ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
от 15 июля 2013 г. N 240/22/2637

ПО ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ В СВЯЗИ С ИЗДАНИЕМ ПРИКАЗА ФСТЭК РОССИИ ОТ 11 ФЕВРАЛЯ 2013 Г. N 17 "ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ" И ПРИКАЗА ФСТЭК РОССИИ ОТ 18 ФЕВРАЛЯ 2013 Г. N 21 "ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ"

В соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и законодательством о персональных данных Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в пределах своих полномочий утверждены Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (приказ ФСТЭК России от 11 февраля 2013 г. N 17, зарегистрирован Минюстом России 31 мая 2013 г., рег. N 28608), и Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ ФСТЭК России от 18 февраля 2013 г. N 21, зарегистрирован Минюстом России 14 мая 2013 г., рег. N 28375).

В связи с изданием указанных нормативных правовых актов в адрес ФСТЭК России поступают обращения о разъяснении отдельных положений Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, и Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21. Данный вопрос обсуждается специалистами в области защиты информации на различных форумах и электронных площадках в сети Интернет.

Учитывая характер наиболее часто обсуждаемых вопросов и в целях разъяснения отдельных положений указанных приказов ФСТЭК России, считаем целесообразным сообщить следующее.

1. По вопросу вступления в действие Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, и Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21, а также необходимости проведения повторной аттестации (оценки эффективности) информационных систем аттестованных (прошедших оценку эффективности) до вступления в действие указанных приказов ФСТЭК России.

В соответствии с пунктом 12 Указа Президента Российской Федерации от 23 мая 1996 г. N 763 "О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти" нормативные правовые акты федеральных органов исполнительной власти вступают в силу одновременно на всей территории Российской Федерации по истечении десяти дней после их официального опубликования, если самими актами не установлен другой порядок введения их в действие.

Таким образом, Состав и содержание мер, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. N 21, вступили в действие со 2 июня 2013 г. Требования, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. N 17, вступают в действие с 1 сентября 2013 г.

Исходя из общих принципов норм права по действию во времени, изданные в установленном порядке нормативные правовые акты не имеют обратной силы и применяются к отношениям, возникшим после вступления актов в силу (если иное не установлено федеральными

законами).

Учитывая изложенное, информационные системы, аттестованные (прошедшие оценку эффективности) по требованиям защиты информации до вступления в действие Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, и Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21, повторной аттестации (оценке эффективности) в связи с изданием указанных нормативных правовых актов не подлежат.

2. По вопросу требований, которыми необходимо руководствоваться для обеспечения безопасности персональных данных при их обработке в государственных информационных системах, а также определения класса защищенности государственной информационной системы, в которой обрабатываются персональные данные.

КонсультантПлюс: примечание.

В официальном тексте документа, видимо, допущена опечатка: имеется в виду часть 5 статьи 16, а не часть 5 статьи 6.

В соответствии с пунктом 7 Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21, меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 6 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Указанные требования утверждены приказом ФСТЭК России от 11 февраля 2013 г. N 17.

Учитывая, что меры по обеспечению безопасности персональных данных и порядок их выбора, установленные Составом и содержанием мер, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. N 21, аналогичны мерам защиты информации и порядку их выбора, установленным Требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. N 17, для обеспечения безопасности персональных данных, обрабатываемых в государственных информационных системах, достаточно руководствоваться только Требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. N 17.

Вместе с тем, в соответствии с пунктом 5 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, при обработке в государственной информационной системе информации, содержащей персональные данные, требования о защите информации, не составляющей государственную тайну, в государственных информационных системах применяются наряду с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119.

Таким образом, для обеспечения безопасности персональных данных при их обработке в государственных информационных системах в дополнение к Требованиям, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. N 17, необходимо руководствоваться требованиями (в том числе в части определения уровня защищенности персональных данных), установленными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119. При этом в соответствии с пунктом 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, должно быть обеспечено соответствующее соотношение класса защищенности государственной информационной системы с уровнем защищенности персональных данных. В случае, если определенный в установленном порядке уровень защищенности персональных данных выше, чем установленный класс защищенности государственной информационной системы, то осуществляется повышение класса защищенности до значения, обеспечивающего выполнение пункта 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17.

3. По вопросу о форме оценки эффективности принимаемых мер по обеспечению безопасности персональных данных, о форме и содержании материалов оценки эффективности, а

также о возможности проведения оценки эффективности при проведении аттестации информационной системы.

В соответствии с пунктом 4 части 2 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" обеспечение безопасности персональных данных достигается в частности оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

В соответствии с пунктом 6 Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21, оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. При этом Составом и содержанием мер, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. N 21, форма оценки эффективности, а также форма и содержание документов, разрабатываемых по результатам (в процессе) оценки, не установлены.

Таким образом, решение по форме оценки эффективности и документов, разрабатываемых по результатам (в процессе) оценки эффективности, принимается оператором самостоятельно и (или) по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных.

Оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации информационной системы персональных данных в соответствии с национальным стандартом ГОСТ РО 0043-003-2012 "Защита информации. Аттестация объектов информатизации. Общие положения".

В части государственных информационных систем, в которых обрабатываются персональные данные, оценка эффективности принимаемых мер по обеспечению безопасности персональных данных проводится в рамках обязательной аттестации государственной информационной системы по требованиям защиты информации в соответствии с Требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. N 17, национальными стандартами ГОСТ РО 0043-003-2012 и ГОСТ РО 0043-004-2013 "Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний".

4. По вопросу о применении Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, в отношении муниципальных информационных систем.

В соответствии с частью 4 статьи 13 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" требования к государственным информационным системам, установленные указанным Федеральным законом, распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

Таким образом, Требования, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. N 17, распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении (в частности, Федеральным законом от 6 октября 2003 г. N 131-ФЗ "Об общих принципах местного самоуправления в Российской Федерации" и принятыми в соответствии с ним иными нормативными правовыми актами Российской Федерации).

5. По вопросу применения "Специальных требований и рекомендаций по технической защите конфиденциальной информации" с учетом издания приказа ФСТЭК России от 11 февраля 2013 г. N 17.

Издание приказа ФСТЭК России от 11 февраля 2013 г. N 17 не отменяет действие методических документов "Специальные требования и рекомендации по технической защите конфиденциальной информации" (далее - СТР-К) и "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования о защите информации" (далее - РД АС).

СТР-К применяется в качестве методического документа при реализации мер по защите

технических средств государственных информационных систем (ЗТС.1), выбранных в соответствии с пунктом 21 и приложением N 2 к Требованиям, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. N 17, в целях нейтрализации угроз безопасности информации, связанных с защитой информации, представленной в виде информативных электрических сигналов и физических полей (защита от утечки по техническим каналам).

Иные положения СТР-К (раздел 3 "Организация работ по защите конфиденциальной информации", раздел 5 "Требования и рекомендации по защите конфиденциальной информации, обрабатываемой в автоматизированных системах") могут применяться по решению обладателей информации, заказчиков и операторов государственных информационных систем в части, не противоречащей Требованиям, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. N 17.

Кроме того, положения СТР-К и РД АС применяются по решению обладателя информации (заказчиков, операторов информационных систем) для защиты информации, содержащей сведения конфиденциального характера (Указ Президента Российской Федерации от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера"), обрабатываемой в информационных системах, которые в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" не отнесены к государственным информационным системам.

6. По вопросу применения понятий "информационная система" и "автоматизированная система".

В Требованиях, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, и Составе и содержании мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21, используется понятие "информационная система", установленное Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом понятие "государственная информационная система", цели и порядок ее создания, а также порядок эксплуатации установлены статьями 13 и 14 указанного Федерального закона.

В иных методических документах и национальных стандартах в области защиты информации используется понятие "автоматизированная система", определенное национальным стандартом ГОСТ 34.003-90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения".

Учитывая, что Требования, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. N 17, и Состав и содержание мер, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. N 21, разрабатывались во исполнение федеральных законов от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и от 27 июля 2006 г. N 152-ФЗ "О персональных данных" соответственно, в которых используется понятие "информационная система", в нормативных правовых актах ФСТЭК России также использовано указанное понятие.

Исходя из родственных определений понятия "информационная система", установленного Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", и понятия "автоматизированная система", установленного национальным стандартом ГОСТ 34.003-90, а также из содержания Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, и Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21, использование в нормативных правовых актах ФСТЭК России понятия "информационная система" не влияет на конечную цель защиты информации.

7. По вопросу отражения в сертификатах соответствия на средства защиты информации результатов их проверки на отсутствие недекларированных возможностей, а также отражения в конструкторской и эксплуатационной документации возможности применения средств защиты информации в государственных информационных системах и информационных системах персональных данных.

В соответствии с Требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. N 17, и Составом и содержанием мер, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. N 21, в государственных информационных системах 1 и 2 классов защищенности, а также для обеспечения 1, 2 уровней защищенности и 3 уровня защищенности персональных

данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей. При этом выбор классов защиты сертифицированных средств защиты информации в зависимости от класса защищенности государственных информационных систем и уровня защищенности персональных данных осуществляется в соответствии с пунктом 26 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, и пунктом 12 Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21, соответственно.

Отмечаем, что требования по безопасности информации к средствам защиты информации, утвержденные ФСТЭК России в пределах своих полномочий начиная с декабря 2011 г., включают требования по соответствующему уровню контроля отсутствия недекларированных возможностей для классов защиты этих средств.

В частности, системы обнаружения вторжений и средства антивирусной защиты, сертифицированные на соответствие Требованиям к системам обнаружения вторжений, утвержденным приказом ФСТЭК России от 6 декабря 2011 г. N 638, и Требованиям к средствам антивирусной защиты, утвержденным приказом ФСТЭК России от 20 марта 2012 г. N 28, по 4 классу защиты соответствуют 4 уровню контроля отсутствия недекларированных возможностей.

При использовании в государственных информационных системах соответствующего класса защищенности и для обеспечения установленного уровня защищенности персональных данных средств защиты информации, сертифицированных на соответствие требованиям безопасности информации, установленным в технических условиях (заданиях по безопасности) и (или) иных нормативных документах ФСТЭК России, соответствие уровню контроля отсутствия недекларированных возможностей указывается в сертификатах соответствия требованиям по безопасности информации на эти средства защиты информации.

Возможность применения в государственных информационных системах соответствующего класса защищенности и для обеспечения установленного уровня защищенности персональных данных средств защиты информации, сертифицированных на соответствие требованиям безопасности информации, установленным в технических условиях (заданиях по безопасности), указывается заявителем (разработчиком, производителем) в эксплуатационной и конструкторской документации на эти средства (формулярах и технических условиях).

8. По вопросу применения дополнительных мер защиты информации, направленных на нейтрализацию актуальных угроз безопасности персональных данных 1-го и 2-го типов.

В соответствии с пунктом 11 Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. N 21, в целях снижения вероятности возникновения угроз безопасности персональных данных 1-го и 2-го типов могут применяться дополнительные меры, связанные с тестированием информационной системы на проникновения и использованием в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Указанные меры применяются для обеспечения безопасности персональных данных по решению оператора. При этом до разработки и утверждения ФСТЭК России методических документов по реализации указанных мер порядок их применения, а также форма и содержание документов определяются оператором самостоятельно.

9. По вопросу разработки методических документов ФСТЭК России в целях реализации Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17.

Приказ ФСТЭК России от 18 февраля 2013 г. N 21 издан во исполнение части 4 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных". Указанным Федеральным законом разработка ФСТЭК России иных документов по обеспечению безопасности персональных данных, в том числе по моделированию угроз безопасности персональных данных, не предусмотрена. Определение типов угроз безопасности персональных данных осуществляется оператором в соответствии с пунктом 7 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119.

Одновременно в рамках полномочий по методическому руководству в области технической защиты информации, а также в целях реализации пунктов 14.3 и 21 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17, в настоящее время в ФСТЭК России завершается разработка методических документов по описанию содержания мер защиты информации в информационных системах и порядку моделирования угроз безопасности информации в информационных системах. Ориентировочный срок утверждения документов - IV квартал 2013 г.

Кроме того, планируется разработка методических документов, определяющих порядок обновления программного обеспечения в аттестованных информационных системах, порядок выявления и устранения уязвимостей в информационных системах, порядок реагирования на инциденты, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации, а также ряда других методических документов, направленных на реализацию Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17.

Одновременно сообщаем, что ФСТЭК России не наделена полномочиями по разъяснению Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, в том числе в части определения типов угроз персональных данных и порядка определения уровней защищенности персональных данных.

Начальник 2 управления
ФСТЭК России
В.ЛЮТИКОВ