105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР «ВУЛКАН»

КОММЕНТАРИИ К ДОКУМЕНТУ «ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ», УТВЕРЖДЕННОМУ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 1 НОЯБРЯ 2012 Г. № 1119

МОСКВА, 2012

105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Введение

Уже около пяти лет[1] решением вопросов обеспечения безопасности персональных данных озадачены сотни тысяч российских организаций.

Практически не прекращающийся итерационный процесс изменения нормативно-правовой базы привел к созданию сложной ситуации. Организации, реализовавшие актуальные (на определенный момент) требования, сталкиваются с изменениями условий игры в области обработки и защиты персональных данных: появляются проекты новых документов, представители регуляторов делают заявления о планируемых изменениях… В конце концов эти изменения вступают в силу, и операторам приходится разбираться в нововведениях и адаптироваться к ним.

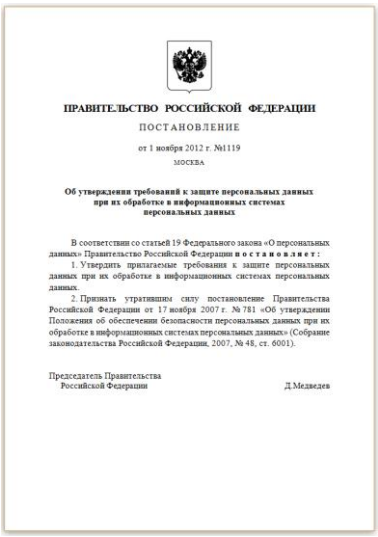
Подобная ситуация произошла и с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781:

– после внесения прошлым летом поправок в Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (и в частности, в статью 19 закона), стало ясно – избежать изменений и обновлений существующих положений, утвержденных постановлениями Правительства, а также методических документов ФСТЭК и ФСБ России не удастся;

– в апреле 2012 года на интернет-сайте ФСБ России появились проекты двух постановлений Правительства – «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»;

– в сентябре 2012 года на том же ресурсе были опубликованы обновленные документы, вызвавшие не меньше количество обсуждений, нежели их первая редакция;

– в итоге, 1 ноября 2012 года был утвержден интегрированный документ «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Требования).



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 1 ноября 2012 г. №1119

МОСКВА

Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных

В соответствии со статьей 19 Федерального закона «О персональных данных» Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые требования к защите персональных данных при их обработке в информационных системах персональных данных.

2. Признать утратившим силу постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2007, № 48, ст. 6001).

Председатель Правительства
Российской Федерации Д.Медведев

Основные положения этих требований будут прокомментированы ниже.

[1] Отсчет ведется с момент выхода в 2008 году четырех методических документов ФСТЭК России, получивших в кругу специалистов по информационной безопасности условное наименование «четверокнижие»

105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Комментарии

1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее – информационные системы) и уровни защищенности таких данных.

Первым делом напомним терминологию, используемую в документе.

Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» *требование по защите информации*[2] – это установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

Как раз данные правила или нормы нас интересуют в первую очередь.

Согласно 152-ФЗ *персональные данные* (ПДн) – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), а *информационная система персональных данных* (ИСПДн) – это совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Обратите внимание, **угрозы должны быть уже определены** в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

Кто же должен это делать? Перечень следующий:

– федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности – **около 80 структур** [4,5];

– органы государственной власти субъектов Российской Федерации – то есть **губернаторы, собрания депутатов, региональные законодательные собрания и т.п., итого – еще несколько десятков нормотворческих «единиц»** [6];

– Банк России;

[2] Стоит отметить, что в отечественной нормативной базе можно встретить практически любые предлоги в словосочетаниях со словами **требования** и **защита информации**: требования о защите информации; требования к защите информации; требование по защите информации (в данном случае будем считать их синонимами)

– органы государственных внебюджетных фондов – например, **органы ПФ РФ, ФОМС, ФСС**;

– иные государственные органы в пределах своих полномочий.

На данный момент нормативных правовых актов указанных органов, учитывающих вводимые Требованиями угрозы 1 – 3 типов, безусловно, нет.

Стоит отметить, что до этого Минздравсоцразвития[3], Банк России, Национальная ассоциация негосударственных пенсионных фондов, Правительство Москвы и некоторые другие органы власти и отраслевые объединения разработали и согласовали с ФСТЭК (а в ряде случаев – и с ФСБ России) документы, в которых определили угрозы безопасности ПДн (т.е. сформировали свои частные модели угроз).

Обратим внимание, что в 152-ФЗ указано, что органы власти, перечисленные в части 5 статьи 19 **принимают** данные документы, т.е. не «могут принимать» или «имеют право принимать», а именно **принимают –** то есть делают это в обязательном порядке. К сожалению, сроки принятия данных актов не указаны ни в федеральном законе, ни в Требованиях, но рано или поздно это все равно должно быть сделано.

Для операторов же получается интересная ситуация: с одной стороны без данных документов нельзя определить организационные и (или) технические меры, а с другой стороны – пунктом 1 части 2 статьи 19 Федерального закона «О персональных данных» обязанность по определению угроз безопасности ПДн при их обработке в ИСПДн возложена на оператора.

С учетом того, что Базовую модель угроз [7] и Методику определения актуальных угроз [8] еще никто не отменял, данным инструментарием все еще можно пользоваться, но… Далее мы увидим, что не все так просто, как хотелось бы.

Перейдем к рассмотрению второго абзаца. Нюансом, на который стоит обратить особое внимание, являются союзы «**и (или)**», которые позволяют создавать системы защиты персональных данных (СЗПДн), включающие в себя:

– только организационные меры;

– только технические меры;

– организационные и технические меры.

Однако, несмотря на наличие союзов, обойтись только организационными или только техническими мерами вряд ли удастся. Лучшие практики в области ИБ, а также существующие отечественные и западные методические документы по защите информации базируются на принципах системности и комплексности, что априори подразумевает применение и технических, и организационных мер.

[3] Ныне преобразовано в Министерство здравоохранения Российской Федерации и Министерство труда и социальной защиты Российской Федерации [5]

105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее – оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

Данный пункт полностью согласуется с частью 3 статьи 6 Федерального закона «О персональных данных». Здесь важно отметить, что в случае, если оператор поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет оператор.

4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

Этот пункт сужает возложенные частью 4 статьи 19 Федерального закона «О персональных данных» на ФСТЭК и ФСБ России обязанности по установлению состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн только до технической составляющей – средств защиты информации.

Что будет на самом деле, мы с вами узнаем после выхода новых методических документов от уполномоченных федеральных органов исполнительной власти.

5. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом – третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

Подход к градации ИСПДн, предложенный в пункте 5, очень похож метод, введенный в отраслевой частной модели угроз Банка России [9], по градации ПДн на четыре категории, с единственным «но»: здесь явно отсутствует понятие обезличенных персональных данных.

Информационные системы, обрабатывающие обезличенные ПДн, методом исключений подпадают к информационным системам, обрабатывающим иные категории персональных данных. Хорошо это или плохо – судить пока рано.

Неоднозначная ситуация складывается с информационной системой, обрабатывающей общедоступные ПДн, т.к. эти данные должны быть получены **только из общедоступного источника персональных данных**, а туда в свою очередь они попадают с письменного согласия субъекта (этому в 152-ФЗ посвящена статья 8). Таким образом, чтобы объявить ИСПДн информационной системой, обрабатывающей общедоступные ПДн, потребуется провести работу по формированию общедоступного источника либо обоснованно использовать существующие «справочники», «адресные книги», созданные «в целях информационного обеспечения». Одним словом, информационная система, обрабатывающая общедоступные ПДн – дело хлопотное.

6. *Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.*

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Согласно РД ФСТЭК России [10] недекларированные возможности (НДВ) – это функциональные возможности программного обеспечения, не описанные или не соответствующие

описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

В рассматриваемом документе не приведены определения системного и прикладного программного обеспечения. Стоит отметить, что более корректно было бы использовать термин «программные средства», т.к. под программным обеспечением понимается еще и документация.

Основываясь на терминологии ГОСТ 19781-90 «Обеспечение систем обработки информации программное. Термины и определения», определим, что:

– системное программное обеспечение (средство) – средство, предназначенное для поддержания работоспособности информационной системы или повышения эффективности ее использования в процессе выполнения прикладных программ;

– прикладное программное обеспечение (средство) – средство, предназначенное для оказания услуг общего характера пользователям и обслуживающему персоналу информационной системы.

Теперь перейдем к рассмотрению определения угрозы и типов угроз.

Анализ показывает, что в данном случае **условиями и факторами** выступает **наличие недокументированных (недекларированных) возможностей.**

А теперь вопрос: если данные возможности являются недокументированными (недекларированными), т.е. о них никто кроме разработчиков не знает, то как можно оценить, будут ли они случайно или намеренно использованы при реализации угрозы?

На наш взгляд, есть два варианта, когда угрозы 1 и 2 типа могут быть признаны не актуальными:

– если используемое в составе ИСПДн системное и прикладное программное обеспечение (средства) имеют действующий сертификат соответствия по какому-либо уровню контроля отсутствия в НДВ [10];

– если согласно Методике определения актуальных угроз [8] задать частоту (вероятность) реализации угроз, связанных с наличием недокументированных (недекларированных) возможностей, маловероятной[4] или низкой[5].

7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 181 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

Не совсем ясно, как оценка возможного вреда может сказаться на признании или непризнании наличия НДВ в системном или прикладном программном обеспечении ИСПДн. Ве-

[4] Отсутствуют объективные предпосылки для осуществления угрозы [8]
[5] Объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию [8]

105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

роятно, следует ожидать, что ответ на данный вопрос будет получен в обновленных методических документах ФСТЭК и ФСБ России.

Дополнительно стоит отметить, что отсутствует шкала и методика оценки вреда, и здесь операторы могут использовать качественные (*высокий, средний и низкий*), нематериальные (*моральный вред, физический вред и т.п.*) и/или количественные показатели (*100, 1 000 или 10 000 рублей*).

И вот здесь мы возвращаемся к комментариям к пункту 2 об ожидании нормативных правовых актов от органов государственной власти, т.к. в существующей Методике определения актуальных угроз [8] нет явной увязки актуальности с недокументированными (недекларированными) возможностями.

8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

9. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий: …

10. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий: …

11. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий: …

12. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий: …

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований: …

14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах …

15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах …

16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах …

Пункты с 9 по 12 и с 13 по 16 для простоты восприятия агрегированы в виде таблиц, наглядно иллюстрирующих условия определения уровней защищенности ПДн и требований к ним.

105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Таблица – Уровни защищенности персональных данных

		Категории обрабатываемых персональных данных									
№	Какой тип угроз актуален для информационной системы	Биометрические персональные данные	Специальные категории персональных данных			Общедоступные персональные данные			Иные категории персональных данных		
			Сотрудники	> 100 000	< 100 000	Сотрудники	> 100 000	< 100 000	Сотрудники	> 100 000	< 100 000
1.	угрозы 1-го типа	1	1	1	1	2	2	2	1	1	1
2.	угрозы 2-го типа	2	2	1	2	3	2	3	3	2	3
3.	угрозы 3-го типа	3	3	2	3	4	4	4	4	3	4

Условные обозначения к таблице:

Сотрудники – обработка персональных данных сотрудников.
> 100 000 – более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.
< 100 000 – менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.
1 – 1-го уровень защищенности персональных данных.
2 –2-ой уровень защищенности персональных данных.
3 –3-ий уровень защищенности персональных данных.
4 –4-ый уровень защищенности персональных данных.

105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Таблица – Требования к уровням защищенности персональных данных

№	Формулировка требования	Уровень защищенности персональных данных			
		4	3	2	1
1.	Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	+	+	+	+
2.	Обеспечение сохранности носителей персональных данных	+	+	+	+
3.	Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
4.	Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	+	+	+	+
5.	Назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе	-	+	+	+
6.	Доступ к содержанию электронного журнала сообщений[6] был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей	-	-	+	+
7.	Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе	-	-	-	+
8.	Создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности	-	-	-	+

Условные обозначения к таблице:

«-» – требование не предъявляется.
«+» – требование предъявляется.

[6] Скорее всего, речь идет об электронном журнале обращений, в котором автоматизированными средствами информационной системы регистрируются запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам (см. п. 15 Положения [13])

105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Обращаем внимание, что в данном пункте речь идет только о **контроле**[7].

В части 8 статьи 19 Федерального закона «О персональных данных» сказано, что **контроль и надзор**[8] за выполнением организационных и технических мер по обеспечению безопасности ПДн при обработке персональных данных в государственных ИСПДн осуществляются ФСТЭК и ФСБ России.

А вот для проведения указанными регуляторами контроля за выполнением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, требуется решение Правительства Российской Федерации. Надзор для данного случая не предусмотрен (см. часть 9 статьи 19 152-ФЗ).

В связи с обновлениями в области лицензирования деятельности по технической защите конфиденциальной информации требуется уточнение, что для организаций, получивших/переоформивших лицензии на данный вид деятельности позднее первого квартала 2012 года, в лицензии должны быть указаны следующие виды работ и услуг [12]:

а) контроль защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации;

б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.

Следует отметить, что установленный период контроля (три года) является классическим сроком действия для сертификатов и аттестатов соответствия, в связи с этим вполне разумно установить данную периодичность и для проведения контроля за выполнением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

[7] Контроль – сравнение фактических (текущих) значений характеристик контролируемого объекта с заданными значениями этих характеристик
[8] Надзор – наблюдение за исполнением обязательных требований (предписаний)

Заключение

Надеемся, что материал был полезен специалистам, в обязанности которых входит организация обработки и защиты персональных данных.

Безусловно, стоит отметить определенную преемственность рассмотренных Требований с ранее изданными нормативными правовыми актами. При этом на первый взгляд количество требований по сравнению с документом-предшественником («Положение…», утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 [13]) сократилось, но на самом деле часть их просто перенесена в статью 19 ФЗ «О персональных данных».

Пока рано делать какие-либо выводы о том, стала ситуация с защитой персональных данных проще и прозрачнее или наоборот – усложнилась и стала более неоднозначной. Для этого необходимо дождаться выхода новых методических документов ФСТЭК и ФСБ России, детально раскрывающих данные требования, а также нормативных актов соответствующих органов государственной власти.

ООО «НТЦ «Вулкан»
Адрес: 105318 г. Москва, ул. Ибрагимова, д. 31 корп. 50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
http://twitter.com/ntc_vulkan
http://www.facebook.com/ntc.vulkan

105318 г. Москва, ул. Ибрагимова, д.31, корп.50
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Список источников

1. Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119.

2. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Дата введения в действие 01 февраля 2008 г.

3. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Распоряжение Администрации Президента Российской Федерации и Аппарата Правительства Российской Федерации от 16 июля 2008 г. № 943/788.

5. Указ Президента Российской Федерации от 21 мая 2012 г. № 636 «О структуре федеральных органов исполнительной власти».

6. Интернет-сайт Совета Федерации: *http://www.council.gov.ru/subject_RF/sub/*

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008 г.

8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14.02.2008 г.

9. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации» (РС БР ИББС-2.4-2010), принятые и введенные в действие распоряжением Банка России от 21 июня 2010 года № Р-705.

10. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», утвержденный решением председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

11. ГОСТ 19781-90 «Обеспечение систем обработки информации программное. Термины и определения». Дата введения в действие 01 января 1992 г.

12. Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

13. Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781.