Ксения Шудрова, shudrova.blogspot.ru

21 Приказ ФСТЭК: что делать оператору персональных данных?

28 мая на сайте ФСТЭК был выложен уже утвержденный Приказ № 21 от 18 февраля 2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ №21). Этот документ определяет состав и содержание организационно-технических мер по защите персональных данных, заменяя старый документ – Приказ ФСТЭК № 58 от 5 февраля 2010 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ № 58). Без преувеличения можно сказать, что все ИБ-сообщество, затаив дыхание, ожидало выхода Приказа №21, который должен был внести ясность – чего регуляторы ждут от операторов? И вот документ утвержден и обязателен к исполнению, давайте его проанализируем.

Законодательство в сфере защиты персональных данных постоянно меняется, изначально состав организационно-технических мер регламентировался **«четверокнижием».**[1] Затем в 2010 году был издан Приказ №58, который действовал еще в этом году до утверждения Приказа № 21, о котором мы сегодня и поговорим. Почву для отмены Приказа №58 подготовило Постановление Правительства № 1119 от 01 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», которое в свою очередь отменило Постановление Правительства № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» **от 17 ноября 2007 г**.

В Постановлении Правительства №1119 был введен новый процесс классификации информационных систем, вместо четырех классов (1К, 2К, 3К, 4К) появилось 4 уровня защищенности, тесно связанных с типами актуальных угроз. Операторам пришлось переклассифицировать свои системы, а вот каким образом их защищать было совершенно непонятно, т.к. в Приказе №58 говорилось о мерах защиты применительно к классам, а не уровням. Возникшее противоречие в законодательстве и исправил Приказ № 21.

[1] Все 4 документа ФСТЭК были помечены грифом «ДСП», и их могли видеть очень немногие, в основном – интеграторы, затем два документа упразднили, с оставшихся сняли гриф и, в конце концов, последние два документа как-то «потерялись».

В сферу действия Приказа №21 не попадают защита государственной тайны и защита персональных данных с использованием криптографических средств[2]. Как и в Приказе №58 оператор может привлекать для защиты персональных данных организацию, имеющую лицензию на деятельность по технической защите конфиденциальной информации, либо выполнять работы самостоятельно. В Приказе №21, как и в его предшественнике, затронут вопрос о применении сертифицированных средств защиты информации:

Меры по обеспечению безопасности персональных данных реализуются, в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда, применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Далее в Приказе №21 приведены требования к классу защищенности при применении сертифицированных средств защиты информации.

Оценка актуальности угроз проводится оператором с учетом оценки возможного вреда субъекту персональных данных. Оценка эффективности применяемых мер проводится не реже, чем раз в три года самостоятельно, либо с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Далее в Приказе №21 дается полный перечень возможных защитных мер с их описанием. В данный перечень входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение вторжений;
- контроль защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

[2] Защита персональных данных криптографическими средствами регламентируется документами ФСБ.

- проверка системного и (или) прикладного программного обеспечения на отсутствие недекларированных возможностей;
- тестирование информационной системы на проникновения;
- использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Оператору предлагается определить список защитных мер следующим образом:

Этап 1. Определяем базовый набор мер защиты. В приложении к Приказу №21 приведена сводная таблица мер по обеспечению безопасности персональных данных. Рассмотрим работу с таблицей на примере следующей строки:

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+

ИАФ.2 обозначает, что мера относится к классу мер «Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)» и является второй в списке мер этого класса. Во втором столбце дается описание меры – в нашем случае это идентификация и аутентификация устройств. Третий столбец разделен на 4 части, что соответствует 4 уровням защищенности. Знак «+» означает, что мера для данного уровня является базовой. Мера ИАФ.2 является базовой для 1 и 2 уровня. Для уровня 3 и 4 данная мера является необязательной и может применяться только для адаптации базового набора.

Итак, оператор на первом этапе должен выделить все меры, напротив которых стоит знак «+» в нужном ему столбце с номером уровня защищенности.

Этап 2. Адаптируем базовый набор мер под свою систему с учетом особенностей ее функционирования, исключаем те меры, которые связаны с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе. Например, для меры ИАФ.2 можно исключить идентификацию и аутентификацию портативных устройств, т.к. они не используются в информационной системе.

Этап 3. Уточняем список мер с учетом не выбранных ранее мер для нейтрализации актуальных угроз. На этом этапе мы можем включить меру ИАФ.2 в список мер для 3 и 4 уровня защищенности.

Этап 4. Добавляем меры, обеспечивающие выполнение требований к защите персональных данных, установленных иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации. Например, добавляем перечень мер, связанных с защитой криптографическими средствами.

Этап 5 (необязательный). Выбираем компенсирующие меры. Очень важным для оператора является оговоренная в документе возможность замены приведенного перечня мер на иные, если предлагаемые меры по техническим причинам невыполнимы, либо экономически нецелесообразны. Такая замена должна проводиться с обязательным обоснованием необходимости применения компенсирующих мер. При использовании новых технологий, для которых характерны угрозы, не рассмотренные в рамках Приказа №21, применение компенсирующих мер обязательно.

Проанализировав Приказ №21 можно сказать, что документ действительно вносит ясность в неразрешенные вопросы защиты персональных данных, некоторые его положения, в первую очередь самостоятельная оценка эффективности и применение компенсирующих мер, значительно облегчают жизнь операторам.