**ОБЩИЙ ПОРЯДОК**

**действий оператора по выполнению требований**

**Федерального закона № 152-ФЗ «О персональных данных»**

Перед началом работ по выполнению требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» органу государственной власти необходимо решить следующие основные задачи:

инициация работ по защите персональных данных и назначение ответственных за организацию обработки и обеспечения безопасности персональных данных (должны быть определены объекты, в границах которых будут осуществляться мероприятия по реализации требований, структурные подразделения или должностные лица, ответственные за обеспечение безопасности ПДн);

определение состава обрабатываемых ПДн, целей, сроков, условий и законных оснований обработки (необходимо определить состав обрабатываемых ПДн, цели и условия обработки, сроки хранения ПДн различных категорий, при необходимости должны быть организованы процессы получения согласий субъектов ПДн на обработку ПДн);

разработка основных организационно-распорядительных документов (необходимо сформировать совокупность согласованных организационных мероприятий, направленных на выполнение правил обработки ПДн и обеспечение их безопасности);

определение порядка взаимодействия с субъектами персональных данных (в целях обеспечения максимальной юридической чистоты в вопросах соблюдения прав субъектов ПДн и во избежание инцидентов, связанных с нарушением этих прав, порядок реагирования на запросы со стороны субъектов ПДн, внесения изменений в ПДн, а также условия прекращения обработки ПДн должны быть также определены документально в соответствующих приказах, инструкциях и процедурах, определяющих степень участия должностных лиц в обработке ПДн и характер их взаимодействия между собой);

определение порядка взаимодействия с другими организациями при обработке персональных данных (требуется определить порядок взаимодействий, в рамках которых возможен обмен персональными данными, в том числе провести разграничение ответственности);

определение перечня информационных систем персональных данных (ИСПДн) и их характеристик (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);

разработка модели угроз для ИСПДн (разработка модели угроз входит в состав мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах, с учетом моделирования угроз определяется уровень защищенности ПДн при обработке в информационных системах и требования, выполнение которых позволит обеспечить указанный уровень).

проектирование и реализация системы защиты персональных данных (в каждой информационной системе, предназначенной для обработки персональных данных, должна быть спроектирована и создана система защиты персональных данных (СЗПДн) соответствующая требованиям руководящих и нормативно-методических документов ФСТЭК России и ФСБ России);

определение необходимости уведомления уполномоченного органа на защите ПДн (выполнив все установленные требования к системе защиты персональных данных 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).

В ряде предусмотренных федеральным законодательством случаев организация, осуществляющая деятельность, связанную с использованием средств криптографической защиты информации, либо деятельность в области технической защиты конфиденциальной информации должна получить соответствующие лицензии.

Федеральным законом от 27.07.2006 №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. Например, вопросы трансграничной передачи персональных данных. При наличии таких оснований требуется выработка специальных мер, разработка процедур и издание внутренних организационно-распорядительных документов, регулирующих данные процессы.

**1. Инициация работ по защите персональных данных и назначение ответственных за организацию обработки и обеспечения безопасности персональных данных**

В начале всех работ по выполнению требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» необходимо назначить ответственного (ответственных) за организацию обработки и защиты персональных данных.

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.

Действующая нормативная база в области обработки персональных данных также предусматривает необходимость наличия в организации лиц, ответственных за организацию обработки и защиты персональных данных.

Наделение полномочиями лиц, ответственных за организацию обработки и обеспечение безопасности персональных данных, рекомендуется оформить соответствующим приказом.

**Цели проведения работ**

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 информационную безопасность;

разработка и утверждение документов, закрепляющих функциональные обязанности и права должностных лиц и структурных подразделений, отвечающих за информационную безопасность.

**Выполняемые работы**

В соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (п. 4 ст. 16), 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 защищенности информации.

Чтобы процесс актуализации системы защиты ПДн, а также поддержания ее 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. Назначение структурных подразделений и ответственных лиц осуществляется приказами руководителя организации-оператора.

Как правило, лицом, ответственным за организацию обработки ПДн, назначается работник, который имеет широкие полномочия и от имени руководителя организации может организовать все работы, необходимые для реализации требований законодательства в области обработки ПДн (в т.ч. способен самостоятельно принимать управленческие решения).

Лицом (или структурным подразделением), ответственным за обеспечение безопасности ПДн, могут быть назначены следующие лица/структурные подразделения:

ИТ-подразделение;

подразделение информационной безопасности;

начальник службы безопасности;

администратор информационной безопасности;

специалист по защите информации;

системный администратор;

и др.

Для небольших и средних организаций, в которых отсутствуют сложные схемы подчиненности, наиболее правильным решением будет совмещение указанных ролей в одном сотруднике в виде лица, ответственного за организацию обработки и защиты персональных данных.

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, ответственного за обеспечение безопасности ПДн, должны быть разработаны индивидуальные, соответствующие его зоне ответственности и обязанностям должностные инструкции.

При достаточно сложной производственной структуре организации-оператора могут 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 (персональных данных).

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 более высокого уровня.

**2. Определение состава обрабатываемых ПДн, целей, сроков, условий и законных оснований обработки**

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

Также необходимо получить информацию о сотрудниках, которые имеют доступ к обрабатываемым персональным данным. Это достигается разработкой перечня сотрудников оператора, допущенных к обработке персональных данных.

**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 персональных данных являются Перечень персональных данных и Перечень лиц, допущенных к обработке персональных данных – подробные, четко структурированные документы, содержащие информацию обо всех категориях и видах персональных данных, основаниях и условиях обработки, а также список лиц, имеющих к ним доступ.

**Выполняемые работы**

Для составления Перечней 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 Перечней должностные лица организации, а в случае проведения работ сторонней организацией – сотрудники организации-исполнителя должны провести анализ всех сторон деятельности оператора. При этом выполняются следующие работы:

изучение внутренней и внешней организационно-распорядительной документации, в том числе организационно-штатной структуры;

интервьюирование должностных лиц и специалистов оператора;

идентификация точек входа и выхода информации, содержащей ПДн, и пути её миграции в структуре оператора;

выявление в информационных потоках, сопровождающих деятельность оператора, ПДн, обрабатываемых как с использованием, так и без использования средств автоматизации

анализ оснований и установление целей обработки ПДн; . выявление условий начала и прекращения и определение сроков обработки (хранения) для ПДн; . определение структурных подразделений и должностных лиц оператора, использующих в своей деятельности ПДн; . составление и представление на утверждение Перечня персональных данных и Перечня лиц, допущенных к обработке персональных данных.

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

оформления трудовых договоров с работниками;

ведения учета 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.

Следует особое внимание уделять основаниям обработки ПДн. Одним из условий обработки персональных данных может являться её осуществление с согласия субъекта персональных данных, за исключением случаев, предусмотренных ч. 2 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Невыполнение условия согласия субъекта на обработку его персональных данных может привести к нарушению прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его 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.

Особенно важной является аналитическая проработка и создание юридически значимой доказательной базы правомерности обработки персональных данных, 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.

Законом также установлен ряд случаев, когда согласие субъекта на обработку его персональных данных должно быть дано исключительно в письменной форме. Доказательной базой наличия согласия субъекта на обработку его ПДн могут быть только официальные, юридически грамотно оформленные документы.

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

Стоит уделить внимание обоснованию целей обработки ПДн, с учетом того, что согласно п. 7 ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», хранение персональных данных должно осуществляться не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в их достижении.

**3. Разработка основных организационно-распорядительных документов (внутренних нормативных документов)**

Получив полное представление о процессах обработки ПДн в организации, необходимо заложить организационные основы в части правил обработки ПДн.

**Цель проведения работ** ‑ документирование всех правил обработки и защиты ПДн, в том числе для повышения осведомленности конечных пользователей. Для этого необходимо разработать пакет организационно-распорядительной документации.

**Выполняемые работы**

Разрабатываемые организационно-распорядительные документы должны соответствовать всем требованиям законодательства РФ, предъявляемым к документационному обеспечению операторов ПДн, отражать внутренние организационные и инфраструктурные особенности процессов обеспечения безопасности ПДн. Разработанные документы могут вводиться в действие приказом или утверждаться по отдельности, в зависимости от принятой процедуры утверждения документов.

К процедурам, направленным на предотвращение и выявление нарушений законодательства РФ и устранение последствий таких нарушений, могут быть отнесены:

порядок учета, хранения и уничтожения электронных и бумажных носителей персональных данных;

предоставление, изменение и отзыв прав доступа к ПДн;

выделение информационных систем персональных данных и выявление актуальных угроз безопасности ПДн;

порядок проведения мероприятий, направленных на обеспечение безопасности ПДн (в том числе планирование, создание, эксплуатация СЗПДн);

функционирование подсистем, входящих в состав СЗПДн;

проведение контрольных мероприятий и действия по их результатам;

реагирование на нарушение правил обработки ПДн;

контроль обеспечения уровня защищенности ПДн;

и др.

Политику обработки и обеспечения безопасности ПДн необходимо опубликовать или иным образом обеспечить к ней неограниченный доступ. В случае, если сбор ПДн осуществляется с использованием информационно-телекоммуникационных сетей, Политика должна быть опубликована в данной информационно-телекоммуникационной сети, и к ней должен быть организован доступ с использованием средств этой сети.

Всех работников, непосредственно осуществляющих обработку ПДн, необходимо ознакомить с положениями законодательства РФ о ПДн, в том числе требованиями к защите ПДн и с локальными актами по вопросам обработки ПДн. Необходимо провести обучение указанных работников правилам обработки ПДн. Все работники, использующие средства защиты информации, применяемые в ИСПДн, должны быть обучены правилам работы с ними.

**4. Определение порядка взаимодействия с субъектами**

**персональных данных**

Основной целью Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» является защита прав субъектов ПДн, поэтому в нем четко определены права субъектов ПДн и соответствующие обязанности оператора ПДн, например:

оператор должен предоставлять субъекту ПДн сведения о его ПДн 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 субъекту информации о содержании, условиях обработки его персональных данных, другой информации, затрагивающей его законные права и интересы, может быть квалифицировано как нарушение установленного порядка обработки ПДн. Некорректная реакция (или ее отсутствие) на запрос субъекта персональных данных может быть поводом для обращения в Роскомнадзор с жалобой на действия оператора.

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

**Цели проведения работ**

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

**Выполняемые работы**

При разработке регламентов реагирования на обращения субъектов ПДн необходимо обратить внимание:

на сроки реагирования, установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

на объем предоставленных субъектам ПД прав по получению информации об обработке ПДн, в том числе случаи ограничения данных прав.

Для достижения целей данного этапа необходимо провести следующие работы:

определить ответственных лиц отвечающих за соблюдение требований в части реагирования на запросы субъектов ПДн;

разработать механизмы реагирования на запросы субъектов ПДн (например, документальные регламенты или процедуры);

ввести в действие в рамках организации-оператора разработанные регламенты реагирования на запросы субъектов;

разработать типизированные шаблоны ответов на запросы субъектов ПДн. провести мероприятия по проверке выполнения разработанных механизмов реагирования на запросы субъектов ПДн.

Регламенты реагирования направлены на сведение к минимуму риска нарушения прав субъектов ПДн при поступлении запроса от субъекта ПДн, а также при наступлении факта достижения целей обработки ПДн и отзыва согласия субъекта ПДн.

**5. Определение порядка взаимодействия с другими организациями при обработке персональных данных**

Практически каждое юридическое лицо в рамках своей деятельности осуществляет обмен информацией (в т.ч. и персональными данным) с другими лицами как для осуществления возложенных на него законодательством РФ функций, полномочий и обязанностей (отчетность, ответы на запросы в соответствующие государственные органы).

В связи с этим организации-оператору требуется определить порядок таких взаимодействий.

**Цели проведения работ**

При анализе взаимодействия с другими организациями важно понимать какова роль вашей организации в этом взаимодействии.

При определении перечня внешних организаций и физических лиц, с которыми осуществляется обмен ПДн, необходимо также определить осуществляется ли трансграничная передача ПДн. Под трансграничной передачей понимается передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Выполняемые работы**

Для достижения целей данного этапа необходимо провести следующие работы:

определить перечень внешних организаций и физических лиц, с которыми осуществляется обмен ПДн, и порядок обмена ПДн;

определить случаи поручения обработки ПДн;

определить случаи трансграничной передачи ПДн.

Среди всех организаций и лиц, с которыми осуществляется обмен ПДн, можно выделить 3 группы в зависимости от типа взаимодействия с ними:

внешние организации и физические лица, которым ваша организация поручает вести обработку ПДн;

внешние организации и физические лица, которые поручают вашей организации вести обработку ПДн;

внешние организации и физические лица, обмен персональными данными с которыми осуществляется для выполнения функций, полномочий и обязанностей, возложенных на вашу организацию законодательством РФ.

В первом и третьем случае организация является оператором ПДн (в терминах Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»), во втором случае – лицом, осуществляющим обработку персональных данных по поручению оператора персональных данных. При этом вполне возможны ситуации, когда организация при взаимодействии с третьими лицами в одном случае будет являться оператором ПДн, а в другом случае – лицом, осуществляющем обработку по поручению. Если организация-оператор поручает обработку ПДн третьим лицам, то необходимо.

проверить наличие правовых оснований для передачи персональных данных (договор, требования закона, согласие и т.д.);

проверить соответствие договоров с третьими лицами на предмет содержания поручения на обработку ПДн согласно п. 3 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Если организация выполняет обработку ПДн по поручению другого лица, то необходимо обеспечить выполнение требований по обеспечению защиты ПДн, предусмотренных договором поручения. Важно учитывать, что в случае, если организация-оператор поручает обработку ПДн другому лицу, ответственность перед субъектом за действия этого лица все равно несет оператор. Лицо, осуществляющее обработку ПДн по поручению, несет ответственность только перед оператором. Согласно п. 3 Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», безопасность ПДн при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает ПДн, или лицо, осуществляющее обработку ПДн по поручению оператора на основании заключаемого с этим лицом договора. Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в информационной системе.

Если организация осуществляет трансграничную передачу ПДн, необходимо определить, относится ли страна, на территорию которой осуществляется передача, к странам, являющимся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн или обеспечивающим адекватную защиту ПДн.

Следует учитывать, что трансграничная передача персональных данных на территорию иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, возможна при соблюдении условий, определенных в Статье 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных.

Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватную защиту прав субъектов персональных данных, возможна только при выполнении любого из нижеследующих условий:

наличие согласия в письменной форме субъекта на трансграничную передачу его персональных данных. в случаях, предусмотренных международными договорами РФ;

в случаях, предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя РФ, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства. для исполнения договора, стороной которого является субъект персональных данных;

для защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

**6. Определение перечня информационных систем персональных данных (ИСПДн) и их характеристик**

ИСПДн представляют собой совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

**Цели проведения работ**

выделение (идентификация) и определение состава ИСПДн, имеющихся в IT инфраструктуре;

определение характеристик ИСПДн в соответствии с нормативно-правовыми актами ФСТЭК России;

документальная фиксация перечня всех идентифицированных ИСПДн и их характеристик.

**Выполняемые работы**

идентификация ИСПДн – выделение в IT-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 IT-инфраструктуры, утверждение перечня защищаемых ИСПДн приказом руководителя предприятия;

определение характеристик ИСПДн в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Идентификация ИСПДн включает в себя следующие блоки работ:

изучение информационных потоков (необходимо идентифицировать и описать процессы, связанные с обработкой ПДн, а также 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);

сегментация сети (используя представление об информационных потоках, схему 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 либо ставятся цели обработки ПДн, отличные от целей обработки ПДн в других сегментах сети).

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

Решение о выделении ИСПДн 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.

Далее для каждой из имеющихся ИСПДн необходимо определить:

1) Тип ИСПДн в зависимости от категории обрабатываемых ПДн:

информационная система, обрабатывающая специальные категории персональных данных;

информационная система, обрабатывающая биометрические персональные данные;

информационная система, обрабатывающая общедоступные персональные данные;

информационная система, обрабатывающая иные категории персональных данных.

2) Тип ИСПДн в зависимости от категории субъектов ПДн:

информационная система, обрабатывающая персональные данные сотрудников оператора;

информационная система, обрабатывающая персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

3) Количество субъектов, ПДн которых обрабатываются в ИСПДн:

>100 000 субъектов;

<100 000 субъектов.

Определившись с составом и типами ИСПДн, рекомендуется разработать документ «Перечень информационных систем персональных данных», в котором для каждой ИСПДн зафиксировать ее физическое месторасположение, программное обеспечение, используемое при обработке персональных данных, а также характеристики ИСПДн и иные сведения.

Вся представленная информация потребуется в дальнейшем при определении уровней защищенности ПДн при обработке в информационных системах.

**7. Разработка модели угроз для ИСПДн**

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 персональных данных:

адекватно оценить необходимость реализации тех или иных мероприятий по обеспечению безопасности ПДн исходя из состояния защищенности 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 моделирования действий различных групп нарушителей, использующих те или иные уязвимости, характерные для анализируемой ИСПДн. Эти действия осуществляются после выделения и обследования ИСПДн и предшествует проектированию и реализации СЗПДн. 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**

Определение актуальных угроз и типов угроз безопасности ПДн при их обработке в ИСПДн и составление модели угроз для каждой ИСПДн, выделенной в информационной инфраструктуре организации-оператора. Определив тип угроз безопасности персональных данных, актуальных для информационной системы, необходимо установить уровень защищенности ПДн при обработке в ИСПДн.

**Выполняемые работы**

В первую очередь, согласно ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и п. 7 Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», необходимо выполнить оценку вреда, который может быть причинен субъекту в случае нарушения безопасности защищаемых ПДн.

При определении возможного вреда для субъекта персональных данных рекомендуется ориентироваться на состав персональных данных, обрабатываемых в рассматриваемой ИСПДн, цели и условия этой обработки.

Результаты проведенной оценки вреда для субъекта персональных данных и определения показателей опасности угроз фиксируются документально.

Следующим шагом для каждой из ИСПДн необходимо определить возможные угрозы безопасности ПДн с учетом имеющихся предпосылок, нарушителей и уже применяемых средств защиты информации и разработать документ под названием «Модель угроз безопасности персональных данных при их обработке в ИСПДн».

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);

расчет актуальности полученных угроз безопасности ПДн для анализируемой ИСПДн (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).

После определения вышеназванных параметров из общего перечня угроз осуществляется выборка актуальных для ИСПДн типов угроз в соответствии с пп. 6–7 Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и определение уровня защищенности.

Результаты вышеперечисленных работ отражаются в документе «Модель угроз безопасности ПДн при их обработке в ИСПДн», который рекомендуется утвердить руководителем организации или другим уполномоченным лицом.

Определение уровня защищенности ПДн при обработке в ИСПДн предусматривает проведение следующих мероприятий:

назначение комиссии (как правило, в состав комиссии включаются руководители (представители) подразделений, осуществляющих обработку персональных данных, сотрудники IT-подразделений и подразделений информационной безопасности предприятия);

изучение характеристик ИСПДн (характеристики ИСПДн, влияющие на определение уровня защищенности ПДн, описаны в пп. 9–12 Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»);

разработка и утверждение актов определения уровня защищенности ПДн при обработке в ИСПДн (акт подписывается председателем комиссии и её членами и утверждается руководителем организации).

**8. Проектирование и реализация системы защиты персональных данных**

Создание системы защиты персональных данных является неотъемлемой частью реализации всего спектра требований, предъявляемых к оператору ПДн Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и соответствующими подзаконными актами. Субъекты ПДн, 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 определенных 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 информационной безопасности и отвечающей требованиям, предъявляемым документами ФСТЭК России и ФСБ России к соответствующему классу ИСПДн.

**Выполняемые работы**

Разработка и создание системы защиты персональных данных 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:

разработка требований по обеспечению безопасности ПДн при обработке в ИСПДн (для каждой из ИСПДн, с учетом уровня защищенности ПДн, выполняется разработка требований по обеспечению безопасности ПДн при обработке в ИСПДн, определяющих необходимые для реализации меры обеспечения безопасности);

разработка технического задания (должны быть определены требования к проведению работ по созданию СЗПДн, в том числе зафиксировано обоснование разработки СЗПДн, исходные данные ИСПДн, конкретные мероприятия СЗПДн, перечень предполагаемых к использованию средств защиты информации, сроки проведения работ по этапам, ссылки на нормативные документы и т.д.);

проектирование СЗПДн (включает в себя выбор необходимых для внедрения средств и мер защиты ПДн, 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).

внедрение и контроль (установку, настройку и ввод в эксплуатацию средств защиты информации следует осуществлять строго в соответствии с эксплуатационной и технической документацией, поставляемой вместе с программным продуктом);

разработка документации (после того, как все необходимые средства защиты установлены, необходимо оформить ввод системы защиты персональных данных в эксплуатацию путем составления и утверждения соответствующих документов, например, акта и приказа).

Необходимо обратить внимание на выбор средств защиты информации. В реестрах сертификатов ФСТЭК и ФСБ указывается, выдан ли сертификат на всю серию или на единичный экземпляр, приводятся сведения о возможности применения данного средства защиты в ИСПДн с заданными характеристиками. Возможна сертификация ранее внедренных в систему средств защиты, если установка имеющихся сертифицированных средств защиты трудоемка или нецелесообразна.

В общей сложности в рамках системы защиты персональных данных должны быть реализованы следующие меры по защите персональных данных:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей персональных данных;

регистрация событий безопасности;

антивирусная защита;

обнаружение вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов и реагирование на них;

управление конфигурацией информационной системы и системы;

защиты персональных данных.

**9. Определение необходимости уведомления уполномоченного органа**

**по защите ПДн**

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 персональных данных. Исключение составляют случаи, предусмотренные частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Невыполнение условия уведомления уполномоченного органа может быть квалифицировано как правонарушение, предусмотренное статьёй 19.7 Кодекса Российской Федерации об административных правонарушениях от 30.12.2001 № 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 персональных данных в уполномоченный орган по защите прав субъектов персональных данных. В случае если выявлен хотя бы один факт обработки персональных данных, не подпадающий под перечень случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», уведомление должно быть подготовлено и отправлено.

**Цели проведения работ**

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 персональных данных, если все обрабатываемые персональные данные подпадают под исключения, предусмотренные частью 2 статьи 22 Федерального закона № 152-ФЗ;

в случае необходимости, подготовить уведомление об обработке персональных данных в соответствии с требованиями регулятора и отправить в уполномоченный орган.

**Выполняемые работы**

Используя представление о составе, условиях и целях обработки персональных данных, сформированное при разработке перечня ПДн, на текущем необходимо проанализировать всю совокупность обрабатываемых в организации ПДн, 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, предусмотренным частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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. 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 персональных данных.

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 способов обработки персональных данных;

описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

сведения о наличии или об отсутствии трансграничной передачи персональных данных;

сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

дата начала обработки персональных данных. срок или условие прекращения обработки персональных данных.

Организация-оператор, подающая уведомление об обработке персональных данных, 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.

**Список терминов**

Безопасность персональных данных ‑ состояние защищенности ПДн от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность ПДн при их обработке, независимо от формы их представления.

Блокирование персональных данных ‑ временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к информации ‑ возможность получения и использования информации.

Доступность персональных данных ‑ возможность беспрепятственного получения санкционированного доступа к персональным данным.

Информационная система персональных данных ‑ совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных ‑ обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта ПДн или 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-распределенное программное (программноаппаратное) 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.

Обезличивание персональных данных ‑ действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту персональных данных.

Обработка персональных данных ‑ любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор ‑ государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные ‑ любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных ‑ действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Процесс обработки персональных данных ‑ деятельность, в рамках которой осуществляется обработка персональных данных.

Распространение персональных данных ‑ действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Система защиты персональных данных ‑ совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Субъект персональных данных ‑ физическое лицо, к которому относятся определенные персональные данные либо которое может быть определено на основании определенных персональных данных.

Трансграничная передача персональных данных ‑ передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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.

Уничтожение персональных данных ‑ действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Список нормативно-правовых документов**

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1981);

2. Конституция Российской Федерации (принята на всенародном голосовании 12.12.1993);

3. Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

6. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;

7. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ;

8. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

9. Указ Президента Российской Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;

10. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

11. Распоряжение Президента Российской Федерации от 10.07.2001 № 366-рп «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;

12. Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

13. Постановление Правительства Российской Федерации от 15.08.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

14. Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

15. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

16. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства российской федерации в области персональных данных»;

17. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 21.12.2011 № 346 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Введение реестра операторов, осуществляющих обработку персональных данных»;

18. Приказ Роскомнадзора от 19.08.2011 № 706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».