ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ПРОПУСКНОЙ РЕЖИМ

Михаил ЕМЕЛЬЯННИКОВ,

автор и преподаватель курсов Учебного центра «Информзащита»

26.01.2007 года вступил в силу Федеральный закон № 152-ФЗ «О персональных данных». В рамках его реализации в стране создана государственная система контроля и надзора за соблюдением закона, включающая федеральные органы исполнительной власти, уполномоченные в области безопасности – ФСТЭК и ФСБ России, и уполномоченный орган по защите прав субъектов персональных данных – Роскомнадзор. В соответствии с частью 3 ст.25 этого закона до 1 января 2010 все информационные системы персональных данных должны быть приведены в соответствие закону, что будет контролироваться указанными выше органами в рамках их компетенции

Гладко было без бумаги

Тема приведения порядка обработки персональных данных в соответствие с требованиями законодательства – самая обсуждаемая профессиональным сообществом последние два года. В 2009 году редкая неделя обходится без проведения конференции, семинара или круглого стола, на которых активно спорят и ищут решения многочисленных проблем, порожденных законом, законодатели, государственные регуляторы, представители операторов персональных данных и компаний, поставляющих продукты и услуги на рынке информационной безопасности. Абсолютное большинство этих обсуждений сводится к вопросу защиты данных в информационных сетях операторов, в то время, как огромное количество сведений о гражданах хранится на бумажных носителях в виде различных форм, анкет, журналов регистрации и т.п.

Мы вписываем практически все свои паспортные данные при размещении в гостинице, получении заказного письма или бандероли на почте, оформлении дисконтной карты в магазине. Что происходит со сведениями о нас, мы не знаем. А проблема-то очень серьезная. С одной стороны, отрезвляющим для многих душем стала публикация 3 ноября с.г. в газете «Ведомости» о найденных на свалке анкетах-заявлениях на кредит людей, которые так и не стали клиентами ярославского отделения банка ВТБ 24. С другой стороны, о том, что может произойти, если паспортные данные попадут в руки нечистоплотных людей, весьма своеобразно проинформировала население налоговая инспекция Санкт-Петербурга. Там предложили гражданам новую платную услугу – блокирование возможности регистрации подставных фирм с использованием их паспортов. Да и памятная история с фальшивыми заемщиками Сбербанка подтверждает опасность бесконтрольного распространения паспортных данных.

Требование о регистрации оператором персональных данных на бумажном носителе чаще всего бывает не только избыточным, но и бессмысленным. Так, для получения заказного письма, пришедшего на вашу фамилию и ваш адрес, паспорт предъявляется работнику почты. Зачем же указывать на извещении еще и паспортные данные? Какова цель обработки этих персональных данных почтовым отделением? На этот вопрос получить вразумительный ответ не удается. Между тем наличие конкретно сформулированной цели обработки является одним из краеугольных положений Федерального закона «О персональных данных».

Особое место в проблеме регистрации персональных данных занимает вопрос организации пропускного режима, актуальный практически для всех предприятий и организаций.

ЧОП как оператор персональных данных

Рассмотрим типичную ситуацию.

Ваша компания арендует помещения в коммерческом бизнес-центре, где, кроме вас, квартирует еще несколько десятков организаций. Как организован пропускной режим в таком случае? Чаще всего функции бюро пропусков выполняет подразделение частного охранного предприятия (ЧОП), на которое возложены функции обеспечения безопасности бизнес-центра в целом. Арендаторы сдают в бюро пропусков заявки на пропуск посетителей, указывая фамилию, имя и отчество (ФИО) визитера, организацию, где он работает, время посещения и номер офиса, где его ждут. Зачем знать, где работает посетитель – непонятно в принципе. А дальше начинается самое интересное. Посетитель предъявляет паспорт (иногда либеральные ЧОПы могут довольствоваться и водительскими правами) и, казалось бы, при совпадении ФИО в заявке и паспорте, идентичности лица посетителя с паспортным фото он должен беспрепятственно проследовать в нужный ему офис. Ан нет. Паспортные данные – кроме ФИО, это номер паспорта, а иногда еще и дата и место его выдачи, и даже место регистрации (прописки по-старому) переписываются хмурым охранником в потрепанный гроссбух или вводятся симпатичной девушкой в компьютер. Иногда идут дальше – страницы паспорта ксерокопируют или сканируют. В некоторых, наиболее «продвинутых» и озабоченных собственной безопасностью организациях, посетителя еще и фотографируют. Зачем все это делается? На этот вопрос, как и на почте в описанном выше случае, ответ получить невозможно. Да и не у кого – охранник или рецепционистка ничего сами не придумывают, они только выполняют имеющуюся инструкцию. Пробиться к автору этой инструкции или лицу, ее утвердившему, невозможно.

А теперь давайте взглянем на эту ситуацию с точки зрения Федерального закона «О персональных данных». ЧОП, регистрирующий паспортные данные посетителей, становится оператором персональных данных, осуществляющим их обработку и определяющим ее цели. При этом составным элементом обработки является использование оператором полученных персональных данных – действия, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных. Такими действиями, в данном случае, является принятие решения охранником о возможности или

невозможности посещения нужного офиса. В случае отсутствия документа, удостоверяющего личность посетителя, попасть в нужное место ему, скорее всего, не удастся, даже если принимающая сторона подтверждает, что это именно тот человек, которого ждут. И последствия для посетителя могут быть самые значительные – в виде конкретных финансовых потерь из-за невозможности заключения сделки или получения нужного документа, вреда здоровью, если речь идет, скажем, о платном медицинском учреждении, моральных страданий из-за возникшей конфликтной ситуации. Готов ли ЧОП принять на себя риски, связанные с возможными исками пострадавших, понимает ли он сложившуюся ситуацию? Очень сомневаюсь.

В соответствии со ст.5 ФЗ-152 оператор (ЧОП) обязан заранее определить и заявить цель обработки, а сам порядок обработки должен эти целям соответствовать. Кто-нибудь видел такие цели, оформленные ЧОПом документально?

Фундаментальной нормой закона является согласие субъекта на обработку персданных, при этом пропускной режим не является основанием для обработки данных без согласия гражданина. Конечно, передача паспорта в бюро пропусков для оформления пропуска может рассматриваться как выражение косвенного согласия, но на это можно посмотреть и по-другому. Поскольку законодательство никак не регулирует порядок доступа в коммерческие предприятия, отказ в проходе без документа может рассматриваться как препятствие реализации прав и свобод гражданина.

Далее. В соответствии с уже упомянутой ст.5 закона, все персданные подлежат уничтожению по достижении целей обработки, т.е. при завершении визита в офис. Как это сделать в гроссбухе охраны или зачем тогда делать копию паспорта? Ответа нет. Ссылки на необходимость хранения сведений о посетителях для расследования возможных инцидентов в дальнейшем абсолютно несостоятельны, поскольку никак не подкреплены законодательно, а выполнение таких действий очень похоже на оперативно-розыскную деятельность, субъектом которой ЧОП не является.

Принимая на себя функции оператора персданных, руководство ЧОП должно четко понимать, что автоматически принимаются и обязательства по выполнению требований ФЗ-152, постановлений Правительства РФ 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (при наличии системы контроля управления доступом и/или ввода персданных в компьютер бюро пропусков), 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (при наличии «бумажных» заявок и гроссбуха на входе), а при обработке и хранении цифровых фото и ксерокопий паспортов – и Постановления 2008 г. «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». Формат статьи не позволяет остановиться на содержании этих требований, но они очень и очень жесткие. Среди принятых ЧОП обязательств в этом случае есть и обязанность по первому требованию любого посетителя сообщить ему информацию о наличии его персональных данных у оператора, предоставить возможность ознакомления с ними при обращении гражданина или в течение десяти рабочих дней с даты получения запроса. При этом должна быть исключена возможность ознакомления обратившегося посетителя с персданными других граждан. Как это сделать – головная боль ЧОП. Посетитель может по закону отозвать согласие на обработку данных, т.е. потребовать немедленного уничтожения.

И что же делать?

Прошедшие 20 октября 2009 года парламентские слушания, посвященные проблематике реализации закона «О персональных данных», показали настоятельную необходимость внесения изменения в огромное количество законодательных и нормативно-правовых актов, касающихся обработки сведений о гражданах. Нуждается в радикальном пересмотре и сложившаяся система организации пропускного режима в коммерческие предприятия, не связанные с обработкой государственной тайны, экологически опасным производством и т.п. Существующий сегодня порядок, унаследованный от предприятий и организаций социалистической экономики, от положений закона и инициировавшей его европейской конвенции бесконечно далек и грубо нарушает права и свободы граждан. А пока государство будет разруливать возникшие проблемы, ЧОПы и их руководители рискуют быть привлеченными к административной ответственности в ходе контрольно-надзорных мероприятий, вплоть до предписания об административной приостановки деятельности в виде наказания за нарушение прав и свобод граждан.