Визитка

ВЯЧЕСЛАВ МЕДВЕДЕВ, *аналитик компании «Доктор Веб»*

Правда и мифы №152-ФЗ

Как выполнить требования закона малой кровью?

Вопрос об актуальности проблемы выполнения требований Федерального закона №152-ФЗ «О персональных данных» на данный момент является одним из основных как для руководителей компаний и организаций, так и для системных администраторов

Окончательное вступление положений закона в силу (сам закон вступил в силу давно, но об этом далее) было в очередной раз перенесено (в этот раз до 16 июля 2011 года), но нет никакой уверенности, что этот срок не будет перенесен вновь. При этом необходимо помнить, что:

- закон вступил в силу достаточно давно, отсрочка касается только сетей, существовавших на момент принятия закона, – все организации, сети которых созданы после вступления в силу данного закона, уже должны выполнить все его требования;
- положение закона о том, что оператор обязан принимать необходимые организационные и технические меры для защиты персональных данных, не отменено и действует в полной мере.

Не будем подробно останавливаться на причинах, приводящих к сложностям в реализации требований этого закона, – они хорошо известны и описаны во многих публикациях. Вместо этого попробуем посмотреть, как можно выполнить требования закона «малой кровью», с помощью имеющихся специалистов и оставаясь в рамках бюджета.

Прежде всего, необходимо дать несколько определений, так как уже из непонимания определений начинается мифология, связанная с законом.

В соответствии с положениями закона, оператором является практически любое физическое или юридическое лицо – исключений достаточно мало. В свою очередь понятие «обработка персональных данных» включает в себя не только их сбор, накопление и хранение, но и такие действия, как удаление, уточнение, блокирование данных. Таким образом, даже если вы на своей машине только уничтожаете данные (например, удаляете письма, приходящие вам по почте, если эти письма содержат персональные данные), ваш компьютер уже должен быть защищен в соответствии с категорией этих персональных данных.

И о вышеупомянутых исключениях. Действие закона не распространяется на действия по обработке архивных документов, в соответствии с законодательством об архивном деле в Российской Федерации.

Еще одним мифом, связанным с Федеральным законом № 152-ФЗ, является утверждение о том, что неподача уведомления о намерении обработки персональных данных автоматически освобождает от необходимости их защиты. В действительности Роскомнадзор, как уполномоченный орган по защите прав субъектов персональных данных, имеет право запрашивать все необходимые данные от оператора (которым, напомним, может являться и простой пользователь), а также предпринимать все необходимые меры вне зависимости от подачи уведомления – вплоть до прекращения обработки персональных данных, подачи в суд исковых заявлений и привлечения к административной ответственности.

И, наконец, необходимо ввести понятие персональных данных. В соответствии с Евродирективой (а закон был принят вследствие присоединения 7 ноября 2001 года Российской Федерации к Европейской конвенции 1981 года «О защите личности в связи с автоматической обработкой персональных данных», определяющей основные принципы защиты персональных данных в европейских странах), для определения того, является ли лицо идентифицируемым, следует принимать в расчет все средства, в равной мере могущие быть реально использованными либо оператором, либо любым иным лицом для идентификации указанного лица. Таким образом, персональными могут быть любые данные, которые могут привести к идентификации человека, а не только данные паспорта.

При этом в соответствии с законом обязанность представлять доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на оператора. В силу вышеизложенного именно оператор должен определять, что является персональными данными, а что нет, и именно оператор должен собирать доказательства своей правоты. Это притом что возможность идентифицировать человека на основании тех или иных данных зависит от очень многих факторов, и в первую очередь от финансовых возможностей того, кто задастся такой целью.

Также на оператора возлагается ответственность за составление списка угроз, определение их значимости

и в конечном итоге, за правильность классификации информационной системы, от чего напрямую зависит список организационных и технических мер, которые необходимо предпринимать для защиты данных. При этом ответственность за порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации. Общий же список документов, на основании которых оператор должен проводить все необходимые работы, далеко не исчерпывается самим законом, постановлениями правительства № 781, 687 и 512, а также документами Роскомнадзора, ФСТЭК и ФСБ – федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных. В связи с этим второе, что необходимо сделать в ходе работ по защите персональных данных (первое – это назначение ответственно за проведение работ лица), – составить список документов, имеющих силу для данного типа предприятий и организаций.

В зависимости от утвержденного списка угроз оператор должен принимать меры по обеспечению целостности, управлению доступом, внедрению антивирусной и криптографической систем, мер по защите от утечек по аудио- и видеоканалам. К сожалению, объем статьи не позволяет подробно рассмотреть порядок определения угроз персональных данных и выбора тех или иных средств защиты в зависимости от класса информационной системы. Поэтому ограничимся только рассмотрением методов защиты от несанкционированного доступа.

Подключение информационных систем к информационно-телекоммуникационным сетям осуществляется в соответствии с Указом Президента Российской Федерации № 351.

При этом для информационных систем первого класса (и только для него, требование использования сертифицированных средств для всех средств защиты – это еще один миф) требуется использование сертифицированных средств защиты информации, соответствующее четвертому уровню контроля отсутствия недекларированных возможностей.

Угрозы несанкционированного доступа требуют защиты:

- линий связи и сетей передачи данных;
- сетевых программных и аппаратных средства, в том числе сетевых серверов;
- файлов и баз данных;
- носителей информации любых типов, в том числе бумажных носителей;
- прикладных и общесистемных программных средств;
- всех помещений компании.

Список программных и аппаратных средств, требуемых для защиты от несанкционированного доступа, также велик и включает в большинстве случаев (но не ограничивается):

- средства антивирусной защиты как рабочих станций, так и серверов;
- средства антивирусной защиты всех каналов передачи данных в сети общего пользования;
- средства резервного копирования;
- средства уничтожения данных и очистки оперативной памяти;
- средства контроля целостности данных и программ;
- средства блокирования исследования, модификации и несанкционированного запуска;
- средства предупреждения пользователей о выполнении опасных действий;
- программные средства администрирования (разграничения полномочий, регистрации и контроля);
- программные и аппаратные средства идентификации и аутентификации;
- средства создания защищенных каналов связи;
- средства ЭЦП;
- средства тестирования сетей и программ;
- средства обнаружения атак и межсетевые экраны.

Если говорить об антивирусной защите, то, согласно закону, требуется:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам;
- предотвращение внедрения в информационные системы вредоносных программ;
- использование средств антивирусной защиты при взаимодействии с сетью Интернет;
- централизованное управление системой защиты персональных данных информационной системы.

Эти меры подразумевают наличие централизованной защиты рабочих станций и серверов, вне зависимости от используемой операционной системы, а также защиту каналов передачи данных (почты и шлюза сети Интернет) и обеспечение недоступности серверов и содержащихся на них данных для несанкционированного доступа.

В связи с тем, что средства защиты от разных производителей могут быть несовместимы, рекомендуется по возможность использовать средства защиты от одного вендора. При закупке таких средств необходимо обращать внимание на возможности продукта. Так, антивирусные продукты компании «Доктор Веб» включают средства защиты от несанкционированного доступа и позволяют определить список ресурсов, к которым пользователь должен иметь доступ. Кроме того, продукты Dr.Web для защиты рабочих станций включают в себя брандмауэр, что также позволяет сэкономить деньги на закупке специализированных решений.

Большую проблему представляет защита сетей компаний, имеющих филиалы либо размещающихся в местах, не позволяющих обеспечить регулярное обслуживание локальных сетей. В качестве примеров таких сетей можно привести банки, крупные компании и учреждения здравоохранения. Для таких организаций необходимо использование централизованно управляемых систем защиты с возможностью построения иерархических сетей любых конфигураций. По возможности должна быть доступна поставка предустановленных средств защиты в виде программно-аппаратного решения.

В качестве примеров также можно привести хорошо себя зарекомендовавшие Dr.Web Enterprise Security Suite и Dr. Web Office Shield. Оба этих продукта имеют интерфейс управления, рассчитанный на использование неподготовленными пользователями, но, с другой стороны, имеют богатый функционал, позволяющий реализовать любую политику информационной безопасности, вплоть до самостоятельного наращивания возможности решений. EOF