

УТЕЧКА ИНФОРМАЦИИ: ПОСЛЕДСТВИЯ И БОРЬБА С НИМИ

**Государство пытается усилить контроль
за сохранностью персональных данных**

• ТЕКСТ | Алексей ГРЕКОВ



Купить диск с базой данных на миллионы жителей города (Ф. И. О., паспортные данные, домашний и мобильный телефон и т. п.) — не проблема у нас в стране уже лет 15. Такие диски сначала продавали на рынках, потом в киосках «CD/DVD», после их закрытия купить базу можно было в метро — по вагонам ходили молодые люди и предлагали «всего за 100 рублей данные на всех», сейчас эти продавцы зачастую стоят прямо на выходе из станций. Какое-то время такие базы данных существовали в интернете в свободном доступе. И любой мошенник до сих пор может воспользоваться вашими паспортными данными, пользуясь недобросовестностью некоторых компаний и структур.

«Подарок» от МТС

С ситуацией незаконного использования паспортных данных я столкнулся прямо во время подготовки этого материала. Получаю по почте на домашний адрес конверт, где на своем фирменном бланке компания «МТС» извещает меня о том, что на телефонном номере, зарегистрированном на мое имя, имеется задолженность в размере 525,81 рубля, и «убедительно просит» заплатить указанную сумму в течение десяти дней с момента получения из-

вещения. Заканчивается письмо фразой: «В случае неоплаты задолженности в указанный срок ОАО «МТС» оставляет за собой право взыскания данной суммы в судебном порядке, с начислением процентов за пользование чужими денежными средствами в соответствии со ст. 395 ГК РФ».

Клиентом этого оператора связи в Петербурге я не являюсь и никаких договоров с ним не заключал, поэтому попытался сразу прояснить ситуацию, позвонив в контактный центр МТС. Убеждаюсь, что действительно такой номер зарегистрирован на мое имя и на нем есть указанный долг. Оказывается, кто-то из дилеров компании МТС заключил договор, используя фиктивные паспортные данные, взятые из имевшейся у них базы данных. Оригинал паспорта для данной сделки не требовался. В результате компания МТС не считает себя виновной, сваливая всю вину на неназванного дилера. Но и не считает зазорным требовать от человека «возврата долга», угрожая ему судом.

Юридические последствия

Комментарий старшего юриста консалтинговой группы «Налоговик» Антона Кротина:

— Если попавший в такую ситуацию человек предъявит иск к МТС о компенсации морального вреда, то подобный иск может иметь перспективу. Дилер является представителем, поэтому все правовые последствия возникают у МТС, а не у дилера. МТС не позаботилась о том, чтобы собрать убедительные доказательства факта сделки с данным лицом — иными словами, проверку-расследование следовало проводить до предъявления претензии человеку. Вина МТС имеется, поскольку она необоснованно обвинила человека в недобросовестности в обязательственных отношениях по договору с МТС (чего не было в действительности).

Еще одна история с МТС

Несмотря на заявление сотрудника компании МТС о том, что такие случаи единичны, нам удалось без труда найти еще более вопиющую историю. Рассказывает жительница Петербурга Светлана:

— На меня в МТС открыли почти два десятка номеров, третий месяц якобы проверяют. Да еще и с нормального номера сняли 1140 рублей в погашение задолженности по «левым». В офисе МТС я написала заявление о том, что я к этим номерам отношения не имею, они же говорят, что раз номеров так много, то расследование будет долгим.

Редакция обратилась в компанию с просьбой разобраться в данной ситуации. Достаточно оперативно был получен ответ. Вся история подтвердилась, но сотрудники МТС не смогли связаться с абонентом, поскольку в заявлении был указан только номер МТС, которым она после данной истории уже перестала пользоваться. Предложили обратиться в салон связи компании и забрать снятые с номера деньги. Однако удалось бы добиться результата без привлечения к ситуации внимания прессы — нельзя утверждать однозначно.

Все ли дилеры добросовестны?

В результате разговора с начальником отдела развития сети салонов сотовой связи, который попросил не упоминать ее название, выяснилось следующее. Подобные ситуации вполне можно назвать обычными. Сеть салонов заключает договор с оператором сотовой связи о том, что обязуется подключить за квартал, предположим, 1000 абонентов. В случае выполнения этого норматива оператор сотовой связи дает скидки/подарки/путевки/много денег — в общем, большие бонусы. В случае невыполнения программы следует не менее жесткий прессинг. Так вот,

чтобы выполнить программу, они подключают по несколько номеров на своих сотрудников, их родственников, соседей и т.п. «абсолютно бесплатно». Часто жертвы ни о чем и не догадываются.

Добавим от себя: а что мешает дилеру «ради выполнения плана» и получения бонусов оформлять договоры на первых попавшихся лиц, используя их паспортные данные из доступной базы? А потом продавать эти сим-карты на улице случайным лицам. Иначе каким образом на этих номерах могут появиться задолженности?

Проблема в данном случае не только с МТС. Утечка персональных данных происходит из разных организаций, владеющих такой информацией. Сотовый оператор — точнее, его дилеры — лишь недобросовестно ими пользуются. В самой же компании, как заявил в недавнем интервью журналу «СЮ» директор департамента информационной безопасности компании МТС Сергей Прадедов, последняя довольно серьезно утечка данных случилась в 2003 году. «И это стало сигналом к тому, чтобы уделять существенное внимание вопросам информационной безопасности: было создано подразделение, которое я сейчас возглавляю; были проведены организационные и технические мероприятия, для того чтобы исключить утечки. И нам удалось добиться контроля над потоками информации. С тех пор утечек не случалось», — отметил он.

В квартиру «подселили» десятки чужих людей

Но долг в 500 или даже 1 тыс. рублей оператору сотовой связи — не самая большая из возможных проблем, связанных с утечкой персональной информации. Гораздо хуже, если ваши паспортные данные были использованы в махинациях с недвижимостью. Вот что рассказала нам Елена, работающая

• Вина МТС имеется, поскольку она необоснованно обвинила человека в недобросовестности в обязательственных отношениях по договору с МТС (чего не было в действительности)



• Известно, что учитывают нас Пенсионный фонд и Федеральная налоговая служба, Фонд социального страхования и Министерство здравоохранения, МВД и коммунальные службы...

в редакции одной из городских газет:

— Пару лет назад выяснилось, что без моего ведома у меня в квартире прописано огромное количество неизвестных мне людей. Начались звонки из милиции — по каким-то делам их разыскивали, каждый день почтовый ящик был забит почтой, приходящей этим людям. В поликлинике на нашей полке стоят десятки карточек — причем эти люди реально приходят туда лечиться! Я запросила в паспортном столе форму 9 — в ней никого из «лишних людей» нет. Могу сделать вывод, что это одна из многочисленных фирмочек, свободно рекламирующих сегодня себя на улицах города — «оформляем регистрацию», — даже на Невском проспекте!

Самое удивительное, что эта история продолжается уже три года, и я ничего не могу поделать! Я даже узнала название компании, которая оформляет регистрацию на мой адрес. Но все госорганы заявляют, что ситуация неразрешима. Милиция заводила уголовное дело — безрезультатно. Я обращалась лично к начальнику миграционной службы — он тоже ничем не смог помочь. Государство просто бросило нас с нашими проблемами. А звонки продол-

жаются, почтовый ящик забит. Безвыходное положение!..

Редакции известна еще одна история, когда человек узнал о незаконно прописанных в своей квартире людях, получив квитанцию о квартплате — ему предлагалось оплатить пользование коммунальными услугами как за себя, так и «за того парня».

Закон о защите персональных данных

О том, в какие неприятные ситуации можно попасть, когда ваши персональные данные находятся практически в открытом доступе, мы говорили. Государство это понимает и борется с утечками данных из компаний и организаций. Заниматься проблемой защиты данных в России начали в 2005 году, когда был подписан Федеральный закон № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». Позднее — в 2006 году — был принят закон № 152-ФЗ «О персональных данных». Он до сих пор продолжает корректироваться и ужесточаться.

Согласно последним внесенным Госдумой изменениям, сделанным 16 декабря 2009 года, срок

приведения информационных систем в соответствие с данным законом был перенесен на один год — до 1 января 2011 года. В пояснительной записке к законопроекту указано на то, что приведение информационных систем в соответствие с законом о персональных данных требует от бизнеса и госорганов значительных затрат, которые не планировались и сложно осуществимы в условиях кризиса.

Кто учитывает и что именно

Известно, что учитывают нас очень многие ведомства: Пенсионный фонд и Федеральная налоговая служба, Фонд социального страхования и Министерство здравоохранения, МВД и коммунальные службы... Но дело в том, что в России практика работы с персональными данными граждан складывалась стихийно. Где-то — в первую очередь, в банках — уже давно предпринимались серьезные меры по защите от утечки информации о клиентах, большинство же организаций защитой данных до поры до времени не было озабочено. В результате незаконная продажа всевозможных баз данных, содержащих персональную информацию о гражданах, была поставлена, по сути, на поток.

Итак, персональными данными, требующими защиты, теперь по закону считаются сведения о фактах, событиях и обстоятельствах частной жизни конкретного гражданина. В здравоохранении конфиденциальны Ф.И.О. пациентов, пол, дата рождения, адрес места жительства, реквизиты документа, удостоверяющего личность, номер полиса медицинского страхования, сведения о наличии льгот, страховой номер индивидуального лицевого счета в Пенсионном фонде, сведения о случаях обращения за медицинской помощью и о состоянии здоровья. Конфиденциальны также ИНН, данные кадрового учета, сведения о заработной плате и про-

че. Суть защиты этой информации — в жестких технических требованиях, которые должны соблюдаться при любых операциях с ней — от сбора и обработки вплоть до уничтожения.

Согласно требованиям закона о персональных данных все предприятия, в той или иной степени участвующие в обработке персональных данных своих клиентов или работников, обязаны привести информационные системы в соответствие с требованиями в сфере защиты информации. В целях исполнения закона осуществляются мероприятия по защите информации — разрабатывается комплекс организационно-распорядительных документов, отражающих регламенты защиты информации, действующие на предприятии. Уровень необходимой защиты информации и серьезность требований зависят от категории, определяемой исходя из способов и объема обработки персональных данных.

Что делать операторам данных

Предприятие, являющееся оператором персональных данных, обязано уведомить федеральный орган в сфере

связи и массовых коммуникаций — Роскомнадзор — о намерении осуществлять такую обработку и указать ее цели. Судя по всему, первыми проверку на соответствие закону пройдут банковская сфера, операторы связи и сфера ЖКХ. Специалисты считают, что тяжело придется и медицинским учреждениям. Это связано тем, что государственные учреждения обладают всеми персональными данными достаточно большой группы населения.

Приведение в порядок информационных баз оборачивается достаточно серьезными затратами даже для банков, которые еще до принятия закона осуществляли защиту конфиденциальной информации о своих клиентах. Рядовой городской поликлинике для защиты информации о своих клиентах нужно изыскать несколько миллионов рублей, чтобы закупить программное обеспечение, провести аттестацию, учебу сотрудников и т. д. Как ни странно это звучит, но может случиться, что больницам и поликлиникам экономнее будет вернуться к карточной системе и заполнять документы вручную...

Как подготовиться к вступлению в силу новых требований?

Для начала руководителям предприятий необходимо изучить закон. Затем заполнить и отправить в Роскомнадзор уведомление об обработке персональных данных. Для этой цели еще в октябре прошлого года был создан портал персональных данных (<http://pd.rsoc.ru/>), где в рамках работы по переходу на предоставление услуг в электронном виде реализована возможность электронного заполнения «Уведомления о намерении осуществлять обработку персональных данных». На первом этапе самое главное — грамотно оформленные документы.

Проверять соблюдение закона предприятиями будут осуществлять Роскомнадзор, ФСБ и ФСТЭК. Кстати, на портале персональных данных должен появиться план проведения проверок на 2010 год.

Роскомнадзор призван контролировать выполнение закона и гарантировать защиту прав граждан. ФСТЭК России, в свою очередь, будет осуществлять контроль защиты информации

КОММЕНТАРИИ



Исполнительный директор «Лаборатории Касперского» в России Сергей Земков:

— Обеспечение безопасности не только персональных, но и любых конфиденциальных данных стало насущной проблемой по всему миру, и Россия здесь — не исключение. Согласно исследованию, опубликованному компани-

ей InfoWatch, в 2008 году произошло свыше 250 крупных инцидентов в сфере информационной безопасности, затронувших интересы более 100 млн человек.

Риск потери конфиденциальной информации значительно вырос именно сейчас, в период массовых сокращений. Уволенные сотрудники могут забрать с собой данные о внутренних процедурах, условиях договоров и клиентах компании, что способно нанести значительный ущерб.

В свете подобных происшествий компаниям надо разработать организационные и технические меры для охраны собственных информационных систем. Согласно ФЗ № 152, информационная система должна пройти проверку на безопасность персональных данных, получить сертификаты Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности. Продукты «Лаборатории Касперского» удовлетворяют этим требованиям, своевременно пройдя процедуры сертификации ФСТЭК и ФСБ.



Начальник управления сетевых платформ Optima Services Владислав Епишкин:

— Федеральный закон о персональных данных касается всех организаций, а не только участников IT- или медиарынка. Всем, кто просто ведет собственную бухгалтерию и платит сотрудникам зарплаты, а значит, обрабатывает персо-

нальные данные, необходимо будет реализовать проект по построению Информационной системы персональных данных (ИСПД) и следовать требованиям по их обработке. Требования зависят от объема и категории данных — соответственно, объем задач по защите ПД может варьироваться.

Компании-аутсорсеры, обслуживающие такого рода системы, тоже должны следовать требованиям ФЗ 152. Причем чем крупнее клиент и шире спектр оказываемых услуг, тем сложнее и дороже проект для аутсорсера. Например, в случае, если сервисная компания поддерживает бизнес-приложения заказчика на собственной инфраструктуре, необходимо будет не только сертифицировать ИСПД, но, возможно, и получать лицензии ФСТЭК и ФСБ.

Поскольку проект создания ИСПД занимает 4–9 месяцев, тем компаниям, которые еще не начали реализацию проекта по защите ПД, давно пора начать это делать...

ЮРИДИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

с применением технических средств, а ФСБ РФ — курировать вопросы защиты информации с использованием средств шифрования (криптографии).

За нарушение правил защиты информации в Кодексе РФ «Об административных правонарушениях», в статье 13.12, подробно прописано пять степеней ответственности. Штрафные санкции для юридических лиц колеблются от 5 до 35 тыс. руб., с конфискацией несертифицированных средств информации. А вообще за нарушение требований Закона «О персональных данных» предусмотрена не только гражданская и административная, но и уголовная ответственность.

Роскомнадзор следит за ситуацией

Надо признать, что управление Роскомнадзора, ведущее реестр операторов, пока занимает достаточно конструктивную позицию. Сейчас его усилия направлены на предварительное выявление несоответствий у операторов требованиям закона, после чего на них указывается оператору. Руководство надзорного органа понимает, что на данном этапе операторам сложно выполнить все регламентации и следовать букве закона, потому работа с организациями ведется, в том числе, в консультативном режиме.

Как отметил недавно в интервью «Российской газете» глава Роскомнадзора Сергей Ситников, «закон должен защищать не систему, не некие данные, а гражданина. Не должно быть закона о персональных данных ради самих персональных данных».

Закон начнет работать, хотя и не сразу

В прессе и в выступлениях экспертов в целом звучит положительная оценка закона о защите персональных данных как способного повлиять на общий уровень информационной безопасности. Но, учитывая большие сложности, реально применять его начнут не сразу, «обкатка» закона может затянуться на два-три года. Главная цель — преодолеть каким-то образом человеческий фактор, который, по данным исследований, почти в 70% случаев и является причиной утечки важных данных. **15**

Чтобы узнать о юридических аспектах вопроса защиты персональных данных, мы обратились к специалистам. На вопросы «Территории бизнеса» отвечает старший юрист консалтинговой группы «Налоговик» Антон Кротин.



— **О каких основных аспектах Закона «О персональных данных», вступившего в силу 1 января 2010 года, должны знать руководители компаний?**

— Важно знать, что Закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» устанавливает общее правило, что персональные данные являются конфиденциальными, если они не обезличены и не являются общедоступными (ст. 7). В соответствии с ч. 2 ст. 8 этого закона по требованию гражданина его данные должны быть исключены из общедоступных источников — например, справочников, словарей, очевидно, что и с сайтов интернета, — т.е. до момента такого требования изменений в обработке персональных данных может быть гражданином отозвано, после чего их следует удалять из баз данных.

В целях информационного обеспечения можно создавать 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.

Письменное согласие субъекта персональных данных можно получать по факсу, электронной почтой — если в документе имеется собственноручная подпись гражданина и нет сомнений, что отправление исходит от самого субъекта.

— **На какие именно компании распространяется действие данного закона?**

— Действие данного закона распространяется на все компании (юридические лица), организации без исключения, в том числе — на государственные, муниципальные органы, юридические или физические лица, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

— **Какие меры должны быть приняты в компаниях, чтобы не попасть под санкции контролирующих органов?**

— Чтобы не попасть под санкции контролирующих органов, в компаниях должны быть приняты меры, исключающие доступ к таким данным посторонних лиц, в том числе через сеть интернет, а также проверяющих лиц, путем шифрования баз данных и их скрытого хранения.

— **Насколько необходим компании свой квалифицированный юрист для устранения конфликтных ситуаций с контролирующими органами?**

— Для устранения конфликтных ситуаций с контролирующими органами свой юрист компании не требуется, целесообразнее прибегать к услугам сторонних юристов (предпочтительнее — адвокатов), с тем чтобы избежать утечки информации, связанной с наполнением объемами баз данных (т.е. исключить возможность появления лишнего свидетеля в деле). **16**

ВЫБОР ПОДХОДЯЩИХ МЕТОДОВ ЗАЩИТЫ

ЗАВИСИТ ОТ ТОГО, ЧТО ЗАЩИЩАЕТСЯ И ОТ КАКИХ УГРОЗ

Об особенностях законодательства по защите персональной информации и мерах, которые должны предпринять компании, чтобы не попасть под санкции контролирующих органов, нам рассказал также руководитель отдела консалтинга и аудита компании Positive Technologies Сергей Гордейчик.

— **Какие основные методы защиты данных существуют сегодня?**

— Методов защиты существует очень много, и выбор подходящих зависит от того, что защищается и от каких угроз. Но если мы говорим о персональных данных, то государство в лице ФСТЭК и ФСБ определило минимальный набор механизмов защиты, который операторы должны реализовать. Прежде всего, от оператора требуется вынести информационные системы, обрабатывающие персональные данные, в отдельный сетевой сегмент, доступ к которому должен ограничиваться межсетевым экраном, а возможные сетевые атаки должны выявляться и блокироваться системами обнаружения и предотвращения вторжений. В дополнение к ним на серверах и рабочих станциях этих систем должны использоваться антивирусные средства. Внутри самой системы оператор должен реализовать адекватное разграничение доступа пользователей к данным, с тем чтобы каждый из пользователей получал ровно те сведения, которые действительно необходимы ему для выполнения своих служебных обязанностей. Кроме того, информационные системы должны генерировать данные аудита, необходимые для разбора возможных инцидентов. При передаче персональных данных по незащищенным каналам связи должны использоваться средства шифрования.

— **Что в плане технической защиты должны делать компании, на которые распространяется действие Закона «О персональных данных»?**

— Единого ответа на этот вопрос нет, поскольку тут регуляторы пошли по единственному правильному пути — дали оператору возможность выбирать адекватные меры защиты. Естественно, комплексы мероприятий по защите для поликлиники или бан-



• **Методические документы ФСТЭК и ФСБ не диктуют, какие именно средства защиты должны применяться. Оператору предоставлена возможность самостоятельно формулировать модель угроз, характерных для его информационных систем**

ковской системы, охватывающей всю страну, должны различаться. В одном случае достаточно стандартного набора средств защиты, таких как антивирус, фаервол, пароль. В других — требуются специализированные средства, включая системы шифрования и защиты от утечек по каналам побочного электромагнитного излучения. Основные требования к средствам защиты изложены в документах ФСТЭК и ФСБ. Для реализации сложных проектов логично привлекать специализированные компании, имеющие лицензии ФСТЭК и ФСБ и опыт построения информационных систем и их аттестации на соответствие требованиям 152 ФЗ «О персональных данных».

— **Насколько квалифицированные ИТ-специалисты должны рабо-**

тать в компании, чтобы проблем с защитой персональных данных было минимум?

— Поскольку вопрос соответствия 152 ФЗ «О персональных данных» — это далеко не только технический вопрос, то в его решение должны быть вовлечены все затрагиваемые подразделения: юристы, специалисты по работе с клиентами, ИТ- и ИБ-специалисты. Ничего принципиально нового требования регуляторов не привносят, все рекомендуемые процессы и средства защиты уже в том или ином виде присутствуют в большинстве компаний — соответственно, есть опыт их внедрения и обслуживания.

Требования к квалификации в значительной степени зависят от сложности системы. В одних случаях будет достаточно пользовательских навыков для эксплуатации системы в соответствии с разработанными инструкциями; в других, особенно если компания получает лицензии ФСТЭК, потребуются специалисты, которые имеют образование в области ИБ или прошли соответствующие курсы повышения квалификации.

— **Насколько велики должны быть вложения компании, чтобы ее оборудование для защиты персональных данных соответствовало требованиям законодательства?**

— Уровень расходов на приведение в соответствие требованиям 152 ФЗ «О персональных данных» и их поддержание в большой степени зависит от категории и объема обрабатываемой информации. Для небольших компаний — например, коллекторских агентств — для целей обработки ПД разумно выделить одно рабочее место, и в этом случае затраты будут исчисляться десятками тысяч рублей. При чем стоимость именно средств защиты в этом случае будет составлять 10–20%. Остальные расходы будут направлены на регламентацию организационных мероприятий, аттестацию и т. д. При масштабировании техническая составляющая затрат растет пропорционально сложности, а организационная — менее интенсивно. **IT**