«Мы строили, строили, и, наконец, построили…»

Небольшое эссе на тему проектов Постановлений Правительства РФ по защите ПДн

С. В. Вихорев,
Заместитель генерального директора
ОАО «ЭЛВИС-ПЛЮС» по развитию

25-30.09.2012 г.

В конце прошлой недели на сайте ФСБ России наконец-то появились долгожданные великомученные проекты Постановлений Правительства РФ «Об установлении уровней защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных» и «О требованиях к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных». Ждали их еще в июне, но, видимо, споры были большие и, говорят, не только в экспертном сообществе. Судя по записи А. Лукацкого в Twitter, этот проект в начале сентября был согласован, по крайней мере, с директором ФСТЭК России. Так что эти проекты, можно считать согласованной позицией основных регуляторов в вопросах защиты персональных данных. Итак, начнем наш анализ…

«Что было, что будет, чем сердце успокоится»

Посмотрим для начала генезис. Надо сказать, что официально опубликованные тексты документов сильно отличаются от тех, которые были в конце прошлого года, когда ФСБ России по поручению Правительства РФ только приступило к их разработке. Концепция первых вариантов была направлена на сохранение преемственности с действующими документами, в частности с «Приказом трех» (Совместный Приказ ФСТЭК России, ФСБ России и Минкомсвязи России от 13.02.2008 г. № 55/86/20) и предполагала возможность использования уже того, что было наработано и прошло некоторую апробацию на практике. Это относится, в том числе и к классификации ИСПДн по трем основным признакам: (a) категория обрабатываемых ПДн, (b) объем обрабатываемых ПДн, (c) степень негативных последствий для субъекта ПДн. (Я умышленно не беру классификацию по признаку заданных оператором характеристик безопасности, так как на практике все равно требовалось определение класса по основным параметрам – иначе нельзя было определить требования по защите). Именно так был построен первый вариант анализируемых документов: классы ИСПДн выбирались по устоявшимся критериям и связывались с уровнями. Правда, так как исполнителем по этому документу была определена ФСБ России, естественно, сей вариант не миновал «родовой признак»: модель нарушителя. Уровни привязывались к определенному типу нарушителя по модели ФСБ России. Еще надо сказать, что этот вариант не учитывал те критерии выбора уровня защищенности персональных данных, которые были впрямую указаны в Законе «О персональных данных» (вред субъекту ПДн, объем и содержание обрабатываемых ПДн, вид деятельности оператора ПДн, актуальность угроз безопасности ПДн). Это не вызывало положительных эмоций у экспертного сообщества и, видимо, не только у него. Иначе бы не появился тот вариант, который мы анализируем.

В официально опубликованной версии документов полностью изменилась парадигма критериев выбора уровня защищенности ПДн. Детальное изучение этих документов показывает, что выделяются четыре основных критерия: (a) тип угроз, (b) содержание обрабатываемых ПДн, (c) объем обрабатываемых ПДн, (d) принадлежность ПДн сотрудникам оператора.

Насколько правильный такой подход к выбору уровня и верны ли эти критерии – покажет практика, которая, как известно, критерий истины, но логика в этом есть. Сначала посмотрим, соответствуют ли эти критерии тем, что определил закон (табл. 1).

Таблица 1.

Критерии по Закону «О персональных данных»	**Критерии по проекту ПП об уровнях защищенности ПДн**
Оценка вреда субъекту ПДн	Оценка отдана на откуп оператору при определении типа угроз
Оценка объема и содержания обрабатываемых ПДн	Учитывается и объем и содержание обрабатываемых ПДн
Определение вида деятельности оператора ПДн	С натяжкой 2 вида: "оператор - не оператор" + ведомственная МУ
Оценка актуальности угроз безопасности ПДн	Учтено через ведомственную МУ и тип угроз

Итак, видно, что практически все критерии закона нашли свое отражение в проектах Постановлений Правительства. И это отрадно. Некоторые сомнения вызывает критерий «Определение вида деятельности оператора ПДн». Дело в том, что в документе это можно проследить только косвенно. В п. 3 Постановления Правительства РФ «Об установлении уровней защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных» сказано:

> *«3. Определение типа угроз безопасности персональных данных, актуальных для информационной системы персональных данных, производится оператором с учетом совокупности условий и факторов, указанных в подпункте «е» пункта 2, а также оценки вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и нормативных правовых актов, принятых во исполнение части 5 статьи 19 Федерального закона «О персональных данных».*

Здесь ключевым для понимания является то, что тип угроз определяется оператором с учетом «…нормативных правовых актов, принятых во исполнение части 5 статьи 19 Федерального закона «О персональных данных». Эта статья обязывает ФОИВ, органы государственной власти субъектов РФ, Банк России, государственные внебюджетные фонды принимать нормативные правовые акты, в которых определяются для соответствующей отрасли актуальные угрозы безопасности ПДн при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки. Получается, что вид деятельности оператора ПДн учитывается в этой отраслевой модели актуальных угроз. Кроме того, выбор уровня защищенности также зависит от того, что оператор обрабатывает ПДн только своих сотрудников или он обрабатывает ПДн «чужих» субъектов. В совокупности получается, что данный критерий учтен.

Примерно то же можно сказать и про оценку актуальности угроз безопасности ПДн. Надо особо обратить внимание на то, что согласно того же п. 3 Постановления Правительства РФ, **оператор самостоятельно не определяет состав актуальных угроз**. Он на основании отраслевой модели **определяет только тип угроз**. Однако, сказать, что актуальность угроз не учитывается при выборе уровня защищенности ПДн – нельзя.

«Не так страшен черт, как его малюют»

Для начала попробуем препарировать текст документа в виде таблицы (табл. 2), которая упростит процесс определения уровня защищенности ПДн. Теперь видно, что угрозы 1-го типа наиболее характерны для 1 уровня защищенности, а угрозы 2-го типа сосредоточены в основном на 2 уровне защищенности.

Попробуем проанализировать какие же угрозы актуальны для тех или иных категорий персональных данных (табл. 3).

Таблица 2

Критерии выбора уровня / Уровень защищенности			1-й уровень	2-й уровень	3-й уровень	4-й уровень
По принадлежности к оператору ПДн	По количеству субъектов	По содержанию обрабатываемых ПДн	По типу угроз			
Обрабатываются ПДн **не сотрудников оператора** ПДн	мене 100 000	ИС, обрабатывающие ПДн, отнесенные к специальным	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к биометрическим	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к общедоступным		Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)
		ИС, не обрабатывающие специальные, биометрические, общедоступные ПДн	Угрозы 1-го типа (НДВ СПО)		Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)
	более 100 000	ИС, обрабатывающие ПДн, отнесенные к специальным	Угрозы 1-го типа Угрозы 2-го типа	Угрозы 3-го типа (нет НДВ)		
		ИС, обрабатывающие ПДн, отнесенные к биометрическим	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к общедоступным		Угрозы 1-го типа Угрозы 2-го типа		Угрозы 3-го типа (нет НДВ)
		ИС, не обрабатывающие специальные, биометрические, общедоступные ПДн	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
Обрабатываются ПДн **только сотрудников** оператора ПДн		ИС, обрабатывающие ПДн, отнесенные к специальным	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к биометрическим	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к общедоступным		Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)
		ИС, не обрабатывающие специальные, биометрические, общедоступные ПДн	Угрозы 1-го типа (НДВ СПО)		Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)

Естественно предположить, что для получения общедоступных ПДн вряд ли будут использоваться возможности, предоставляемые наличием НДВ в специальном и прикладном ПО. Зачем ломиться в открытую дверь? На то они и общедоступные ПДн, что их можно получить из открытых источников не прибегая ни к каким хитростям. Поэтому изменим их «цветовую дифференциацию».

Таблица 3.

Уровень защищенности / Критерии выбора уровня			1-й уровень	2-й уровень	3-й уровень	4-й уровень
По принадлежности к оператору ПДн	По количеству субъектов	По содержанию обрабатываемых ПДн	По типу угроз			
Обрабатываются ПДн **не сотрудников оператора** ПДн	мене 100 000	ИС, обрабатывающие ПДн, отнесенные к специальным	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к биометрическим	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к общедоступным		Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)
		ИС, не обрабатывающие специальные, биометрические, общедоступные ПДн	Угрозы 1-го типа (НДВ СПО)		Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)
	более 100 000	ИС, обрабатывающие ПДн, отнесенные к специальным	Угрозы 1-го типа Угрозы 2-го типа	Угрозы 3-го типа (нет НДВ)		
		ИС, обрабатывающие ПДн, отнесенные к биометрическим	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к общедоступным		Угрозы 1-го типа Угрозы 2-го типа		Угрозы 3-го типа (нет НДВ)
		ИС, не обрабатывающие специальные, биометрические, общедоступные ПДн	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
Обрабатываются ПДн **только сотрудников** оператора ПДн		ИС, обрабатывающие ПДн, отнесенные к специальным	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к биометрическим	Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)	
		ИС, обрабатывающие ПДн, отнесенные к общедоступным		Угрозы 1-го типа (НДВ СПО)	Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)
		ИС, не обрабатывающие специальные, биометрические, общедоступные ПДн	Угрозы 1-го типа (НДВ СПО)		Угрозы 2-го типа (НДВ ППО)	Угрозы 3-го типа (нет НДВ)

Биометрические ПДн обрабатываются для целей идентификации с использованием специального ПО и далеко не во всех организациях. Можно сделать предположение, что в таком ПО, написанном под заказ и прошедшем строгий выходной контроль со стороны заказчика, маловероятно наличие НДВ. Поэтому, думаю, что и для угроз 2-типа при обработке биометрических ПДн можно изменить цветовую дифференциацию.

Учтем также, что обработка специальных категорий ПДн – явление редкое, даже можно сказать экзотическое. Поэтому не скажу, что для всех, но в большинстве случаев и здесь можно изменить цветовую дифференциацию. Тем более, что если уж в редких случаях такие ПДн и обрабатываются, то средств на их защиту жалеть не стоит.

Маловероятно также и то, что сложные и дорогие методы несанкционированного доступа к информации, основанные на использовании НДВ ПО, будут применяться в том случае, ели обрабатываются только ПДн сотрудников самого оператора. Масштабы не те. Так что и здесь можно смело изменить цветовую дифференциацию.

Отмечу, что это конечно же весьма грубая оценка. Более точную картину можно будет получить, когда появятся отраслевые модели актуальных угроз. Но и такая оценка показывает, что не так страшен черт, как его малюют. Для большинства ИСПДн основным все таки будет 3 или 4 уровень защищенности, что значительно облегчает жизнь операторам ПДн.

Давайте попробуем разобрать ситуацию на примере обычной среднестатистической школы. Положим в школе имеется ИСПДн, которая обрабатывает ПДн постоянного состава (преподавателей) для целей исполнения трудовых отношений и ИСПДн обрабатывающая ПДн переменного состава (школьников).

Согласно данным из книги А. Б. Вифлеемского и И. Г. Лозицкого «Персональные данные и информационные технологии в образовании», в первой ИСПДн (преподаватели) обрабатываются: паспортные данные, ИНН, СНИЛС, сведения об образовании, квалификации и наличии специальных знаний, анкетные данные, сведения о малолетних детях, сведения о состоянии здоровья (инвалидность, беременность), трудовой договор, копии приказов о назначении, форма Т-2, заявления, результаты аттестации. Однозначный вывод о том, что данная ИСПДн обрабатывает только ПДн сотрудников оператора напрашивается сам собой, так что в дальнейшем будем использовать нижнюю часть таблицы. Перечень показывает, что биометрические ПДн для идентификации преподавателей не используются. Есть, конечно специальные ПДн (о состоянии здоровья преподавателя и его родственников), но вероятность, что для получения этих сведений будут применяться методы, основанные на использовании возможностей НДВ - маловероятно. Таким образом, к данной ИСПДн можно применять требования по 3 – 4 уровню защищенности ПДн.

В книге тех же авторов приведен и типовой перечень ПДн, обрабатываемых в ИСПДн второго типа (школьники): сведения, из документов удостоверяющих личность школьника, сведения о составе семьи, паспортные данные родителей, номер полиса медицинского страхования, сведения о состоянии здоровья, сведения о праве на дополнительные гарантии и компенсации, предусмотренные законом. Можно с уверенностью сказать, что число учащихся в среднестатистической школе менее 100 000 человек. Также видно. Что биометрические данные для идентификации личности школьника не используются. Получается, что за исключением сведений о состоянии здоровья, приведенные ПДн можно отнести к «обычным» ПДн, а к такой ИСПДн можно применять требования по 3 – 4 уровню защищенности ПДн. Что же делать со сведениями о состоянии здоровья? Мне почему-то кажется, что для среднестатистической школы здесь проблемы нет. Не думаю, что использовать возможности НДВ для получения таких сведений проще, чем обыкновенный и тривиальный подкуп школьной медсестры. Хотя, все бывает… Но я бы в данном случае использовал бы требования по 3 уровню защищенности ПДн.

Таким образом, в среднестатистической школе имеются информационные системы, обрабатывающие ПДн 3 уровня (школьники) и 4 уровня (преподаватели) защищенности. А это не так уж и страшно.

Рассмотрим общие требования, которые должен выполнить оператор ПДн и которые установлены Законом «О персональных данных» и частные требования, которые выделены в проектах документов (табл. 4):

Таблица 4.

Уровень защищенности / Критерии выбора уровня	1-й уровень защищенности	2-й уровень защищенности	3-й уровень защищенности	4-й уровень защищенности
Общие требования к защите ПДн (по Закону "О персональных данных" ФЗ-152)				
Содержание требования	**Необходимость применения по уровням защищенности**			
Определение и издание политики оператора в отношении обработки ПДн [ст. 18^1.1.(2)]	+	+	+	+
Применением организационных и технических мер по обеспечению безопасности ПДн [ст.181.1.(3)]	+	+	+	+
Осуществление внутреннего контроля (аудита) соответствия обработки ПДн требованиям [ст.18^1.1.(4)]	+	+	+	+
Оценка вреда, который может быть причинен субъектам ПДн при нарушении режима обработки Пдн [ст. 18^1.1.(5)]	+	+	+	+
Ознакомление работников оператора с положениями законодательства по ПДн [18^1.1.(6)]	+	+	+	+
Оценка эффективности мер по обеспечению безопасности ПДн до ввода в эксплуатацию [ст. 19.2.(4)]	+	+	+	+
Восстановление ПДн, модифицированных или уничтоженных вследствие НСД к ним [ст. 19.2.(7)]	+	+	+	+
Установление правил доступа к ПДн обрабатываемым в ИСПДн [19.2.(8)]	+	+	+	+
Обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн [19.2.(8)]	+	+	+	+
Контроль мер по обеспечению безопасности ПДн и уровня защищенности ИСПДн [19.2.(9)]	+	+	+	+
Частные требования к защите ПДн (по проекту Постановления Правительства РФ)				
Организован режим обеспечения безопасности помещений, где находится ИСПДн	+	+	+	+
Обеспечивается сохранность носителей ПДн	+	+	+	+
Утвержден перечень лиц, допущенных к ПДн для выполнения (трудовых) обязанностей	+	+	+	+
Назначено должностное лицо, ответственное за обеспечение безопасности ПДн в ИСПДн	+	+	+	
Доступ к содержанию электронного журнала сообщений имеет только уполномоченный сотрудник	+	+	+	
СЗИ, используемые в ИСПДн прошли установленным порядком процедуру оценки соответствия	+	+		
Изменение полномочий субъектов регистрируется автоматизированными средствами	+			
Имеется структурное подразделение, ответственное за обеспечение безопасности ПДн в ИСПДн	+			

Цветом в таблице выделены те мероприятия, которые требуют применения специальных средств защиты, то есть наиболее затратные. Остальные мероприятия - организационные. Судить какие будут предъявляться технические способы защиты пока не выйдут подзаконные акты ФСТЭК и ФСБ России рано. Но одно уже можно сказать с уверенностью: для 3 и 4 уровней защищенности ПДн применение СЗИ, прошедших процедуру оценки соответствия установленным требованиям – не обязательно.

То есть, в нашем примере, для среднестатистической школы вполне можно обойтись средствами защиты, встроенными в ОС. Не думаю, что это ляжет тяжким бременем (в экономическом смысле) на образовательные учреждения.

«На чужой каравай рот не разевай»

Многие эксперты оценивают тот факт, что для 3 и 4 уровней защищенности ПДн применение СЗИ, прошедших процедуру оценки соответствия установленным требованиям не является обязательным, как некую индульгенцию на право использования зарубежных средств криптографической защиты информации (СКЗИ). На мой взгляд, есть подвох. Дело в том, что ввоз/вывоз зарубежных СКЗИ определяется «Положением о порядке ввоза на таможенную территорию таможенного союза и вывоза с таможенной территории таможенного союза шифровальных (криптографических) средств». Это достаточно интересный документ сам по себе. Но сейчас главное, то, что данное Положение относит к средствам шифрования в том числе:

> *«… аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее передаче по каналам связи и (или) при ее обработке и хранении…»*

В России ввоз/вывоз шифровальных средств осуществляется на основании разовых лицензий, выдаваемых ФСБ России. При этом, заявитель обязан предоставить в контрольный орган много чего, но самое главное:

- *копию лицензии на осуществление лицензируемого вида деятельности*
- *техническую документацию на шифровальное средство*
- *образцы шифровального обрудования для проведения научно-технической экспертизы.*

Такой порядок ввоза зарубежных СКЗИ очень напоминает мне процедуру сертификации, но без выдачи сертификата.

Правда есть в Положении и оговорки. Не требуется получения лицензий, например:

> *«…при ввозе и вывозе шифровальных средств в целях обеспечения собственных нужд организаций без права их распространения и оказания третьим лицам услуг в области шифрования».*

Но предоставление технической документации и образца СКЗИ – требуется.

Надо честно отметить, что Положение для определенных шифровальных средств допускает применение упрощенной процедуры нотификации:

- *средства, имеющие симметричный криптографический алгоритм, использующий криптографический ключ длиной, не превышающей 56 бит*
- *средства, имеющие асимметричный криптографический алгоритм, использующий множители целых чисел, размер которых не превышает 512 бит*
- *средства, обладающие ограниченными функциями (аутентификацией, контроля доступа, где нет шифрования файлов или текстов, электронной цифровой подписи)*
- *средства, являющиеся компонентами программных операционных систем, криптографические возможности которых не могут быть изменены пользователями*
- *персональные смарт-карты (интеллектуальные карты)*
- *оборудование, криптографические возможности которого недоступны пользователю*
- *оборудование, специально разработанное и ограниченное применением для банковских или финансовых операций*

Но даже эти послабления вряд ли позволят широко и легально использовать зарубежные СКЗИ для целей защиты ПДн, если ключ превышает 56 бит для симметричного

алгоритма или 512 бит для ассиметричного алгоритма. Так что не все так гладко с применением зарубежных СКЗИ.

«Не мытьем, так катаньем»

И еще один подводный камень, который заложен в п. 9 проекта Постановления Правительства РФ по требованиям к защите ПДн:

> *«9. Контроль исполнения настоящих Требований организуется и проводится операторами …самостоятельно или с привлечением на договорной основе юридических лиц …, имеющих лицензию по технической защите конфиденциальной информации …»*

Действительно, требования о наличии у оператора ПДн лицензии на работы по технической защите информации в данных документах нет. Однако, проект Постановления Правительства РФ дает право контроля самому оператору ПДн. Здесь уместно вспомнить Постановление правительства РФ от 03.02.2012г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации», где сказано:

> *(п.2) «Под технической защитой конфиденциальной информации понимается выполнение работ и или) оказание услуг по ее защите...» (п.4) «...лицензированию подлежат следующие виды работ и услуг:... б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации».*

Контроль, исходя из смысла ПП-79, это как раз и есть выполнение работ (в своих или чужих интересах – Постановление не оговаривает). Так что контролировать можно, но имея для этого лицензию, так как этот вид работ подлежит лицензированию. Оператор задумается: надо ли ему получать лицензию или пригласить лицензиата. Думаю, что перевесит второе. А вот срок он может определить сам и сделать периодичность в 3 года.

«Сухой остаток»

Анализ документов показывает:

1. Вместо классов ИСПДн, требования по защите ПДн теперь задаются уровнем защищенности ПДн. Это потребует отмены совместного Приказа ФСТЭК России, ФСБ России и Минкомсвязи России от 13.02.2008 г. № 55/86/20 и, как следствие, дополнительных работ от операторов ПДн по определению уровня защищенности обрабатываемых ПДн.

2. Критерии выбора уровня защищенности ПДн не совпадают с критериями классификации ИСПДн, существовавшими до настоящего времени. Это потребует некоторой перестройки в умах операторов и, как следствие, на первом этапе возможна путаница, усложняющая процесс приведения обработки ПДн в соответствие требованиям.

3. Признание утратившим силу постановления Правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и привязка требований по защите ПДн к уровням защищенности ПДн потребует отмены Приказа ФСТЭК России от 05.02.2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» и, как следствие, обнародования новых технических требований.

4. Выход в свет данных документов требует дальнейшей работы и, в частности, разработки отраслевых моделей угроз, а также состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обра-

ботке в ИСПДн. Учитывая, темпы разработки аналогичных документов во ФСТЭК России и ФСБ России, рассчитывать на то, что такие требования появятся хотя бы до конца 2012 года – не приходится.

5. Проект требований не предусматривает проведение мероприятий по защите от ПЭМИН, хотя некоторые требования по этому вопросу могут появится в разрабатываемых ФСТЭК России и ФСБ России документах по составу и содержанию организационных и технических мер по обеспечению безопасности ПДн.

6. Проекты определяют, что для 3 и 4 уровней защищенности ПДн применение СЗИ, прошедших процедуру оценки соответствия установленным требованиям не является обязательным. Однако, это не освобождает их от другого регулирования – экспортного контроля. Данные проекты Постановлений Правительства РФ не дают право бесконтрольного использования СКЗИ, ели их ключ превышает 56 бит для симметричного алгоритма и 512 бит для ассиметричного алгоритма. В месте с тем, даже таких размеров ключа во многих случаях может быть достаточно для обеспечения адекватной защиты. Более подробно об этой проблеме скорее всего будет в документах ФСБ России. И уж, конечно, как минимум потребуется лицензия ФСБ, если используемая ИСПДн не обрабатывает ПДн только сотрудников самого оператора.

7. Контроль выполнения требований стал обязательным элементом защиты ПДн. Оператор может осуществлять такой контроль самостоятельно, но для этого ему требуется получить лицензию на деятельность по технической защите информации или пригласить другое юридическое лицо, имеющее такую лицензию.

Ну, вот в первом приближении – все. Теперь надо ждать документов ФСТЭК России и ФСБ России. И еще отраслевых моделей угроз (странно, но в анализируемых документах ни разу не упоминается «Модель нарушителя»). И только потом можно будет сказать: «к добру это или к худу…»