АНДЭК-ИНФО

Безопасность бизнеса

Мобильная революция. Возможности и угрозы

Выпуск №2

Срочно в номер! Изменения в законодательстве

Владимир Гайкович,
Председатель Правления компании «Андэк»

Вячеслав Максимов,
заместитель генерального директора компании «Андэк».

Что день грядущий нам готовит: о проектах Постановлений Правительства РФ по защите персональных данных

25.04.2012 на сайте ФСБ России появились проекты двух долгожданных Постановлений Правительства Российской Федерации (ПП РФ):

- «Об установлении уровней защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных»;
- «О требованиях к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных».

Данные документы определяют новые правила защиты персональных данных, вводят новые понятия, и призваны заменить ныне действующее «Положение об обеспечении безопасности персональных данных в информационных системах персональных данных» (ПП РФ № 781 от 17.11.2007).

Ниже представлен краткий содержательный анализ этих документов.

Уровни защищенности

В этих документах впервые введено понятие «Уровень защищенности».

Пункт 2 проекта ПП РФ «Об установлении уровней защищенности…» разъясняет это понятие:

> *Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах.*

Ожидалось, что вместо классов ИСПДн будут уровни защищенности. Но этого не произошло. Теперь классы ИСПДн и модели нарушителей являются исходной информацией для определения уровня защищенности.

Фактически, введение уровней защищенности способно сделать обеспечение безопасности персональных данных риск-ориентированным процессом. Для этого уровень защищенности должен определяться на основе ценности защищаемого актива (класса ИСПДн) и применимых угроз. Именно эта мысль и сформулирована в п.2 проекта ПП РФ «Об установлении уровней защищенности…».

Но в соответствии с п.16 того же ПП РФ, при определении уровня защищенности вместо угроз безопасности используется категория нарушителя. Если это несоответствие не будет устранено, требования безопасности, формулируемые для каждого из уровней защищенности, рискуют потерять связанность с реальными угрозами безопасности ПДн. То есть сформулированная мысль останется без реализации.

Способ определения уровней защищенности и их документальное оформление, по сути, аналогичны уже давно известному процессу классификации ИСПДн. Процесс определения уровня защищенности формально определен, а его результаты оформляются все теми же актами.

Проект ПП РФ «О требованиях к защите персональных данных…» определяет общие требования к защитным мерам для всех уровней защищенности. Однако данный проект не определяет меры обеспечения безопасности для каждого уровня защищенности. В соответствии с п.4 ст.19 ФЗ №152-ФЗ «О персональных данных» (в редакции ФЗ №261-ФЗ от 25.07.2011) конкретные требования к мерам защиты, обеспечивающим заданные уровни защищенности, определяют ФСБ России и ФСТЭК России в пределах их полномочий. Но именно этих требований пока нет, поэтому рано говорить о повышении или снижении сложности в реализации мер защиты ПДн.

Для организаций, принявших решение обеспечивать защиту персональных данных с помощью отраслевых стандартов (например, принявших Комплекс БР ИББС), все становится интереснее.

В соответствии с п.3 ст.19 ФЗ №152-ФЗ «О персональных данных» (в редакции ФЗ №261-ФЗ от 25.07.2011) уровни защищенности для таких организаций определяет Правительство РФ. Типовые модели угроз разрабатываются организациями, перечисленными в п.5 ст.19 ФЗ №152-ФЗ «О персональных данных» в редакции ФЗ №261-ФЗ от 25.07.2011 (в том числе — Банк России). А перечень защитных мер, обеспечивающих заданные Правительством уровни защищенности, определяют ФСТЭК России и ФСБ России в пределах их полномочий. Таким образом, Банк России не уполномочен выдвигать требования по защите персональных данных, использующихся в рамках банковских технологических процессов. В частности, «лишними» становятся «Методические

рекомендации по выполнению законодательных требований при обработке ПДн в организациях банковской системы Российской Федерации», «Требования по обеспечению безопасности ПДн в ИСПДн организаций банковской системы Российской Федерации» (РС БР ИББС-2.3-2010).

С другой стороны, в феврале 2012 года появился еще один законопроект — проект «Положения о защите информации в национальной платежной системе», в соответствии с которым операторы по переводу денежных средств и банковские платежные агенты должны реализовывать защитные меры в соответствии с требованиями по защите информации, установленными Банком России. Другими словами, все кредитные организации должны будут принять документы Комплекса БР ИББС, неотъемлемой частью которых являются и требования по защите ПДн.

В письме Банка России «О реализации в организациях банковской системы Российской Федерации отраслевого комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», сказано, что требования по защите ПДн сформулированные в документах Комплекса БР ИББС, действительны до выхода новых подзаконных актов, которые устанавливают уровни защищенности и требования к защите ПДн.

То есть, если рассматриваемые в данной статье ПП РФ будут приняты без изменений, эти требования становятся недействительными. Какие изменения претерпят документы Комплекса БР ИББС в связи с измененными правилами, и как будет обеспечена легитимность защиты ПДн по новым требованиям Банка России — увидим в будущем. Важно, что работы, направленные на обеспечение согласованности требований регуляторов уже ведутся.

Модель нарушителя

Пунктом 13 ПП РФ «Об установлении уровней защищенности…» введена необходимость включения в модель угроз модели нарушителя. Следующий пункт (14) ПП РФ раскрывает категории нарушителей, которые должны учитываться при определении уровня защищенности.

Само по себе определение категории нарушителя и уровней защищенности можно только приветствовать, поскольку это вводит новую размерность при определении требований к защите ПДн. В результате требования к мерам защиты ПДн могут стать более гибкими: в зависимости от категории нарушителя и класса соответствующей ИСПДн должны применяться те меры защиты, которые наиболее адекватны актуальным угрозам. То есть введение категорий нарушителя и уровней защищенности способно снизить затраты на меры защиты ПДн, не обоснованные реальными рисками.

При этом ключевыми характеристиками нарушителя, категорирование по которым позволит достичь этих преимуществ, будут: уровень квалификации нарушителя; доступные ресурсы (людские, финансовые, временные); методы атаки (физическое проникновение, социальная инженерия, эксплуатация известных уязвимостей в системном и прикладном ПО, реверс-инжиниринг); и т.п.

К сожалению, предложенные в ПП РФ категории нарушителей пока не обеспечивают желаемой гибкости требований к защите.

Предложенное категорирование нарушителей фактически вводит новую систему классификации, которая не согласуется с уже известной моделью нарушителей ФСБ России («Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21.02.2008), что может

привести к необходимости построения операторами ПДн ***нескольких различных*** моделей нарушителей в случае, если для защиты ПДн будут использоваться криптографические средства защиты. То есть к увеличению сложности и количества разрабатываемых документов внутри организации.

В то же время классификация, на наш взгляд, противоречива.

Для разделения нарушителей на внутренних и внешних введено понятие контролируемой зоны (пункт 15 ПП РФ «Об установлении уровней защищенности…»):

> *Контролируемая зона — это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.*

Такое определение контролируемой зоны попросту не предполагает наличие в ней злоумышленников («исключено» = «невозможно ни при каких обстоятельствах»). Поэтому при сохранении этого определения неизменным речь о внутренних нарушителях не может идти.

Кроме того, на наш взгляд, фактически вырожденной является категория КН2, так как сложно представить себе нарушителя, способного реализовать атаки за счет недокументированных возможностей прикладного ПО, но не способного эксплуатировать уязвимости операционных систем. Обычно те, кто знает уязвимости в прикладном ПО до этого изучили уязвимости операционных систем.

Также, поскольку оценить возможности и квалификацию внешних нарушителей априори невозможно, логично предположить, что регулятор всех внешних нарушителей будет относить к категории КН3 (высокий потенциал), а операторы — наоборот, к категории КН1 (низкий потенциал). Таким образом, определение категории внешнего нарушителя становится потенциальной зоной конфликта между регулятором и операторами, в которой решения будут приниматься от случая к случаю.

Обезличивание ПДн

В соответствии с пунктом 9 ПП РФ «Об установлении уровней защищенности…», значение показателя Хпд (содержание обрабатываемых персональных данных), характеризующее обезличенные ПДн, определяется следующим образом:

> *тип 4 — результат обезличивания персональных данных, представляющего действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (далее — обезличенные персональные данные).* ***В случае, если имеется возможность получения оператором такой дополнительной информации, информационная система считается обрабатывающей персональные данные того типа содержания, который был определен до прохождения процедуры обезличивания.***

В большинстве случаев сам оператор и производил действия по

разделению информации о субъектах персональных данных, поэтому у него, как правило, всегда есть возможность получения дополнительной информации о субъекте.

Поэтому снижение класса ИСПДн за счет разделения систем на части, ПДн и прочую информацию о субъекте, в будущем, скорее всего, будет невозможно, а операторы, уже снизившие классы ИСПДн за счет их дробления и отделения идентифицирующих персональных данных субъектов (ФИО, паспортные данные и пр.) от дополнительной значимой информации (остаток на счете, состояние здоровья и т.п.), фактически окажутся вне закона.

Кроме того, данный тип Хпд не включает общедоступные ПДн. Если это не будет исправлено, общедоступные ПДн придется защищать так, как все остальные. Что приведет к росту расходов на защиту ПДн в целом.

Необходимость сертификации средств защиты

К сожалению, пункт 4 ПП РФ «О требованиях к защите персональных данных…» не раскрыл процедуру оценки соответствия. То есть формально вопросы о необходимости обязательной сертификации СЗИ пока еще не сняты.

Однако, пункты (5 и 6) требуют согласования с ФСБ и ФСТЭК правил пользования СЗИ, и получения от них же индексов или условных наименований и регистрационных номеров на используемые для защиты ПДн СЗИ, что может служить свидетельством о необходимости использования исключительно сертифицированных средств защиты.

Но все это наши догадки и рассуждения по косвенным признакам. Участникам рынка, и нам в том числе, хотелось бы получить официальную недвусмысленную позицию регулятора, а не различные позиции отдельных его представителей.

Мониторинг и аудит

Пункт 12 ПП РФ «О требованиях к защите ПДн…» вводит новое требование по защите журналов регистрации событий от несанкционированного доступа.

Еще одно позитивное нововведение: пункт 13 фактически вводит необходимость проведения внутреннего и/или внешнего аудита защиты ПДн не реже одного раза в 2 года, что является шагом навстречу процессному подходу обеспечения защиты ПДн.

Выводы:

На наш взгляд, рассматриваемые ПП РФ реально направлены в сторону обеспечения безопасности персональных данных на основе оценки рисков.

Несмотря на то, что основная идея представленных ПП РФ вполне современна (насколько она вообще может быть современной при текущем уровне развития рынка), эти документы нуждаются в доработке.

Последствия воздействия этих ПП РФ на рынок сильно зависят от того, прислушается ли регулятор к мнению экспертного сообщества или нет.

Новые правила способны повысить не только «бумажный», но и реальный уровень безопасности ПДн, за счет частичного введения процессного подхода к обеспечению информационной безопасности.

Если ПП РФ останутся в том же виде, в котором были опубликованы — будет очередное изменение сил, действующих на рынке. Если же регулятор прислушается к мнению экспертного сообщества — появится реальная возможность действительно защитить персональные данные, а не заниматься вопросами написания большого количества бумажных документов.

Комментарий Владимира Гайковича, председателя Правления компании «Андэк».

Появление этих постановлений, само по себе, не может не радовать, потому как ПП РФ от 2007 года уже все меньше и меньше выполняет те функции, для которых оно было предназначено.

Эти постановления задают более сложные правила игры на рынке защиты персональных данных, причем снова предполагается, что государство лучше всех знает, как именно защищать персональные данные в каждой конкретной компании. Вполне возможно, для текущего уровня развития рынка это и справедливо.

Но для того, чтобы эти правила игры были приняты рынком необходимо, чтобы они дали требуемый уровень гибкости и устранили разночтения, присущие предыдущему ПП РФ.

Необходимые конструкции в этих постановлениях уже есть, нужно просто сделать так, чтобы они заработали в полную силу. А это будет зависеть от того, насколько регулятор воспримет замечания экспертного сообщества.

В общем, поживем — увидим.

Компания «Андэк» специализируется на результатах в области безопасности бизнеса.
Под безопасностью бизнеса мы понимаем устойчивость, развитие, сохранение денег и репутации благодаря умению компании управлять рисками и критически важными данными.

Сферы деятельности «Андэк» — это консалтинг по безопасности бизнеса и информационная безопасность.
Консалтинг, аудит, поставку средств защиты информации, проектирование, внедрение, любые проекты и решения мы рассматриваем как инструменты, позволяющие нашим клиентам достигать самого главного для них результата — развивать свой бизнес, используя новые возможности и контролируя риски.

Наша конечная цель — создание такой системы безопасности, которая бы максимально соответствовала бизнесу компании с учетом его особенностей и отраслевой специфики.

Деятельность «Андэк» в сфере информационной безопасности подтверждена всеми необходимыми лицензиями органов государственного регулирования и сертификатами на предлагаемые решения. Все инновационные решения проходят всестороннее тестирование в центре компетенции, который мы организовали совместно с нашими партнерами — ведущими поставщиками средств защиты информации.

За более подробной информацией Вы можете обратиться к Наталии Тесаковой, шеф-редактору АНДЭК-ИНФО
n.tesakova@andek.ru

Над выпуском работали:

Шеф-редактор: Наталия Тесакова.
Редакционный совет: Олег Глебов, Наталья Зосимовская, Марина Медведева.
Дизайн и вёрстка: Анна Артюшенкова.

Андэк

127083 Москва, ул. 8-го Марта, д.1, стр. 12 (корп. 2, 4 этаж)
Тел.: +7 495 921-44-82
www.andek.ru