



**Код безопасности**  
ГК «Информзащита»

## Защита персональных данных в организациях ТЭК

Эксклюзивный полный вариант статьи М.Ю. Емельяникова, написанной на основе экспертной аналитики компании «Код Безопасности». Сокращенная версия статьи была опубликована на [snews.ru](http://snews.ru) некоторое время назад. Данная статья может рассматриваться как экспертная инструкция для отрасли ТЭК, полностью описывающая все действия (и их этапы) компаний данной отрасли, которые необходимо предпринимать в процессе приведения информационных систем и процедур в соответствие с требованиями ФЗ-152 «О персональных данных».

## Об авторе



**Михаил Емельяников**  
 Эксперт в области информационной безопасности и безопасности бизнеса.  
 Управляющий партнер Консалтингового агентства «Емельяников, Попова и партнеры»

## Персональные данные и сбыт электроэнергии

Принятие федерального закона № 261-ФЗ на длительный период сняло с повестки дня обсуждение изменений законодательства о персональных данных, проблемы излишних обременений для оператора, баланса интересов участников правоотношений и прочее, и прочее.

Новая редакция закона принята, все точки на сегодняшний день расставлены, правила определены. Остается лишь ждать документов Правительства, которые завершат процесс «вписывания» проблем охраны приватности в реалии российской жизни: определение уровней защищенности персональных данных, требований к защите персональных данных при их обработке в информационных системах персональных данных (ИСПДн), исполнение которых обеспечит установленные уровни защищенности, полномочий ФСБ и ФСТЭК России по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных в ИСПДн, не являющихся государственными, и тех видов деятельности, где с учетом значимости и содержания обрабатываемых персональных данных необходим контроль этих ведомств.

Крайне важным представляется то, каким образом будут реализовываться положения части второй ст. 4 Федерального закона «О персональных данных» (далее – ФЗ-152), в соответствии с которыми государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты (НПА), касающиеся обработки персональных данных. Новая редакция ФЗ-152, к сожалению, фактически сводит на нет возможность отраслевого регулирования, которое совсем еще недавно казалось единственным

возможным направлением для учета специфических особенностей деятельности в различных сферах. Полномочия различного рода отраслевых объединений операторов персональных данных в таких жестко завязанных на их обработку отраслях, как страховое дело, телекоммуникации, медицина, ЖКХ и других, сведены к определению дополнительных угроз безопасности к тем, что предложат ФСБ, ФСТЭК России и отраслевые министерства. Вряд ли стоит ожидать большого энтузиазма профессиональных ассоциаций в этом направлении. Поэтому остается уповать на усилия отраслевых государственных органов и Банка России, которые хоть как-то помогут соотнести практику бизнес-процессов и крайне жесткие требования законодательства.

Не являются исключением в этом процессе и энергосбытовые компании. Весь набор проблем, присущих крупным операторам персональных данных, в наличии и у них. Не случайно, что на двухдневной конференции «Стратегии развития бэк-офиса в энергосбытовых компаниях», которая прошла в Москве 24–25 ноября, два мероприятия – бизнес-кейс и круглый стол – были полностью посвящены тематике персональных данных.

Попробуем разобраться, какие подводные камни возникают на пути реализации законодательства о персональных данных у энергетиков, и как их можно было бы преодолеть.

## Первые шаги

Представляется, что первым шагом, который в условиях фактически нового федерального закона должна сделать любая компания, независимо от того, решала ли она вопросы, связанные с персональными данными, ранее или решила этим заняться только теперь, – это назначить лицо (физическое или юридическое), ответственное за организацию обработки персональных данных. Эта новая норма закона, обязательная для всех юридических лиц, продекларирована, но плохо проработана в ФЗ-152. А от этого шага зависит очень многое. У ответственного лица весьма сложные обязанности:

- 1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к их защите;
- 2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

При этом следует учитывать, что в соответствии с новой редакцией статьи 22.1 закона лицо, ответственное за организацию обработки персональных данных, должно получать указания непосредственно от исполнительного органа организации (чаще всего – генерального директора) и подотчетно только ему. Поэтому вряд ли стоит перекладывать эту проблему на системного администратора, инженера отдела автоматизации или инспектора по кадрам, как это часто делают в российских компаниях. Стоит сразу подумать над тем, как такое назначение «впишется» в требования, предъявляемые законом. Именно это ответственное лицо будет организовывать выполнение всех необходимых мер, предусмотренных российским законодательством в области персональных данных, причем, что очень важно, не только ФЗ-152, но и другими законами и НПА.

Как уже отмечено выше, закон допускает в качестве такого ответственного назначать и юридическое лицо, с которым будет необходимо заключить соответствующий договор. Несмотря на непроработанность норм, связанных, в частности, с необходимостью получения согласия субъектов персональных данных на доступ к сведениям о них представителей этой сторонней организации, практика привлечения аутсорсеров в качестве ответственных лиц выглядит весьма перспективной именно из-за сложности и многогранности проблем соответствия законодательству. Позиция некоторых надзорных органов, высказываемая, но пока не объявленная официально, о необходимости согласия каждого субъекта на допуск аутсорсера к его данным представляется весьма спорной. Обработка персональных данных в форме предоставления их ответственному юридическому лицу вполне может рассматриваться как предусмотренная п. 7 части первой ст. 6 ФЗ-152, когда обработка необходима для осуществления прав и законных интересов оператора при условии, что при этом не нарушаются права и свободы субъекта персональных данных. Права и законные интересы оператора заключаются в предусмотренной законом возможности передачи организации обработки внешней организации (обязательности согласия в этом случае закон не содержит), а соблюдение прав субъекта будет обеспечиваться соответствующими положениями договора между оператором и ответственным юридическим лицом о соблюдении требования конфиденциальности в отношении персональных данных.

## Информационные системы персональных данных в энергосбытовых компаниях

Следующий шаг на пути достижения соответствия требованиям законодательства – инвентаризация информационных систем, систематизированных собраний и картотек энергосбытовой компании, содержащих сведения о субъектах. Обработка персональных данных именно в этих базах регулируется новой редакцией закона.

Информационных систем, содержащих и обрабатывающих персональные данные, может оказаться несколько больше, чем кажется с первого взгляда. Помимо собственно учетной системы, выполняющей функции биллингования предоставленной потребителям электроэнергии, к ИСПДн должны быть отнесены системы кадрового и бухгалтерского учета, сайты сети Интернет, на которых созданы личные кабинеты клиентов – физических лиц, и даже почтовые серверы компании, которые также накапливают и обрабатывают персональные данные. Если обработка жалоб и обращений потребителей электроэнергии также ведется с использованием средств вычислительной техники (а увидеть пишущую машинку, на которой печатаются ответы гражданам, сегодня довольно сложно), эти компьютеры и офисные приложения также должны рассматриваться как ИСПДн, так как в соответствии с законом в них входят обеспечивающие обработку персональных данных информационные технологии и технические средства.

Как минимум, в энергосбытовой компании имеются персональные данные четырех групп субъектов: (1) работников компании; (2) клиентов – физических лиц; (3) акционеров и аффилированных лиц; (4) субъектов, которые являются работниками предприятий-контрагентов (потребителей – юридических лиц, партнеров, сервисных организаций и т.д.) и представителей органов власти, с которыми взаимодействует компания (надзорных органов, органов власти и муниципального управления, регуляторов и т.д.).

Обработка этих сведений производится, как правило, в различных целях, на различных основаниях и в различных информационных системах (приложениях).

Затем необходимо определить и цели обработки персональных данных, и все те категории персональных данных, которые обрабатываются в ИСПДн, и оценить правомерность их обработки.

ФЗ-152 очень жестко требует, чтобы операторы обрабатывали только те персональные данные, которые отвечают заранее сформулированным целям. Может оказаться, что некоторые сведения о гражданах, собранные оператором, являются излишними по отношению к определенным целям, а их обработка является неправомерной. Так, требует тщательного обоснования обработка сведений о лицах, проживающих совместно с владельцем жилья или ответственным квартиросъемщиком, практикуемая некоторыми энергосбытовыми компаниями. На тарификацию отпущенной электроэнергии эти данные, как правило, влияния не оказывают, и их истребование может быть оспорено в суде.

После уточнения правомерности обработки сведений может потребоваться некоторая корректировка бизнес-процессов, связанных с обработкой персональных данных.

Когда все эти подготовительные процессы будут завершены, необходимо проведение классификации информационных систем персональных данных в соответствии с трехсторонним приказом ФСТЭК, ФСБ и Минкомсвязи России от 13.02.2008 № 55/86/20 и документальное (в форме актов) оформление ее результатов. До выхода Постановления Правительства, которое определит уровни защищенности, по разъяснениям регуляторов следует руководствоваться именно этим приказом. Перед классификацией неплохо было бы подумать о снижении класса ИСПДн, например, за счет обезличивания части данных (для этого достаточно, например, вместо ФИО потребителя в биллинговой системе использовать номер лицевого счета) или сегментирования ИСПДн на несколько частей с использованием сертифицированных межсетевых экранов, что в некоторых случаях позволяет каждой из подсистем присвоить более низкий класс и, значит, снизить затраты на их защиту.

Для каждой ИСПДн (или групп однотипных ИСПДн) необходимо определить угрозы безопасности в соответствии с методическими документами ФСБ и ФСТЭК России и оформить результаты в виде модели (моделей) угроз.

## Работы бюрократические, но необходимые

Важнейшей частью работ по приведению порядка обработки в соответствие закону является разработка пакета локальных нормативных актов компании по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление

нарушений законодательства Российской Федерации, устранение последствий таких нарушений, порядок осуществления внутреннего контроля или аудита соответствия обработки персональных данных ФЗ-152 и принятым в соответствии с ним НПА, требованиям к защите персональных данных, а также политике оператора в отношении обработки персональных данных и локальным актам оператора.

Новым требованием к «бумаготворческой работе» является необходимость разработки и опубликования политики оператора в отношении обработки персональных данных. Причем закон требует, чтобы к документу, определяющему политику оператора и сведениям о реализуемых требованиях к защите персональных данных, был обеспечен неограниченный доступ. Причем, если сбор персональных данных осуществляется оператором с использованием информационно-телекоммуникационных сетей (ИТКС), например, сети Интернет, политика и сведения о предпринятых мерах защиты должны быть опубликованы в этой сети.

Поэтому эти документы должны быть доступны в тех помещениях, где энергосбытовая компания ведет прием населения, а если сведения потребителей – физических лиц она получает через веб-формы своих сайтов (например, личные кабинеты или системы формирования платежных документов), то политику необходимо выложить и на сайте, как это уже сделали некоторые компании.

В силу новизны и плохой проработанности методологии формирования политики оператора уже видны характерные ошибки, допускаемые некоторыми предприятиями и организациями. Не очень вникая в содержание этих документов, операторы часто пользуются типовыми, выкладываемыми в различного рода информационных системах. Необходимо понимать, что, изучив опубликованную политику, как клиенты, так и надзорные органы вправе рассчитывать, что оператор реализовал изложенные в ней положения в полном объеме, а в случае если это не так, может быть привлечен к ответственности за введение потребителей в заблуждение. Тем не менее ряд компаний уже принял на себя весьма серьезные, но вряд ли подкрепленные фактическими действиями обязательства, например, в виде использования выделенных каналов оптоволоконной связи для передачи персональных данных потребителей, применения сертифицированных средств шифрования, электронной подписи и криптографической аутентификации как средства подтверждения санкционированности доступа субъекта к объекту.

Другой характерной ошибкой является излишняя детализация описания предпринимаемых в информационной системе мер безопасности, которая может привести к получению потенциальным злоумышленником сведений, которые облегчат ему преодоление средств защиты, используемых оператором.

Да и при разработке всех остальных локальных актов следует быть весьма скрупулезным и внимательным. Обязательные требования могут содержаться в самых различных документах, недаром новая редакция ФЗ-152 так часто адресует нас не к «настоящему Федеральному закону», а к «федеральным законам». Так, например, в глубине Трудового кодекса (ст. 88) содержится требование о том, что локальным нормативным актом, с которым работник должен быть ознакомлен под роспись, должен быть определен порядок передачи персональных данных работников в пределах одной организации, т.е. между ее структурными подразделениями.

Особую сложность представляет определение сроков хранения персональных данных. С одной стороны, в соответствии с ФЗ-152 в случае достижения цели обработки или отзыва согласия на обработку оператор обязан незамедлительно прекратить обработку персональных данных или обеспечить ее прекращение и уничтожить соответствующие персональные данные (обеспечить их уничтожение) в срок, не превышающий тридцати дней с даты достижения цели обработки или поступления отзыва. Однако там же содержится разъяснение – «если оператор не вправе осуществлять обработку персональных данных без согласия субъекта на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами». А таких оснований, не просто допускающих обработку, но и прямо требующих ее продолжения, довольно много. Начиная с Гражданского кодекса, устанавливающего по умолчанию срок исковой давности в три года (а энергосбытовая компания – участник потребительского рынка, и вопросы разрешения споров с потребителями для нее весьма актуальны) и не заканчивая Налоговым кодексом, обязывающим хранить данные, необходимые для исчисления налогов субъектов, в частности, бывших работников, в течение четырех лет.

В заключение рассмотрения данного вопроса вспомним и о том, что Трудовой кодекс требует ознакомления под роспись работников и их представителей с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области. А ФЗ-152 в составе мер по выполнению закона содержит и обязательность ознакомления работников оператора, непосредственно осуществляющих обработку персональных данных, с поло-

жениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и обучения указанных работников.

## Взаимоотношения с субъектами

У энергосбытовых компаний есть несколько особенностей, связанных с наличием законных оснований на обработку персональных данных определенных категорий субъектов.

Первая заключается в том, что во многих случаях между предприятием и его клиентами отсутствуют договоры о предоставлении услуг. Сложилось это исторически, в силу особенностей формирования отношений в ЖКХ вообще, но в ряде случаев может создать негативные последствия для оператора, которым компания и является. Дело в том, что применительно к деятельности участников потребительского рынка основанием для обработки персональных данных физических лиц, помимо их согласия, может быть только договор, стороной которого является субъект, или выполнение возложенных законодательством на оператора функций, полномочий и обязанностей. Но последнее положение касается скорее работников и аффилированных лиц акционерных обществ, поскольку законодательных актов, регулирующих порядок обработки сбытовыми компаниями сведений о клиентах – физических лицах, аналогичных, например, тем, которые регулируют порядок обработки персональных данных участников системы обязательного медицинского страхования или Единого государственного экзамена, у нас в стране нет.

Попытки же получить сведения о субъектах от других организаций ЖКХ иногда приводят к административным правонарушениям. Характерно в этом отношении решение районного суда г. Омска, посчитавшего неправомерным передачу управляющей компанией персональных данных потребителя в энергосбытовую компанию.

Тем не менее даже при отсутствии договоров между сбытовыми компаниями и клиентами – физическими лицами или согласий субъектов их персональные данные обрабатываются поставщиками энергии. Понимая двусмысленность ситуации, некоторые компании идут по пути заключения договоров на энергообеспечение непосредственно с потребителями, однако сталкиваются с нормой ч. 7 ст. 155 Жилищного кодекса, предусматривающей, что собственники помещений в многоквартирном доме, в кото-

ром не созданы товарищество собственников жилья либо жилищный кооператив и управление которым осуществляется управляющей организацией, плату за коммунальные услуги должны вносить этой управляющей организации, а не поставщику ресурсов. Исключения из этого правила допускаются только на основании решения общего собрания собственников помещений.

Не надо забывать и о праве доступа субъекта к своим персональным данным и сведениям, имеющим значение для обеспечения законных интересов субъекта. Попытка не допустить это в том же Омске привела к проигрышу еще одного иска к поставщику, который не предоставил необходимых сведений, в том числе – касающихся других субъектов, но затрагивающих права заявителя.

Существуют особенности и раскрытия информации об акционерах и аффилированных лицах акционерных обществ. С одной стороны, необходимо обеспечить выполнение положений закона, касающихся раскрытия и обязательного опубликования сведений, а с другой – не распространять те категории персональных данных, которые законами не предусмотрены.

Особые сложности вызывает обоснование обработки персональных данных контрагентов, которые должны быть уведомлены о начале обработки персональных данных либо оператором, либо своим работодателем.

Особую проблему вызывает использование энергосбытовыми компаниями биллинговых систем для тарификации потребленной электроэнергии. В данном случае выставление счетов на оплату биллинговой системой является классическим случаем принятия решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы на основании исключительно автоматизированной обработки персональных данных. ФЗ-152 обставляет такую возможность целым рядом обязательных условий, главным из которых является наличие согласия субъекта персональных данных на это в письменной форме, установленной законом. Не только согласия, но и договора с субъектом у сбытовой компании часто нет. Кроме того, даже при наличии согласия оператор должен выполнить целый ряд дополнительных требований, в частности, разъяснить порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных, возможные юридические последствия такого решения и порядок защиты субъектом персональных данных своих прав и законных

интересов, а также предоставить субъекту возможность заявить возражение против такого решения. Вряд ли удастся найти большое количество энергосбытовых компаний, именно таким образом урегулировавших свои отношения с клиентами.

Еще один сложный вопрос – обеспечение конфиденциальности персональных данных. Именно в силу необходимости выполнения этого требования большинство поставщиков услуг населению отказалось от доставки счетов в открытом виде. Не миновала чаша сия и энергетиков. В конце января этого года за рассылку счетов, нарушающих конфиденциальность указанных в них данных, был привлечен к административной ответственности один из топ-менеджеров «Воронежской энергосбытовой компании». Результат не заставил себя ждать. Уже с августа 2011 года все счета доставляются потребителям в запечатанном виде, для чего было закуплено и установлено соответствующее оборудование. Спрос рождает предложение. Одна из крупнейших мировых компаний, специализирующихся на полиграфическом оборудовании для оформления расчетов, предложила российскому рынку специальные технологии бесконвертной упаковки, больше знакомые по счетам, выставляемым банками, операторами связи и расчетными центрами ЖКХ.

## Проектирование подсистемы информационной безопасности

Завершающим этапом работ по приведению обработки персональных данных граждан в соответствие с требованиями закона является проектирование и построение системы защиты этой категории сведений ограниченного доступа. Несмотря на то, что документы Правительства, определяющих уровни защищенности персональных данных и требования по их обеспечению, пока нет, многие вопросы технической защиты очевидны и сейчас, исходя из общей практики построения информационных систем и требований, уже заложенных в законе.

Ясно, что ни в одной современной системе не обойтись без антивирусной защиты. Естественно, она должна быть лицензионной и сертифицированной.

Если информационная сеть компании имеет подключение к сети Интернет, необходимо использовать межсетевые экраны.

Положения ст. 19 ФЗ-152 о необходимости обнаружения фактов несанкционированного доступа (НСД) к персональным данным, регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн, требует применения средств защиты от НСД.

Норма о восстановлении персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, влечет создание системы резервного копирования.

Обработка персональных данных на сайте в сети Интернет вынуждает использовать средства анализа защищенности, поскольку взлом сайта и потеря контроля над ним могут привести к серьезным последствиям, в том числе и для начисления оплаты за услуги компании, т.е. к финансовым потерям.

Помня, что все средства защиты информации, используемые в ИСПДн, должны пройти в установленном порядке процедуру оценки соответствия, в качестве которой на сегодняшний день регуляторы рассматривают только обязательную сертификацию, выбор возможных решений весьма сужается. А учитывая, что техническая защита конфиденциальной информации является лицензируемым видом деятельности, придется сузить и круг возможных интеграторов, которые могут выполнить данную работу.

Строя подсистему информационной безопасности, владельцы информационных систем зачастую сталкиваются с проблемой «зоопарка» применяемых средств защиты и их совместимости. Одну из наиболее интересных и длинных линеек продуктов, обеспечивающих выполнение закона, предлагает российская компания «Код Безопасности», в арсенале которой практически полный набор средств защиты – от предотвращения НСД (Secret Net, «Соболь») до криптографии («Континент») и межсетевое экранирование (TrustAccess). Для таких пользователей, как энергосбытовые компании, эксплуатирующих высокопроизводительные центры обработки данных, важнейшим показателем является наличие среди продуктов средств обеспечения безопасности в виртуальной среде, качество которых подтверж-

дено как российским регулятором, так и производителем средств виртуализации (VMware).

И, наконец, в арсенале компании – комплексное решение по защите рабочих станций Security Studio Endpoint Protection, включающее в себя антивирус, антиспам и антишпион, персональный межсетевой экран, IDS уровня хоста и средства веб-фильтрации.

Все без исключения продукты имеют сертификаты ФСТЭК и/или ФСБ России (в зависимости от области ответственности).

## Уведомление Роскомнадзора

Заключительным этапом работ по приведению системы обработки персональных данных в соответствие с законом является направление уведомления в Роскомнадзор, предусмотренное Ф3-152. В силу особенностей обрабатываемых категорий персональных данных и их субъектов, о которых говорилось выше, энергосбытовыми компаниям не приходится рассчитывать, что они подпадают под исключения, предусмотренные законом. Таких уведомивших уполномоченный орган по защите прав субъектов среди сбытовиков сегодня порядка 40, но Роскомнадзор активно ведет работу по увеличению числа юридических лиц, направляющих уведомления, привлекая те из них, которые не смогут доказать наличие для них исключений, к административной ответственности по ст. 19.7 КоАП РФ.

Как видно, соответствовать закону трудно. Но можно. И лучше не откладывать эту работу до прихода надзорных органов и привлечения должностных лиц оператора к ответственности. А она может быть в конечном итоге весьма серьезной, вплоть до дисквалификации руководителей и иных ответственных лиц.



## Код безопасности

ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: [info@securitycode.ru](mailto:info@securitycode.ru)

Запрос дополнительной информации о продуктах: [info@securitycode.ru](mailto:info@securitycode.ru)

По вопросам стоимости и покупки продуктов [sales@securitycode.ru](mailto:sales@securitycode.ru)

По вопросам партнерства и сотрудничества [info@securitycode.ru](mailto:info@securitycode.ru)

Вы можете узнать подробную информацию о продуктах на сайте

[www.securitycode.ru](http://www.securitycode.ru)

### **О компании «Код Безопасности»**

Компания «Код Безопасности» – лидирующий российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.