Российская нормативная база обеспечения информационной безопасности

Оглавление

По следующим ссылкам можно познакомиться с общими вопросами, связанными с обеспечением безопасности при передаче данных:

1.1. Российская нормативная база обеспечения информационной безопасности

У каждой группы специалистов, занимающихся проблемами безопасности информационных технологий, имеется свой взгляд на безопасность и средства ее достижения, а, следовательно, и свое представление о том, что должна представлять собой защищенная система. Для согласования всех точек зрения на проблему создания защищенных систем разработаны и продолжают разрабатываться *стандарты информационной безопасности, принимаются международные, государственные и ведомственные нормативные акты.* Эти документы, регламентируют основные понятия и концепции информационной безопасности на государственном и межгосударственном уровне, определяют понятие «защищенная система» посредством стандартизации требований и критериев безопасности, образуют шкалу оценки степени защищенности вычислительных систем.

Ниже дан перечень (далеко не полный) основных стандартов, имеющих отношение к защите информации:

ГОСТ 1.0-92 «Межгосударственная система стандартизации. Основные положения».

ГОСТ Р 1.0-92 «Государственная система стандартизации Российской Федерации. Основные положения».

ГОСТ Р ИСО 9000-2001 «Система менеджмента качества. Основные положения и словарь».

ГОСТ Р ИСО 9001-2001 «Система менеджмента качества. Требования».

ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

ГОСТ 15971-90 «Системы обработки информации. Термины и

определения».

ГОСТ Р ИСО 7498-1-99, 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель». Часть 1 Базовая модель. Часть 2 Архитектура защиты информации.

ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».

ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения».

ГОСТ Р ИСО/МЭК 15408-1-2002, 15408-2-2002, 15408-3-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (три части).

ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хеширования».

ГОСТ Р 34.11-95 «Информационная технология. Криптографическая защита информации. Функция кэширования».

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

1.1.1 Обзор Федеральных законов

1.1.1.1. Основные определения сферы защиты информации

Анализ терминологических источников по информационной безопасности (ИБ), в том числе законодательных актов Российской Федерации,

руководящих документов Федеральной службы по техническому и экспортному контролю Министерства обороны, ФСТЭК (ранее Государственной технической комиссии при Президенте Российской Федерации), отечественных и зарубежных стандартов, показывает, что в этой области пока нет единой точки зрения. Основными терминологическими источниками для целей данного учебного пособия являются:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации».
2. Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных».
3. Федеральный закон Российской Федерации от 10 января 2002 г. №1-ФЗ «Об электронной цифровой подписи».
4. Руководящий документ Гостехкомиссии «Защита от несанкционированного доступа к информации. Термины и определения».
5. ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (Общие критерии, ОК). Часть 1.

1.1.1.2. Федеральный закон «Об информации, информационных технологиях и о защите информации»

Закон № 149-ФЗ от 27 июля 2006 года регулирует отношения, возникающие при:

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

Закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности.

В Законе используются следующие основные понятия:

- *информация* сведения (сообщения, данные) независимо от формы

их представления;

- *информационные технологии* процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- *информационная система* совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- *информационно-телекоммуникационная сеть* технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- *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;
- *доступ к информации* возможность получения информации и ее использования;
- *конфиденциальность информации* обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- *предоставление информации* действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- *распространение информации* действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
- *электронное сообщение* информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- *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;

• *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 перечислены основные принципы правового регулирования отношений в сфере информации, а именно:

• свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

• установление ограничений доступа к информации только федеральными законами;

• открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

• равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

• обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

• достоверность информации и своевременность ее предоставления;

• неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

• 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.

Статья 5 закона описывает информацию как объект правовых отношений. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом

и передаваться одним лицом другому лицу, если не установлены ограничения, либо иные требования к порядку ее предоставления или распространения.

Информация в зависимости от категории доступа к ней, подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Статья 6 закона определен обладатель информации, который вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Общедоступная информация (статья 7) информация, к которой относятся общеизвестные сведения, и доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении условий её распространения. Обладатель

общедоступной информации, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве её источника.

Физические и юридические лица имеют право на доступ к информации, право осуществлять поиск и право на получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами (статья 8). Доступ не может быть ограничен к:

- нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды;
- информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Статья 9 закона описывает ограничение доступа к информации в следующих случаях:

- защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
- соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами;
- защиты информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о

государственной тайне;

- отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Закон предусматривает, что информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда. Законом запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Статья 11 закона признаёт электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, как документ, подписанный 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. Обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью, рассматривается как обмен документами.

Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных, что определено в статье 13 закона.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно- технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании. (Статья 14. Государственные информационные системы)

Статья 16 определяет вопросы защиты информации и представляет собой

принятие 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.

Обладатель информации, оператор информационной системы 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.

1.1.1.3. Федеральный закон «О персональных данных»

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. Целью 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.

Действие закона не распространяется на отношения, возникающие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- 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;
- 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;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

В законе используются следующие основные понятия:

- *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;

- *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;

- *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;
- *распространение персональных данных* действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных

персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- *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;
- *блокирование персональных данных* временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- *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;
- *обезличивание персональных данных* действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
- *информационная система персональных данных*

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

- *конфиденциальность персональных данных* обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
- *трансграничная передача персональных данных* передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;
- *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.

Статья 5 закона определяет принципы обработки персональных данных:

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

• 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.

Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев, когда:

• обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

• обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

• обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

• обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

• обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

• обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной,

литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

• осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на

выборные государственные или муниципальные должности.

Конфиденциальность персональных данных обеспечиваться операторами и третьими лицами, за исключением случаев:

- обезличивания персональных данных;
- общедоступных персональных данных.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (справочники), но персональных данных могут быть в любое время исключены из общедоступных источников по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Статья 19 закона определяет меры по обеспечению безопасности персональных данных при их обработке:

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.

Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных определены в статье 21 Закона, в которой регламентируются действия оператора. Так при выявлении неправомерных действий, оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя.

1.1.1.4. Положения Гражданского кодекса Российской Федерации по защите информации

Важнейшее значение для правоотношений в информационной сфере имеет Гражданский кодекс Российской Федерации, определяющий базовые положения для этой области.

В свою очередь, данные положения Гражданского кодекса (ГК) конкретизируются в рассмотренных выше федеральных законах. Поэтому здесь приведем лишь основные статьи ГК, чтобы проиллюстрировать соответствие нормативных правовых актов.

Глава 6. Общие положения.

Статья 138. Интеллектуальная собственность.

В случаях и в порядке, установленных настоящим Кодексом и другими законами, признается исключительное право (интеллектуальная собственность) гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.).

Использование результатов интеллектуальной деятельности и средств индивидуализации, которые являются объектом исключительных прав, может осуществляться третьими лицами только с согласия правообладателя. *Статья 139.* Служебная и коммерческая тайна.

1. 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. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Данная статья предусматривает защиту прав обладателя сведений, для определения которых применено широкое понятие «информация», не подпадающих под охрану норм патентного, авторско-правового или иного специального законодательства. Правила статьи распространяются также на охраноспособные решения (изобретения, полезные модели и др.), не запатентованные правообладателем по каким-либо, как правило, экономическим, мотивам.

Статья не раскрывает содержание сведений, составляющих служебную или коммерческую тайну, и не приводит их перечень. Установлен только один общий признак, которым должна обладать охраняемая информация -«коммерческая ценность», т.е. способность быть объектом рыночного оборота. Условием предоставления защиты служит принятие правообладателем всех необходимых мер для обеспечения ее конфиденциальности. При соблюдении этих требований под правила статьи подпадают, таким образом, любые знания, включая практический опыт специалистов, применяемые не только в производстве, но и в других областях хозяйственной деятельности: торговле, маркетинге, менеджменте, иных управленческих услугах.

Глава 9. Сделки.

Статья 160. Письменная форма сделки.

3. Сделка в письменной форме должна быть совершена путем составления документа, выражающего ее содержание и подписанного лицом или лицами, совершающими сделку, или должным образом уполномоченными ими лицами.

Двусторонние (многосторонние) сделки могут совершаться способами,

установленными пунктами 2 и 3 статьи 434 настоящего Кодекса. Законом, иными правовыми актами и соглашением сторон могут устанавливаться дополнительные требования, которым должна соответствовать форма сделки (совершение на бланке определенной формы, скрепление печатью и т.п.), и предусматриваться последствия несоблюдения этих требований. Если такие последствия не предусмотрены, применяются последствия несоблюдения простой письменной формы сделки (пункт 1 статьи 162).

4. Использование при совершении сделок *факсимильного воспроизведения подписи* с помощью средств механического или иного копирования, *электронно-цифровой подписи* либо *иного аналога собственноручной подписи* допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

5. Если гражданин вследствие физического недостатка, болезни или неграмотности не может собственноручно подписаться, то по его просьбе сделку может подписать другой гражданин. Подпись последнего должна быть засвидетельствована нотариусом либо другим должностным лицом, имеющим право совершать такое нотариальное действие, с указанием причин, в силу которых совершающий сделку не мог подписать ее собственноручно.

Однако при совершении сделок, указанных в пункте 4 статьи 185 настоящего Кодекса, и доверенностей на их совершение подпись того, кто подписывает сделку, может быть удостоверена также организацией, где работает гражданин, который не может собственноручно подписаться, или администрацией стационарного лечебного учреждения, в котором он находится на излечении.

1.1.1.5. Федеральный закон «О техническом регулировании»

Федеральный закон «О техническом регулировании» является системообразующим для построения принципиально новой системы сертификации и стандартизации, в которой бы учитывались демократические

принципы нормативного регулирования, повышался бы уровень безопасности потребителей продукции и услуг, а также учитывались реалии рыночного устройства экономических отношений.

Основной упор в данном Федеральном законе делается на сужение сферы обязательной стандартизации и подтверждения соответствия и расширении добровольности таких действий. При этом подразумевается, что именно рыночная конъюнктура подтолкнет производителей осуществлять данную деятельность, чтобы обеспечить конкурентоспособность производимой продукции.

В законе даны определения ряда понятий.

Аккредитация официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия.

Знак соответствия — обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту.

Сертификация — форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

Сертификат соответствия — документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров.

Стандарт документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания

услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

Стандартизация деятельность по установлению правил и

характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышения конкурентоспособности продукции, работ или услуг.

Техническое регулирование правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнение работ или оказание услуг и правовое регулирование отношений в области оценки соответствия.

Технический регламент — документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством, или федеральным законом, или указом Президента, или постановлением Правительства, и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации).

В качестве основных принципов технического регулирования в Законе приняты следующие:

- независимость органов по аккредитации и сертификации от изготовителей, продавцов, исполнителей и приобретателей;
- единая система и правила аккредитации;
- единство правил и методов исследований (испытаний) и измерений при проведении процедур обязательной оценки соответствия;
- единство применения требований технических регламентов независимо от видов или особенностей сделок;
- недопустимость совмещения одним органом полномочий на аккредитацию и сертификацию и др.

В Законе предписано федеральным органам исполнительной власти издавать в сфере технического регулирования акты только рекомендательного

характера, за исключением случаев, связанных с оборонной продукцией и продукцией, сведения о которой составляют государственную тайну.

Основное новшество в новом Законе — технический регламент, который устанавливает минимально необходимые требования, обеспечивающие безопасность в различных сферах, а также электромагнитную совместимость в части обеспечения безопасности работы приборов и оборудования, а также единство измерений.

В качестве основы технического регламента могут использоваться международные и/или национальные стандарты.

Технический регламент принимается федеральным законом или постановлением Правительства РФ и вступает в силу не ранее чем через 6 месяцев со дня его официального опубликования.

В России действуют общие и специальные технические регламенты. В качестве разработчика технического регламента может выступить любое лицо. Проект технического регламента должен быть опубликован в печатном издании или в информационной системе общего пользования. Федеральным органом исполнительной власти в области технического регулирования определено *Федеральное агентство по техническому регулированию и метрологии,* входящее в Министерство промышленности и энергетики. Публичное обсуждение проекта технического регламента должно быть не менее 2-х месяцев. Подробно описан механизм прохождения закона о техническом регламенте в Госдуме и перечень необходимых документов. В исключительных случаях Президент России вправе издать технический регламент без его публичного обсуждения. До вступления в силу Федерального закона о техническом регламенте Правительство России вправе издать постановление о соответствующем регламенте.

Большое внимание в Законе уделено вопросам стандартизации. Определены цели и принципы стандартизации. Одним из принципов является *добровольное* применение стандартов.

К документам в области стандартизации, используемых на территории

Российской Федерации относятся:

- национальные стандарты;
- правила стандартизации, нормы и рекомендации в области стандартизации;
- общероссийские классификаторы технико-экономической и социальной информации;
- стандарты организаций.

Стандарты организаций, в том числе коммерческих, общественных, научных и саморегулируемых организаций, объединений юридических лиц могут разрабатываться в целях, не противоречащих настоящему закону. Проект стандарта может представляться в технический комитет по стандартизации, который проводит его экспертизу.

Четвертая глава закона посвящена подтверждению соответствия, означающему, что представляемая продукция, процессы и др. соответствует техническим регламентам, стандартам, условиям договоров. Подтверждение соответствия на территории РФ может носить добровольный или обязательный характер. Подробнее об этом будет сказано в главе настоящего учебника, посвященном сертификации.

В пятой главе закона рассмотрены вопросы, связанные с аккредитацией органов по сертификации и испытательных лабораторий (центров).

Шестая глава посвящена государственному контролю (надзору) за соблюдением технических регламентов.

Седьмая глава посвящена ответственности за несоответствие продукции и др. требованиям технических регламентов и порядка отзыва продукции из обращения.

Глава 8 «Информация о технических регламентах и документах по стандартизации» определяет порядок публикации информации о технических регламентах. Здесь также описано назначение Федерального информационного фонда технических регламентов и стандартов.

В заключительных положениях записано, что технические регламенты должны быть приняты в течение 7 лет со дня вступления в силу этого закона. Здесь также

описан порядок работы до вступления в силу технических регламентов.

Реализация положений этого закона и контроль за их исполнением возложена на *Федеральное агентство по техническому регулированию и метрологии* (ФАТР и М). Положение о нем утверждено постановлением Правительства от 17 июня 2004 г. № 294.

Для реализации положений Закона Центром стратегических разработок, Академией народного хозяйства при Правительстве РФ, Институтом экономики переходного периода, Российским союзом промышленников и предпринимателей, объединениями «Деловая Россия» и «ОПОРа» в июле 2004 г. создан Национальный институт технического регулирования НИТР (по аналогии с американским институтом стандартов ANSI — American National Standard Institute).

К настоящему времени НИТР создана «Система объектов технического регулирования и технических регламентов». Готова к выпуску брошюра «Система технического законодательства в Российской Федерации». Сформировано более сорока экспертных советов по подготовке отраслевых технических регламентов. Специалистами НИТР разработана типовая структура технического регламента и стандартные процедуры их подготовки. НИТР периодически проводит обучающие семинары. На рассмотрение в Госдуму передан «Типовой шаблон специального технического регламента».

Распоряжением Правительства от 6 ноября 2004 г. № 1421-р была утверждена «Программа разработки технических регламентов на 2004-2006 годы». Распоряжением Правительства от 23 ноября 2004 г. № 1511 -р в нее были внесены изменения.

Правила финансирования всех мероприятий в области технического регулирования определены в постановлении Правительства РФ от 15 декабря 2004 г. № 791. В нем, в частности, перечислены основные направления работ, финансирование которых производится за счет средств федерального бюджета:

- контроль за соблюдением требований технических регламентов (ТР);
- создание и ведение федерального информационного фонда ТР и стандартов;

- реализация федеральных программ по созданию ТР и стандартов;
- проведение экспертизы отдельных проектов ТР;
- разработка общероссийских классификаторов;
- уплата взносов в международные организации по стандартизации. Следует отметить, что в Законе «О техническом регулировании» недостаточно уделено

внимания информационной безопасности. Так, в статье 7 Закона среди перечисленных в ней видов безопасности информационная безопасность отсутствует, что, возможно, связано с юридической неопределенностью данного понятия.

Тем не менее, законодатель, осознавая важность отношений в сфере защиты информации, в статье 5 Закона предусмотрел особый порядок технического регулирования в данной области. Однако сделано это в некоторой степени непоследовательно. Исходя из презумпции о том, что возможны случаи отсутствия требований технических регламентов в отношении продукции (работ, услуг), используемой для защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, требования к процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации таких средств защиты информации (работ или услуг в области защиты информации), устанавливаются федеральными органами исполнительной власти, являющимися в пределах своей компетенции государственным заказчиком оборонного заказа, и (или) государственным контрактом.

Отсюда следует, что сфера, в которой будет осуществляться регулирование со стороны данных органов это только государственная сфера, в связи с тем, что оборонный заказ, а равно и государственные контракты предназначены исключительно для удовлетворения определенных потребностей государства. Между тем, сфера защиты конфиденциальной информации в ряде случаев должна регулироваться на основании обязательных

требований. Такие требования должны вырабатываться по отношению к персональным данным, сведениям, составляющим банковскую тайну, тайну страхования и т.п., т.к. совокупность относимой к ним информации формируется императивно, и законодательство содержит обязанность соответствующих субъектов по их защите.

Из вышеизложенного следует, что применительно к потребностям сферы защиты информации, напрямую затрагивающей права и свободы человека, а также его безопасность, законодательство о техническом регулировании необходимо совершенствовать.

1.1.2. Другие федеральные нормативные правовые акты

1.1.2.1. Указ Президента Российской Федерации № 611 от 12 мая 2004 г.

Указ Президента Российской Федерации от 12 мая 2004 г. №611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» определяет правила использования информационных систем, сетей и сетей связи, включая международную ассоциацию сетей «Интернет»:

1. Субъектам международного информационного обмена в Российской Федерации не осуществлять включение информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, и служебная информация ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам, в состав средств международного информационного обмена, в том числе в международную ассоциацию сетей «Интернет» (далее сеть «Интернет»),

Владельцам открытых и общедоступных государственных информационных ресурсов осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

Владельцам и пользователям указанных ресурсов осуществлять размещение технических средств, подключаемых к открытым информационным системам, сетям и сетям связи, используемым при международном информационном обмене, включая сеть «Интернет», вне помещений, предназначенных для ведения закрытых переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

2. Службе специальной связи и информации при Федеральной службе охраны Российской Федерации обеспечивать поддержание и развитие сегмента сети «Интернет» для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

3. Администрации Президента Российской Федерации Аппарату Совета Федерации Федерального Собрания Российской Федерации, Аппарату Государственной Думы Федерального Собрания Российской Федерации, Аппарату Правительства Российской Федерации, аппаратам Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации и Генеральной прокуратуре Российской Федерации осуществлять взаимодействие с сетью «Интернет» и представлять в нее информацию через сегмент сети «Интернет» для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Службы специальной связи и информации при Федеральной службе охраны Российской Федерации.

1.1.2.2. Постановление Правительства РФ от 26 июня 1995 г . № 608 «О сертификации средств защиты информации» (с изменениями от 23 апреля

1996 г., 29 марта 1999 г.)

Данным Постановлением утверждено Положение о сертификации средств защиты информации, которое устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом.

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 являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам.

Системы сертификации создаются Государственной технической комиссией при Президенте Российской Федерации, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, Службой внешней разведки Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации.

Сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции. Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны. В каждой системе сертификации разрабатываются и согласовываются с Межведомственной комиссией положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

Основными схемами проведения сертификации средств защиты

информации являются:

• для единичных образцов средств защиты информации проведение испытаний этих образцов на соответствие требованиям по защите информации;

• для серийного производства средств защиты информации проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований. Кроме того, допускается предварительная проверка производства по специально разработанной программе. Срок действия сертификата не может превышать пяти лет.

1.1.2.3. Постановление Правительства РФ от 11 февраля 2002 г № 135 «О лицензировании отдельных видов деятельности»

Устанавливает перечень федеральных органов исполнительной власти, осуществляющих лицензирование в определенных областях, а также виды деятельности, лицензируемые органами исполнительной власти субъектов Российской Федерации.

1. МВД России:

• негосударственная (частная) охранная деятельность,

• негосударственная (частная) сыскная деятельность.

2. МЧС России:

• производство работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений;

3. ФСБ России:

• разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

• деятельность по выявлению 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);

- деятельность по распространению шифровальных (криптографических) средств;
- деятельность по техническому обслуживанию шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей.

4. ФСТЭК России:

- деятельность по технической защите конфиденциальной информации;
- деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

1.1.2.4. Постановление Правительства РФ от 27 мая 2002 г № 348 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»

Это Положение определяет порядок лицензирования деятельности юридических и физических лиц по разработке и (или) производству средств защиты конфиденциальной информации.

Лицензирование осуществляет ФСТЭК России, а в части разработки средств защиты для объектов Администрации Президента РФ, Совбеза РФ, Федерального Собрания РФ, Правительства РФ, Конституционного, Верховного и Высшего Арбитражного судов ФСБ России.

Разрабатываемые устройства должны удовлетворять требованиям

госстандартов РФ, соответствующей документации и иных нормативных актов, а также по уровню подготовки специалистов и выдерживать соответствие помещений и оборудования требованиям по защите информации. Для деятельности, лицензируемой ФСБ России в данной сфере набор лицензионных требований значительно шире.

Перечень необходимых документов для получения лицензии, порядок ее выдачи, срок действия лицензии и контроль за ее выполнением установлены

132

Положением практически аналогично Постановлению №290, рассмотренному выше.

1.1.2.5- Постановление Правительства РФ от 23 сентября 2002 г № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»

Данным документом утверждаются четыре положения, касающиеся лицензирования отдельных видов деятельности в области криптографических

средств:

1. Положение о лицензировании деятельности по распространению

шифровальных (криптографических) средств.

2. Положение о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств.

3. Положение о лицензировании предоставления услуг в области шифрования информации.

4. Положение о лицензировании разработки, производства шифровальных (криптографических) средств защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

В перечисленных положениях дан перечень средств шифрования, имитозащиты, электронной цифровой подписи, кодирования, изготовления ключей

и ключевых документов. При этом указано, что *не требуется* лицензирование для криптографических средств, осуществляющих преобразование информации с длиной ключа до 40 бит при использовании симметричного алгоритма и 128 бит при использовании асимметричного алгоритма.

В качестве лицензирующего органа выступает ФСБ России. Здесь также определены лицензионные требования, а также перечень необходимых документов, представляемых в лицензионный орган и порядок рассмотрения и выдачи лицензии.

1.1.2.6. Постановление Правительства РФ от 30 мая 2003 г № 313 «Об уполномоченном федеральном органе исполнительной власти в области использования электронной цифровой подписи»

В соответствии с Федеральным законом «Об электронной цифровой подписи» функции уполномоченного федерального органа исполнительной власти в области использования электронной цифровой подписи возлагаются на Министерство информационных технологий и связи Российской Федерации. При этом его деятельность в области использования ЭЦП в органах государственной власти России должна согласовываться с ФСБ России.

1.1.3. Законодательное регулирование использования ЭЦП в РФ

1.1.3.1. Стандарты, описывающие методы формирования и проверки ЭЦП

В России были опубликованы несколько ГОСТов:

1. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
2. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».
3. ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».
4. ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой

подписи».

Государственный стандарт РФ «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (ГОСТ Р 34.10-2001) содержит описание процессов формирования и проверки ЭЦП, реализуемой с использованием операций группы **точек эллиптической кривой, определенной над конечным простым полем.** Этот ГОСТ разработан вместо ГОСТ Р 34.10-94, срок действия которого истекает к началу 2008 года, и обеспечивает повышенную стойкость ЭЦП к несанкционированным изменениям. Стойкость ЭЦП основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11-94. Стандарт рекомендуется к использованию в новых СОД (СОИ), а также при модернизации действующих систем.

1.1.3.2. Федеральный закон «Об электронной цифровой подписи»

Электронная цифровая подпись, как реквизит электронного документа, обеспечивает решение следующих задач информационной безопасности:

• **целостность** гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения;

• **аутентичность** гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения;

• **неотказуемость** гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой.

Разница в последних двух категориях (аутентичность и неотказуемость) заключается в том, что при нарушении аутентичности, кто-то другой пытается заявить, что он автор сообщения, а при нарушении неотказуемости — сам автор пытается отказаться от авторства сообщения. При защите информации не

обязательно обеспечивать выполнение всех категорий безопасности. Это зависит от режима защиты информации и определяется ее собственником либо собственником информационных ресурсов, либо уполномоченным лицом (уполномоченным собственником). Например, информационно-справочные материалы, не являющими документами, закрепляющими отношения сторон, могут потребовать обеспечения целостности и аутентичности при передаче, и

не требуют обеспечения неотказуемости. С другой стороны, публичный договор-оферта требует обеспечения целостности, аутентичности и неотказуемости. В тоже время, задачи информационной безопасности, в части обеспечения аутентичности и неотказуемости, могут быть решены с точки зрения обеспечения юридической значимости электронных документов.

Закон «Об электронной цифровой подписи» № 1- ФЗ от 10.01.2002 года

Закон обеспечивает правовые условия использования ЭЦП. В законе введены и описаны определения следующих терминов:

- электронный документ (ЭД);
- электронно-цифровая подпись (ЭЦП);
- владелец сертификата ключа подписи;
- средства ЭЦП;
- сертификат ЭЦП;
- закрытый ключ ЭЦП;
- открытый ключ ЭЦП;
- сертификат ключа подписи (СКП);
- подтверждение подлинности ЭЦП в ЭД;
- пользователь сертификата ключа подписи;
- информационная система общего пользователя;
- корпоративная ИС.

Здесь также определены условия, при которых ЭЦП в ЭД равнозначна собственноручной подписи в документе на бумажном носителе:

1. Сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу на момент проверки или на момент подписания ЭД.

2. Подтверждена подлинность ЭЦП в ЭД.

3. ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Для создания ключей ЭЦП должны использоваться только сертифицированные средства, прошедшие сертификацию в соответствие с законодательством РФ.

Согласно закону об ЭЦП сертификат ключа ЭЦП дожжен содержать следующие сведения:

1. Уникальный регистрационный номер сертификата ключа подписи (СКП), даты начала и окончания срока действия СКП, находящегося в реестре удостоверяющего центра (УЦ).

2. Фамилия, имя и отчество владельца СКП или псевдоним владельца.

3. Открытый ключ ЭЦП.

4. Наименование средств ЭЦП, с которыми используется данный ключ.

5. Наименование и местонахождение удостоверяющего центра, выдавшего СКП.

6. Сведения об отношениях, при осуществлении которых ЭД с ЭЦП будет иметь юридическое значение.

Кроме того, в СКП могут указываться должность и местонахождения организации, квалификация владельца, а по заявлению в письменной форме и иные сведения, подтверждаемые соответствующими документами. СКП может

быть выдан в форме документа на бумажном носителе (на бланке удостоверяющего центра с подписями и печатью). Если СКП выдается в электронной форме, то и подписывается он ЭЦП **уполномоченного лица удостоверяющего центра.** По истечении срока хранения СКП он исключается из реестра СКП и переводится в режим архивного хранения со сроком хранения не менее 5 лет.

Основным элементом применения ЭЦП в системе юридически значимого электронного документооборота является организация удостоверяющего центра. В соответствии с Федеральным законом «Об электронной цифровой

подписи» под удостоверяющим центром понимается субъект права, являющегося носителем субъективных прав и юридических обязанностей в части:

- изготовления и выдачи ключей электронной цифровой подписи;
- изготовления и выдачи сертификатов ключей электронной цифровой подписи;
- регистрации владельцев сертификатов ключей электронной цифровой подписи;
- аннулирования, приостановления и возобновления действия сертификатов ключей электронной цифровой подписи;
- предоставления информации о действии сертификатов ключей электронной цифровой подписи;
- подтверждения подлинности электронных цифровых подписей. Деятельность УЦ, выдавшего СКП, может быть прекращена в порядке,

установленном гражданским законодательством, а его функции, по согласованию с владельцами СКП, могут быть переданы другому УЦ, в противном случае, СКП аннулируются и передаются на хранение Федеральному органу исполнительной власти.

Для автоматизации деятельности удостоверяющего центра при реализации своих целевых функций по предназначению используется специализированное программное обеспечение.

Участники системы электронного документооборота вступают с удостоверяющим центром в некоторые отношения, условия которого закрепляются либо договором (если участники системы электронного документооборота являются представителями других юридических лиц) либо положением, утверждаемым приказом по организации (если участники системы электронного документооборота являются сотрудниками той же организации, что выполняет функции удостоверяющего центра). Основное предназначение такого договора (положения) обеспечить неотказуемость пользователей (владельцев сертификатов ключей подписи) от факта обладания ключом подписи и соответствующим сертификатом ключей подписи, а также определения

статуса действия сертификата ключа подписи в каждый конкретный момент времени.

В виду того, что на текущий момент не отрегулировано (отсутствует) законодательная база по электронным документам, необходимо заключение соглашения между участниками системы электронного документооборота о принятии к исполнению электронных документов с электронной цифровой

подписью при соблюдении условий, определенных в соглашении. Такое соглашение может быть оформлено также либо

договором (если участники системы электронного документооборота являются представителями других юридических лиц) либо положением, утверждаемым приказом по организации (если участники системы электронного документооборота являются сотрудниками той же организации, что выполняет функции удостоверяющего центра). Соглашение предназначено для детализации условий равнозначности ЭЦП собственноручной подписи с целью выполнения требований, изложенных в действующем законодательстве РФ, в соответствующих рекомендациях Высшего Арбитражного суда, и минимизации рисков организатора системы электронного документооборота по ущербам, связанным с применением ЭЦП.

1.1.3.3. Проблемы при использовании стандартов и нормативных документов, касающихся ЭЦП

Как отечественные, так и зарубежные стандарты описывают лишь процедуры выработки и проверки ЭЦП и хэш-функции. Вне их действия остаются такие вопросы как:

- распространение и генерация ключей;
- защита от НСД к ключевой информации и др.

Поэтому зачастую продукты, реализующие один и тот же стандарт, несовместимы между собой. Следует также отметить, что стандарты описывают алгоритм математическим языком, в то время как пользователи сталкиваются уже с его реализацией. Однако при реализации алгоритма могут быть допущены различные ошибки, которые сводят на нет все достоинства алгоритма.

Кроме того, эффективное применение систем ЭЦП зависит от их правильной эксплуатации. Например, хранение секретных ключей для генерации ЭЦП на доступном всем жестком диске позволяет злоумышленнику получить к ним доступ и в дальнейшем подделывать документы, подписанные на этих ключах.

Производители различных систем ЭЦП в России особое внимание уделяют математическим аспектам реализованных алгоритмов (криптостойкость, сколько лет уйдет на подделку и др.), но практиков эти вопросы волнуют мало. Тем более что проверить правильность приводимых в документации выкладок способен только математик-криптограф. Пользователей, в первую очередь, интересуют следующие параметры системы ЭЦП:

1.Скорость.

2.Длина подписи.

3.Интеграция ЭЦП в принятую технологию обработки.

4.Механизм защиты от НСД.

5Юридическая поддержка системы ЭЦП.

Скорость является одним из основных параметров, на который следует обращать внимание при выборе системы ЭЦП. Это особенно актуально в системах связи, в которых осуществляется очень интенсивный обмен данными и передаваемая информация должна защищаться от подделки.

Этот параметр слагается из следующих составляющих:

- скорость генерации подписи;
- скорость проверки подписи.

Параметр «скорость» существенно зависит от скорости выработки хэш-функции и типа ПК, на котором осуществляется генерация или проверка ЭЦП,

Длина подписи также является важным параметром, особенно для систем, в которых передается большое число сообщений малой длины. В этом случае использование российского стандарта для подписи всех данных неэффективно.

Вопросы интеграции приобретаемой системы ЭЦП в существующую технологию обработки информации также достаточно актуальны. Например, если в качестве средства отправки электронной почты используется Microsoft Outlook то

необходимо, чтобы система ЭЦП могла быть встроена в почтовую программу. Такую возможность предоставляют как российские, так и зарубежные производители ЭЦП. Если приобретаемая система ЭЦП не поддерживает используемое у заказчика ПО, то поставщик должен поставлять интерфейс прикладного программирования (API) для встраивания системы ЭЦП в систему заказчика.

Механизмы защиты от НСД должны предусматривать действия, выполняемые в случае компрометации ключей одного из пользователей. Кроме того, они должны позволять контролировать целостность как системы ЭЦП в целом, так и ее компонентов.

Юридическая поддержка при приобретении системы ЭЦП важна при изучении проекта договора об обмене электронными документами. Если та или иная компания предлагает обслуживание с применением системы ЭЦП, то в договоре должно быть предусмотрено решение следующих вопросов:

- наличие процедуры урегулирования конфликтных ситуаций;
- описание состава комиссии, расследующей возникающие конфликты;
- ответственность сторон (в том числе и фирмы-разработчика).

Окончательный выбор системы ЭЦП должен осуществляться с анализом

следующих дополнительных ее возможностей:

1. Постановка нескольких подписей под одним из документов и их выборочная проверка.
2. Хранение ЭЦП не только в подписываемом документе, но ив отдельном файле.
3. Возможность использования командной строки для работы с системой ЭЦП.
4. Возможность подписи и проверка группы файлов.
5. Постановка и проверка подписи под заданными фрагментами (полями) документа.
6. Выработка и проверка групповой подписи.

7. Совместное использование функций шифрования и ЭЦП.

8. Постановка подписи и ее проверка для участка ОП.

9. Архивация использованных ключей и др.

Использование ЭЦП позволяет значительно повысить надежность и сохранность передаваемых электронных документов. Однако и при использовании ЭЦП используются различные способы атак.

Существует следующая классификация атак на схемы ЭЦП:

1. Атака с известным ключом.

2. Атака с известными сообщениями противник, кроме открытого ключа имеет и набор подписанных сообщений.

3. Простая атака с выбором подписанных сообщений противник имеет возможность выбирать сообщения, при этом открытый ключ он получает после выбора сообщения.

4. Направленная атака с выбором сообщения.

5. Адаптивная атака с выбором сообщения.

Каждая атака преследует определенные цели, которые можно разделить на несколько классов:

1. Полное раскрытие. Противник находит секретный ключ пользователя ЭЦП.

2. Универсальная подделка. Противник находит алгоритм, функционально аналогичный алгоритму генерации ЭЦП.

3. Селективная подделка. Подделка подписи под выбранным сообщением.

4. Экзистенциальная подделка. Подделка подписи хотя бы для одного случайно выбранного сообщения.

На практике применение ЭЦП позволяет выявить или предотвратить следующие действия нарушителя:

1. Отказ одного из авторов документа от своих действий.

2. Модификация принятого электронного документа.

3. Подделка документа.

4. Навязывание сообщений в процессе передачи противник

перехватывает обмен сообщениями и модифицирует их.

5. Имитация передачи сообщения.

Также существуют нарушения, от которых невозможно оградить систему обмена сообщениями это повтор передачи сообщения и фальсификация времени отправления общения. Противодействие данным нарушениям может основываться на использовании временных вставок и строгом учете входящих сообщений.

Следует обратить внимание на то, что некоторые разработчики, несмотря на наличие в РФ государственных стандартов, пытаются разработать свои собственные алгоритмы, которые из-за низкой квалификации авторов не обладают свойствами алгоритмов, разработанных математиками-криптографами. Чаще всего в подобных алгоритмах периодически повторяются одни и те же значения случайных чисел, возможна генерация одинаковых хэш-функций и др. С определенной долей скептицизма следует относиться к публикациям о модернизации существующих стандартов.

Много критики высказывается в настоящее время и по отношению к самому российскому закону об ЭЦП, поправки в который давно назрели. Наиболее спорными вопросами в регулировании сферы ЭЦП являются:

1. Неудобная процедура аннулирования сертификатов подписей при ликвидации выдавшего их удостоверяющего центра.

2. Неясности в синхронизации деятельности различных УЦ, поскольку возможны варианты, когда разные УЦ выдадут сертификаты с одинаковыми ключами подписей.

3. Неудобство в ограничении сферы действия того или иного сертификата, порождающего необходимость приобретения нового сертификата, например, при смене места работы.

4. Ограничение действительности самой ЭЦП датой действия сертификата на нее, тогда как было бы целесообразнее разработать механизм фиксации даты подписи документа, и именно ее привязывать к срокам действия сертификата при проверке действительности ЭЦП.

Приложение

Приложение 1

ФЗ РФ от 27.07.2006г. № 149-ФЗ

«Об информации, информационных технологиях и о защите информации»

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

И О ЗАЩИТЕ ИНФОРМАЦИИ

Принят Государственной Думой 8 июля 2006 года

Одобрен Советом Федерации 14 июля 2006 года

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Статья 2. Основные понятия, используемые в настоящем

Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

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.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

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.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Обладатель информации

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать

осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 7. Общедоступная информация

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Статья 8. Право на доступ к информации

1. Граждане (физические лица) и организации (юридические лица) (далее - организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

3. Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

4. Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

7. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации

были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

8. Предоставляется бесплатно информация:

1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

9. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Статья 9. Ограничение доступа к информации

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.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами

возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) **устанавливается федеральным законом о персональных данных.**

Статья 10. Распространение информации или предоставление информации

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

3. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

4. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Статья 11. Документирование информации

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

2. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

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.

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Статья 12. Государственное регулирование в сфере применения информационных технологий

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей.

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 13. Информационные системы

1. Информационные системы включают в себя:

1) государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

2. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

4. Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

5. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

6. Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами

таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

Статья 14. Государственные информационные системы

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются с учетом требований, предусмотренных Федеральным законом от 21 июля 2005 года N 94-ФЗ "О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд".

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления - Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами.

5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

6. Правительство Российской Федерации вправе устанавливать обязательные требования к порядку ввода в эксплуатацию отдельных

государственных информационных систем.

7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами.

Статья 15. Использование информационно-телекоммуникационных сетей

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

2. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.

3. Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или

ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

5. Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

6. Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

Статья 16. Защита информации

1. 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.

2. 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.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

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

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных

систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения

информации.

Статья 18. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

1) Федеральный закон от 20 февраля 1995 года N 24-ФЗ "Об информации, информатизации и защите информации" (Собрание законодательства Российской Федерации, 1995, N 8, ст. 609);

2) Федеральный закон от 4 июля 1996 года N 85-ФЗ "Об участии в международном информационном обмене" (Собрание законодательства Российской Федерации, 1996, N 28, ст. 3347);

3) статью 16 Федерального закона от 10 января 2003 года N 15-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2003, N 2, ст. 167);

4) статью 21 Федерального закона от 30 июня 2003 года N 86-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации, признании утратившими силу отдельных законодательных актов Российской Федерации, предоставлении отдельных гарантий сотрудникам органов внутренних дел, органов по контролю за оборотом наркотических средств и психотропных веществ и упраздняемых федеральных органов налоговой полиции в связи с осуществлением мер по совершенствованию государственного управления" (Собрание законодательства Российской Федерации, 2003, N 27, ст. 2700);

5) статью 39 Федерального закона от 29 июня 2004 года N 58-ФЗ "О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления" (Собрание законодательства Российской

Федерации, 2004, N 27, ст. 2711).

Президент
Российской Федерации
В.ПУТИН

Москва, Кремль

Приложение 2

Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных

Опубликовано 29 июля 2006 г. Вступает в силу 26 января 2007 г.

Принят Государственной Думой 8 июля 2006 года

Одобрен Советом Федерации 14 июля 2006 года

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Федерального 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.

Статья 2. Цель настоящего 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.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

В целях настоящего Федерального закона используются следующие основные понятия:

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 распространение 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.

Статья 4. Законодательство Российской Федерации в области персональных данных

1. Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

2. На основании и во исполнение федеральных законов государственные органы в пределах своих полномочий могут принимать нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных. Нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных, не могут содержать положения, ограничивающие права субъектов персональных данных.

Указанные нормативные правовые акты подлежат официальному опубликованию, за исключением нормативных правовых актов или отдельных положений таких нормативных правовых актов, содержащих сведения, доступ к которым ограничен федеральными законами.

3. Особенности обработки персональных данных, осуществляемой без

использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

4. Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

Глава 2. Принципы и условия обработки персональных данных

Статья 5. Принципы обработки персональных данных

1. Обработка персональных данных должна осуществляться на основе принципов:

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.

2. 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 6. Условия обработки персональных данных

1. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев,

предусмотренных частью 2 настоящей статьи.

2. Согласие субъекта персональных данных, предусмотренное частью 1 настоящей статьи, не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) 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;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

3. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются

соответственно статьями 10 и 11 настоящего Федерального закона.

4. В случае, если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Статья 7. **Конфиденциальность персональных данных**

1. Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обеспечение конфиденциальности персональных данных не требуется:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, 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.

2. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статья 9. Согласие субъекта персональных данных на обработку своих персональных данных

1. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных частью 2

настоящей статьи. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

2. Настоящим Федеральным законом и другими федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

4. В случаях, предусмотренных настоящим Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва.

5. Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительное согласие не требуется.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные являются общедоступными;

3) персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся

медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима в связи с осуществлением правосудия;

7) 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.

3. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

Статья 11. Биометрические персональные данные

1. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Статья 12. Трансграничная передача персональных данных

1. До начала осуществления трансграничной передачи персональных данных оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

2. Трансграничная передача персональных данных на территории иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

3. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных;

2) предусмотренных международными договорами Российской Федерации по вопросам выдачи виз, а также международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам;

3) предусмотренных федеральными законами, если это необходимо в

целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;

4) исполнения договора, стороной которого является субъект персональных данных;

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

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

Глава 3. Права субъекта персональных данных

Статья 14. Право субъекта персональных данных на доступ к своим персональным данным

1. 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.

2. Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

3. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в

электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

4. 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.

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

1) обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление

подозреваемого или обвиняемого с такими персональными данными;

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

Статья 15. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

2. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в части 1 настоящей статьи.

Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

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.

Статья 17. Право 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.

Глава 4. Обязанности оператора

Статья 18. **Обязанности оператора при сборе персональных данных**

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 4 статьи 14 настоящего Федерального закона.

2. Если обязанность предоставления персональных данных установлена федеральным законом, оператор обязан разъяснить субъекту персональных

данных юридические последствия отказа предоставить свои персональные данные.

3. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных.

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

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.

Статья 20. Обязанности оператора при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

1. Оператор обязан в порядке, предусмотренном статьей 14 настоящего Федерального закона, сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

2. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 5 статьи 14 настоящего Федерального закона или иного федерального

закона, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

3. Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса.

Статья 21. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных

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.

4. В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом

персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

Статья 22. Уведомление об обработке персональных данных

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

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

4) являющихся общедоступными персональными данными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных

аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

3. Уведомление, предусмотренное частью 1 настоящей статьи, должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. 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, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных.

4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке

персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

7. В случае изменения сведений, указанных в части 3 настоящей статьи, оператор обязан уведомить об изменениях уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений.

Глава 5. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований настоящего Федерального закона

Статья 23. Уполномоченный орган по защите прав субъектов персональных данных

1. 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 федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

2. 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.

3. Уполномоченный орган по защите прав субъектов персональных данных 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;

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.

4. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

5. Уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных;

2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;

3) вести реестр операторов;

4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;

5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;

6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;

7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.

6. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

7. Уполномоченный орган по защите прав субъектов персональных данных ежегодно направляет отчет о своей деятельности Президенту Российской Федерации, в Правительство Российской Федерации и Федеральное Собрание Российской Федерации. Указанный отчет подлежит опубликованию в средствах массовой информации.

8. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.

9. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

Статья 24. Ответственность за нарушение требований настоящего Федерального закона

Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Глава 6. Заключительные положения

Статья 25. Заключительные положения

1. Настоящий Федеральный закон вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.

2. После дня вступления в силу настоящего Федерального закона обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с настоящим Федеральным законом.

3. 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.

4. Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 настоящего Федерального закона, уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2008 года.

Президент
Российской Федерации
В. Путин

Приложение 3

Федеральный закон Российской Федерации от 10 января 2002 г. N 1-ФЗ об электронной цифровой подписи

Принят Государственной Думой 13 декабря 2001 года

Одобрен Советом Федерации 26 декабря 2001 года

Глава I. Общие положения

Статья 1. Цель и сфера применения настоящего Федерального закона 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.

Статья 2. Правовое регулирование отношений в области использования электронной цифровой подписи Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с настоящим Федеральным законом, Гражданским кодексом Российской Федерации, Федеральным законом "Об информации, информатизации и защите информации", Федеральным законом "О связи", другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а также осуществляется соглашением сторон.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе Для целей настоящего Федерального закона используются 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 которые 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.

Глава II. Условия использования электронной цифровой подписи

Статья 4. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи 1. 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. 2. Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Статья 5. Использование средств электронной цифровой подписи 1. Создание ключей электронных цифровых подписей осуществляется для использования в: информационной системе общего пользования ее участником или по его обращению удостоверяющим центром; корпоративной информационной системе в порядке, установленном в этой системе. 2. При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей несертифицированными средствами электронной цифровой подписи, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством Российской Федерации. 3. Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается. 4. Сертификация средств

электронной цифровой подписи осуществляется в соответствии с законодательством Российской Федерации о сертификации продукции и услуг.

Статья 6. Сертификат ключа подписи 1. Сертификат ключа подписи должен содержать следующие сведения: 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 удостоверяющим центром вносится запись об этом 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 место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи; сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение. 2. В случае необходимости в сертификате ключа подписи на основании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владельца сертификата ключа подписи, а по его заявлению в письменной форме - иные сведения, подтверждаемые соответствующими документами. 3. Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи. 4. Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего

центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра.

Статья 7. Срок и порядок хранения сертификата ключа подписи в удостоверяющем центре 1. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи. 2. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть не менее установленного федеральным законом срока исковой давности для отношений, указанных в сертификате ключа подписи. По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее чем пять лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Российской Федерации. 3. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Глава III. Удостоверяющие центры

Статья 8. Статус удостоверяющего центра 1. Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом. При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести

гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей. Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти. Статус удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы. 2. Деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности.

Статья 9. Деятельность удостоверяющего центра 1. Удостоверяющий центр: изготавливает сертификаты ключей подписей; создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи; приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их; ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем; проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра; выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии; осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей; может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги. 2. Изготовление сертификатов ключей подписей осуществляется на основании заявления

участника информационной системы, которое содержит сведения, указанные в статье 6 настоящего Федерального закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов. 3. При изготовлении сертификатов ключей подписей удостоверяющим центром оформляются в форме документов на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица удостоверяющего центра, а также печатью удостоверяющего центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата ключа подписи, второй - остается в удостоверяющем центре. 4. Услуги по выдаче участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов оказываются безвозмездно.

Статья 10. Отношения между удостоверяющим центром и уполномоченным федеральным органом исполнительной власти 1. Удостоверяющий центр до начала использования электронной цифровой подписи уполномоченного лица удостоверяющего центра для заверения от имени удостоверяющего центра сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью удостоверяющего центра. 2. Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют

выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц удостоверяющих центров. 3. Электронные цифровые подписи уполномоченных лиц удостоверяющих центров могут использоваться только после включения их в единый государственный реестр сертификатов ключей подписей. Использование этих электронных цифровых подписей для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается. 4. Уполномоченный федеральный орган исполнительной власти: осуществляет по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей; осуществляет в соответствии с положением об уполномоченном федеральном органе исполнительной власти иные полномочия по обеспечению действия настоящего Федерального закона.

Статья 11. Обязательства удостоверяющего центра по отношению к владельцу сертификата ключа подписи Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи: вносить сертификат ключа подписи в реестр сертификатов ключей подписей; обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем; приостанавливать действие сертификата ключа подписи по обращению его владельца; уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи; иные установленные нормативными правовыми актами или соглашением сторон обязательства.

Статья 12. Обязательства владельца сертификата ключа подписи 1. Владелец сертификата ключа подписи обязан: не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее; хранить в тайне закрытый ключ электронной цифровой подписи; немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена. 2. При несоблюдении требований, изложенных в настоящей статье, возмещение причиненных вследствие этого убытков возлагается на владельца сертификата ключа подписи.

Статья 13. Приостановление действия сертификата ключа подписи 1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования. 2. Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен. 3. Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию. 4. В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем

внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

Статья 14. Аннулирование сертификата ключа подписи 1. Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его: по истечении срока его действия; при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования; в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи; по заявлению в письменной форме владельца сертификата ключа подписи; в иных установленных нормативными правовыми актами или соглашением сторон случаях. 2. В случае аннулирования сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание об аннулировании сертификата ключа подписи.

Статья 15. Прекращение деятельности удостоверяющего центра 1. Деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, может быть прекращена в порядке, установленном гражданским законодательством. 2. В случае прекращения деятельности удостоверяющего центра, указанного в пункте 1 настоящей статьи, сертификаты ключей подписей, выданные этим удостоверяющим центром, могут быть переданы

другому удостоверяющему центру по согласованию с владельцами сертификатов ключей подписей. Сертификаты ключей подписей, не переданные в другой удостоверяющий центр, аннулируются и передаются на хранение в соответствии со статьей 7 настоящего Федерального закона уполномоченному федеральному органу исполнительной власти. 3. Деятельность удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, прекращается по решению владельца этой системы, а также по договоренности участников этой системы в связи с передачей обязательств данного удостоверяющего центра другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы.

Глава IV. Особенности использования электронной цифровой подписи

Статья 16. Использование электронной цифровой подписи в сфере государственного управления 1. Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций. 2. Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр сертификатов ключей подписей, который ведется уполномоченным федеральным органом исполнительной власти, и выдаются пользователям сертификатов ключей подписей из этого реестра в порядке, установленном настоящим Федеральным законом для удостоверяющих центров. 3. Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов Российской Федерации и уполномоченных лиц органов местного самоуправления устанавливается нормативными правовыми актами соответствующих органов.

Статья 17. Использование электронной цифровой подписи в корпоративной информационной системе 1. Корпоративная информационная система, предоставляющая участникам информационной системы общего пользования услуги удостоверяющего центра корпоративной информационной системы, должна соответствовать требованиям, установленным настоящим Федеральным законом для информационных систем общего пользования. 2. Порядок использования электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы. 3. Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

Статья 18. Признание иностранного сертификата ключа подписи Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Российской Федерации в случае выполнения установленных законодательством Российской Федерации процедур признания юридического значения иностранных документов.

Статья 19. Случаи замещения печатей 1. Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица. 2. В случаях, установленных законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о

правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

Глава V. Заключительные и переходные положения

Статья 20. Приведение нормативных правовых актов в соответствие с настоящим Федеральным законом 1. Нормативные правовые акты Российской Федерации подлежат приведению в соответствие с настоящим Федеральным законом в течение трех месяцев со дня вступления в силу настоящего Федерального закона. 2. Учредительные документы удостоверяющих центров, выдающих сертификаты ключей подписей для использования в информационных системах общего пользования, подлежат приведению в соответствие с настоящим Федеральным законом в течение шести месяцев со дня вступления в силу настоящего Федерального закона.

Статья 21. Переходные положения Удостоверяющие центры, создаваемые после вступления в силу настоящего Федерального закона до начала ведения уполномоченным федеральным органом исполнительной власти реестра сертификатов ключей подписей, должны отвечать требованиям настоящего Федерального закона, за исключением требования предварительно представлять сертификаты ключей подписей своих уполномоченных лиц уполномоченному федеральному органу исполнительной власти. Соответствующие сертификаты должны быть представлены указанному органу не позднее чем через три месяца со дня вступления в силу настоящего Федерального закона.

Президент
Российской Федерации
В. Путин