Ксения Шудрова, shudrova.blogspot.ru

О новом Постановлении Правительства в области защиты персональных данных

Вышло в свет едва ли не самое ожидаемое Постановление Правительства № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Данное Постановление отменяет постановление Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", согласно которому разрабатывали свои документы операторы. В связи с этим многих беспокоит вопрос, неужели все придется заново переделывать? Попробуем ответить на него в этой статье.

Согласно ФЗ «О персональных данных» Правительство устанавливает уровни защищенности, если раньше ИТ-сообщество могло только предполагать, какими они будут, то новое постановление внесло окончательную ясность в этот вопрос. Определено 4 уровня защищенности (просматривается аналогия с 4мя классами ИСПДн, т.е. документу присуща преемственность, что должно облегчить работу оператора). Данные уровни определяются, исходя из типов угроз. Выделяется 3 типа угроз. Стоит отметить, что данная классификация угроз на типы является новшеством. Как мы помним, ранее угрозы определялись в соответствии с нормами «Базовой модели угроз», утвержденной ФСТЭК (часть «четверокнижия») и не подразделялись на типы.

Угрозы 1го типа связаны с наличием недекларированных возможностей (так называемых закладок) в системном программном обеспечении, угрозы 2го типа – с наличием НДВ в прикладном программном обеспечении, угрозы 3 типа – все остальные. Определение актуального типа угроз проводится после определения возможного вреда (п. 5, ч. 1, ст. 18.1 ФЗ «О персональных данных»). Первый тип угроз – наивысший.

Как мы уже говорили, уровни определяются, исходя из актуального типа угроз. Целесообразно изобразить процесс классификации в виде таблицы:

	Угрозы 1 типа	**Угрозы 2 типа**	**Угрозы 3 типа**
Специальные категории персональных данных			
-сотрудников	1 уровень	2 уровень	3 уровень
-не сотрудников	1 уровень	1 уровень (если более 100000 субъектов) 2 уровень (если менее 100000)	2 уровень (если более 100000 субъектов) 3 уровень (если менее 100000 субъектов)
Биометрические персональные данные			

-сотрудников	1 уровень	2 уровень	3 уровень
-не сотрудников	1 уровень	2 уровень	3 уровень
Общедоступные персональные данные			
-сотрудников	2 уровень	3 уровень	4 уровень
-не сотрудников	2 уровень	2 уровень (если более 100000 субъектов) 3 уровень (если менее 100000 субъектов)	4 уровень
Иные персональные данные (не специальные, не биометрические, не общедоступные)			
-сотрудников	1 уровень	3 уровень	4 уровень
-не сотрудников	1 уровень	2 уровень (если более 100000 субъектов) 3 уровень (если менее 100000 субъектов)	3 уровень (если более 100000 субъектов) 4 уровень (если мене 100000 субъектов)

Таким образом, всем без исключения операторам придется переделывать модель угроз и акты классификации систем персональных данных – теперь вместо класса ИСПДн будет указан уровень защищенности, который будет определяться исходя из следующих характеристик:

- тип угрозы (в свою очередь, согласно постановлению, он определяется возможным вредом для субъекта);
- тип субъектов (выделено две категории – сотрудники и «не сотрудники»: клиенты, соискатели на вакантные должности, поставщики и другие лица, с которыми работает организация);
- тип обрабатываемых данных (биометрия, специальные категории, общедоступные данные или иная информация);
- объем обрабатываемых данных лиц, не являющихся сотрудниками (введены две категории – более 100000 субъектов и менее 100000 субъектов).

Классифицировать систему по этим признакам достаточно просто, однако, необходимо помнить, что присутствие в системе хотя бы нескольких записей

специальных персональных данных делает ее специальной информационной системой, обрабатывающей специальные категории персональных данных. То же самое распространяется на биометрию. Информационная система, обрабатывающая общедоступные данные может быть признана таковой только в случае отсутствия иных типов личной информации – все данные получены из общедоступных источников.

Проведем классификацию на примере небольшой организации, которая работает только с юридическими лицами и не собирает биометрическую информацию, а также персональные данные специальных категорий. Персональные данные сотрудников не могут быть целиком общедоступными, значит, они относятся к «иным персональным данным». Очевидно, что для такой фирмы уровень защищенности будет определяться типом угрозы и может быть 1, 3 или 4.

Обосновать неактуальность угрозы недокументированных возможностей программного обеспечения можно с помощью сертифицированного как раз по уровню НДВ программного обеспечения. Таким образом, при использовании сертифицированной версии ОС актуальными остаются угрозы 2 типа. Для того чтобы дополнительно повысить уровень защищенности придется устанавливать исключительно сертифицированное прикладное программное обеспечение, что не всегда выполнимо, так как многие организации используют довольно специфичное ПО, в том числе самописанное. Сертифицированная операционная система также вряд ли установлена в большинстве организаций, а, следовательно, актуальным будет как раз 1 тип угроз. Если в информационной системе обрабатывается что-либо кроме общедоступных ПДн, уровень защищенности – первый.

Какие же требования определяются для первого уровня защищенности? Во-первых, должны быть выполнены все требования для второго, третьего и четвертого уровня:

- введение режима безопасности помещений, в которых расположена информационная система. Должно быть предотвращено несанкционированное проникновение посторонних лиц. Здесь стоит отметить, что для этих целей обычно используется контрольно-пропускной режим, т.е. используются пропуска, которые могут содержать биометрическую информацию;
- обеспечение сохранности носителей информации. Целесообразно вести учет съемных носителей;
- создание перечня лиц, которые могут иметь доступ к персональным данным;

- использование средств защиты информации, прошедших процедуру оценки соответствия (по нормам законодательства РФ) в случаях, если они нужны для нейтрализации актуальных угроз. Скорее всего, имеются в виду сертифицированные средства защиты информации, хотя фраза «прошедшие процедуру оценки соответствия» вызывает частые споры среди специалистов. Одно можно сказать с уверенностью – сертифицированные средства защиты информации являются достаточным условием выполнения этого требования (необходимость, как уже говорилось выше, спорна);
- ограничение доступа к электронному журналу сообщений,

а также дополнительно:

- должна производиться фиксация в электронном журнале изменения полномочий доступа к персональным данным сотрудников оператора;
- должно быть создано структурное подразделение, отвечающее за безопасность персональных данных, или же такие функции должны быть возложены на существующий отдел.

В заключение можно отметить, что контроль выполнения требований производится оператором самостоятельно, либо с привлечением сторонней организации, имеющей лицензию, периодичность проведения проверок – не менее 1 раза в 3 года и определяется оператором. Можно отметить, что в требованиях нет принципиально новых пунктов, даны достаточно общие рекомендации. Те организации, которые защищали персональные данные по старым правилам, могут оставить многие свои внутренние документы без изменений, исключением будет являться лишь акт классификации и модель угроз.