О защите персональных данных и иной конфиденциальной информации

31.05.2012 НОВОСТИ КОМПАНИЙ

**ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ
И ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. ПЕРВЫЕ РЕЗУЛЬТАТЫ ПРОВЕРОК И КОНТРОЛЯ РОСКОМНАДЗОРА,
НОВОВВЕДЕНИЯ И ОЖИДАНИЯ 2012 ГОДА**

Особенности и условия защиты персональных данных, первые результаты проверок и контроля Роскомнадзора, перспективы развития законодательного регулирования защиты персональных данных стали главной темой обсуждений в рамках пресс-завтрака, проведенного 29 мая 2012 года юристами группы правовой защиты информации «Пепеляев Групп».

Юристы «Пепеляев Групп» прокомментировали официальную статистику Роскомнадзора по проверкам и нарушениям в сфере защиты персональных данных, а также поделились прогнозами относительно развития законодательства в области защиты информации.

В выступлениях руководителя группы по правовой защите информации «Пепеляев Групп» **Андрея Слепова** и руководителя группы административно-правовой защиты бизнеса «Пепеляев Групп» **Елены Овчаровой** были затронуты следующие темы:

- Рейтинг главных событий 2011-2012 г. в сфере правовой защиты информации, прогнозы 2012 г.
- Основные нарушения и направления проверок в сфере защиты персональных данных в

2011-2012 гг. (комментарии официальной статистики и отчета Роскомнадзора).

> Ответственность за несоблюдение требований законодательства, предусматривающего защиту персональных данных, методы контроля и надзора.

Мы предлагаем вашему вниманию лишь отдельные и очень важные аспекты, обозначенные и раскрытые в докладах юристов «Пепеляев Групп».

ГЛАВНЫЕ СОБЫТИЯ В СФЕРЕ ПРАВОВОЙ ЗАЩИТЫ ИНФОРМАЦИИ – 2011-2012 были представлены в виде специального рейтинга.

1 место в рейтинге главных событий в сфере правовой защиты информации, по мнению юристов «Пепеляев Групп», можно отдать **Закону «О персональных данных»** (в ред. Федерального закона от 25.07.2011 № 261-ФЗ).

Также планируется принятие целой череды подзаконных актов. В конце апреля 2012 года ФСБ опубликовал *проекты* двух постановлений Правительства РФ, устанавливающих уровни защищенности персональных данные и технические требования к безопасности данных, которые пока еще не приняты в качестве нормативно-правовых актов.

2 место достается Закону «О национальной платежной системе», устанавливающему, среди прочего, обязанности операторов по переводу денежных средств, банковских платежных агентов, операторов платежных систем и операторов услуг платежной инфраструктуры по обеспечению защиты информации в платежной системе.

Закон устанавливает регулирование многих платежных инструментов (например, виртуальных платежей), которые до этого находились практически вне рамок правового поля.

Однако редакция Закона, которая посвящена защите информации и банковской тайне,

представляется крайне запутанной и несогласованной с другими законодательными актами. И, очевидно, это приведет к трудностям и проблемам правоприменения.

Закон полностью вступит в силу с 1 января 2013 года, при этом положения, касающиеся защиты информации, будут обязательны уже с 1 июля 2012 года.

3 место занимает **Закон «О лицензировании отдельных видов деятельности»** и новое положение о лицензировании, которые устанавливают, что деятельность по технической защите конфиденциальной информации является лицензируемой вне зависимости от того, осуществляется ли она для обеспечения собственных нужд или нет.

4 место в рейтинге было отдано **Закону «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»**.

Закон призван сделать российский фондовый рынок, который всегда славился как «инсайдерский», более прозрачным, менее манипулятивным.

Недостатком Закона является его непроработанность. Как в случае с некоторыми другими законами в сфере защиты информации (включая Закон о персональных данных), принимая антиинсайдерский закон, государство стремилось обеспечить или обязать обеспечить максимальный контроль за потоками информации.

5 место принадлежит **Закону «Об электронной подписи»**.

Одно из несомненных достоинств нового Закона заключается в том, что он вариативен в отличие от старого законодательства – в обороте допускается (с определенными оговорками) использовать как технически достаточно простые аналоги собственноручных подписей (в сущности, простые пароли), так и технически сложные (с использованием криптографии) и, соответственно, более безопасные виды электронных подписей. Однако без внесения изменений в ряд законов и принятия некоторых подзаконных актов данный

Закон фактически не будет работать. Кроме того, Закон не столь известен и популярен в бизнес-среде, как хотелось бы. И, тем более, Закон практически не известен широким слоям населения. А если бы каждый гражданин имел бы свою электронную подпись, то это сильно бы упростило многие вопросы, включая заключение договоров и совершение покупок через интернет и т. д.

1 июля 2012 года прекращает свое действие старый Закон «Об электронной цифровой подписи», и все отношения, связанные с использованием электронных подписей, будут регулироваться только новым Законом.

Применительно к вопросам защиты персональных данных стоит заметить, что в Российской Федерации запрет на обработку информации (её сбор, хранение, использование и распространение) о частной жизни лица без его согласия установлен ч. 1 ст. 24 Конституции РФ.

Административная ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) введена с 1 июля 2002 г. статьей 13.11. КоАП РФ. Между тем, конкретика в требованиях к защите и порядку использования персональных данных появилась значительно позже – лишь в январе 2007 г., но и в ней по сей день много неясного.

Федеральным законом от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности» было введено лицензирование деятельности по технической защите конфиденциальной информации (в том числе и персональных данных) (п. 1 ст. 17). С 1 июля 2002 г. была введена административная ответственность за занятие видами деятельности в области защиты информации без получения в установленном порядке специального разрешения (лицензии), если его получение обязательно, частью 1 ст. 13.13. КоАП РФ.

Существенный толчок в развитии российского законодательства о защите персональных данных, хранящихся в автоматизированных базах данных, дала ратификация РФ в конце

2005 г. Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981[1].

26.01.2007 вступил в силу ФЗ «О персональных данных», цель которого – обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни[2], личную и семейную тайну.

Данный закон установил принципы и условия обработки персональных данных, обязанность оператора уведомить уполномоченный государственный орган об обработке персональных данных, определил права субъекта персональных данных и обязанности оператора, в том числе при сборе персональных данных, организационные и технические меры по обеспечению безопасности персональных данных при их обработке.

Однако сложность исполнения данного закона заключалась в том, что не были приняты подзаконные нормативные правовые акты, без которых требования к информационным системам персональных данных не могли быть реализованы операторами.

29.11.2007 вступило в силу Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Постановлением Правительства РФ от 17.11.2007 № 781, которое ввело обязательные для соблюдения требования к обеспечению безопасности персональных данных при их автоматической обработке.

Принятие иных необходимых для реализации ФЗ «О персональных данных» подзаконных актов потребовало еще несколько лет: 28.10.2008 вступило в силу Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации[3], 16.03.2010 – Положение о методах и способах защиты информации в информационных системах персональных данных[4]; 21.06.2010 – Рекомендации в области стандартизации Банка России[5].

Но как только появилась хотя бы какая-то ясность в мероприятиях, которые операторы

должны принимать для защиты персональных данных, требования изменились. 1 июля 2011 г. вступили в силу изменения в ФЗ «О персональных данных», существенно изменившие требования к защите персональных данных. И до настоящего момента, Правительством РФ не приняты постановления, призванные регламентировать новый порядок защиты персональных данных. Это, конечно, не означает, что меры защиты операторами не должны быть приняты.

В части защиты персональных данных работников регулирование более «стройное» и с более долгой историей. Режим защиты персональных данных *работника* был конкретизирован Трудовым кодексом, введенным в действие с 1 февраля 2002 г. Административная ответственность за его несоблюдение установлена статьей 5.27. «Нарушение законодательства о труде и об охране труда» КоАП РФ.

Несмотря на столь существенный массив нормативных правовых документов, обязывающих защищать персональные данные физических лиц и устанавливающих порядок и инструменты защиты персональных данных, операторы, за исключением очень узкого сегмента (например, операторы связи, выполнение которыми законодательства, в том числе о персональных данных, было условием осуществления ими лицензируемой деятельности, а также банки, соответствующую нормативную документацию для которых разрабатывает и проверяет её соблюдение Банк России) продолжали и многие продолжают до сих пор игнорировать данные требования, предъявляемые законодательством к защите персональных данных.

С 01.01.2008 Россвязьохранкультура (в настоящее время Роскомнадзор) был наделен функциями по контролю и надзору за соответствием обработки персональных данных требованиям законодательства[6]. В эту же дату операторы, осуществляющие обработку персональных данных, обязаны были направлять уведомление Россвязьохранкультуры (Роскомнадзор) об обработке персональных данных.

17 мая 2012 г. на сайте Роскомнадзора опубликован отчет данного ведомства о его

деятельности в качестве уполномоченного органа по защите прав субъектов персональных данных за 2011 г., в нем, в частности, заявлен следующий итог работы за все 4 года существования: им «создана стройная система защиты прав и законных интересов граждан, эффективность которой подтверждается ежегодным ростом основных качественных и количественных показателей» (http://www.rsoc.ru/plan-and-reports/reports/).

«Статистика показывает, что из-за неподготовленности бизнеса к изменениям законодательства в сфере защиты персональных данных, почти каждая проверка выявляет нарушения», — комментирует отчет Елена Овчарова, руководитель группы административно-правовой защиты бизнеса «Пепеляев Групп».

Проанализировав практику, складывающуюся в сфере контроля (надзора) за соблюдением требований законодательства в сфере персональных данных, можно сделать вывод, что наиболее частые нарушения операторов неизменны с 2008 г. по 2012 г.:

- ненаправление к определенному сроку в территориальный орган Роскомнадзора сведений уведомления об обработке ПДн;
- непредставление или несвоевременное представление оператором информации по запросу Роскомнадзора (например, для рассмотрения обращения гражданина или в ходе проверки);
- несоответствие сведений, указанных в уведомлении об обработке ПДн, фактической деятельности оператора;
- невыполнение в установленный срок законного предписания территориального органа Роскомнадзора об устранении нарушений;
- обработка оператором ПДн без согласия субъектов ПДН или несоответствие содержания письменного согласия субъекта на обработку его ПДн требованиям Закона о

персональных данных;

- непринятия операторами мер, обеспечивающих сохранность ПДн и исключающих несанкционированный доступ к ним;
- нарушение требования конфиденциальности;
- избыточность обрабатываемых персональных данных субъекта персональных данных применительно к целям обработки; обработка ПДн дольше, чем этого требуют конкретные цели и др.

По оценке группы административно-правовой защиты бизнеса, в настоящее время операторами персональных данных совершается большое количество нарушений законодательства РФ в сфере персональных данных, поэтому от Роскомнадзора следует ожидать «на постоянной основе мониторинга деятельности Операторов, направленного на предупреждение, выявление и пресечение нарушений в области персональных данных». «А в ближайшем будущем, возможна, полагаем, дифференциация составов административных правонарушений в области персональных данных», уверена Елена Овчарова.

[1] См.: Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». Он вступил в силу с 02.01.2006.

[2] См.: Статья 2 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее по тексту – ФЗ «О персональных данных»).

[3] Утверждено Постановлением Правительства РФ от 15.09.2008 № 687.

[4] Утверждено Приказом ФСТЭК РФ от 05.02.2010 № 58.

[5] Приняты и введены в действие Распоряжением Банка России от 21.06.2010 № Р-705 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации РС БР ИББС-2.4-2010 и Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации РС БР ИББС-2.3-2010».

[6] См.: Постановление Правительства РФ от 15.12.2007 № 878 «О некоторых вопросах деятельности Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия».