Заблуждение № 1.

Закон «О персональных данных» вступает в силу только 1.01.2011. Пока время есть.

Реальность.

Закон вступил в силу через 180 дней с даты его опубликования, т.е. 29.01.2007 года. Законом РФ от 27 декабря 2009 года N 363-ФЗ продлен срок приведения в соответствие информационных систем персональных данных, созданных до 01.01.2010 г. Однако все остальные нормы закона №152 (в т.ч. определяющие и иные обязанности оператора, например, обязанности по защите ПДн – ст.19 ФЗ №152) действуют в настоящее время. Это же относится и к положениям иных нормативных документов. Например, работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ по созданию ИСПДн (п.4 Приложения к Постановлению Правительства РФ № 781 от 17.11.2007 г.). О чем это говорит? О том, что любые работы или услуги по проектированию или внедрению ИСПДн в обязательном порядке должны учитывать и создание подсистем обеспечения информационной безопасности. Создается ИСПДн для бухучета и кадровой работы? Тогда срок 1.01.2010 – не для этой ИСПДн, так как она создается не до, а после вступления в силу закона.

Организационные меры по защите ПДн также должны быть реализованы оператором вне всякой связи с датой 1.01.2011. Причина: эти меры в большинстве случаев связаны с фактами обработки ПДн не только в составе ИСПДн, и, следовательно, не подпадают под действие ст. 25 ФЗ№152. Правоприменительная практика Роскомнадзора подтверждает изложенное.

Заблуждение №2.

Важно защититься от претензий контрольных и надзорных органов (т.е. от государства), в первую очередь – Роскомнадзора. Для этого нужно направить уведомление в Роскомнадзор и создать комплекс внутренних документов, требуемых при проверке.

Реальность.

Введение свода локальных организационно-распорядительных документов – конечно же, обязательный этап работ по защите ПДн. Однако эти первоначальные и необходимые меры **не являются достаточными!** Действительно, многие операторы полагают, что нужно защититься от государства, а не защищать ПДн. Часто в понимании оператора задача защиты от государства в лице Роскомнадзора является вообще единственной, что противоречит смыслу и цели (она одна и простая, почему бы не посмотреть эту цель?) закона "О персональных данных". Это тупиковый путь, чреватый осложнениями.

Во-первых, не следует забывать о том, что ФЗ № 152 (ч.1 ст.19) установил, что, наряду с организационными мерами защиты оператор обязан принимать и технические меры защиты. Какие именно – вопрос вне рамок данной статьи, можно лишь подчеркнуть, что в большинстве случаев необходимость принятии технических мер защиты обоснована, и такие меры должны быть приняты в сроки, установленные ст. 25 ФЗ№ 152.

Во-вторых, Роскомнадзор РФ осуществляет надзорные функции только в рамках, установленных действующим законодательством, Положением о Роскомнадзоре и административными регламентами. Иных (выходящих за пределы своей компетенции) мероприятий по проверке системы защиты ПДн Роскомнадзор не выполняет, но это не означает, что государство не имеет возможностей контроля полноты и соответствия закону мероприятий по защите ПДн, проведенных конкретным оператором. Роскомндазор – не единственный орган, надзирающий за соблюдением прав граждан. Органы прокуратуры, например, наделены правами по возбуждению административного производства (в т.ч. и по ст.13.11 КоАП РФ), а достаточное количество предписаний органов прокуратуры и судебных решений позволяет говорить о формировании правоприменительной практики.

В-третьих, недальновидность такой стратегии оператора заключается в том, что не учитываются права самого субъекта ПДн и возможные негативные последствий для оператора из-за нарушения прав субъекта ПДн. Тем более тогда, когда такие нарушения действительно имеют место. Субъект будет жаловаться, и его жалоба будет рассмотрена вне зависимости от количества и качества подготовленных оператором положений, инструкций и регламентов! Права субъекта ПДн весьма обширны (ст.14

ФЗ 152). К сожалению, большинство операторов и не подозревают о том, в какие сроки и какой объем информации оператор обязан предоставить субъекту ПДн. А ведь субъект ПДн, не подозревающий о выстроенной оператором «системе документарной защиты от Роскомнадзора», по своей душевной простоте может обратиться с обоснованной жалобой (обращением, заявлением, иском) в прокуратуру, органы внутренних дел, суд. Безусловно, указанные органы будут обязаны реагировать на такие обращения. Длительность и последствия такого реагирования находятся в прямой зависимости от настойчивости грамотного субъекта ПДн (а его знания эволюционируют весьма быстро) и содержательной части его обращений. Именно поэтому стратегия оператора по реализации требований ФЗ № 152 должна заключаться не в подготовке «дециметров» внутренних нормативных документов, а в создании сбалансированной системы защиты ПДн, исключающей наступление инцидентов информационной безопасности. Исключение таких инцидентов будет являться залогом отсутствия обоснованных жалоб субъектов ПДн.

Заблуждение №3.

Направлять уведомление в Роскомнадзор не следует, т.к. в этом случае оператора «возьмут на заметку», обязательно проверят и накажут.

Реальность.

Территориальные подразделения Роскомнадзора обладают вполне очевидными, доступными и законными способами установить факт деловой активности лица (оператора), и сделать вывод о том, что такое лицо является оператором ПДн. Отсутствие уведомления в этом случае только усугубит положение оператора, не направившего уведомления в случаях, предусмотренных ФЗ№152. Роскомнадзор же вправе расценить отсутствие уведомления от оператора как административное правонарушение, предусмотренное ст. 19.7. КоАП РФ. То есть «накажут», скорее, из-за нерасторопности оператора и отсутствия уведомления, а не в силу направления уведомления в надзорный орган. Задача же сбора уведомлений – не тотальный контроль операторов со стороны государства, а подготовка реестра операторов в целях упорядочения обработки ПДн и, в конечном счете, надлежащей защиты прав субъектов ПДн. Форму уведомления можно найти на сайте Роскомнадзора www.rsoc.ru .

Остается только добавить, что подготовка уведомления – достаточно простая процедура, имеющая, правда, свои особенности, связанные с формулированием целей и правовых оснований обработки ПДн.

Заблуждение №4.

Направлять уведомление в Роскомнадзор не нужно, если оператор обрабатывает ПДн только своих сотрудников на основании трудового договора (ч.2 ст22 ФЗ 152).

Реальность.

Формально такое исключение предусмотрено указанной статьей. Однако на практике осмысленная и вдумчивая попытка применения этого исключения не приводит к аргументированному выводу об отсутствии обязанности оператора по направлению уведомления. Этот парадокс касается большинства операторов. Для примера рассмотрим обработку ПДн субъекта, являющего работником оператора. Как правило, помимо обработки ПДн работника, оператор на законных основаниях обрабатывает ПДн иных лиц, имеющих отношение к работнику. Таковыми могут быть лица, получающие алименты по решению суда или в добровольном порядке (супруги, дети, родители работников). Оператор также может обрабатывать ПДн в целях предоставления работникам стандартных налоговых вычетов на детей и (или) социальных налоговых вычетов в связи с обучением или лечением детей или иных родственников; несовершеннолетних детей работников в целях их оздоровления (направление детей в оздоровительные лагеря) и т.п. Наконец, оператор обрабатывает ПДн физических лиц в целях их трудоустройства (резюме кандидатов), при этом обработка ПДн этих лиц происходит до установления трудовых отношений. Поэтому к применению такого исключения нужно относиться очень внимательно.

Часто оператор, поверхностно ознакомившись с ФЗ №1 52, приходит и к следующему нелогичному выводу: отсутствие необходимости направления уведомления означает вообще отсутствие обязанности выполнения закона «О персональных данных»! Что это - труднообъяснимый парадокс российского менталитета, болезненная потребность во вмешательстве надзорных органов, или банальная самонадеянность в сочетании с завесой коллективной безответственности? Вероятнее всего – безграмотность и халатность сотрудников оператора, вводящих руководителя оператора в заблуждение.

Заблуждение №5.

Защищать персональные данные нужно лишь тем, кто оказывает какие-либо услуги гражданам и обрабатывает ПДн этих граждан. Защита персональных данных «своих» сотрудников необязательна, либо такая защита может быть менее строгой.

Реальность.

Подобное утверждение является предпосылкой к нарушению принципа равенства всех перед законом. Этот принцип закреплен в Конституции РФ (ст. 19). Действительно, разве могут конституционные права работника на тайну личной жизни (ст. 23 Конституции РФ) отличаться от прав другого лица, не являющегося работником предприятия? Еще более важным является вопрос: согласится ли работник предприятия (организации) с фактическим положением дел, при котором его (работника) конституционные права ущемлены? Даже если работников немного, и все они крайне лояльны по отношению к оператору, то нужно понимать, что защита любых конституционных прав – это сфера публичных интересов. Положения же Конституции РФ все органы власти будут защищать вне зависимости от желания субъекта ПДн и вопреки воле оператора - это аксиома. Иными словами, органы прокуратуры, например, вправе отреагировать на указанную позицию оператора вполне предсказуемым образом.

Практика показывает, что работник оператора может быть гораздо более требовательным, чем любой иной субъект ПДн по отношению к оператору в части соблюдения последним своих обязанностей по защите ПДн работника. Многие операторы (и профессиональное сообщество) считают, что в действующей редакции ФЗ 152 права субъекта ПДн чрезмерны и абсолютизированы. Действительно, это так – права субъекта ПДн должны быть «уравновешены» здравым смыслом и правами оператора, а требования субъекта – быть обоснованными. Так или иначе, оператору пора привыкать к тому, что конституционные права субъектов (его работников) – непреложный факт, требующий выполнения установленных законом действий. Не следует забывать о том, что и Трудовой Кодекс РФ (ст.87) устанавливает обязанности работодателя по хранению и использованию ПДн работника. В этой связи можно подумать о том, готов ли работодатель столкнуться с еще одним органом государственного надзора и контроля – Государственной инспекцией труда.

Заблуждение №6

Безопасность ПДн и конфиденциальность ПДн – это одно и то же. Если обеспечена конфиденциальность, то требования закона выполнены.

Реальность.

Очень часто операторы понимают под конфиденциальностью (режимом конфиденциальности) весь комплекс мер по обеспечению безопасности. Это заблуждение находит свое отражение и в нормативных документах оператора, в которых понятие «конфиденциальность» подразумевает комплекс мер по защите информации. Это ошибка. Серьезная, опасная, системная ошибка. Природа и смысл этих терминов (и, как следствие, мер по реализации защиты) различны.

Закон дает (п.10 ч.1 ст. 3 ФЗ 152) определение конфиденциальности информации. **Совсем коротко, конфиденциальность – это требование о неразглашении ПДн. Безопасность же – это состояние защищенности.** Определение термину безопасность дает ФЗ РФ «О безопасности». Определение безопасности информации дано в ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Крайне важным представляется и тот факт, что законодатель (ч.4 ст. 6 ФЗ 152) разграничил эти понятия и указал их отдельно при установлении обязанностей оператора при передаче ПДн третьим лицам для обработки. Кстати, такая практика передачи встречается очень часто (например, при передаче на аутсорсинг бухучета, при направлении работников на медосмотр и т.п). Необходимо помнить об этом и потому, что закон установил

Требование по обеспечению безопасности и конфиденциальности ПДн в качестве существенного условия договора. Отсутствие такого условий может привести к признанию договора недействительным.

Заблуждение №7

Лицензия ФСТЭК нужна, если оказываются услуги по технической защите конфиденциальной информации третьим лицам. Если оператор защищает ПДн «для собственных нужд», не за деньги – то никакой лицензии не нужно.

Реальность.

Такое заблуждение – результат псевдоправовых изысканий некоторых операторов, пытающихся выдать желаемое за действительное и сэкономить на защите персональных данных. Наше развернутое и аргументированное мнение по этому вопросу будет являться предметом отдельной статьи. Коротко же можно пояснить следующее. Не существует у оператора «собственных нужд» по защите персональных данных, и существовать не может в силу закона. Единственной целью ФЗ152 является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных. Иных целей (в том числе и удовлетворения нужд операторов) закон не указывает. Кстати, для всех была бы очевидной абсурдность утверждений застройщика, о том, что ему не нужна лицензия на строительство, т.к. он возводит жилое здание «для собственных нужд». Или – отсутствие необходимости в лицензии на оказание медицинских услуг, так как организация будет лечить только своих сотрудников. Сторонникам этого заблуждения нужно обратиться и к ст.4 ФЗ 128-ФЗ «О лицензировании отдельных видов деятельности»: «…к лицензируемым видам деятельности относятся виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам, законным интересам, здоровью граждан…». В нашем же случае речь идет о конституционном праве гражданина на личную тайну! Как мы уже указывали, закон не делает различий между интересами субъекта ПДн (работника) и субъекта ПДн (стороннего лица). Иное положение вещей было бы дискриминацией. Законодатель же (через институт лицензирования) защищает любого субъекта ПДн от последствий некачественного выполнения работ по ТЗКИ. Вероятно, точку в этом вопросе поставит судебная власть, но для профессионального сообщества истина очевидна уже сейчас.

Заблуждение №8

Сначала надо создать информационную систему, а уж потом решать вопрос с защитой персональных данных в ней. Тем более что сметой (бюджетом) эти расходы не предусмотрены.

Реальность.

Работы по обеспечению безопасности персональных данных при их обработке в ИСПД являются неотъемлемой частью работ по созданию ИСПДн (п.4 Приложения к Постановлению правительства РФ от 17.11.2007 г. № 781). Неотъемлемой! Создавать какие-либо ИСПДн без системы защиты ПДн в ИСПДн запрещено. Помимо этого недвусмысленного требования, нарушать которое мы не советуем, есть еще логика бизнес-процессов и доводы экономического характера – создаваемая одновременно с информационной системой система защиты обойдется оператору значительно дешевле, чем созданная потом «надстройка». Касательно сметы и бюджетирования можно лишь напомнить, что времени для планирования таких расходов было достаточно – с января 2007 года.

Заблуждение №9

Защита ПДн – это дело системного администратора (или IT службы), и эта задача может быть ими успешно выполнена.

Реальность.

Вряд ли разумный человек, нуждающийся в операции на сердце, доверит ее проведение даже очень квалифицированному стоматологу. Профессиональный же стоматолог никогда и не возьмется за это. Защита информации – это профессиональная специализация, а не хобби. В РФ существует шесть образовательных стандартов в сфере защиты информации, и это не случайно! Конечно, желательно поручить решение комплекса вопросов по защите ПДн специалисту, имеющему диплом по защите информации, или хотя бы прошедшему курсы повышения квалификации. Но и этого недостаточно.

Ведь оператору придется решить массу вопросов организационно-административного и правового характера, привлекая к мероприятиям по защите ПДн юридическую, финансовую, кадровую службу, а далеко не всякий оператор обладает достаточными людскими ресурсами. Вот почему лучшим решением является привлечение специализированной организации, имеющей соответствующие лицензии. Самолечение опасно!

Существует и еще один аспект проблемы. Как известно, в большинстве случаев причиной наступления инцидентов информационной безопасности является человеческий фактор, а источником угроз – собственные сотрудники оператора (т.н. внутренние угрозы). IT-специалист или системный администратор организации - лицо, облеченное доверием. Поэтому (и в силу специфики работы) оно обладает и неограниченными правами доступа к инфоресурсам. Но как раз по этой причине и нельзя «класть яйца в одну корзину», сосредотачивая двойную ответственность в функционале одного человека (подразделения). IT-служба не должна контролировать себя! Информационная безопасность – дело отдельного специалиста (подразделения).

Заблуждение №10

Если заставить всех сотрудников оператора подписать согласие о том, что их ПДн являются общедоступными, то никаких мер по защите ПДн предпринимать не нужно.

Реальность.

Как правило, у оператора нет никаких оснований требовать такого согласия, а у субъектов – нет желания его давать. Понуждение работников к такому согласию влечет создание скрытых конфликтов с работодателем, а «тлеющие риски» более опасны, чем явные. В относительно крупной организации далеко не все работники пожелают выразить такое согласие, а часть работников сделают весьма неблагоприятные для оператора выводы. **Помимо этого, любой работник (субъект ПДн) вправе отозвать такое согласие, что не будет являться основанием для расторжения с ним трудового контракта. Подчеркиваем – речь не о согласии на обработку ПДн, а о согласии на общедоступность ПДн.** Порой такую манипуляцию сделать попросту невозможно, т.к. статус общедоступности ПДн будет конфликтовать со статусом конфиденциальности этих сведений в рамках иных (помимо ФЗ 512) законов. Пример – тайна связи, налоговая тайна, семейная тайна и т.п.

И, наконец, такую стратегию оператора надзорные органы могут счесть злоупотреблением правом.

Существенную лепту в сумятицу, связанную с реализацией ФЗ «О персональных данных» вносит «демонизация» проблемы защиты ПДн, подогреваемая сенсационными сообщениями жителей (когда же они работают?) различных тематических форумов и «авторитетными» заключениями безымянных доброхотов.

Огромные затраты, невыполнимые требования, запутанные и противоречивые документы – вот аргументы «экспертов», якобы подтверждающие существование тайного плана, призванного выкачивать (непонятно, правда, как и в чьих интересах) миллиарды из карманов доверчивых операторов. Эти же псевдоэксперты склоняют операторов быть «более отважными» во взаимоотношениях с государством путем построения экзотических политик противодействия надзорным органам. Политик столь же дешевых (в прямом смысле), сколь и сомнительных, суть которых – не выполнять закон, а «аргументировано» торпедировать его требования. Сама постановка вопроса в таком ключе заставляет более пристально приглядеться к "чародеям" с повадками серийных бизнес-самоубийц, но, что более важно – критически воспринимать их советы, руководствуясь законом, здравым смыслом и чувством самосохранения.

Одновременно многим операторам стоит задуматься – а по какой причине флагманы российской экономики и ее отдельных отраслей (СИБУР, Роснефть, РусГидро, Еврохим, Газпром, Северсталь, Сбербанк, Мегафон, МТС, Билайн, и многие, многие другие) уже второй год поступательно и непрерывно реализуют в своих компаниях мероприятия по защите персональных данных? Неужели эти организации испытывают излишек денежных средств и людских ресурсов? Или все же причина лежит на поверхности, и называется она – закон, неукоснительные требования которого подкреплены целенаправленными действиями государственных институтов?

Любые точки зрения на нормы закона и порядок его реализации имеет право на существование. Любые, кроме опасных как для оператора, так и для субъекта ПДн. Рассмотрим вторую десятку популярных заблуждений, которые могут оказаться для оператора весьма дорогостоящими….

Заблуждение №11

При защите персональных данных нужно руководствоваться ведомственными инструкциями или указаниями вышестоящей организации. Пока их нет, можно ничего не делать. Законы и иные нормативно-правовые акты не играют роли.

Реальность.

Такая точка зрения свойственна организациям, входящим в структуры с жестко выстроенной вертикалью управления. Руководители этих организаций, однако, должны помнить, что возглавляемые ими организации являются операторами и несут все бремя ответственности за неисполнение требований по защите ПДн. Именно на операторов (а не на «вышестоящие организации») закон возлагает обязанности по исполнению комплекса мер по защите ПДн и предусматривает ответственность за нарушение порядка обработки. Так, кстати, за нарушение противопожарных норм или условий труда работника ответственность будет нести собственник объекта пожарной опасности или руководитель организации, а не «вышестоящая организация». Здесь – аналогичная ситуация.

Заблуждение №12

Компьютеры нам переданы вышестоящей организацией (министерством, департаментом и т.п.), значит, она и должна защищать ПДн. Наша же организация не является собственником этих компьютеров, значит, ничего не обязана (или не имеет права) делать.

Реальность.

Ст. 3 ФЗ 152 дает определение оператора. При этом закон не увязывает это понятие (а, следовательно, и обязанности оператора) с правом собственности на объекты информатизации (локальные сети, коммутационное оборудование, отдельные компьютеры, серверы и т.п.). Оператор – это тот, кто обрабатывает ПДн, а не тот, кто является собственником. Такое открытие весьма огорчительно для операторов. Но вывод очевиден – пора приступать к реализации мер по защите ПДн. Первоочередные из которых – организационные.

Заблуждение №13

Хранение персональных данных – это никакая не обработка, на порядок хранения требования ФЗ-152 не распространяются.

Реальность.

Хранение – это одно из действий (операций) по обработке ПДн. Если оператор не выполняет никаких иных действий, кроме хранения (в т.ч. и не в составе ИСПДн, например, в виде бумажных документов) – он, тем не менее, является оператором со всеми вытекающими отсюда обязанностями. Определение обработки дано в ст. 3 ФЗ 152. В то же время, действие ФЗ 152 не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования архивных документов в соответствии с требованиями архивного законодательства РФ. При этом нужно понимать, что недостаточно назвать помещение (шкаф, хранилище) архивом, от этого архив у оператора не появится. Надлежащий порядок организации архивного хранения и перевода документов на архивное хранение может быть описан в результатах обследования, проводимого в интересах оператора специализированными компаниями (лицензиатами). Советуем операторам требовать такое описание при проведении обследования. Благоприятным же фактором является то, что, если оператор (вне архива) только хранит ПДн (даже в электронном виде), то издержки на защиту этих ПДн будут, скорее всего, минимальными.

Заблуждение №14

Можно купить базу данных с ПДн на рынке, и использовать ее в своих целях. В случае проверки или жалоб - заявить, что ПДн являются общедоступными, подтверждая это фактом свободного обращения базы данных. Желательно еще иметь кассовый чек.

Реальность.
Действительно, существуют общедоступные источники ПДн. Однако стихийные рынки, на которых продаются базы данных, к числу таких не относятся. Почему? Общедоступными ПДн могут являться только в двух случаях – либо в силу закона, либо в тех случаях, когда субъект ПДн своей волей сделал (путем совершения каких-либо действий) свои ПДн общедоступными. Первый случай мы не рассматриваем (не существует закона, который именовал бы продающиеся на стихийных рынках базы данных общедоступными источниками). Рассмотрим второй случай. ФЗ 152 (ч. 3 ст.9) возлагает на оператора обязанность доказать факт получения им согласия субъекта на обработку, а в случае обработки общедоступных ПДн – доказать что обрабатываемые ПДн являются общедоступными. В случае приобретения пресловутой БД на рынке оператор лишен такой возможности, т.к. ни один субъект ПДн не подтвердит (тем более, задним числом) своего согласия на обработку таких ПДн. При проведении проверки оператора надзорным органом может быть сделан вывод о незаконности происхождения такой БД, и, следовательно, обработки ПДн. Законодатель же предусмотрел такое поведение оператора и дал ему определение – «недобросовестность» (ст. 5 ФЗ 152). Многие операторы нарушают принцип добросовестности при сборе ПДн – иногда в силу незнания закона, иногда имея прямой умысел, что гораздо опаснее. Таким синдромом «повышенной осведомленности» страдают практически все банки, коллекторские агентства, страховые компании и т.д. Они же проводят и взаимное внутрицеховое «перекрестное опыление» актуальной информацией, содержащей ПДн. Спору нет, для снижения кредитных рисков это важно. Но законно ли? Иногда такие действия оператора содержат состав преступления, предусмотренного ст. 137 УК РФ. Оставляя за рамками статьи методику доказывания противоправных действий (к слову, по данному составу преступления она проста и незамысловата), советуем задуматься о следующем. Готов ли оператор рисковать своей свободой, имиджем, клиентской базой и стабильным бизнесом ради достижения призрачных целей, к тому же противоречащих закону?

Заблуждение №15

Если ПДн не собраны оператором самостоятельно, а получены на основании договора (с субъектом ПДн или с другим оператором), или, тем более, по указанию вышестоящей организации, то защищать ПДн не нужно.

Реальность.
Налицо смешение понятий «право на обработку» и «обязанность по защите». Законные и обоснованные цели обработки не исключают необходимости принятия мер по защите ПДн. Иногда же и передача ПДн от одного оператора к другому неожиданно для обоих участников такого информационного обмена оказывается не основанной на законе!
Скорее всего, в указанном случае нарушителями будут являться обе организации – оператор, который передал ПДн, и оператор, который их принял в обработку. Первый – за отсутствие в договоре существенного условия (ч.4 ст. 6 ФЗ 152, см выше) и за передачу ПДн без согласия субъекта ПДн. Второй – за нарушение порядка обработки (ст. 13.11 КоАП РФ). Почему? Потому, что закон не делает исключений для тех операторов, которые не осуществляли сбор ПДн непосредственно от субъектов, но получили ПДн от другого оператора (даже во исполнение своих функций и полномочий, закрепленных каким-либо законом). Оператор – тот, кто осуществляет обработку, т.е. любое лицо, осуществляющее хотя бы одно из указанных в ст. 3 ФЗ№152 действий (операций) с ПДн. Надзорный же орган (Роскомнадзор), реализуя свои полномочия по защите прав субъектов ПДн и устранению нарушений в этой сфере, вправе запланировать (или провести внеплановые) проверки обоих операторов. О полномочиях Роскомнадзора при проведении проверок подробно указано в Административном Регламенте на официальном сайте Роскомнадзора.

Заблуждение №16

Будем собирать и использовать любые ПДн из любых источников. В случае проверки – заплатим штраф (он небольшой), и все!

Реальность.
Вне всяких сомнений такие действия являются нарушением принципов обработки ПДн (ст. 5 ФЗ№ 152). Такие непродуманные действия могут привести к крайне негативным последствиям для опера-

тора. Штраф – далеко не все меры воздействия, которые предусмотрены законом. Так, в случае выявления нарушений при обработке ПДн оператор обязан или устранить эти нарушения в течение 3 дней, или уничтожить ПДн. Но этим обязанности оператора не исчерпываются. Оператор обязан уведомить субъекта ПДн об устранении (например, путем уничтожения ПДн) выявленных нарушений. Купленные на рынке базы данных могут содержать ПДн десятков, а то и сотен тысяч лиц. В состоянии ли оператор уведомить такое количество граждан об уничтожении их ПДн? Какие последствия будет иметь такое уведомление, как субъекты ПДн воспримут действия оператора? И это еще не все. Роскомнадзор имеет право принимать меры по прекращению обработки ПДн или приостановлению деятельности оператора вплоть до аннулирования лицензии, если обработка ПДн осуществляется (ч.3 ст. 23 ФЗ-152) с нарушениями. Готов ли оператор идти на такие риски?

Заблуждение №17

Если от субъекта ПДн поступило обращение (или жалоба) о порядке обработки его ПДн, но фактов утечки информации наверняка не было, то нужно ответить гражданину, что с конфиденциальностью ПДн в организации все в порядке. Ответы на каверзные вопросы субъекта ПДн не входят в обязанности оператора и раскрывают конфиденциальные сведения (или коммерческую тайну) оператора. Если нет времени или желания, то можно и не отвечать субъекту ПДн.

Реальность.

Права субъекта ПДн изложены в ст. 14 ФЗ 152. По мнению многих они избыточны, но именно по этой причине оператор должен быть крайне осмотрителен при рассмотрении обращения (жалобы) субъекта! Оператор обязан дать исчерпывающий и полный ответ субъекту ПДн на все вопросы, предусмотренные ст. 14 ФЗ 152 в течение 10 рабочих дней, а в случае обоснованного отказа в предоставлении информации – в течение 7 рабочих дней. Ответы, не отражающие реального положения дел (либо отсутствие ответа) могут быть истолкованы субъектом как нарушение его прав, что может повлечь для оператора еще более негативные последствия – обращение субъекта ПДн за защитой своих прав в орган по надзору за соблюдением прав субъекта ПДн. Практика же показывает, что оператор, ранее никогда не обращавший внимания на вопросы обработки и защиты ПДн, не в состоянии справиться с подготовкой правильного и всестороннего ответа на запрос субъекта ПДн. В данном случае имеются ввиду правовые основания, цели, способы обработки и многие другие положения, формулировку которых необходимо осуществить заблаговременно.

Заблуждение №18

Мероприятия по защите ПДн – это очень дорого. Лучше будем платить штрафы, они совсем маленькие.

Реальность.

Негативные последствия отсутствия системы защиты (помимо действительно незначительных пока штрафов) приведены выше. Про дороговизну системы защиты можно сказать, что все относительно. Например, затраты на построение такой системы в образовательном учреждении или лечебно-профилактическом учреждении районного уровня на порядок меньше, нежели затраты на создание системы пожарной безопасности или видеонаблюдения. Квалифицированный лицензиат сумеет спроектировать такую систему защиты ПДн, затраты на которую будут оптимальны. Более того, на этапе обследования уполномоченная организация (лицензиат) предложит решения, позволяющие сократить издержки при создании системы защиты. Проведение же первого этапа (обследования) как правило, не превышает 20% от общей стоимости работ по защите ПДн.

Заблуждение №19

Система защиты персональных данных – это некие технические средства. Нужно их купить и установить. Обследование, аудит, проектирование – это избыточно, это придумано, чтобы побольше заработать на проблемах оператора.

Реальность.

Аналогия с лечением пригодится и тут. Любому лечению предшествует диагностика заболевания. Так и этап обследования предшествует организационно-административным и техническим мero-

приятиям по защите. Обследование помогает не только достоверно выявить слабые места информационных систем и разработать замысел защиты, но и, как ни странно, сэкономить деньги. Каким же образом? Квалифицированное обследование определяет, как именно можно сократить издержки при построении системы защиты. Способов много: оправданное снижение класса ИСПДн, пересмотр перечня ПДн, подлежащих обработке, сегментирование информационных систем, оптимизация топологии сети и т.п. Все эти способы известны специализированным организациям – лицензиатам. Мы не советуем выбрасывать деньги на ветер.

Заблуждение №20

Уже существующая у оператора мощная система защиты конфиденциальной информации (коммерческой тайны) наверняка решит и проблемы защиты ПДн. Ничего дополнительно делать не нужно.

Реальность.

С технической точки зрения – возможно, и решит. Однако есть множество требований, предъявляемых как к способам и методам защиты ИСПДн, так и к техническим средствам защиты информации. Эти требования установлены регуляторами (ФСТЭК России и ФСБ РФ) в пределах их компетенции. Игнорирование этих требований не только является нарушением, но и может привести к наступлению негативных последствий как для оператора, так и для субъекта ПДн. К числу таких требований относится, например, необходимость применения средств защиты информации, прошедших процедуру оценки соответствия. Специфические требования предъявляются и на этапе ввода в эксплуатацию системы защиты персональных данных (процедуры оценки состояния защищенности подсистем). Поэтому, как правило, любую существующую систему защиты (если она строилась не в целях защиты ПДн и не в соответствии с нормативными документами) необходимо пересмотреть и модернизировать. Возможно, затраты при этом могут оказаться незначительными, а выгоды – очевидными. Специализированная организация при проектировании системы защиты обязательно учтет существующие компоненты системы защиты и постарается эффективно их применить.

Что же касается организационной компоненты работ по защите ПДн, то смело можно утверждать, что в подавляющем большинстве организаций, в которых задача по защите ПДн (а не любой иной конфиденциальной информации) не ставилась, состояние этой работы плачевное.

Заблуждение №21 (бонусное).

Нужно провести предпроектное обследование, руководствуясь только одним критерием для выбора исполнителя – ценой. Все равно все исполнители создают примерно одинаковые документы.

Реальность.

Во-первых, цель обследования – вовсе не создание документов, которые ждут своего часа для представления проверяющим органам. В результате правильного и квалифицированного обследования оператор получает в свое распоряжение стратегию защиты.

Во-вторых, результаты обследования, проведенного разными организациями, могут радикально отличаться. Некачественно проведенное обследование вводит в заблуждение оператора относительно существующего и требуемого уровня защищенности ПДн, дезориентирует его при реализации единой технической политики, подвергает опасности возникновения инцидентов информационной безопасности, и, главное, создает предпосылки для нарушения прав субъектов ПДн. А когда такое нарушение произойдет, то результаты некачественного обследования только добавят неприятностей оператору. Порой оператор в качестве результатов обследования получает лишь частную модель угроз, акты классификации ИСПД и некие шаблоны неадаптированных к специфике оператора документов. Впрочем, рынок, как ни странно, приемлет и такой дешевый во всех смыслах подход к проблеме.

Стоит ли экономить на безопасности? Стоит, если Вас не интересует результат.