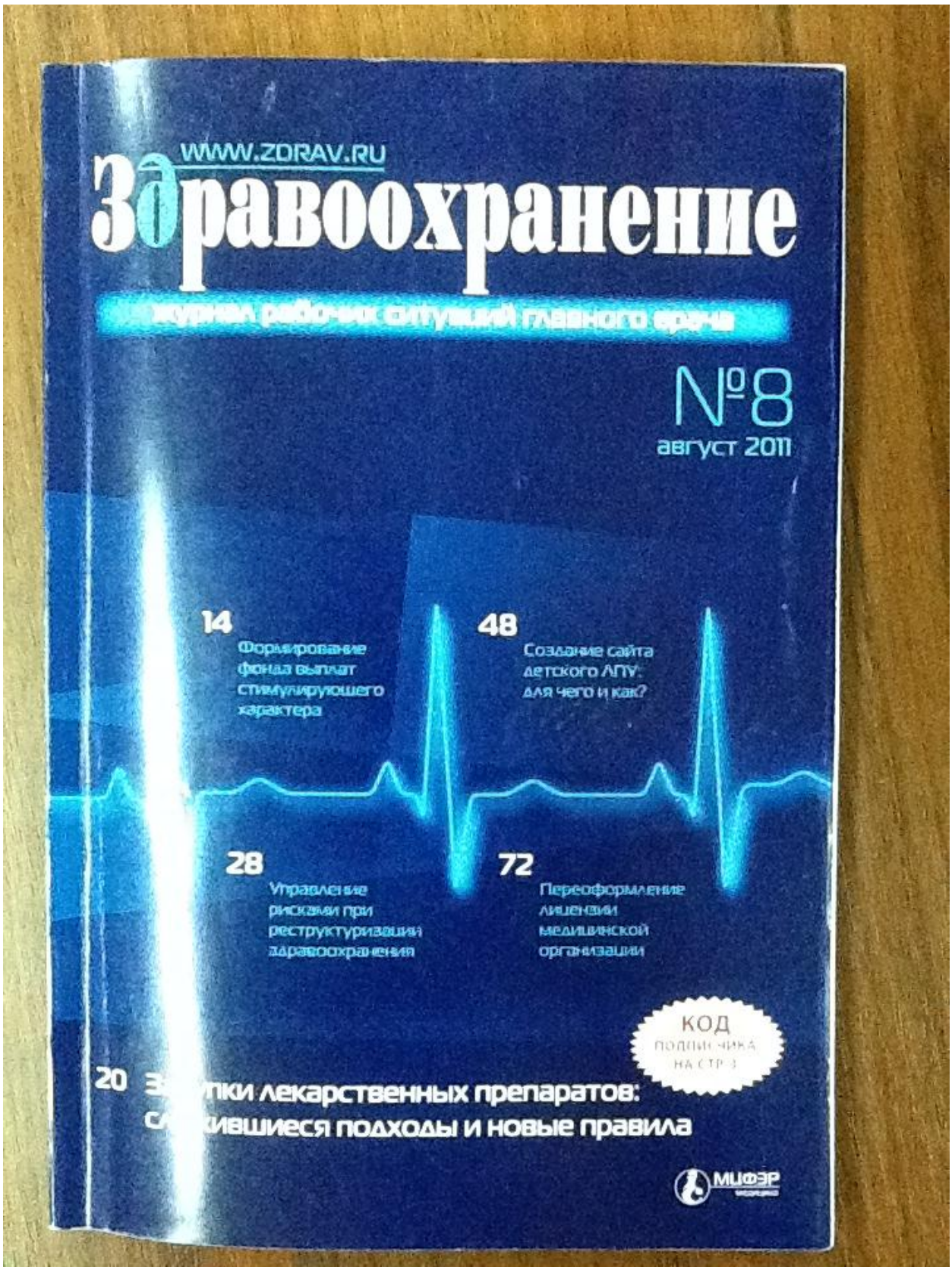
WWW.ZDRAV.RU
Здравоохранение
журнал рабочих ситуаций главного врача
№8
август 2011
14
Формирование фонда выплат стимулирующего характера
48
Создание сайта детского ЛПУ: для чего и как?
28
Управление рисками при реструктуризации здравоохранения
72
Переоформление лицензии медицинской организации
КОД
ПОДПИСЧИКА
НА СТР 3
20
МИФЭР

www.zdrav.ru

Здравоохранение

№8 август 2011

ЖУРНАЛ РАБОЧЕЙ СИТУАЦИИ ГЛАВНОГО ВРАЧА

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

ЭКСПЕРТНЫЙ СОВЕТ

Организация автоматизированной обработки и защиты персональных данных в медицинском учреждении

ключевые слова информатизация здравоохранения, персональные данные

П.П. Кузнецов, д-р мед. наук, профессор, директор

А.П. Столбов, д-р техн. наук, профессор, зам. директора

Медицинский информационно-аналитический центр РАМН

РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТ ПРИВЕЛО К ЗНАЧИТЕЛЬНОМУ ПОВЫШЕНИЮ РИСКОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА.

С ОДНОЙ СТОРОНЫ, ОГРОМНЫЕ МАССИВЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ СЕГОДНЯ ПЕРЕВЕДЕНЫ В ЦИФРОВОЙ ФОРМАТ. С ДРУГОЙ СТОРОНЫ, ШИРОКОЕ РАСПРОСТРАНЕНИЕ ПОЛУЧИЛИ КОМПЬЮТЕРНЫЕ ПРОГРАММЫ, ОБЕСПЕЧИВАЮЩИЕ УДАЛЕННЫЕ ОПЕРАЦИИ С ИНФОРМАЦИЕЙ БЕЗ ВЕДОМА ЕЕ ВЛАДЕЛЬЦА (ШПИОНСКИЕ, ТРОЯНСКИЕ, ЧЕРВИ И Т. Д.). С ТРЕТЬЕЙ – ПОЯВИЛИСЬ СОЦИАЛЬНЫЕ СЕТИ, ПОДРАЗУМЕВАЮЩИЕ АКТИВНЫЙ ПОСТОЯННЫЙ ОБМЕН ИНФОРМАЦИЕЙ МЕЖДУ БОЛЬШИМ КОЛИЧЕСТВОМ ЛЮДЕЙ (В Т. Ч. ЗНАКОМЫХ ЛИШЬ ВИРТУАЛЬНО ИЛИ АНОНИМОВ).

УПРОЩЕНИЕ ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (НАПРИМЕР, О СОСТОЯНИИ ЗДОРОВЬЯ) ОТКРЫЛО ВОЗМОЖНОСТИ ДЛЯ ПРИЧИНЕНИЯ ВРЕДА С ЕЕ ПОМОЩЬЮ (КАК ВАРИАНТ – ДИСКРИМИНАЦИЯ ПРИ ПРИЕМЕ НА РАБОТУ). ЭТА УГРОЗА СТАЛА ПРИЧИНОЙ ПОВЫШЕНИЯ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.

В СООТВЕТСТВИИ С ФЕДЕРАЛЬНЫМ ЗАКОНОМ "О ПЕРСОНАЛЬНЫХ ДАННЫХ" ОТ 27.07.2006 № 152-ФЗ (В РЕД. ФЕДЕРАЛЬНОГО ЗАКОНА ОТ 23.12.2010 № 359-ФЗ) ВСЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ, В КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, ДО 01.07.2011 ДОЛЖНЫ БЫТЬ ПРИВЕДЕНЫ В СООТВЕТСТВИЕ С ТРЕБОВАНИЯМИ УКАЗАННОГО ЗАКОНА.

Конфиденциальность персональной информации не является новшеством последних лет. Конституция РФ декларирует право гражданина на неприкосновенность частной жизни и личной тайны (ст. 23) и устанавливает обязательность его согласия на сбор, хранение, использование и распространение таких сведений (ст. 24).

Этот вопрос не остался без внимания и в законодательстве, регулирующем оказание медицинской помощи. Так, "Основы законодательства Российской Федерации об охране здоровья граждан"

УВЕЛИЧЕНИЕ РИСКОВ ПОТЕРИ ДАННЫХ ПРИ РАБОТЕ В ГЛОБАЛЬНЫХ СЕТЯХ ТРЕБУЕТ ПЕРЕСМОТРА КОНЦЕПЦИИ ИСПОЛЬЗОВАНИЯ ПРОСТОЙ АУТЕНТИФИКАЦИИ. ПАРОЛИ В СОВРЕМЕННОМ МИРЕ НЕ ТОЛЬКО НЕ МОГУТ ОБЕСПЕЧИТЬ СООТВЕТСТВУЮЩИЙ УРОВЕНЬ ЗАЩИТЫ, НО И УПРАВЛЕНИЕ ИМИ СТАНОВИТСЯ ВСЕ БОЛЕЕ ДОРОГОСТОЯЩИМ.

В. Мамыкин, директор по информационной безопасности Майкрософт Рус

(далее – Основы) относят к конфиденциальной информацию о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе заболевания и иные сведения, полученные при обследовании и лечении гражданина (ст. 61). Условия предоставления такой информации третьим лицам в отдельных случаях (при отсутствии согласия, несовершеннолетии или недееспособности гражданина) приведены в ст. 61 и 31 Основ.

Статья 192 Трудового кодекса, ст. 13.14 Кодекса об административных правонарушениях и ст. 137 Уголовного кодекса Российской Федерации предусматривают дисциплинарную, административную и уголовную ответственность за нарушения этих прав граждан. Однако на практике случаи наступления такой ответственности ранее были достаточно редки и касались, как правило, работников, непосредственно разгласивших конфиденциальные сведения.

Принятие Федерального закона "О персональных данных" от 27.07.2006 № 152-ФЗ (далее – Закон № 152-ФЗ)[1] заставило руководителей медицинских организаций по-новому взглянуть на проблему обеспечения конфиденциальности информации (как пациентов, так и работников).

Были конкретизированы права граждан – субъектов персональных данных, а также обязанности организаций, осуществляющих обработку персональных данных. Уполномоченным органом по защите прав субъектов персональных данных стала Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

К персональным данным относятся сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (Указ Президента РФ от 06.03.1997 № 188 "Об утверждении перечня сведений конфиденциального характера"), любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу – субъекту персональных данных (ст. 3 Закона № 152-ФЗ).

Под обработкой персональных данных (далее – ПД) понимаются любые действия (операции) с персональными данными, включая: сбор, систематизацию, накопление, хранение, уточнение (обновление, из-

[1] На рассмотрении Государственной Думы находится новая редакция этого закона.

Оценка рисков

●●●●● НЕСОБЛЮДЕНИЕ ТРЕБОВАНИЯ О ПРИВЕДЕНИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЛПУ В СООТВЕТСТВИЕ С ФЕДЕРАЛЬНЫМ ЗАКОНОМ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"

●●●●○ ПРИНЯТИЕ В НЕПОЛНОМ ОБЪЕМЕ ЛОКАЛЬНЫХ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫХ АКТОВ ЛПУ ПО ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

●●●○○ ПРИВЛЕЧЕНИЕ ДЛЯ СОЗДАНИЯ В ЛПУ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПОДРЯДЧИКОВ, НЕ ИМЕЮЩИХ НЕОБХОДИМЫХ ЛИЦЕНЗИЙ ФСТЭК РОССИИ И ФСБ РОССИИ

менение), использование, распространение (в т. ч. передачу), обезличивание, блокирование, уничтожение.

Любое юридическое или физическое лицо, организующее и/или осуществляющее обработку ПД, а также определяющее цели и содержание их обработки, является оператором ПД.

Конфиденциальность данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Новые требования к автоматизированной обработке ПД и обеспечению их конфиденциальности (помимо обязательного применения специальных программных и технических средств защиты информации) предопределяют необходимость изменения в организации рабочих процессов; уточнения должностных инструкций и регламентов взаимодействия между подразделениями; а также других локальных нормативных актов медицинского учреждения. Должна быть скорректирована и профессиональная подготовка персонала ЛПУ.

Во исполнение и для реализации требований Закона № 152-ФЗ Правительством РФ, Минкомсвязи России, Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Федеральной службой безопасности (ФСБ России) и Роскомнадзором был издан целый ряд нормативных документов, рекомендаций и разъяснений; организован официальный интернет-портал Роскомнадзора по вопросам защиты персональных данных (www.pd.rsoc.ru).

Минздравсоцразвития России были подготовлены и опубликованы на его официальном сайте "Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости" (утв. 23.12.2009), "Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости" (утв. 23.12.2009) и 26 приложений к ним (письмо Минздравсоцразвития России от 05.03.2010 № 328-29), "Модель угроз типовой медицинской информационной системы типового лечебно-профилактического учреждения" (письмо от 27.11.2009 № 240/2/4009). Федеральным фондом ОМС направлено письмо от 22.04.2008 № 2170/90-и "Об организации работ по технической защите информации".

СОГЛАСНО ФЕДЕРАЛЬНОМУ ЗАКОНУ ОТ 23.12.2010 № 359-ФЗ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ, В КОТОРЫХ ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ДО 01.07.2011 ДОЛЖНЫ БЫТЬ ПРИВЕДЕНЫ В СООТВЕТСТВИЕ С ТРЕБОВАНИЯМИ ЗАКОНА № 152-ФЗ.

При создании комплексной системы защиты и безопасности информации ЛПУ потребуется подготовить и принять около 40 ранее необязательных организационно-распорядительных документов (приказов, положений, инструкций, журналов, ведомостей и т. д.). Для этого нужны и время, и специальные знания.

Важно ❯ Для проектирования и создания в ЛПУ системы защиты информации целесообразно привлекать специализированные организации, имеющие соответствующие лицензии Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и Федеральной службы безопасности (ФСБ России) ■

Операторы персональных данных (медицинские организации, фонды ОМС, страховые медицинские организации) должны выполнить следующие действия:

- провести комиссионное обследование информационной системы (организации) и выделить в ее составе подсистемы, в которых обрабатываются персональные данные (далее – ИС ПД), провести их классификацию и оформить соответствующий акт в соответствии с "Порядком проведения классификации информационных систем персональных данных" (утв. приказом ФСТЭК России № 55, ФСБ России № 86, Мининформсвязи России № 20 от 13.02.2008);
- зарегистрироваться в качестве оператора ПД, для чего направить в территориальный орган Роскомнадзора уведомление, заполненное в соответствии с "Рекомендациями по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных" (утв. приказом Роскомнадзора от 16.07.2010 № 482);
- организовать получение, учет и хранение письменного согласия субъектов ПД (как пациентов, так и работников своей организации) на обработку их персональных данных (ст. 6, 9 и 10 Закона № 152-ФЗ).

  Важно › Частью 2 ст. 6 закона № 152-ФЗ предусмотрены случаи, не требующие оформления согласия на обработку ПД. К ним относятся случаи обработки ПД пациента при бесплатном оказании ему медицинской помощи по программе ОМС в соответствии с Федеральным законом от 29.11.2010 № 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации". ■
- организовать информирование пациентов (по их запросам) о целях, способах и сроках обработки и хранения их ПД, лицах, имеющих к ним доступ (ч. 4 ст. 14 Закона № 152-ФЗ), а также об обработке их ПД, полученных от третьих лиц (ст. 18 Закона № 152-ФЗ). Ответ на запрос пациента должен быть подготовлен и направлен ему в течение десяти рабочих дней. Напомним, что согласно ст. 31 Основ пациент имеет право непосредственно знакомиться с медицинской документацией, отражающей его состояние здоровья, и получать копии документов, если в них не затрагиваются интересы третьей стороны.

  Важно › Пациент имеет право ознакомиться со своими персональными данными, которые обрабатывает оператор, и, в случае обнаружения их недостоверности или неправомерных действий с ними, запретить оператору их обрабатывать (ст. 21 Закона № 152-ФЗ). ■
- создать и поддерживать систему защиты информации, представляющую собой совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованных и функционирующих по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации. Состав применяемых методов и средств защиты информации определяется в соответствии с классом ИС ПД. Самые жесткие требования к защите информации установлены для ИС ПД класса К1: предусматривается обязательное применение специальных сертифицированных средств защиты информации;
- получить лицензию на техническую защиту информации (письмо ФСТЭК России от 18.06.2010 № 240/2/2520);
- провести аттестацию объекта информатизации, на котором эксплуатируется ИС, по требованиям к безопасности информации, установленным для ИС ПД данного класса (письмо управления ФСТЭК России по ЦФО от 24.06.2010 № 957). Объектом информатизации является совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией.

средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров (ГОСТ Р 51275-2006 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию").

Должно быть предусмотрено обучение персонала и выделение необходимых финансовых и материальных средств на создание, ввод в действие и эксплуатацию системы защиты информации в учреждении. Безусловно, в первую очередь необходимо соответствующими приказами определить ответственных за обеспечение защиты информации, определить перечень конфиденциальных сведений, утвердить приказом список работников, имеющих к ним допуск, и их полномочия по работе с этой информацией.

Контроль и надзор за выполнением операторами установленных требований к обработке персональных данных осуществляется органами Роскомнадзора, ФСТЭК России и ФСБ России. Процедуры проверки операторов регламентируются следующими документами:

- Правилами подготовки органами государственного контроля (надзора) и органами муниципального контроля ежегодных планов проведения плановых проверок юридических лиц и индивидуальных предпринимателей (утв. постановлением Правительства РФ от 30.06.2010 № 489);
- Типовым регламентом проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. руководством ФСБ России 08.08.2009);
- Административным регламентом проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (утв. приказом Роскомнадзора от 01.12.2009 № 630).

В следующей статье будет рассказано о том, как должно проводиться обследование информационной системы медицинского учреждения; как правильно определить и выделить подсистемы, в которых обрабатываются персональные данные, определить класс информационной системы учреждения в целом; как оформить акт классификации и подготовить уведомление в органы Роскомнадзора для регистрации в качестве оператора персональных данных. Авторы будут признательны всем, кто пришлет свои замечания и предложения по рассмотренным вопросам по электронной почте на адрес AP100Lbov@mail.ru.

Указы Президента РФ, нормативные и методические документы Правительства РФ, Минкомсвязи России, Роскомнадзора, ФСТЭК России и ФСБ России

- Перечень сведений конфиденциального характера (Указ Президента РФ от 06.03.1997 № 188, от 23.09.2005 № 1111);
- О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена (Указ Президента РФ от 17.03.2008 № 351).

- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 17.11.2007 № 781);
- Требования к материальным носителям биометрических персональных данных и технологии хранения таких данных вне информационных систем персональных данных (утв. постановлением Правительства РФ от 06.07.2008 № 512);
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. постановлением Правительства РФ от 15.09.2008 № 687);
- Порядок проведения классификации информационных систем персональных данных (утв. совместным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20);
- Методика определения актуальных угроз безопасности персональным данным при их обработке в информационных системах персональных данных (утв. ФСТЭК России 14.02.2008, гриф "Для служебного пользования" снят 16.11.2009);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 15.02.2008, выписка опубликована на сайте ФСТЭК России www.fstec.ru);
- Положение о методах и способах защиты информации в информационных системах персональных данных (утв. приказом ФСТЭК России от 05.02.2010 № 58);
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ России 21.02.2008);
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ России 21.02.2008);
- Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции "Ведение реестра операторов, осуществляющих обработку персональных данных" (утв. приказом Минкомсвязи России от 30.01.2010 № 18);
- Образец формы уведомления об обработке персональных данных (утв. приказом Роскомнадзора от 16.07.2010 № 482);
- О лицензировании деятельности по технической защите информации (постановление Правительства РФ от 15.08.2006 № 504);
- Положение о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами (утв. постановлением Правительства РФ от 29.12.2007 № 957, с учетом Федерального закона от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности");
- Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством РФ информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг) (постановление Правительства РФ от 15.05.2010 № 330, имеет гриф "Для служебного пользования").