**Что такое законодательный уровень информационной безопасности и почему он важен**

В деле обеспечения информационной безопасности успех может принести только *комплексный подход*. Для защиты интересов *субъектов информационных отношений* необходимо сочетать меры следующих уровней:

* законодательного;
* административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
* процедурного (меры безопасности, ориентированные на людей);
* программно-технического.

***Законодательный уровень***является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

* меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их ***мерами ограничительной направленности***);
* ***направляющие и координирующие меры***, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех *субъектов информационных отношений*, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно.

Самое важное на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий.

### Обзор российского законодательства в области информационной безопасности

#### Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со **статьей 24 Конституции**, 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 41** гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, **статья 42** - право на знание достоверной информации о состоянии окружающей среды.

В принципе, *право на информацию* может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

**Статья 23** Конституции гарантирует *право на личную и семейную тайну*, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, **статья 29** - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к *средствам защиты информации*.

В Гражданском кодексе Российской Федерации фигурируют такие понятия, как *банковская*, *коммерческая* и *служебная тайна*. Согласно статье 139, информация составляет служебную или *коммерческую тайну* в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности. (Примечание:Утратила силу с 1 января 2008 года. - Федеральный закон от 18.12.2006 N 231-ФЗ.)

Весьма продвинутым в плане информационной безопасности является *Уголовный кодекс* Российской Федерации (редакция от 14 марта 2002 года). Глава 28 - "Преступления в сфере компьютерной информации" - содержит три статьи:

* **статья 272**. Неправомерный доступ к компьютерной информации;
* **статья 273**. Создание, использование и распространение вредоносных программ для ЭВМ;
* **статья 274**. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-*телекоммуникационных сетей*.

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности *информационных сервисов* представляется нам очень своевременным.

**Статья 138 УК РФ**, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О *государственной тайне*" (с изменениями и дополнениями на 22 августа 2004 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих *государственную тайну*; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

#### Закон "Об информации, информационных технологиях и о защите информации"

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ (принят Государственной Думой 8 июля 2006 года).

В нем даются основные определения, намечаются направления, в которых должно развиваться законодательство в данной области, регулируются отношения, возникающие при:

1. осуществлении права на поиск, получение, передачу, производство и распространение информации;
2. применении информационных технологий;
3. обеспечении защиты информации.

Процитируем основные определения:

1. **информация** - сведения (сообщения, данные) независимо от формы их представления;
2. **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
3. **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
4. **информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
5. **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
6. **доступ к информации** - возможность получения информации и ее использования;
7. **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
8. **предоставление информации** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
9. **распространение информации** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
10. **электронное сообщение** - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
11. **документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
12. **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

В **статье 3** Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. установление ограничений доступа к информации только федеральными законами;
3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. достоверность информации и своевременность ее предоставления;
7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Отметим, что в этих принципах явным образом фигурируют целостность (достоверность) и доступность (своевременность предоставления) информации.

**В статье 9** Закона содержатся следующие положения:

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.
3. Защита информации, составляющей *государственную тайну*, осуществляется в соответствии с законодательством Российской Федерации о *государственной тайне*.
4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим *коммерческую тайну*, *служебную тайну* и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Отметим, что в этой статье упор делается на конфиденциальность информации.

**Статья 11 "Документирование информации"** содержит следующие важные положения:

**3**. Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

**4**. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

**Статья 16** целиком посвящена вопросам защиты информации. Процитируем ее полностью. «Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на»:

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

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

* предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
* своевременное обнаружение фактов несанкционированного доступа к информации;
* предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
* недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
* возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
* постоянный контроль за обеспечением уровня защищенности информации.

#### Другие законы и нормативные акты

**Закон «О лицензировании отдельных видов деятельности» от 8 августа 2001 года номер 128-ФЗ** (Принят Государственной Думой 13 июля 2001 года, последняя учтенная редакция от 04.05.2011 номер 99-ФЗ). Начнем с основных определений.

***Лицензия*** - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

***Лицензируемый вид деятельности*** - вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.

***Лицензирование*** - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, *аннулированием* лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, ведением реестров лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании.

***Лицензирующие органы*** - федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.

***Лицензиат*** - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности."

**Статья 12** Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:

* распространение шифровальных (криптографических) средств;
* техническое обслуживание шифровальных (криптографических) средств;
* предоставление услуг в области шифрования информации;
* разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (*криптографических) средств* информационных систем, телекоммуникационных систем;
* выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* разработка и (или) производство средств защиты конфиденциальной информации;
* техническая защита конфиденциальной информации;
* разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими *предпринимательскую* деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

* деятельность, связанная с защитой государственной тайны;
* деятельность в области связи;
* образовательная деятельность.

10 января 2002 года Президентом был подписан очень важный закон **«Об электронной цифровой подписи» номер 1-ФЗ** (принят Государственной Думой 13 декабря 2001 года, рассматривается в редакции Федерального закона от 08 ноября 2007 года номер 258-ФЗ). Его роль прекрасно выражена в статье 1. (Закон с 1 июля 2013 будет недействителен, в силу вступит Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».)

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.
2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Закон вводит следующие основные понятия:

***Электронный документ*** - документ, в котором информация представлена в электронно-цифровой форме.

***Электронная цифровая подпись*** - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием *закрытого ключа*электронной цифровой подписи и позволяющий идентифицировать владельца *сертификата ключа подписи*, а также установить отсутствие искажения информации в электронном документе.

***Владелец сертификата ключа подписи*** - физическое лицо, на имя которого *удостоверяющим центром* выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

***Средства электронной цифровой подписи*** - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием *закрытого ключа*электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

***Сертификат средств электронной цифровой подписи*** - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия *средств электронной цифровой подписи* установленным требованиям.

***Закрытый ключ электронной цифровой подписи*** - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

***Открытый ключ электронной цифровой подписи*** - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием *средств электронной цифровой подписи* подлинности электронной цифровой подписи в электронном документе.

***Сертификат ключа подписи*** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица *удостоверяющего центра*, которые включают в себя открытый ключ электронной цифровой подписи и выдаются*удостоверяющим центром* участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца *сертификата ключа подписи*.

***Подтверждение подлинности электронной цифровой подписи в электронном документе*** - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием *сертификата ключа подписи* принадлежности электронной цифровой подписи в электронном документе владельцу *сертификата ключа подписи* и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

***Пользователь сертификата ключа подписи*** - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу *сертификата ключа подписи*.

***Информационная система общего пользования*** - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

***Корпоративная информационная система*** - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Согласно Закону, *электронная цифровая подпись* в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

* *сертификат ключа подписи*, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
* подтверждена подлинность электронной цифровой подписи в электронном документе;
* *электронная цифровая подпись* используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет сведения, которые должен содержать сертификат ключа подписи:

* уникальный регистрационный номер *сертификата ключа подписи*, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре *удостоверяющего центра*;
* фамилия, имя и отчество владельца *сертификата ключа подписи* или псевдоним владельца. В случае использования псевдонима запись об этом вносится *удостоверяющим центром* в сертификат ключа подписи;
* открытый ключ электронной цифровой подписи;
* наименование *средств электронной цифровой подписи*, с которыми используется данный открытый ключ электронной цифровой подписи;
* наименование и местонахождение *удостоверяющего центра*, выдавшего *сертификат ключа подписи*;
* сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

**Федеральный закон "О Персональных данных"** от 27 июля 2006 года номер 152-ФЗ (принят Государственной Думой 8 июля 2006 года) можно назвать долгожданным. И в целом он оправдал ожидания.

В статье 2 сформулирована цель Федерального закона:

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В статье 1 определяется сфера действия рассматриваемого закона:

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами (далее - муниципальные органы), юридическими лицами, физическими лицами с использованием средств автоматизации 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.
2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:
   1. обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
   2. организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
   3. обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;
   4. обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим *государственную тайну*.

В статье 3 сформулированы основные понятия, используемые в Федеральном законе:

1. **персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
2. **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;
3. **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;
4. **распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-*телекоммуникационных сетях* или предоставление доступа к персональным данным каким-либо иным способом;
5. **использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
6. **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
7. **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
8. **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
9. **информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
10. **конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
11. **трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;
12. **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Обычно персональные данные не обрабатываются изолированно, они сосуществуют с другими видами данных, поэтому введенное понятие информационной системы персональных данных представляется искусственным.

В рассматриваемом законе сформулированы следующие принципы обработки персональных данных:

1. законности целей и способов обработки персональных данных и добросовестности;
2. соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
3. соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
4. достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
5. недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Кроме того, хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Статья 14 главы 3 декларирует право субъекта персональных данных на доступ к своим персональным данным. Приведем наиболее важные положения этой статьи.

Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных частью 5 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

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

Это очень важная статья, и хочется надеяться, что она действительно будет работать.

Весьма любопытны, особенно в сопоставлении с законом "Об электронной цифровой подписи", следующие положения статьи 16:

1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.
2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.
3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.
4. Оператор обязан рассмотреть возражение, указанное в части 3 настоящей статьи, в течение семи рабочих дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Очень хорошо, что аргументы типа "но мой компьютер говорит..." не рассматриваются законом как истина в последней инстанции.

В статье 17 сформулировано естественное право субъекта на обжалование действий или бездействия оператора:

1. 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.
2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Известно множество случаев нарушения конфиденциальности персональных данных. Все эти нарушения могут повлечь для оператора юридические последствия, способные заставить его обеспечить информационную безопасность персональных данных, если потенциальные последствия действительно могут быть серьезными. Здесь важна реальная весомость карательной составляющей закона.

В контексте информационной безопасности центральной является статья 19, регламентирующая меры по обеспечению безопасности персональных данных при их обработке. Процитируем ее целиком.

1. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для *защиты персональных данных* от неправомерного или *случайного доступа* к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.
2. Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.
3. Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации в соответствии с частью 2 настоящей статьи, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.
4. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или *случайного доступа* к ним, уничтожения, изменения, блокирования, копирования, распространения.

И вновь важнейшая статья закона носит исключительно декларативный характер. Все зависит от того, какие требования к обеспечению безопасности персональных данных устанавливает Правительство Российской Федерации, и как осуществляется контроль и надзор за выполнением этих требований. Правда, упомянуты все основные аспекты информационной безопасности - доступность (отметим, что в пункте 1 статьи термин "блокирование" понимается не так, как это определено в числе основных понятий), целостность и конфиденциальность, однако отдельное упоминание шифровальных (*криптографических) средств* выглядит наивно. Как же без них, без заверения данных цифровой подписью, например? Криптография - обязательный элемент реальной информационной безопасности, и она отнюдь не сводится исключительно к шифрованию, она много шире. Не очень ясно и повышенное внимание к защите биометрических персональных данных. Кроме них, есть и другие критически важные персональные данные, хранящиеся, например, на картах.

Важна и статья 21, регламентирующая обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных. Процитируем первые три пункта из нее.

1. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.
2. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.
3. В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

К сожалению, не очень понятно, как в случае нарушения конфиденциальности персональных данных блокировать их и устранить допущенные нарушения. Остается жаловаться в уполномоченный орган по защите прав субъектов персональных данных (статья 23) на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона. Таким органом является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

Права уполномоченного органа весьма широки. Он, в частности, 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 в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;
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.

Будет ли реально работать эта статья? Хватит ли у уполномоченного органа ресурсов и напора, чтобы реально защищать интересы многочисленных субъектов?

Согласно пункту 3 статьи 25, информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года.

На этом мы заканчиваем обзор законов РФ, относящихся к информационной безопасности.