# Раздел 1. Персональные данные. Защита персональных данных. Утечка персональных данных

# Защита персональных данных как исполнение конституционных прав граждан на неприкосновенность частной жизни

Право на неприкосновенность частной жизни, личную и семейную тайну является неотъемлемым конституционным правом человека и гражданина и подлежит защите независимо от гражданской или национальной принадлежности.

В 1993 году была принята Конституция Российской Федерации, предусматривающая неприкосновенность частной жизни. В соответствии со статьей 23: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Статья 24 также дополняет, что «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом».

Статья 2 Конституции России провозглашает, что человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства. Права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (часть 3 статьи 55 Конституции России). Аналогичные основания ограничения закреплены и в отношении гражданских прав (п. 2 ст. 1 ГК РФ) При этом Конституция Российской Федерации не определяет иных оснований, позволяющих ограничить права человека.

Введенной статьей 152.2 Гражданского кодекса РФ определено «если иное прямо не предусмотрено законом, не допускаются без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни». При этом не являются нарушением указанных правил сбор, хранение, распространение и использование информации о частной жизни гражданина в государственных, общественных или иных публичных интересах, а также в случаях, если информация о частной жизни гражданина ранее стала общедоступной либо была раскрыта самим гражданином или по его воле.

Современная трактовка конституционного права на частную жизнь, личную и семейную тайну, в рамках взятых на себя Российской Федерацией обязательств в связи с ратификацией Европейских Конвенций о защите прав человека и основных свобод и о защите физических лиц при автоматизированной обработке персональных данных, предполагает защиту: во-первых, деятельности личности в частной сфере, ее поступков, образа жизни и поведения, и, во-вторых, непосредственно персональных данных человека. Таким образом, объектом конституционного права на частную жизнь, личную и семейную тайну выступают две группы общественных отношений, первая из которых связана с действиями, вторая с информацией (персональными данными).

# *Международное законодательство о защите персональных данных*

В настоящее время конституционные права на частную (личную) и семейную жизнь, тайну телефонных переговоров и на неприкосновенность жилища предусматриваются большинством конституций государств. В частности, Политическая Конституция Перу от 29 декабря 1993 г. (ст. 2) закрепляет право каждого на неприкосновенность частной и семейной жизни, также на свой голос и образ; на секретность и неприкосновенность личной корреспонденции и документов; право хранить в тайне свои политические, философские, религиозные и другие виды убеждений, а также профессиональную тайну.

Вопросы защиты частной жизни и персональных данных регулируются в Великобритании законодательными актами, а Европейская конвенция о защите прав человека и основных свобод инкорпорирована Законом о защите прав человека 1998 г. В современной Великобритании под правом на неприкосновенность частной жизни принято понимать «право быть одному». В контексте деятельности Европейского Суда по правам человека по делам против Соединенного Королевства, право на частную жизнь включает в себя неприкосновенность коммуникаций, дома и офисных помещений, защиту окружающей среды, физическую неприкосновенность, защиту от несправедливости обвинения, свободу сексуального поведения. При этом на публичные органы возлагается ограниченная обязанность защищать право на частную жизнь от посягательств третьих лиц.

Положения о возможности раскрытия информации, касающейся личности (личной жизни), только на основании закона закреплено в Конституциях Албании и Польши

# *Персональные данные*

Необходимость обеспечения безопасности персональных данных в наше время - объективная реальность. Современный человек не может самостоятельно противодействовать посягательству на его частную жизнь. Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных.

Рассмотрим несколько примеров из повседневной жизни, когда нарушаются права человека на конфиденциальность персональных данных. Бывает так, что при оформлении дисконтной карты в магазине покупатель указывает следующие сведения: фамилию, номер телефона, электронный адрес, а затем получает сообщения и письма совершенно из других магазинов, в которых даже никогда не бывал. То есть магазин без согласия покупателя передал его данные третьим лицам. Если газета печатает ФИО и суммы выигрыша победителей лотереи без их ведома, или ТСЖ вывешивает на подъезде списки должников и сумму их долга - это примеры "безобидных " утечек. Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах или информации о сбережениях в банке. Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт (скиминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию (фишинг). На самом деле зачастую даже трудно установить источник утечки персональных данных вследствие высокой информатизации современного общества.

Государство на законодательном уровне требует от организаций и физических лиц, обрабатывающих персональные данные, обеспечить их защиту. Законодательство Российской Федерации в области защиты персональных данных основывается на Конституции РФ, международных договорах Российской Федерации, Федеральном законе РФ от 27 июля 2006 г. N 152-ФЗ "О персональных данных", Федеральном законе от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" и других определяющих случаи и особенности обработки персональных данных федеральных законов.

Целью российского законодательства в области защиты персональных данных является обеспечение защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Законодательством регулируются отношения, связанные с обработкой персональных данных, осуществляемой государственными органами власти, органами местного самоуправления, юридическими лицами и физическими лицами.

Основополагающим законом в области защиты персональных данных является Федеральный закон "О персональных данных" №152, который был принят Государственной думой 8 июля 2006 года и вступил в силу с 26 января 2007 года. Закон определяет:

1. основные понятия, связанные с обработкой персональных данных;
2. принципы и условия обработки персональных данных;
3. обязанности оператора персональных данных;
4. права субъекта персональных данных;
5. виды ответственности за нарушение требований ФЗ-№152;
6. государственные органы, осуществляющие контроль за соблюдением требований ФЗ-№152.

В соответствии с Законом **персональные данные** - любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПД). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПД.

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

**Информационная система персональных данных (далее ИСПД)** – 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.

**Регуляторами** называются органы государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований федерального закона. В ФЗ "О персональных данных" установлены три регулятора:

* Роскомнадзор (защита прав субъектов персональных данных)
* ФСБ (требования в области криптографии)
* ФСТЭК России (требования по защите информации от несанкционированного доступа и утечки по техническим каналам).

Так как ФЗ "О персональных данных" является лишь основой правового обеспечения защиты ПД, его требования в дальнейшем были конкретизированы в актах Правительства РФ и Министерства связи, нормативно-методических документах регуляторов.

# *Категории персональных данных*

ФЗ "О персональных данных" выделяет следующие категории персональных данных.

**Общедоступные ПД -** данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПД или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Общедоступные источники персональных данных создаются в целях информационного обеспечения (например, справочники и адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Важно отметить, что сведения о субъекте ПД могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

**Специальные категории ПД -**персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

* субъект ПД дал согласие в письменной форме на обработку своих персональных данных;
* персональные данные являются общедоступными;
* персональные данные относятся к состоянию здоровья субъекта ПД и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
* обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПД;
* обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" определяет следующие **категории персональных данных**, которые обрабатываются в ИСПД:

Категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Категория 2 – персональные данные, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Категория 3 – персональные данные, позволяющие идентифицировать субъекта ПД.

Категория 4 – обезличенные и (или) общедоступные персональные данные.

**Биометрические персональные данные** – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПД. Обработка биометрических персональных данных без согласия субъекта ПД может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно - розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Определение биометрических данных в российском законодательстве предоставляет оператору персональных данных возможность принятия самостоятельного решения об отнесении тех или иных данных к биометрическим. Это породило немало споров. Рассмотрим пример с фотографией. С одной стороны, она характеризует физиологические особенности человека. Но человек с течением времени может сильно измениться или злоумышленник может подделать внешние признаки под законного субъекта. Так ли однозначно в данном случае установление личности? В настоящее время представители регуляторов подтверждают, что фотография и видеоизображения относятся к биометрическим данным.

# *Персональные данные в системе документооборота предприятия*

 Деятельность любого работодателя связана с подбором персонала, а также с накоплением, обработкой, хранением и использованием значительных объемов сведений о работниках.

Закон распространяется абсолютно на все организации. Поскольку в каждой организации есть работники, то их данные так или иначе используются при заключении трудового договора, начислении зарплаты и в других случаях.

Персональные данные вносятся в личные дела сотрудников, которые хранятся у работников кадровой службы.

Под обработкой персональных данных подразумеваются действия по сбору, систематизации, накоплению, хранению, уточнению, использованию, передаче, обезличиванию, блокированию и уничтожению персональных данных. Распространение персональных данных - это действия, направленные на раскрытие персональных данных неопределенному кругу лиц. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Операторами персональных данных, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными, могут быть государственные органы, муниципальные органы, юридические или физические лица. На это указывает пункт 2 статьи 3 Закона N 152-ФЗ.

Персональные данные работника могут накапливаться по месту работы и содержаться в кадровой документации, включающей в себя:

* личные дела и трудовые книжки работников;
* документы, возникающие при оформлении трудовых правоотношений (при решении вопросов о приеме на работу, переводе, увольнении, поощрении и тому подобном);
* документы по анкетированию, тестированию и тому подобные;
* приказы (распоряжения) по личному составу;
* документация по аттестации сотрудников, служебным расследованиям и тому подобному;
* учетная документация (картотеки, книги, журналы и другие);
* аналитическая и справочная документация, как используемая руководством, так и выдаваемая работникам для представления в заинтересованные органы;
* отчетная документация, передаваемая в государственные органы статистки, налоговые органы и другие учреждения.

# *Угрозы утечки персональных данных*

## 

Утечки персональных данных нередки в работе компаний и государственных органов. Часто они связаны с недобросовестным отношением к их защите. Следствия утечек могут быть и очень серьезными, и незначительными. Защита от них должна стать задачей и операторов, и субъектов персональных данных.

Персональные данные – это любая информация о человеке, которая связана с ним, позволяет идентифицировать его в полной мере, получить иные сведения о нем, совершать какие-либо посягательства на тайну его личной жизни или на имущество. В группе риска утраты важной информации при проведении обработки персональных данных оказываются многие люди, среди них:

* граждане, пользующиеся банковскими картами;
* граждане, получающие медицинские услуги;
* владельцы пенсионных накоплений;
* вкладчики банков;
* владельцы недвижимости.

Это не исчерпывающий перечень, пострадать от утечки персональных данных могут и многие другие. Поэтому государство выстроило систему защиты персональных данных. В ее основу лег Федеральный закон «О защите персональных данных», систему технических мер регламентируют правительство, ФСТЭК, ФСБ.

Любая организация, которая в своей деятельности обрабатывает персональные данные, обязана предпринять комплекс организационных и технических мер, направленных на их защиту. Перечень этих мер и способов регламентируется для каждой группы данных. При разработке системы таких технических и административных решений используется модель угроз, в которой учитываются риски двух типов:

1. внешние;
2. инсайдерские.

Первый тип угроз, представляющих собой неправомерное проникновение в защищенный информационный периметр организации-оператора, – хакерские атаки, которые в России редко становятся серьезными угрозами для жизни и здоровья граждан. Прекратились появления в Сети баз данных ЦБ РФ, ГИБДД, Пенсионного фонда – информационные системы защищены серьезно, а утечка массива сведений, защищенных средствами криптографической защиты, без возможности персонификации, не несет серьезных рисков. Сократилось и количество внешних атак на сайты банков.

Вторые реализуются наиболее часто. Гражданин предоставляет сведения о себе во множестве случаев в медицинском учреждении, в туристическом агентстве, в котором для оформления визы он практически полностью раскрывает сведения о своем финансовом статусе. Согласие на обработку персональных данных зачастую не подписывается. Таким образом, паспортные данные, сведения о недвижимости, доходах, операциях по банковской карте оказываются в незащищенном виде в компьютере, на котором может не быть даже антивирусной защиты. В этом случае доступ к ним становится возможным:

* при прямом проникновении недобросовестного сотрудника агентства в компьютер или к материальным носителям информации;
* при размещении их в облачных сетях, иногда на множестве серверов, зачастую расположенных не в России. Законодательство требует обязательного хранения персональных данных внутри страны, но эти требования выполняют не все операторы, зачастую даже не знающие о существовании такой обязанности;
* при хищении ноутбука или портфеля сотрудника компании, в котором находится интересующая злоумышленника информация.

Частые случаи, появляющиеся в судебной практике, в которых штрафуются или наказываются иным образом врачи или сотрудники банковских учреждений, допустившие утечку сведений, например, паспортных данных, говорят о существовании проблемы и ее серьезности.

Последствия утечек могут оказаться серьезными и для владельцев данных, и для операторов. Для первой группы существуют многочисленные риски стать жертвой злоумышленников. Они могут пострадать:

* от разглашения любой информации, имеющей отношение к личности;
* от шантажа;
* от неправомерного списания средств с банковской карты;
* от вмешательства в личную жизнь;
* от угроз детям, например, в случае публикации в СМИ данных о школах, где они учатся.

Минимальным риском станет неправомерная передача сведений, например, адреса электронной почты, каким-либо компаниям, которые начнут преследовать их обладателя рекламными объявлениями. Но даже это дает возможность возбудить дело и о неправомерной рекламе, и об утечке данных и приведет к штрафам, налагаемым на операторов, если источник утечки или спама удастся достоверно установить.

Операторы, в свою очередь, допустившие утечку персональных данных, понесут ответственность:

* гражданскую, в виде взыскания в судебном порядке понесенных гражданами убытков и морального вреда;
* административную, в виде наложения штрафа, приостановления или запрета деятельности, связанной с обработкой персональных данных;
* уголовную, в случае неправомерного распространения ПД, причинившего существенный ущерб и передаче информации в правоохранительные органы.

# Раздел 2. Основные положения Федерального закона "О персональных данных"

# ***Сфера действия закона***

Закон регулирует отношения связанные с обработкой персональных данных (Рис.1), осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.



Рис.1. Область применения закона

В категорию тех, на кого распространяются требования ФЗ-152, попадают все организации, в силу должностных и профессиональных особенностей обязанные собирать, систематизировать и защищать личные данные.

Перечень отраслей, для которых работа с защитой персональных данных является приоритетной – огромен, но если обобщить возможные варианты, он будет выглядеть так:

* медицина (независимо от собственника);
* кредитно-финансовые структуры;
* страховые организации;
* компании-операторы сотовой связи;
* туристическая индустрия;
* рынок транспортных и пассажирских перевозок;
* риелторский бизнес;
* провайдеры систем безопасности.

**Основные понятия, используемые в области персональных данных**

**персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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;

**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;

**автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

**распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

**предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

**блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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;

**обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

**информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

**трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

# ***Защита персональных данных***

Это комплекс правовых, организационных и технических мер исключающих доступ к информации, содержащей персональные данные, лиц, не обладающих соответствующими полномочиями, а также исключающих возможность неправомерного использования такой информации. В соответствии с Федеральным законом "О персональных данных" Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) [требования](consultantplus://offline/main?base=LAW;n=72596;fld=134;dst=100009) к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) [требования](consultantplus://offline/main?base=LAW;n=78154;fld=134;dst=100009) к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Для граждан основным способом защиты их персональных данных - проявление бдительности при предоставлении кому-либо информации личного характера, а также знание прав и обязанностей, которыми наделяет Федеральный закон операторов информационных систем и субъектов персональных данных.

# ***Уполномоченный орган по защите прав субъектов персональных данных***

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор),осуществляющая деятельность непосредственно и через свои территориальные органы во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, общественными объединениямии иными организациями. На службу возложены функции по ведению реестра операторов персональных данных, проведение контрольно-надзорных мероприятий в отношении юридических и физических лиц, осуществляющих обработку персональных данных, работа с жалобами и обращениями граждан и юридических лиц, принимать в установленном законодательством РФ меры по приостановлению или прекращению обработки персональных данных.

Роскомнадзор, как уполномоченный орган по защите прав субъектов персональных данных, помимо вышеуказанных функций, обладает правом обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде; направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью; вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных.

# *Обработка персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение*

**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;

**автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники, при этом такая обработка не может быть признана осуществляемой исключительно с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее;

**обработка персональных данных без использования средств автоматизации (неавтоматизированная обработка)**- действия с персональными данными, такие как использование, уточнение, распространение, уничтожение, осуществляемые при непосредственном участии человека;

**распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

**предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

**блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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;

**обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

**трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Обработка персональных данных  осуществляется путем смешанной (как автоматизированной, так и неавтоматизированной) обработки, в том числе, с использованием внутренней сети и сети Интернет.

В случаях, установленных законодательством РФ, основным условием обработки персональных данных является получение согласие соответствующего субъекта персональных данных, в том числе, в письменной форме.

Письменное согласие субъекта персональных данных на обработку его 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;

* фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
* наименование и адрес организации, получающей согласие субъекта персональных данных;
* цель обработки персональных данных;
* перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных
* перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
* срок, в течение которого действует согласие, а также порядок его отзыва;
* подпись субъекта персональных данных.

Согласие субъекта на обработку его персональных данных не требуется в следующих случаях:

* обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
* обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
* обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
* в иных случаях, установленных законом.

В случаях, когда требуется согласие субъекта персональных данных на обработку персональных данных, но не требуется согласие в письменной форме, субъект персональных данных может предоставить согласие средствами электронной связи, Интернет, по электронной почте или по факсу.

**Сбор**

Источником информации обо всех персональных данных является непосредственно субъект персональных данных. Если иное не установлено законом, Компания вправе получать персональные данные субъекта персональных данных от третьих лиц только при уведомлении об этом субъекта, либо при наличии письменного согласия субъекта на получение его персональных данных от третьих лиц.

Уведомление субъекта персональных данных о получении его персональных данных от третьих лиц должно содержать:

* наименование Оператора и адрес его местонахождения,
* цель обработки персональных данных и ее правовое основание,
* предполагаемые пользователи персональных данных,
* установленные законом права субъекта персональных данных,
* источник получения персональных данных.

**Хранение**

При хранении персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных. Документы, включающие в себя персональные данные, содержащиеся на бумажных носителях, находятся в специально отведенных для этого местах с ограниченным доступом в условиях, которые обеспечивают их защиту от несанкционированного доступа. Перечень мест хранения документов определяется руководством организации (предприятия). Персональные данные, хранящиеся в электронном виде, защищаются от несанкционированного доступа с помощью специальных технических и программных средств защиты. Хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, но не дольше, чем этого требуют цели их обработки, если иной срок не установлен законодательством РФ или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Сроки хранения персональных данных субъекта определяются, в том числе, в соответствии с Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», а также иными требованиями законодательства и нормативных документов. Если иное не предусмотрено законодательством, обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки, в случае утраты необходимости в достижении этих целей или по истечении сроков их хранения. Уничтожение или обезличивание персональных данных должно производиться способом, исключающим дальнейшую обработку этих персональных данных. При этом в случае необходимости следует сохранять возможность обработки иных данных, зафиксированных на соответствующем материальном носителе (удаление, вымарывание). При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

**Использование**

Доступ к персональным данным предоставляется только тем работникам, служебные обязанности которых предполагают работу с персональными данными, и только на период, необходимый для работы с соответствующими данными. Перечень таких лиц определяется руководителем. В случае возникновения необходимости предоставить доступ к персональным данным работникам, не входящих в перечень лиц с доступом к персональным данным, им может быть предоставлен временный доступ к ограниченному кругу персональных данных по распоряжению руководителя или иного лица, уполномоченного на это руководителем. Соответствующие работники должны быть ознакомлены под роспись со всеми локальными нормативными актами организации (предприятия) в области персональных данных, а также должны подписать обязательство неразглашения персональных данных. Работники, осуществляющие обработку персональных данных без использования средств автоматизации, информируются о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных законодательством. Работникам, не имеющие надлежащим образом оформленного допуска, доступ к персональным данным запрещается.

При необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

Уточнение персональных данных при их обработке без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

**Передача**

Передача персональных данных субъектов третьим лицам допускается в минимально необходимых  объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных. Передача персональных данных третьим лицам, в том числе, в коммерческих целях, допускается только при наличии согласия субъекта, либо иного законного основания.

При передаче персональных данных третьим лицам субъект должен быть уведомлен о такой передаче, за исключением случаев, определенных законом, в частности, если:

* субъект персональных данных уведомлен об осуществлении обработки его персональных данных оператором, который получил от Компании соответствующие данные;
* персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
* персональные данные обрабатываются для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных.

Передача информации, содержащей персональные данные, должна осуществляться способом, обеспечивающим защиту от неправомерного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий в отношении такой информации

Лица, получающие персональные данные, должны предупреждаться о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и с соблюдением режима конфиденциальности. Организация вправе требовать от этих лиц подтверждение того, что это правило соблюдено.

В случаях, когда государственные органы имеют право запросить персональные данные, или персональные данные должны быть предоставлена в силу закона, а также в соответствии с запросом суда, соответствующая информация может быть им предоставлена в порядке, предусмотренном действующим законодательством РФ.

Все поступающие запросы должны передаваться лицу, ответственному за организацию обработки персональных данных в организации, для предварительного рассмотрения и согласования.

**Поручение обработки**

В договоре с лицом, осуществляющим обработку персональных данных по поручению организации, данных должны быть определены:

* перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
* цели обработки;
* обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с требованиями федерального законодательства и ответственность за несоблюдение таких требований.

**Защита**

Под защитой персональных данных понимается ряд правовых, организационных и технических мер, направленных на:

* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа;
* реализацию права на доступ к информации.

Для защиты персональных данных организация (предприятие) принимает необходимые предусмотренные законом меры, включая, но не ограничиваясь:

* ограничивает и регламентирует состав работников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные (в том числе, путем использования паролей доступа к электронным информационным ресурсам);
* обеспечивает условия для хранения документов, содержащих персональные данные, в ограниченном доступе;
* организует порядок уничтожения информации, содержащей персональные данные, если законодательством не установлены требования по хранению соответствующих данных;
* контролирует соблюдение требований по обеспечению безопасности персональных данных, в том числе, установленных настоящим Положением (путем проведения внутренних проверок, установления специальных средств мониторинга и др.);
* проводит расследование случаев несанкционированного доступа или разглашения персональных данных с привлечением виновных работников к ответственности, принятием иных мер;
* внедряет программные и технические средства защиты информации в электронном виде;
* обеспечивает возможность восстановления персональных данных модифицированных или уничтоженных вследствие несанкционированного доступа к ним; и др.

# *Цели обработки персональных данных*

Обработка персональных данных субъектов персональных данных осуществляется в следующих целях:

* осуществление и выполнение функций, полномочий и обязанностей, возложенных на организацию законодательством РФ и международными договорами РФ;
* предоставление родственникам работников льгот и компенсаций;
* организация медицинского и иного страхования работника;
* рассмотрение возможности трудоустройства кандидатов;
* проверка кандидатов (в том числе их квалификации и опыта работы);
* обеспечение безопасности, сохранение материальных ценностей и предотвращение правонарушений;
* проведение мероприятий и обеспечение участия в них субъектов персональных данных;
* иные цели, направленные на обеспечение соблюдения трудовых договоров, законов и иных нормативных правовых актов.

# *Принципы обработки персональных данных*

Обработка персональных данных должна осуществляться на законной и справедливой основе. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если иное не предусмотрено федеральным законом или договором. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

# *Права субъекта персональных данных*

Субъект персональных данных – это физическое лицо, которое может быть однозначно идентифицировано на основе персональных данных, то есть фактически тот, чьи данные необходимо защищать. Рассмотрим основные *права* субъекта ПД, установленные ФЗ-№152.

1. Право субъекта персональных данных на доступ к своим персональным данным. Это предполагает право субъекта на получение сведений об операторе персональных данных и о том, какие ПД, относящие к этому субъекту, он обрабатывает, а также непосредственный доступ к этим ПД. Субъект вправе требовать от оператора уточнения ПД, их блокирования или уничтожения, если они устаревшие, неполные или не являются необходимыми для заявленной цели обработки. Доступ к своим ПД предоставляется субъекту (или его представителю) при обращении либо на основании запроса. Полученная информация может содержать следующие сведения:

* цель обработки ПД
* способы обработки ПД
* сроки обработки ПД
* перечень допущенных к обработке ПД лиц
* перечень обрабатываемых ПД и источник их получения
* сведения о возможных юридических последствиях обработки ПД для субъекта ПД.

Закон определяет случаи, когда данное право субъекта ПД ограничивается, например, если речь идет о безопасности страны, нарушении конституционных прав и свобод других лиц или оперативно-розыскной деятельности.

1. Права субъектов ПД при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации. В данном случае обработка осуществляется только при условии предварительного согласия субъекта. При этом важно отметить, что обработка признается осуществленной без согласия субъекта, если оператор не доказал обратное. Оператор обязан немедленно прекратить обработку ПД по требованию субъекта.
2. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных. Закон запрещает принятие решений в отношении субъекта ПД исключительно на основании автоматизированной обработки, если не получено его согласия в письменной форме или в случаях, предусмотренных федеральными законами.
3. Право на обжалование действий или бездействия оператора. Если субъект ПД считает, что оператор обрабатывает его ПД ненадлежащим образом, то есть нарушает его права, он может обратиться в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Необходимо отметить, что субъект ПД имеет право на возмещение убытков и компенсацию материального вреда в судебном порядке.

Обработка персональных данных субъекта, по общему правилу, должна осуществляться с его согласия (ч. 1 ст. 6 закона о персональных данных). В тех случаях, когда это прямо предусмотрено законом, согласие должно быть письменным. Утвержденной формы такого документа нет, но в нем как минимум следует указать:

* ФИО, адрес субъекта персональных данных и его паспортные данные;
* ФИО, адрес и паспортные данные его представителя, реквизиты доверенности или иного документа, подтверждающего его полномочия (если согласие дает представитель субъекта);
* наименование (или ФИО) и адрес оператора, а также лица, которому оператор поручил обработку данных (если обработка поручена третьему лицу);
* цель обработки персональных данных;
* перечень персональных данных, на обработку которых дается согласие субъекта;
* перечень действий с персональными данными, на совершение которых дается согласие;
* срок, в течение которого действует согласие субъекта, а также способ его отзыва;
* подпись субъекта персональных данных (ч. 4 ст. 9 закона о персональных данных).

Равнозначным согласию в письменной форме признается согласие в электронной форме, скрепленное электронной подписью субъекта.

Стоит также отметить, что лицо вправе в любой момент отозвать свое согласие на обработку его персональных данных (ч. 2 ст. 9 закона о персональных данных).

# *Обязанности оператора персональных данных*

Все без исключения организации являются операторами ПД, так как они накапливают, собирают и обрабатывают информацию о своих сотрудниках в рамках Трудового кодекса РФ. Помимо этого многие организации собирают сведения о своих клиентах, подрядчиках, поставщиках и партнерах в рамках своей основной деятельности. Главными обязанностями оператора ПД является уведомление Роскомнадзора об обработке ПД и ,собственно, защита ПД.

Законом предусмотрены случаи, когда оператор не обязан уведомлять Роскомнадзор об обработке ПД:

* если его связывают с субъектом трудовые отношения;
* если между оператором и субъектом существует договор и данные необходимы для исполнения обязательств по нему;
* если данные относятся к членам религиозных объединений и общественных организаций и обрабатываются в соответствии с учредительными документами и с законом.
* если данные являются общедоступными;
* если включают в себя только ФИО;
* данные необходимы для однократного пропуска на территорию оператора или аналогичных целей;
* если данные включены в федеральные автоматизированные информационные системы и государственные информационные системы персональных данных;
* если данные обрабатываются без использования средств автоматизации в соответствии с законами РФ.

Важно отметить, что оговаривается обязанность оператора не передавать персональные данные третьим лицам.

При этом многие организации допускают ошибку в том, что если они не обязаны уведомлять уполномоченный орган об обработке ПД, то можно не выполнять обязанности, возлагаемые законом на операторов ПД. Такие действия являются противозаконными, однозначно трактуются как невыполнение требований законодательства и караются мерами, предусмотренными Законом.

Рассмотрим основные обязанности оператора персональных данных, предусмотренные ФЗ-№152:

Обеспечение безопасности обработки персональных данных, что означает обязанность "принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий".

Уведомительный характер обработки персональных данных. В соответствии со статьей 2 ФЗ-№152 оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов ПД (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. Роскомнадзор вносит сведения об операторе в реестр операторов. Информация, содержащаяся в реестре, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, является общедоступной.

При получении персональных данных (в том числе от третьих лиц) оператор ПД до начала обработки обязан получить у субъекта этих ПД письменное разрешение на их обработку (за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если они являются общедоступными). Важно отметить, что субъект имеет право отозвать данное разрешение.

Оператор обязан предоставить субъекту ПД по требованию все имеющиеся сведения о нем, целях и условиях обработки, способах защиты его персональных данных.

Оператор также должен уничтожить или блокировать соответствующие персональные данные, внести в них необходимые изменения по предоставлении субъектом ПД 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.

Более того, оператор ПД обязан предоставить доказательство получения согласия субъекта ПД на обработку его персональных данных, а в случае обработки общедоступных персональных данных на него возлагается обязанность доказать, что обрабатываемые ПД являются общедоступными.

Подконтрольность и поднадзорность деятельности операторов персональных данных государственным органам. Это означает обязанность оператора сообщать в уполномоченный орган по защите прав субъектов ПД по его запросу информацию, необходимую для осуществления деятельности указанного органа. Функциями контроля и надзора государство наделило Роскомнадзор, ФСТЭК и ФСБ.

Законом также предусмотрены случаи, когда не требуется согласие субъекта ПД на обработку сведений о нем:

* обработка персональных данных осуществляется на основании других федеральных законов, например, некоторыми Федеральными законами предусматриваются случаи обязательного предоставления субъектом ПД своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
* оператор и субъект ПД связаны договором на выполнение действий, которые требуют обработки персональных данных этого субъекта, например, договор, по которому туристическая фирма (оператор) имеет право использовать персональные данные субъекта для бронирования гостиницы;
* обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД, если получение его согласия невозможно, например, госпитализация человека при несчастном случае;
* 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 ПД;
* осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПД лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Во всех других случаях оператор должен соблюдать требования российского законодательства по обработке персональных данных. Законом предусмотрена гражданская, уголовная, административная, дисциплинарная и иная ответственность за нарушение его требований.

Так, Кодекс об административных правонарушениях предусматривает максимальный штраф в 500000 рублей за невыполнение законного предписания Роскомнадзора (ст. 19.5 КоАП). Тот же Кодекс предусматривает приостановку деятельности организации на срок до 90 суток при осуществлении деятельности по защите персональных данных без лицензии (ст. 19.20 КоАП).

В уголовном кодексе говорится о штрафе в 300000 руб., обязательных работах на срок до 1-го года, аресте до 6 месяцев и лишении права занимать должность на срок до 5 лет в случае осуществления защиты персональных данных без лицензии в случаях, если это деяние причинило крупный ущерб гражданам (ст. 171 УК).

При систематических и грубых нарушениях Роскомнадзор имеет право ходатайствовать об отзыве лицензий на основной вид деятельности.

# *Уведомление Роскомнадзора о начале обработки персональных данных*

Уведомить Роскомнадзор о начале обработки персональных данных (ст. 22 закона о персональных данных). Такое уведомление необходимо направить в ведомство до начала обработки данных, указав в нем:

* наименование (ФИО), 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;
* меры защиты персональных данных;
* ФИО физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
* дату начала обработки персональных данных;
* срок или условие прекращения обработки персональных данных;
* данные о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
* информацию о месте нахождения базы данных информации, содержащей персональные данные россиян;
* сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ (речь, в частности, идет об уровнях защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности, требованиях к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных, а также о требованиях к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных).

При этом есть ситуации, когда уведомлять Роскомнадзор об обработке персональных данных не нужно. Это, например, обработка работодателем данных работников, получение оператором данных клиента при заключении с ним договора (если эта информация не предоставляется третьим лицам без согласия на то субъекта и используется исключительно для исполнения указанного договора), обработка общедоступных персональных данных, оформление лицу однократного пропуска на территорию оператора, использование только ФИО субъекта и др. (ч. 2 ст. 22 закона о персональных данных).

Распространять персональные данные без согласия на то субъекта нельзя (ст. 7 закона о персональных данных). Данная обязанность лиц, получивших доступ к персональным данным, является одной из основных. В частности, при передаче персональных данных работников работодатель обязан:

* не сообщать персональные данные работника третьей стороне без его письменного согласия (за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, и в других предусмотренных законом случаях – например, при передаче данных в ФСС, ПФР, налоговые органы, военные комиссариаты, прокуратуру, правоохранительные органы, ГИТ и др.);
* предупредить лиц, получающих персональные данные работника, что эта информация может быть использована лишь в целях, для которых она сообщена – более того, работодатель даже может требовать от таких лиц подтверждения того, что это правило соблюдено;
* осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под подпись;
* разрешать доступ к персональным данным работников только специально уполномоченным лицам, причем они должны иметь право получать лишь те данные работника, которые необходимы для выполнения конкретных функций;
* не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
* ограничивать информацию, передаваемую представителям работников, лишь теми данными работника, которые необходимы для выполнения указанными представителями их функций (ст. 88 ТК РФ).

Для этого организации следует назначить лицо, ответственное за организацию обработки персональных данных (ст. 22.1 закона о персональных данных). Такое лицо обязано осуществлять внутренний контроль за соблюдением оператором и его работниками требований к защите персональных данных, доводить до сведения работников положения закона о персональных данных, локальных актов по вопросам обработки персональных данных, а также организовывать прием и обработку обращений и запросов субъектов персональных данных. Кроме того, в этих же целях следует применять технические меры по обеспечению безопасности обработки, а также издать документы, определяющие политику компании в отношении обработки персональных данных, и др.

При этом политику обработки персональных данных организация должна сделать публичной (ч. 2 ст. 18.1 закона о персональных данных). Наиболее оптимальным способом является размещение документа на сайте оператора. Но в том случае, когда это невозможно, достаточно установить "кармашек" с политикой на бумажном носителе в любом доступном для посетителей организации месте. Исключение составляют операторы, собирающие персональные данные непосредственно через Интернет, – им необходимо опубликовать политику именно на сайте и обеспечить возможность доступа к указанному документу. На официальном сайте Роскомнадзора можно ознакомиться с рекомендациями по составлению политики в отношении обработки персональных данных.

Не стоит путать политику, распространяющуюся в основном на третьих лиц (контрагентов, клиентов и др.), с Положением о защите, хранении, обработке и передаче персональных данных работников – этот документ в отличие от политики является локальным нормативным актом, поэтому делать его публичным не нужно, а вот ознакомить с ним под роспись работников следует обязательно (ст. 22 ТК РФ).

С 1 сентября 2015 года все операторы при сборе персональных данных обязаны обеспечить их обработку с использованием баз данных, находящихся в России (ч. 5 ст. 18 закона о персональных данных). Так называемая локализация персональных данных поначалу вызвала большой резонанс среди специалистов и операторов – требования закона были сформулированы таким образом, что у экспертов возникло немало вопросов. Среди них отсутствие ясности, на какие именно персональные данные будет распространяться данное требование, каких операторов это затронет, допускается ли обработка персональных данных одновременно на российском и иностранном сервере, как определить гражданство субъекта и т. д. На большую часть этих вопросов Роскомнадзор ответил еще до вступления новых требований закона в силу. Так, например, ведомство предоставило операторам право самостоятельно решать вопрос определения гражданства лица, чьи данные обрабатываются, либо применять требование о локализации к персональным данным всех субъектов. Кроме того, Роскомнадзор уточнил, что в том случае, когда при сборе персональные данные были записаны в российскую базу данных, в дальнейшем они могут обрабатываться и в электронной базе, находящейся за пределами страны.

И в политике обработки персональных данных, и в Положении о защите, хранении, обработке и передаче персональных данных работников следует прописать, что при сборе персональных данных оператор обязуется обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных россиян с использованием баз данных, находящихся на территории России, а также указать место нахождения такой базы данных.

Своевременно прекратить обработку персональных данных – одна из важных составляющих ЗПД. Если цель обработки персональных данных достигнута или субъект отозвал свое согласие на их обработку, оператор должен прекратить обработку этих данных и удалить их в 30-дневный срок, если иной срок не определен в соглашении (ч. 4-5 ст. 21 закона о персональных данных).

# *Ответственность за нарушение требований по обращению с персональными данными*

Лицам, нарушившим требования закона о персональных данных, в зависимости от конкретных обстоятельств и серьезности деяния может грозить не только административная и уголовная ответственность, но также гражданско-правовая и даже дисциплинарная (таблица 1). При этом административная ответственность с 1 июля 2017 года ужесточилась – вместо одного состава правонарушения ст. 13.11 КоАП РФ теперь предусматривает семь, а максимальный штраф составляет 75 тыс. руб.

Таблица 1. "Виды ответственности за нарушение закона о персональных данных"

|  |  |  |  |
| --- | --- | --- | --- |
| **Вид ответственности** | **Нарушение** | **Санкция** | **Норма** |
| Административная | Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено законом, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации | Административный штраф на должностных лиц в размере от 5 тыс. до 10 тыс. руб. | Статья 5.39 КоАП РФ |
| Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных | Предупреждение или административный штраф:   * на граждан – от 1 тыс. до 3 тыс. руб.; * на должностных лиц – от 5 тыс. до 10 тыс. руб.; * на юридических лиц – от 30 тыс. до 50 тыс. руб. | Часть 1 ст. 13.11 КоАП РФ |
| Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие | Административный штраф:   * на граждан – от 3 тыс. до 5 тыс. руб.; * на должностных лиц – от 10 тыс. до 20 тыс. руб.; * на юридических лиц – от 15 тыс. до 75 тыс. руб. | Часть 2 ст. 13.11 КоАП РФ |
| Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике обработки персональных данных | Предупреждение или административный штраф:   * на граждан – от 700 до 1 тыс. руб.; * на должностных лиц – от 3 тыс. до 6 тыс. руб.; * на индивидуальных предпринимателей – от 5 тыс. до 10 тыс. руб.; * на юридических лиц – от 15 тыс. до 30 тыс. руб. | Часть 3 ст. 13.11 КоАП РФ |
| Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных | Предупреждение или административный штраф:   * на граждан – от 1 тыс. до 2 тыс. руб.; * на должностных лиц – от 4 тыс. до 6 тыс. руб.; * на индивидуальных предпринимателей – от 10 тыс. до 15 тыс. руб.; * на юридических лиц – от 20 тыс. до 40 тыс. руб. | Часть 4 ст. 13.11 КоАП РФ |
| Невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении (если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки) | Предупреждение или административный штраф:   * на граждан – от 1 тыс. до 2 тыс. руб.; * на должностных лиц – от 4 тыс. до 10 тыс. руб.; * на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; * на юридических лиц – от 25 тыс. до 45 тыс. руб. | Часть 5 ст. 13.11 КоАП РФ |
| Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении них | Административный штраф:   * на граждан – от 700 до 2 тыс. руб.; * на должностных лиц – от 4 тыс. до 10 тыс. руб.; * на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; * на юридических лиц – от 25 тыс. до 50 тыс. руб. | Часть 6 ст. 13.11 КоАП РФ |
| Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных для этого требований или методов | Предупреждение или наложение административного штрафа на должностных лиц в размере от 3 тыс. до 6 тыс. руб. | Часть 7 ст. 13.11 КоАП РФ |
| Непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено законом либо предоставление таких сведений в неполном объеме или в искаженном виде | Административный штраф:   * на граждан – от 100 до 300 руб.; * на должностных лиц – от 300 до 500 руб.; * на юридических лиц – от 3 тыс. до 5 тыс. руб. | Статья 19.7 КоАП РФ |
| Уголовная | Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ | Штраф до 200 тыс. руб., либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо принудительные работы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арест на срок до четырех месяцев, либо лишение свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет) | Статья 137 Уголовного кодекса |
| То же деяние, совершенное с использованием служебного положения | Штраф от 100 тыс. до 300 тыс. руб., либо лишение права занимать определенные должности на срок от двух до пяти лет, либо принудительные работы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет или без такового), либо арест на срок до шести месяцев, либо лишение свободы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет) |
| Незаконное публичное распространение информации, указывающей на личность лица, не достигшего 16 лет, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий | Штраф от 100 тыс. до 300 тыс. руб., либо лишение права занимать определенные должности на срок от трех до пяти лет, либо принудительные работы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет или без такового), либо арест на срок до шести месяцев, либо лишение свободы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет) |
| Неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление ему неполной или заведомо ложной информации, если это причинило вред правам и законным интересам граждан | Штраф до 200 тыс. руб., либо лишение права занимать определенные должности на срок от двух до пяти лет | Статья 140 УК РФ |
| Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование | Штраф до 200 тыс. руб., либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок | Статья 272 УК РФ |
| Гражданско-правовая | Причинение лицу убытков в результате нарушения правил обработки его персональных данных.  Под убытками при этом понимаются:   * расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права; * утрата или повреждение его имущества; * неполученные доходы, которые лицо получило бы, не будь его право нарушено. | Возмещение убытков | Статья 15 Гражданского кодекса |
| Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных | Компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков) | Статья 24 закона о персональных данных, [ст. 151 ГК РФ](http://base.garant.ru/10164072/8/#block_151) |
| Дисциплинарная | Разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей | Увольнение | Подпункт "в" п. 6 ч. 1 ст. 81 Трудового кодекса |
| Иные нарушения в области персональных данных при их обработке | Замечание или выговор | Статья 90, [ст. 192 ТК РФ](http://base.garant.ru/12125268/30/#block_192) |

# Раздел 3. Работа с персональными данными на предприятии

# *Информация, подлежащая защите в информационной системе предприятия*

Действующее законодательство подразделяет информацию на два вида: общедоступная и информация ограниченного доступа (ч. 2 ст. 5 Федерального закона от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации"). Информацию ограниченного доступа можно разделить на две большие группы – это государственная тайна и сведения конфиденциального характера.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (ст. 2 Закона РФ от 21.07.1993 г. № 5485-1 "О государственной тайне").

Перед началом обработки сведений, составляющих государственную тайну, организация должна получить соответствующую лицензию. Санкции за нарушение порядка обработки жесткие. Кроме того, количество субъектов, имеющих подобную информацию, невелико.

К сведениям конфиденциального характера относится порядка 50 видов тайн, наиболее распространенными из них являются коммерческая тайна и личная (семейная) тайна, разновидностью которой являются персональные данные.

Персональные данные в корпоративной информационной системе предприятия (далее – КИС) есть практически всегда. В частности, любая организация, у которой есть хотя бы один работник или паспортные данные хотя бы одного клиента, будет являться оператором персональных данных в понимании Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных". То есть если в корпоративной CRM-системе обрабатываются данные о клиентах (например, ФИО и адрес доставки) или эти данные находятся в файле MS Excel на рабочей станции, можно с уверенностью говорить о том, что в КИС обрабатываются персональные данные и, следовательно, организация обязана выполнять требования по их защите. На практике же руководители большинства организаций этого не понимают и считают, что персональные данные у них не обрабатываются, в связи с чем мер по защите информации до наступления какого-либо инцидента не предпринимают.

Помимо персональных данных, практически в любой КИС есть информация, которая имеет действительную или потенциальную ценность в силу ее неизвестности третьим лицам, разглашения или неконтролируемой передачи которой организация стремится избежать (коммерческая тайна). На практике распространенной является такая ситуация, когда перечень этой информации содержится исключительно в сознании руководителя или собственника организации.

Ключевым является обучение персонала правилам информационной безопасности, которое должно проводиться с определенной периодичностью.

Поэтому нередко персонал неумышленно передает (пересылает участнику информационного обмена, которому она не предназначена) хранящуюся в КИС информацию или разглашает ее (выкладывает в открытый доступ). При этом в отсутствие утвержденного перечня информации, составляющей коммерческую тайну, привлечь сотрудника к дисциплинарной ответственности за совершение указанных действий невозможно.

С учетом изложенного актуальным становится вопрос принятия в организации комплекса мер защиты информации, обрабатываемой в корпоративной информационной системе.

# *Мероприятия по защите сведений ограниченного доступа.*

Одно  из наиболее важных направлений деятельности предприятия, осуществляющего работу со сведениями конфиденциального характера — планирование мероприятий по защите конфиденциальной информации. Планирование указанных мероприятий занимает особое место в системе управления деятельностью как предприятия в целом, так и его структурных подразделений (отдельных должностных лиц). Трудно также переоценить значение этого направления в общей системе организационных мер обеспечения информационной безопасности предприятия.      Основными целями планирования мероприятий по защите информации являются:

* организация проведения комплекса мероприятий по защите конфиденциальной информации, направленных на исключение возможных каналов утечки этой информации;
* установление  персональной ответственности всех должностных лиц предприятия за решение вопросов защиты информации в ходе производственной и иной деятельности предприятия;  - определение сроков (времени, периода) проведения конкретных мероприятий по защите информации; - систематизация (объединение) всех проводимых на плановой основе мероприятий по различным направлениям защиты конфиденциальной информации;
* установление  системы контроля за обеспечением защиты информации на предприятии, а также  системы отчетности о выполнении конкретных мероприятий; - уточнение (конкретизация) функций и задач, решаемых отдельными должностными лицами и структурными подразделениями предприятия.

Основой для планирования мероприятий по защите информации на предприятии служат:

* требования  законодательных и иных нормативных  правовых актов по защите конфиденциальной информации, соответствующих нормативно-методических документов федерального органа исполнительной власти (при наличии ведомственной принадлежности), вышестоящей организации, а при планировании мероприятий по защите информации филиалом или представительством предприятия — указания головного предприятия;
* требования  заказчиков проводимых предприятием  в рамках соответствующих договоров  (контрактов) совместных и других  работ;
* положения международных договоров (соглашений) и иных документов, определяющих участие предприятия в тех или иных формах международного сотрудничества;
* положения внутренних организационно-распорядительных  документов предприятия (приказов, директив, положений, инструкций),определяющих  порядок ведения производственной  и иной деятельности, а также конкретизирующих вопросы защиты конфиденциальной информации на предприятии;
* результаты  комплексного анализа состояния  дел в области защиты информации, проводимого службой безопасности (режимно-секретным подразделением) на основании материалов проверок структурных подразделений (филиалов, представительств) предприятия;
* результаты проверок состояния защиты информации, проведенных вышестоящими организации, федеральными органами исполнительной власти (при наличии ведомственной принадлежности) и заказчиками работ (в рамках выполняемых договоров или контрактов), выработанные на основании этих результатов предложения и рекомендации;
* результаты контроля за состоянием защиты  информации, проводимого органами  безопасности и иными контролирующими органами (в части, их касающейся);  - особенности повседневной деятельности предприятия и специфика выполнения на предприятии работ с использованием различных видов конфиденциальной информации.

Планирование  мероприятий по защите конфиденциальной информации проводится одновременно с планированием основной производственной и иной деятельности предприятия. Планирование может осуществляться на календарный год, календарный месяц, неделю, а также на иной определенный срок, обусловленный проведением важных мероприятий (работ) по видам деятельности предприятия, если они связаны с вопросами конфиденциального характера. Планы мероприятий, разрабатываемые на срок более одного календарного года, относятся, как правило, к стратегическому планированию, остальные планы решают тактические задачи.

В целях эффективного решения задач  по защите конфиденциальной информации в рамках наиболее важных и масштабных работ, а также в ходе реализации на предприятии федеральных целевых, государственных, ведомственных и  других программ могут разрабатываться отдельные планы, носящие характер программно-целевого планирования. Такими программами могут быть реконструкция предприятия, внедрение новых технологий, в том числе информационных, и т.п.

Планы мероприятий по защите информации относятся к документам с ограниченным доступом, учитываются и хранятся в службе безопасности (режимно-секретном подразделении) предприятия в порядке, установленном для документов соответствующей степени конфиденциальности (секретности).

Разработка  планирующих документов по защите информации на предприятии осуществляется службой безопасности (режимно-секретным подразделением) в тесном взаимодействии с подразделениями (отдельными должностными лицами), в ведении которых находятся задачи, непосредственно касающиеся вопросов защиты информации (подразделение противодействия иностранным техническим разведкам, служба охраны, кадровый орган и др.). Кроме того, при подготовке планов учитываются предложения структурных подразделений предприятия, занимающихся производственной (финансово-хозяйственной) деятельностью или ее обеспечением.

 От полноты и качества разработки организационно-планирующих  документов в полной мере зависит  эффективность проведения мероприятий, направленных на исключение утечки конфиденциальной информации, утрат ее носителей, а также возникновения предпосылок подобных происшествий.

Основным организационно-планирующим документом предприятия является План мероприятий по защите конфиденциальной информации на календарный год.

Данный план наиболее полно и всесторонне отражает мероприятия по защите информации, предполагаемые к проведению в ходе повседневной деятельности предприятия в течение календарного года. При подготовке плана учитываются вновь принятые (подписанные, утвержденные) нормативные правовые акты и методические документы по защите конфиденциальной информации, действующие приказы и текущие указания вышестоящих органов государственной власти и организаций (при наличии ведомственной принадлежности или иной подчиненности).

План мероприятий по защите конфиденциальной информации на предприятии на календарный год утверждается руководителем предприятия до начала календарного года, на который он разработан. При необходимости план согласовывается с соответствующим органом безопасности. Утвержденный план под расписку доводится до сведения заместителей руководителя предприятия, руководителей структурных подразделений и отдельных должностных лиц, ответственных за проведение указанных в плане мероприятий.

Типовой план мероприятий по защите конфиденциальной информации на календарный год содержит следующие основные разделы:

* организаторская работа руководства предприятия — разработка организационно-планирующих документов в ходе повседневной деятельности предприятия и при выполнении предприятием всех видов работ;
* представляемые в вышестоящий орган государственной власти или в вышестоящую организацию доклады и донесения о состоянии защиты информации; подготовка и издание приказов руководителя предприятия по различным вопросам в сфере защиты конфиденциальной информации; переработка и уточнение должностных обязанностей сотрудников и др.

Особое внимание уделяется планированию проводимых по окончании календарного года мероприятий по проверке наличия носителей информации комиссией предприятия. Для предприятий, работающих со сведениями, составляющими государственную тайну, проведение проверок наличия носителей этих сведений планируется в соответствии со сроками, определенными в нормативных правовых актах по обеспечению режима секретности.

При наличии у предприятия подчиненных организаций, филиалов и представительств планируются проверки состояния защиты информации в этих организациях комиссиями головного предприятия.

При необходимости отдельным пунктом отражаются вопросы организации учета осведомленности лиц в сведениях особой важности и совершенно секретных сведениях, подготовки соответствующих заключений.

При планировании мероприятий по защите информации учитываются все возможные  виды и способы проявления чрезвычайных ситуаций, мероприятия по защите информации при возникновении чрезвычайных ситуаций отражаются в соответствующих планах работы предприятия (его структурных подразделений) на календарный месяц.

В данном разделе плана (либо в отдельном приложении к плану) указываются также:

* фамилия, имя, отчество, домашний адрес и контактные телефоны (в том числе мобильной связи) каждого сотрудника, принимающего участие в ликвидации последствий чрезвычайной ситуации на объектах предприятия;
* очередность и порядок вызова (оповещения) всех сотрудников, участвующих в выполнении работ по ликвидации последствий чрезвычайной ситуации, в зависимости от ее вида, сроки прибытия этих сотрудников на объекты предприятия;
* обязанности каждого сотрудника предприятия и последовательность выполнения им мероприятий (работ) в соответствии с конкретным планом действий; перечень сил и средств (в том числе транспортных средств и средств связи), привлекаемых к решению задач ликвидации последствий чрезвычайных ситуаций.

Контроль  за выполнением конкретных мероприятий, включенных в план, осуществляется руководителем предприятия и  его заместителем, в ведении которого находятся вопросы защиты конфиденциальной информации.

# *Ограничение доступа к персональным данным*

В соответствии с п.8 ст. 14 Закона N 152-ФЗ, ограничения могут быть наложены в случае, если:

* обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
* 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;
* обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
* доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
* обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

За лицом, так называемом субъекте, чьи персональные данные подлежат обработке, закреплено право на обжалование действий или бездействия оператора. Так, если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке (п.1 ст. 18 Закона N 152-ФЗ).

# *Локальные акты по вопросам обработки персональных данных*

1. Локальный нормативный акт должен (далее – ЛНА) быть утвержден генеральным директором, директором, советом директоров или другими уполномоченными лицами, определенными уставом компании.

2. При утверждении ЛНА не обязательно учитывать мнение представительного органа работников.

3. Закон не устанавливает требований к количеству ЛНА по работе с персональными данными. Часто у работодателей целый свод таких положений.   
  
Например, ЛНА могут определять:

* общие принципы обработки данных,
* порядок обработки данных на бумажных носителях,
* порядок обработки данных в информационных системах,
* порядок хранения персональных данных,
* порядок передачи данных,
* порядок обработки данных должностными лицами и проч.

4. В каждый ЛНА стоит включить раздел «Общие положения».  В нем указать значение ЛНА, основные термины и понятия:

* «персональные данные»,
* «оператор»,
* «обработка персональных данных»,
* «трансграничная передача персональных данных» и проч.

Также можно указать права и обязанности сторон: работодателя как оператора и сотрудников — субъектов персональных данных.

5. Сотрудников компании под роспись нужно ознакомить со всеми внутренними актами компании, которые устанавливают порядок обработки персональных данных (ст. 86 ТК РФ).

Цели обработки персональных данных и содержание   
должны быть конкретными и законными.

Могут опираться на регламенты деятельности работодателя, бизнес-процессы.  
Примеры целей:

* использование персональных данных в информационных системах, с которыми работает компания,
* использование данных при составлении документов,
* передача данных в государственные инстанции (ФСС, ПФР, ФНС и проч.) и другие организации (банки, страховые компании, гостиницы и проч.),
* сбор данных для принятия решения о приеме кандидата на работу и проч.

В ЛНА нужно указать всех субъектов обработки персональных данных (бывшие и настоящие сотрудники и их родственники, соискатели, клиенты, контрагенты и их представители), цели обработки персональных данных и их перечень.

Указанные в ЛНА персональные данные не должны быть избыточными по отношению к целям.

Например, если речь об обработке персональных данных соискателя, цель — рассмотрение кандидатуры на конкретную должность. Для этой цели достаточно фамилии, имени, отчества, даты, месяца и года рождения, уровня образования, опыта работы, квалификации, знания иностранных языков, контактных телефонов, email.

Если нужно, в ЛНА можно прописать обработку биометрических и специальных персональных данных субъектов (расовая и национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья).

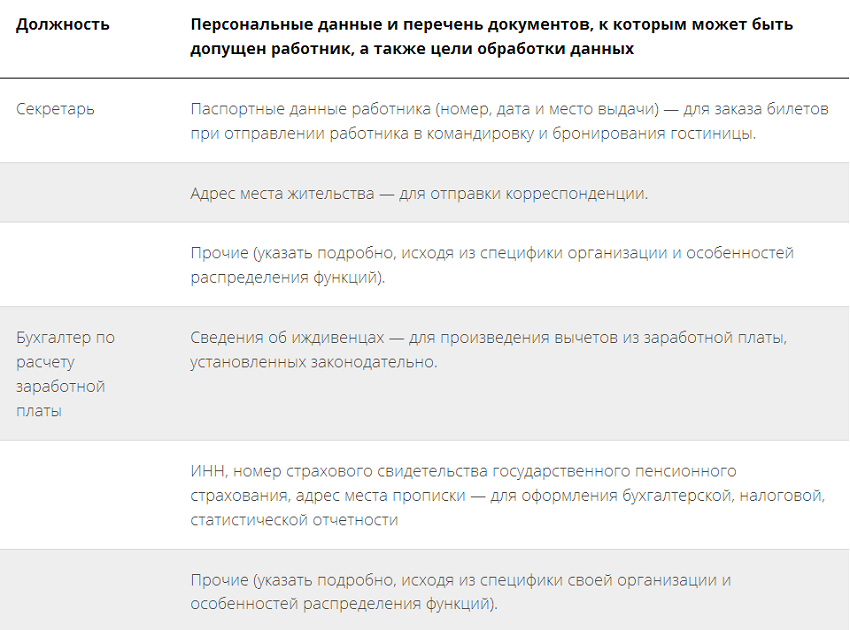
В ЛНА нужно указать перечень должностных лиц, у которых будет внутренний и внешний доступ к персональным данным.

Внутренний доступ может быть полным и ограниченным (таблица 2).

При полном доступе достаточно указать перечень должностей, которым дан такой доступ к персональным данным сотрудников.

При ограниченном — указать должности, перечень персональных данных и действий с ними (с указанием целей обработки).

Таблица 2. Внутренний доступ к персональным данным



Также нужно назначить сотрудника, который будет отвечать за обработку персональных данных в компании (ч. 1 п. 1 ст. 18.1 Закона № 152-ФЗ «О персональных данных»).

Назначить можно прямым приказом работодателя или прописать должность в ЛНА.

Желательно, чтобы сотрудник имел отношение к работе с персональными данными: IT-специалист, HR, специалист по подбору и проч. Он будет получать указания от исполнительного органа компании (дирекция, правление, генеральный директор и проч.).   
Ответственный сотрудник будет:

* контролировать соблюдение законодательства РФ о персональных данных, в том числе требований к их защите;
* информировать сотрудников о новых нормах, локальных актах о персональных данных;
* принимать и обрабатывать обращения и запросы сотрудников и (или) их представителей по вопросам обработки персональных данных.

Нужно прописать в ЛНА условия передачи персональных данных третьим лицам, в том числе за пределы РФ (трансграничная передача): это можно делать на основании договора, поручения на обработку данных и прочее (Таблица 3).

В ЛНА нужно указать:

* наименование и местонахождение третьих лиц,
* цели передачи данных и объемы,
* перечень действий по обработке,
* способы обработки,
* требования к защите данных.

Таблица 3. Трансграничная передача



Необходимо также прописать порядок хранения данных и документов, в которых они содержатся (копии паспортов сотрудников, СНИЛС, ИНН и т.д.).

Базы данных с персональными данными работников должны находиться на территории Российской Федерации. В ЛНА нужно указать место нахождения таких баз.

Нужно отдельно указать сроки хранения данных (не дольше, чем этого требуют цели обработки) в информационных системах и на бумажных носителях. Исключение, когда сроки хранения данных установлены федеральным законом, договором с субъектом персональных данных (сотрудником, партнером и проч.).

Уточните в локальном нормативном акте порядок действий при получении запросов (других обращений) на исправление, удаление, уничтожение персональных данных и прочих требований. Включите в ЛНА формы таких запросов (обращений).

В ЛНА стоит прописать меры, которые компания предпримет для сохранения конфиденциальности персональных данных.

Основные требования к компании (ст. 18.1, 19 Закона № 152- ФЗ «О персональных данных», Приказ ФСТЭК России от 18.02.2013 № 21):

* определение угроз безопасности,
* обнаружение фактов несанкционированного доступа,
* применение мер по обеспечению безопасной обработки данных,
* защита технических средств, на которых хранятся данные,
* установка антивирусов.

«Одноразовая» обработка персональных данных

Речь об информации о лицах, которые один раз прошли на территорию предприятия. При этом у охраны есть распоряжение при пропуске гостей спрашивать у них ФИО, брать у них паспортные данные.

В таких ситуациях можно вести бумажный журнал однократного пропуска на территорию компании (Постановление Правительства РФ от 15.09.2008 № 687). Копировать информацию из журнала нельзя.  
 В ЛНА нужно закрепить:

* порядок пропуска гостей на территорию предприятия (ведение журнала),
* данные, которые охрана запрашивает у гостей и вносит в журнал,
* цели сбора и обработки данных гостей,
* сроки обработки данных,
* перечень лиц (имена или должности), которые ведут журнал и отвечают за его сохранность.

Наконец, компания должна обеспечить неограниченный доступ к документу, в котором определена политика работы с персональными данными (п. 2 ст. 18.1 Закона № 152-ФЗ «О персональных данных»).

Локальный нормативный акт можно опубликовать на сайте компании, на внутреннем портале организации, наконец, на стендах в офисе. Главное — донести информацию до реальных и потенциальных субъектов персональных данных (сотрудников, партнеров).

Подготовка уведомлений об обработке персональных данных в уполномоченный орган

В соответствии с ч. 1 ст. 22 Закона «О персональных данных» операторы обязаны до начала обработки персональных данных уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

Уведомление, предусмотренное ч. 1 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных статьями 18.1 и 19 настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

8) 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;

9) дата начала обработки персональных данных;

10) срок или условие прекращения обработки персональных данных;

11) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

12) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

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

В случае представления оператором уведомления, содержащего неполные или недостоверные сведения, Управление вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

В соответствии с ч. 7 ст. 22 Закона  «О персональных данных в случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Уведомление об изменении сведений представляется Оператором  в территориальное управление Службы на бланке оператора в виде информационного письма с указанием основания изменения сведений в письменной форме, подписанное уполномоченным лицом, с указанием сведений в соответствии с ч. 3 ст. 22 Закона «О персональных данных».

Уведомление об обработке персональных данных, в соответствии с требованиями ч. 3 ст. 22 ФЗ «О персональных данных» необходимо направить в виде документа на бумажном носителе, подписанного уполномоченным лицом, при этом направление сопроводительного письма к уведомлению законом не предусмотрено.

# Раздел 4. Техническая защита персональных данных в информационных системах

# *Автоматизированная и неавтоматизированная обработка персональных данных*

Существует два вида обработки персональных данных: **автоматизированный** и **неавтоматизированный**.

Неавтоматизированная обработка персональных данных осуществляется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 г. "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

Обработка персональных данных является **неавтоматизированной**, если осуществляется при непосредственном участии человека.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков). Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПД для каждой из них должен использоваться отдельный материальный носитель.

Пункты 1 и 2 Постановления РФ помогают решить вопрос о том, какие системы являются автоматизированными, а какие нет. Процитируем их:

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

При этом оператор также может совершить ошибку, неправильно трактуя данные пункты. Дело в том, что почти во всех операциях по обработке ПД участвует человек, но это не значит, что обработка неавтоматизированная. Достаточно просто сохранить информацию в виде файла на компьютере – и обработка тут же станет автоматизированной. Примером неавтоматизированной обработки может стать выдача бумажного одноразового пропуска на территорию организации или талончика к врачу.

Для более детального определения автоматизированной системы обработки ПД обратимся к Конвенции "О защите физических лиц при автоматизированной обработке ПД" от 28 января 1981 года. Данный документ вводит понятие "автоматизированный файл" – любой комплекс данных, подвергающихся автоматизированной обработке. И, соответственно, "**автоматизированная обработка** " включает следующие операции, осуществляемые полностью или частично с помощью автоматизированных средств: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение.

# *Особенности обеспечения безопасности персональных данных в автоматизированных системах*

Автоматизированные системы обработки информации (АС) в общем случае классифицируются по следующим признакам:

* наличие в АС информации различного уровня конфиденциальности;
* уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
* режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается 9 классов защищенности АС от несанкционированного доступа. Каждый класс характеризуется установленным набором требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Деление АС на классы производится в целях выбора оптимальных и достаточных мер защиты для достижения требуемого уровня защищенности.

АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.

В зависимости от структуры АС и способа обработки информации руководящими документами предусмотрены требования и рекомендации к нижеследующим случаям обработки информации:

1. Обеспечение безопасности в автоматизированных рабочих местах (АРМ) на базе автономных ПЭВМ при использовании съемных накопителей большой емкости. Такие рабочие места обладают всеми признаками автоматизированной системы, соответственно, должны удовлетворять определенным требованиям по защите информации. Основной особенностью является исключение хранения на ПЭВМ информации, подлежащей защите.

Обмен информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей. На рабочих местах исполнителей не должно быть неучтенных носителей информации. В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть "закрыты на запись".

При использовании в данном случае Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности, как перед началом работ, с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.

Должна быть согласована и утверждена технология обработки защищаемой информации, предусматривающая такие вопросы, как защита информации, учет носителей, размещения, эксплуатации АРМ и т.п.

1. Обеспечение безопасности в локальных вычислительных сетях. Основными особенностями ЛВС являются распределенное хранение информации, удаленная обработка данных, а также сложность контроля за работой пользователей и общей защищенностью сети. В данном случае средства защиты информации должны использоваться во всех узлах сети, независимо от того, обрабатывают они конфиденциальную информацию или нет.

Персональные данные могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или с использованием межсетевого экрана соответствующего уровня.

Для управления ЛВС и распределения системных ресурсов могут быть назначены администраторы безопасности, имеющие соответствующие права и квалификацию.

Состав пользователей ЛВС должен утверждаться по письменному разрешению руководства, а все изменения регистрироваться. Каждый пользователь и администратор должен иметь уникальные идентификаторы и пароли, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств.

1. Обеспечение безопасности при межсетевом взаимодействии. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах контролируемой зоны. Рекомендуется учитывать разделение трафика по производственной основе и видам деятельности предприятия при построении сети и конфигурировании коммуникационного оборудования.

Подключение ЛВС к другой автоматизированной системе иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:

* в АС класса 1Г - МЭ не ниже класса 4;
* в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.

Если каналы связи выходят за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

# *Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных*

Статья 19 Федерального Закона "О персональных данных" гласит, что оператор при обработке ПД обязан принимать необходимые организационные и технические меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Обеспечение безопасности в соответствии ФЗ-№152 не требуется лишь для обезличенных и общедоступных персональных данных.

Персональные данные могут быть обезличенными, в случае, если над ними были произведены действия, в результате которых невозможно определить их принадлежность конкретному субъекту ПД.

Персональные данные могут быть общедоступными только с письменного согласия субъекта ПД. Они могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом ПД.

Автоматизированная обработка ПД осуществляется в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 г. "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", а также конкретизируются в нормативно-методических документах ФСТЭК и ФСБ.

Во второй лекции мы уже рассматривали определение информационной системы персональных данных.

Информационная система персональных данных (ИСПД) – 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.

Безопасность ПД при их обработке в ИСПД обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных – уполномоченное лицо. При этом оператор должен заключать договор с уполномоченным лицом. Существенным условием этого договора является обязанность уполномоченного лица обеспечить конфиденциальность и безопасность ПД при их обработке в ИСПД.

Обеспечение безопасности ПД при их обработке в ИСПД достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование и распространение персональных данных. Обязанность по обеспечению безопасности ПД при их обработке в ИСПД полностью возлагается на оператора персональных данных.

В связи с этим оператор обязан:

* проводить мероприятия, направленные на предотвращение несанкционированного доступа (далее НСД) к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;
* своевременно обнаруживать факты НСД к персональным данным;
* не допускать воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование;
* незамедлительно восстанавливать ПД, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
* осуществлять постоянный контроль за обеспечением уровня защищенности ПД.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах оператором может назначаться структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности персональных данных.

Информационные системы персональных данных представляют собой совокупность информационных и программно- аппаратных элементов, основными из которых являются:

* ПД, содержащиеся в базах данных, как совокупность информации и ее источников, используемых в информационных системах;
* информационные технологии, применяемые при обработке ПД;
* технические средства, осуществляющие обработку ПД;
* программные средства, применяемые при обработке.
* средства защиты информации.

# *Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПД*

Для обеспечения безопасности персональных данных оператор ПД или уполномоченное лицо обязаны провести следующие мероприятия:

1. определить угрозы безопасности персональных данных при их обработке и построить модель угроз;
2. разработать на основе модели угроз системы защиты персональных данных, обеспечивающих нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
3. проверить готовность средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
4. установить и ввести в эксплуатацию средства защиты информации в соответствии с эксплуатационной и технической документацией;
5. обучить персонал работе со средствами защиты информации;
6. вести учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
7. вести учет лиц, допущенных к работе с персональными данными в информационной системе;
8. контролировать соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
9. разбирать и составлять заключения по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных; осуществить разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
10. составить описание системы защиты персональных данных.

# *Основные принципы обеспечения безопасности персональных данных*

При построении системы защиты персональных данных оператор ПД должен руководствоваться следующими принципами:

1. принцип законности;
2. принцип максимальной дружественности и прозрачности;
3. принцип превентивности;
4. принцип оптимальности и разумной разнородности;
5. принцип адекватности и непрерывности;
6. принцип адаптивности;
7. принцип доказательности и обязательности контроля;
8. принцип самозащиты и конфиденциальности самой системы защиты информации;
9. принцип многоуровневости и равнопрочности;
10. принцип простоты применения и апробированности защиты;
11. принцип преемственности и совершенствования;
12. принцип персональной ответственности и минимизации привилегий для пользователей всех уровней.

**Принцип законности**. Проведение защитных мероприятий должно быть согласовано с действующим законодательством в области информации, информатизации и защиты информации с применением всех дозволенных методов обнаружения и пресечения нарушений при работе с информацией.

**Принцип максимальной дружественности и прозрачности**. Противодействие угрозам безопасности информации всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу ИС, так как меры по защите информации всегда налагают ограничения на работу организационного и технического характера. Поэтому принимаемые меры должны максимально совмещаться с используемыми операционной и программно-аппаратной структурой ИС, а также должны быть понятны и оправданы для пользователей.

**Принцип превентивности.** Меры по защите информации и внедряемые СЗИ должны быть нацелены, прежде всего, на недопущение (пресечение) реализации угроз безопасности информации, а не на устранение последствий их проявления.

**Принцип оптимальности и разумной разнородности.** Для сокращения расходов на создание систем обеспечения безопасности должен осуществляться оптимальный выбор соотношения между различными методами и способами противодействия угрозам безопасности информации. Дополнительно внедряемые средства защиты должны дублировать основные функции защиты, уже используемые в программно-аппаратной среде ИС, и по возможности иметь другое происхождение, чем сама эта среда, что позволяет существенно затруднить процесс преодоления защиты за счет иной логики построения защиты.

**Принцип адекватности и непрерывности.** Решения, реализуемые системами защиты информации, должны быть дифференцированы в зависимости от важности защищаемой информации и вероятности возникновения угроз ее безопасности. Безопасность информации в государственных информационных системах должна обеспечиваться непрерывно в течение всего жизненного цикла систем.

**Принцип адаптивности.** Системы обеспечения информационной безопасности должны строиться с учетом возможного изменения конфигурации ИС, роста числа пользователей, изменения степени конфиденциальности и ценности информации.

**Принцип доказательности и обязательности контроля**. Должны реализовываться организационные меры внутри сети и применение специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации. Должны обеспечиваться обязательность, своевременность и документированность выявления, сигнализации и пресечения попыток нарушения установленных правил защиты.

**Принцип самозащиты и конфиденциальности самой системы защиты информации**.

**Принцип многоуровневости и равнопрочности.** ИС должна реализовывать защиту информации на всех уровнях своей жизнедеятельности (технологическом, пользовательском, локальном, сетевом). Защита должна строиться эшелонировано, и иметь несколько последовательных рубежей таким образом, чтобы наиболее важная зона безопасности находилась внутри других зон. Все рубежи защиты должны быть равнопрочными к возможности реализации угрозы.

**Принцип простоты применения и апробированности защиты**. Должны применяться средства защиты, для которых формально или неформально возможно доказать корректность выполнения защитных функций, проверить согласованность конфигурации различных компонентов, а их применение пользователями и обслуживающим персоналом должно быть максимально простым, чтобы уменьшить риски, связанные с нарушениям правил их использования. По той же причине целесообразно использовать средства защиты информации, допускающие возможность централизованного администрирования.

**Принцип преемственности и совершенствования.** Система защиты информации должна постоянно совершенствоваться на основе преемственности принятых ранее решений и анализа функционирования ИС.

**Принцип персональной ответственности и минимизации привилегий для пользователей всех уровней**. Принимаемые меры должны определять права и ответственности каждого уполномоченного лица. Распределение прав и ответственности должно в случае любого нарушения позволять определить круг виновных. Система обеспечения информационной безопасности должна обеспечивать разделение прав и ответственности между пользователями.

# Раздел 5. Лицензирование деятельности по технической защите конфиденциальной информации

# *Сертификация средств защиты ПД*

Порядок сертификации средств защиты информации в России устанавливается "Положением о сертификации средств защиты информации" от 26 июня 1995г. Сертификация по требованиям безопасности информации представляет собой процедуру оценки соответствия характеристик продукта, услуги или системы, требованиям стандартов, федеральных законов и других нормативных документов.

Участниками процесса сертификации являются:

1. заявители – те, кто хочет получить сертификат соответствия. Заявителями могут быть продавцы продукции, исполнители продукции.
2. федеральный орган по сертификации;
3. центральный орган сертификации – орган, возглавляющий сертификацию однородной продукции (необязательный участник).
4. органы по сертификации средств защиты информации – те, кто проводит сертификацию определенной продукции.
5. испытательные лаборатории – лаборатории, проводящие сертификационные испытания определенной продукции.

В России действуют 4 Федеральных органа по сертификации, но в области защиты персональных данных их два – ФСБ России и ФСТЭК России. В основные обязанности Федерального органа по сертификации входит:

1. создание системы сертификации;
2. выбор способа подтверждения соответствия средств защиты информации;
3. определение перечня средств защиты, для которых необходима сертификация;
4. установление правил аккредитации центральных органов систем сертификации, органов по сертификации средств защиты информации, испытательных лабораторий и проведение соответствующих аккредитаций;
5. выдача сертификатов и лицензий на применение знака соответствия;
6. ведение реестра сертифицированных средств и участников сертификации;
7. осуществление контроля и надзора за соблюдением участниками сертификации правил сертификации и за сертифицированными средствами защиты информации;
8. рассмотрение апелляции по вопросам сертификации;
9. периодическая публикация информации о сертификации;
10. организация подготовки и аттестации экспертов-аудиторов;
11. приостановление, продление или отмена действия выданных сертификатов.

Органы сертификации:

1. участвуют в определении схемы проведения сертификации средств защиты информации с учетом предложений заявителя;
2. уточняют требования, на соответствие которым проводятся сертификационные испытания;
3. рекомендуют заявителю испытательный центр (лабораторию);
4. утверждают программы и методики проведения сертификационных испытаний;
5. проводят экспертизу технической, эксплуатационной документации на средства защиты информации и материалов сертификационных испытаний;
6. оформляют экспертное заключение по сертификации средств защиты информации и представляют их в федеральный орган по сертификации;
7. организуют, при необходимости, предварительную проверку (аттестацию) производства сертифицируемых средств защиты информации;
8. участвуют в аккредитации испытательных центров (лабораторий) и органов по аттестации объектов информатизации;
9. организуют инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации и участвуют в инспекционном контроле за деятельностью испытательных центров (лабораторий);
10. хранят документацию (оригиналы), подтверждающую сертификацию средств защиты информации;
11. ходатайствуют перед федеральным органом по сертификации о приостановке или отмене действия выданных сертификатов;
12. формируют и актуализируют фонд нормативных и методических документов, необходимых для сертификации, участвуют в их разработке;
13. представляют заявителю необходимую информацию по сертификации.

Испытательные центры (лаборатории) в пределах установленной области аккредитации:

1. осуществляют отбор образцов средств защиты информации для проведения сертификационных испытаний;
2. разрабатывают программы и методики сертификационных испытаний, осуществляют сертификационные испытания средств защиты информации, оформляют протоколы сертификационных испытаний и технические заключения;
3. маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном правилами системы сертификации;
4. участвуют в аттестации производства сертифицируемых средств защиты информации.

Испытательные центры (лаборатории) несут ответственность за полноту испытаний средств защиты информации, достоверность, объективность и требуемую точность измерений, своевременную проверку средств измерений и аттестацию испытательного оборудования.

Органы сертификации средств защиты информации и испытательные лаборатории проходят процедуру аккредитации на право проведения работ по сертификации, в ходе которой федеральный орган по сертификации проверяет их способность на проведение данных работ и выдает разрешение.

Сертификация проводится на материально-технической базе аккредитованных испытательных лабораторий. В отдельных случаях возможно проведение испытаний на базе заявителя при надлежащем контроле со стороны органа сертификации.

Изготовители обязаны извещать орган по сертификации, который выдал сертификат на их продукцию, об изменениях в технологии изготовления или составе сертифицированного средства защиты информации.

Процедура сертификации включает:

1. подачу и рассмотрение заявки на проведение сертификации (продления срока действия) средства защиты информации в Федеральный орган по сертификации. Заявка оформляется на бланке заявителя и заверяется печатью. Федеральный орган назначает орган по сертификации и испытательную лабораторию, после чего заявитель отправляет туда сертифицируемое средство защиты информации.
2. сертификационные испытания средств защиты информации и (при необходимости) аттестацию их производства. Сроки проведения испытаний устанавливаются на договорной основе между заявителем и лабораторией. По результатам испытаний оформляется заключение, которое отправляется в орган по сертификации и заявителю.
3. экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия. На основании заключения испытательной лаборатории орган сертификации делает заключение и отправляет его в Федеральный орган по сертификации. После присвоения сертификату регистрационного номера, его получает заявитель. Срок действия сертификата – 3 года.
4. осуществление государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации. По результатам контроля Федеральный орган по сертификации может приостановить или аннулировать сертификат в следующих случаях:

* изменения на законодательном уровне, касающиеся требований к средствам защиты информации, методам испытаний и контроля;
* изменение технологии изготовления, конструкции (состава), комплектности средств защиты информации и системы контроля их качества;
* невыполнение требований технологии изготовления, контроля и испытаний средств защиты информации;
* несоответствие сертифицированных средств защиты информации техническим условиям или формуляру, выявленное в ходе государственного или инспекционного контроля;
* отказ заявителя в допуске (приеме) лиц, уполномоченных осуществлять государственный контроль и надзор, инспекционный контроль за соблюдением правил сертификации и за сертифицированными средствами защиты информации.

1. информирование о результатах сертификации средств защиты информации.
2. рассмотрение апелляций. Апелляция подается в федеральный орган по сертификации и рассматривается в месячный срок с участием независимых экспертов и заинтересованных сторон.

Органы по сертификации и испытательные лаборатории несут ответственность за выполнение своих функций, обеспечение сохранности информации ограниченного доступа, материальных ценностей, предоставленных заявителем, а также за соблюдение авторских прав разработчика при испытаниях его средств защиты информации.

# *Требования законодательства к средствам защиты ПД*

Важным моментом при построении СЗПД является пункт 5 "Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденного Постановлением Правительства Российской Федерации от 17.11.2007 № 781, которое гласит, что средства защиты информации, используемые в ИСПД, должны в установленном порядке проходить процедуру соответствия (сертификацию). Порядок сертификации устанавливается уполномоченными органами, которыми в случае защиты ПД являются ФСТЭК и ФСБ России. Сертификации подлежат системы, продукты и услуги защиты информации от НСД. В рамках систем обязательной сертификации организации должны сертифицировать средства и продукты. Например, в руководящих документах Гостехкомиссии России продуктом может выступать средство вычислительной техники (СВТ), средство защиты информации (СЗИ), межсетевой экран (МЭ), программное обеспечение (ПО) и др.

Система – это объект информатизации, где обрабатывается реальная информация. По этой причине к системам предъявляются дополнительные требования, касающиеся в том числе организационных мер и физической защиты.

Программное обеспечение СЗПД для защиты от угроз конфиденциальности, целостности и доступности, применяемое в ИСПД 1 класса, подлежит сертификации на отсутствие недекларированных возможностей согласно п.2.12 Приказа ФСТЭК России №58.

В соответствии с Руководящим документом Гостехкомиссии России "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей", утвержденным приказом Председателя Гостехкомиссии от 04.06.1999 № 114,  **недекларированные возможности** - функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. Порядок классификации по уровню контроля отсутствия недекларированных возможностей определен указанным выше руководящим документом Гостехкомиссии. Данное требование обусловлено тем, что большинство современных атак использует уязвимости в программном обеспечении системы. Основной метод нахождения уязвимостей в программе – детальное изучение программного кода. Данное требование может привести к выводу из эксплуатации в ИСПД зарубежных средств защиты информации, так как для сертификации необходимо предоставить код в открытом виде.

При просмотре сертификата к средству защиты информации необходимо обратить внимание, на соответствие каким документам проводились сертификационные испытания.

# *Требования законодательства к ИСПД*

До февраля 2010 года проведение аттестации ИСПД было обязательным этапом построения системы защиты. После введения Приказа ФСТЭК №58 ситуация изменилась, так как документ отменил обязательность аттестации, предоставив операторам самим решать, проводить ее или нет. Тем не менее, это не отменяет необходимости проведения оценки соответствия принятых мер по обеспечению безопасности требованиям законодательства, о чем говорят в частности – постановление Правительства РФ № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке и ИСПДн" и 184-ФЗ "О техническом регулировании".

Аттестация ИСПД предназначена для официального подтверждения эффективности и достаточности мер по обеспечению безопасности ПД в данной ИСПД. Аттестация должна предшествовать началу обработки данных. Порядок проведения аттестации регламентирован "Положением по аттестации объектов информатизации по требованиям безопасности информации" от 25 ноября 1994 г.

Результатом аттестации является документ, называемый "Аттестат соответствия", который подтверждает, что ИСПД удовлетворяет требованиям стандартов и нормативно-технических документов по безопасности ПД ФСТЭК и Гостехкомиссии России (в настоящее время это другая организация).

Этапы аттестации включают в себя:

* разработка программы и методики аттестационных испытаний;
* подачу и рассмотрение заявки на аттестацию;
* предварительное ознакомление с аттестуемым объектом;
* испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
* заключение договоров на аттестацию;
* проведение аттестационных испытаний объекта информатизации;
* оформление, регистрация и выдача "Аттестата соответствия";
* осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
* рассмотрение апелляций.

Испытания, в процессе которых производится оценка эффективности защищенности информации от несанкционированного доступа (c применением специализированного программного обеспечения). После окончания испытаний подготавливаются отчетные документы, на основании которых принимается решение об аттестации ИСПД.

Органы по аттестации объектов информатизации аккредитуются Гостехкомиссией России и получают от нее лицензию на право проведения аттестации объектов информатизации. Такими органами могут быть отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры Гостехкомиссии России.

Аттестационные испытания предполагают проведение следующих проверок:

* проверка состояния технологического процесса автоматизированной обработки персональных данных в ИСПД;
* проверка ИСПД на соответствие организационно-техническим требованиям по защите информации;
* испытания ИСПД на соответствие требованиям по защите информации от несанкционированного доступа.

Результатом аттестации являются:

* Протокол аттестационных испытаний;
* Заключение по результатам аттестационных испытаний;
* Аттестат соответствия на ИСПД (выдается в случае положительного Заключения);
* Акт о переводе СЗПД в промышленную эксплуатацию (в случае наличия положительного заключения по результатам аттестационных испытаний ИСПД).

Следует указать, что если заявитель пожелает только аттестовать ИСПД как объект информатизации, то пока действуют традиционные нормативные требования по аттестации объектов информатизации, в которых обрабатывается конфиденциальная информация.

# *Лицензирование деятельности по защите персональных данных*

Для проведения деятельности по защите ПД операторы должны получить лицензию в соответствии с Постановлением правительства РФ "Об организации лицензирования отдельных видов деятельности" от 26.01.2006 г. Это требование касается обработки ПД в ИСПД 1, 2 класса и распределенных информационных систем 3 класса.

Лицензирование деятельности по технической защите информации осуществляет ФСТЭК России. Порядок лицензирования деятельности определяется "Положением о лицензировании деятельности по технической защите конфиденциальной информации".

Лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

1. наличие в штате соискателя лицензии 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 технической защиты информации;
2. наличие у соискателя лицензии помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;
3. наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;
4. использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;
5. использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;
6. наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю

Для получения лицензии соискатель направляет в ФСТЭК следующие документы:

1. заявление на предоставление лицензии;
2. копии документов, подтверждающих квалификацию специалистов;
3. копии документов, подтверждающих право соискателя на помещения (например, свидетельство о собственности или договор аренды);
4. копии аттестатов соответствия защищаемых помещений требованиям безопасности;
5. копия технического паспорта АС;
6. копии документов, подтверждающих право использования программных средств;
7. сведения о наличии производственного и контрольно-измерительного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемой деятельности, с приложением копий документов о проверке контрольно-измерительного оборудования;
8. сведения о том, что соискатель имеет все нормативно- правовые акты, нормативно-методические и методические документы по вопросам технической защиты информации.

Лицензия выдается на 5 лет и по окончании срока действия может быть продлена.

# *Регуляторы в области защиты персональных данных*

В соответствии с ФЗ "О персональных данных" выделяют три регулятора в области защиты персональных данных:

* Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее Роскомнадзор) в части, касающейся соблюдения норм и требований по обработке персональных данных и защиты прав субъектов персональных данных;
* Федеральная служба безопасности РФ (далее ФСБ) в части, касающейся соблюдения требований по организации и обеспечению функционирования шифровальных (криптографических) средств в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПД;
* Федеральная служба по техническому и экспортному контролю (далее ФСТЭК) в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПД (не криптографическими методами) при их обработке в ИСПД.

В целях контроля соблюдения операторами требований безопасности в области защиты ПД регуляторы проводят плановые и внеплановые проверки.

Роскомнадзор проводит плановые проверки с целью контроля сведений, указанных в уведомлении уполномоченного органа по защите ПД, а также внеплановые – на основании заявления физических лиц с целью проверки информации, указанной в данном заявлении.

ФСБ России имеет право проводить плановые проверки:

* представление по запросу отчета по лицензируемым видам деятельности;
* представление копий аттестатов соответствия по требованиям информационной безопасности на автоматизированные системы, в составе которых эксплуатируются системы криптографической защиты информации (СКЗИ);
* явочная проверка выполнения организационных мер на объектах лицензируемых видов деятельности.
* ФСТЭК РФ уполномочен осуществлять плановые проверки:
* представление по запросу отчета по лицензируемым видам деятельности;
* представление копий аттестатов соответствия по требованиям информационной безопасности на автоматизированные системы;
* представление копий аттестатов соответствия на защищаемые помещения по требованиям безопасности;
* явочная проверка выполнения организационных мер на объектах лицензируемых видов деятельности.

Плановые и внеплановые проверки осуществляются в соответствии с Федеральным законом от 26 декабря 2008 г. N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

В рамках межведомственного сотрудничества между Роскомнадзором, ФСТЭК России и ФСБ РФ достигнута договоренность о проведении совместных мероприятий по контролю и надзору в области персональных данных.

# *Проверки Роскомнадзора*

Роскомнадзор осуществляет проверку выполнения требований законодательства в области обеспечения безопасности персональных данных с целью защиты прав субъектов.

В соответствии с ФЗ "О персональных данных" Роскомнадзор имеет право:

1. запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
2. осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
3. требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
4. принимать решение по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований ФЗ "О персональных данных";
5. обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;
6. направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;
7. направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;
8. вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;
9. привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

Контроль осуществляется с помощью плановых и внеплановых проверок и в строгом соответствии с установленным порядком проведения данных проверок. Проверки осуществляет Роскомнадзор или его территориальные органы.

Плановые проверки проводятся на основании ежегодного плана проведения проверок:

* в отношении Операторов, включенных в Реестр операторов, осуществляющих обработку персональных данных;
* в отношении Операторов, не включенных в Реестр, но осуществляющих обработку персональных данных.
* Внеплановые проверки проводятся по следующим основаниям:
* истечение срока исполнения оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных.
* поступление в Роскомнадзор или его территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:

1. возникновение угрозы причинения вреда жизни, здоровью граждан;
2. причинение вреда жизни, здоровью граждан;
3. нарушение прав и законных интересов граждан действиями (бездействием) Операторов при обработке их персональных данных;
4. нарушение Операторами требований законодательства в области персональных данных, а также о несоответствии сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

Обращение гражданина РФ, не позволяющее установить его лицо, либо не содержащее сведения о фактах, указанных выше, не может являться основанием для внеплановой проверки.

О проведении внеплановой выездной проверки оператор уведомляется не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом.

Если в результате деятельности оператора причинен или причиняется вред жизни, здоровью граждан, предварительное уведомление оператора о начале проведения внеплановой выездной проверки не требуется.

**Срок проведения, как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней.**

В исключительных случаях срок проведения проверки может быть продлен, но не более чем на 20 рабочих дней, в отношении малых предприятий и микропредприятий – на 15 часов.

В ходе проверки осуществляется следующее:

1. рассмотрение документов оператора, таких как уведомление об обработке, письменное согласие субъекта, локальных документов, регламентирующих порядок хранения и обработки ПД;
2. исследование ИСПД в части, касающейся субъектов ПД.
3. Основанием для приостановления проверки является:

* необходимость получения заключений экспертов по вопросам обработки персональных данных, связанным с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований;
* мотивированное решение руководителя контролирующего органа, принятое по причине изъятия документов, являющихся объектами контроля, проведенного ранее сотрудниками прокуратуры, правоохранительных органов, болезни должностных лиц, проводящих проверку. Оператору представляется копия приказа, в котором указываются причины приостановления проверки и период, на который данная проверка приостановлена.

Основанием для принятия решения об исключении Оператора из плана проведения плановых проверок является:

* ликвидация или реорганизация Оператора;
* прекращение Оператором деятельности по обработке персональных данных.

Проверка соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных завершается:

* составлением и вручением Оператору акта проверки;
* выдачей Оператору предписания об устранении выявленных нарушений требований законодательства Российской Федерации в области персональных данных;
* составлением протокола об административном правонарушении в отношении Оператора;
* подготовкой и направлением материалов проверки в органы прокуратуры, другие правоохранительные органы для решения вопроса о возбуждении дела об административном правонарушении, о возбуждении уголовного дела по признакам правонарушений (преступлений), связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

# *Проверки ФСБ*

Проверка ФСБ проводится на основании распоряжения или приказа начальника 8 Центра ФСБ России либо лица его замещающего. Проверка осуществляется должностными лицами, указанными в данном приказе. В приказе указывается следующее:

1. наименование органа государственного контроля (надзора);
2. фамилии, имена, отчества, должности должностного лица или должностных лиц, уполномоченных на проведение проверки, а также привлекаемых к проведению проверки экспертов, представителей экспертных организаций;
3. наименование юридического лица или фамилия, имя, отчество индивидуального предпринимателя, проверка которых проводится;
4. цели, задачи и предмет проверки;
5. правовые основания проведения проверки;
6. перечень мероприятий по контролю (надзору), необходимых для достижения целей и задач проведения проверки;
7. даты начала и окончания проведения проверки.

**Общий срок проверки** не может превышать 20 рабочих дней, для малого предпринимательства – не более 50 часов, для микропредприятия – 15 часов.

При проведении проверки ФСБ не вправе:

1. проверять выполнение требований, не относящихся к компетенции ФСБ России;
2. осуществлять плановую или внеплановую проверку в случае отсутствия при ее проведении руководителя или уполномоченного представителя юридического лица, индивидуального предпринимателя, его уполномоченного представителя;
3. требовать представления документов, информации, если они не являются объектами проверки и не относятся к предмету проверки, а также изымать оригиналы документов, относящихся к предмету проверки;
4. распространять информацию, составляющую охраняемую законом тайну и полученную в результате проведения проверок, за исключением случаев, предусмотренных законодательством Российской Федерации;
5. превышать установленные сроки проведения проверки;
6. осуществлять выдачу юридическим лицам, индивидуальным предпринимателям предписаний или предложений о проведении за их счет мероприятий по контролю.

Ниже приведен перечень проверяемых в рамках проверки требований:

1. Организация системы организационных мер защиты персональных данных:

* область применения средств криптографической защиты информации (далее - СКЗИ) в информационных системах персональных данных;
* наличие ведомственных документов и приказов по организации криптографической защиты информации;
* выполнение рекомендаций и указаний ФСБ России (при их наличии) по вопросам организации связи с использованием криптосредств.

1. Организация системы криптографических мер защиты информации:

* наличие модели угроз нарушителя;
* соответствие модели угроз исходным данным;
* соответствие требуемого уровня криптографической защиты полученной модели нарушителя;
* соответствие используемых СКЗИ полученному уровню криптографической защиты;
* наличие документов по поставке СКЗИ оператору.

1. Разрешительная и эксплуатационная документация:

* наличие необходимых лицензий для использования СКЗИ в информационных системах персональных данных;
* наличие сертификатов соответствия на используемые СКЗИ;
* наличие эксплуатационной документации на СКЗИ (формуляров, правил работы, руководств оператора и т.п.);
* порядок учета СКЗИ, эксплуатационной и технической документации к ним;
* выявление несертифицированных ФСБ России (ФАПСИ) СКЗИ.

1. Требования к обслуживающему персоналу:

* порядок учета лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных в информационной системе;
* наличие функциональных обязанностей ответственных пользователей СКЗИ;
* укомплектованность штатных должностей личным составом, а также достаточность имеющегося личного состава для решения задач по организации криптографической защиты информации;
* организация процесса обучения лиц, использующих СКЗИ, применяемых в информационных системах, правилам работы с ними и другим нормативным документам по организации работ (связи) с использованием СКЗИ.

1. Эксплуатация СКЗИ:

* проверка правильности ввода СКЗИ в эксплуатацию и соответствие условий эксплуатации технических средств удостоверяющего центра (при наличии) требованиям эксплуатационной документации и сертификатов соответствия;
* оценка технического состояния СКЗИ, соблюдения сроков и полноты проведения технического обслуживания, а также проверка соблюдения правил пользования СКЗИ и порядка обращения с ключевыми документами к ним.

1. Оценка соответствия применяемых СКЗИ:

соответствие программного обеспечения, реализующего криптографические алгоритмы используемых СКЗИ, эталонным версиям, проходившим сертификацию в ФСБ России;

проведение (при необходимости) на местах осуществления проверки оперативных тематических исследований используемых СКЗИ.

1. Организационные меры:

* выполнения требований по размещению, специальному оборудованию, охране и организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, а также соответствия режима хранения СКЗИ и ключевой документации предъявляемым требованиям;
* оценка степени обеспечения оператора криптоключами и организации их доставки.
* проверка наличия инструкции по восстановлению связи в случае компрометации действующих ключей к СКЗИ.
* порядок проведения разбирательств и составления заключений по фактам нарушения условий хранения носителей персональных данных или использования СКЗИ.

По результатам проверки составляется акт проверки в двух экземплярах. В акте указываются результаты проверки, в том числе нарушения, если они есть.

# *Проверка ФСТЭК*

ФСТЭК осуществляет плановые и внеплановые проверки лицензиатов (тех, кто имеет лицензии ФСТЭК). Плановая проверка в отношении одной организации может проводиться не чаще 1 раза в год. Предметом плановой проверки является соблюдение лицензиатом лицензионных требований и условий в процессе осуществления деятельности по технической защите конфиденциальной информации. Плановые проверки осуществляются согласно ежегодному плану.

Основанием для включения лицензиата в план является истечение трех лет со дня:

1. государственной регистрации;
2. последней плановой проверки.

Плановая проверка проводится в документарной или выездной форме. Порядок проведения проверок регламентируется Федеральным законом "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

О проведении проверки лицензиата уведомляют не позднее, чем за 3 дня до проведения.

Основанием для проведения внеплановой проверки является:

1. истечение срока действия предписания об устранении нарушений;
2. поступление обращений и заявлений в ФСТЭК о фактах:

* возникновения угрозы причинения вреда безопасности государства;
* причинение вреда безопасности государства.

Если обращение или заявление не позволяет идентифицировать заявителя, а также не содержат фактов, перечисленных выше, оно не может быть основанием для внеплановой проверки.

В ходе документарной проверки проверяются сведения, содержащиеся в документах лицензиата, устанавливающих его организационно-правовую форму, права и обязанности, документы, используемые при осуществлении его деятельности и связанные с исполнением им лицензионных требований и условий, исполнением предписаний ФСТЭК России.

Документарная проверка (как плановая, так и внеплановая) проводится по месту нахождения ФСТЭК России (управления ФСТЭК России по федеральному округу).

Предметом выездной проверки являются содержащиеся в документах лицензиата сведения, а также соответствие лицензиата лицензионным требованиям и условиям.

Выездная проверка (как плановая, так и внеплановая) проводится по месту нахождения лицензиата -юридического лица, месту осуществления деятельности лицензиата - индивидуального предпринимателя и (или) месту фактического осуществления их деятельности[[44](https://www.intuit.ru/studies/courses/697/553/literature#literature.44)].

Выездная проверка проводится в случае, если при документарной проверке не представляется возможным:

* удостовериться в полноте и достоверности сведений, содержащихся в имеющихся в распоряжении ФСТЭК России (управления ФСТЭК России по федеральному округу) документах лицензиата;
* оценить соответствие деятельности лицензиата лицензионным требованиям и условиям без проведения соответствующего мероприятия по контролю.

**Срок проведения каждой из проверок** не может превышать двадцать рабочих дней.

Проверка проводится на основании приказа ФСТЭК России.

При проведении проверки проверяющие не вправе:

1. требовать представления документов, информации, если они не являются объектами проверки или не относятся к предмету проверки, а также изымать оригиналы таких документов;
2. распространять информацию, полученную в результате проведения проверки и составляющую государственную, коммерческую, служебную, иную охраняемую законом тайну, за исключением случаев, предусмотренных законодательством Российской Федерации;
3. превышать установленные сроки проведения проверки;
4. осуществлять выдачу юридическим лицам, индивидуальным предпринимателям предписаний или предложений о проведении за их счет мероприятий по контроля.

В результате проверки составляется акт в двух экземплярах. В случае выявления нарушений, проверяющие должны выдать предписание об их устранении и проконтролировать его выполнение.

Общая схема взаимодействия регуляторов и операторов персональных данных представлена на рисунке 2.

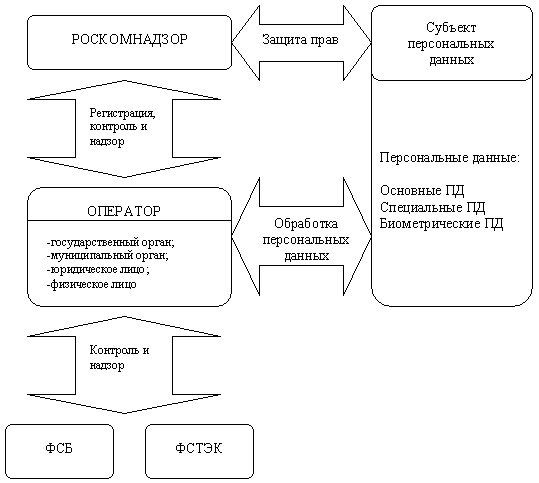


Рисунок 2**.**Взаимодействие регуляторов и операторов персональных данных

В случае выявления в ходе плановых и внеплановых проверок нарушений в области обеспечения безопасности персональных данных, предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность, которая может применяться в отношении руководителя организации, подразделения или виновного в разглашении работника. Наказанием за нарушение требований Федерального закона "О персональных данных" могут стать исправительные работы до 1 года или лишение свободы на срок до 2-х лет.