Некоторые теоретические аспекты защиты персональных данных в органах внутренних дел

Лебедев
Вадим Николаевич,
заместитель начальника кафедры информационных технологий управления органами внутренних дел Академии управления МВД России, к.т.н., доцент, полковник полиции

В данной статье предпринята попытка на основе требований законодательства и иных нормативных правовых актов системно рассмотреть процесс защиты персональных данных, которые обрабатываются в информационных системах органов внутренних дел с целью дальнейшего совершенствования и развития ведомственной системы её защиты.

В соответствии со ст. 17 федерального закона «О полиции» полиция имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в банки данных[1].

Вместе с тем само понятие «данные о гражданах» не имеет законодательного закрепления, однако на основе положений, закреплённых в ст. 24 Конституции РФ, а также ряда других нормативных правовых актов[2], в данное понятие входит, прежде всего, информация о частной жизни, личная и семейная тайна, персональные данные[3].

Данные о гражданах представляются в качестве информации, неразрывно связанной с личностью её обладателя, относящейся прямо или косвенно к определенному или определяемому физическому лицу (субъекту ПДн). Таким образом, применительно к деятельности полиции, понятие «данные о гражданах» полностью отождествляется с персональными данными (ПДн) граждан.

Министерство внутренних дел Российской Федерации является оператором, организующим и осуществляющим обработку ПДн[4], обязано принимать правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, а также от иных неправомерных действий в отношении данных сведений.

В целях обеспечения реализации требований законодательства Российской Федерации в области защиты ПДн при их обработке в органах внутренних дел необходимо создание соответствующей системы, т. е. системы защиты ПДн (СЗПДн). Данная система призвана обеспечивать конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн органов внутренних дел.

Система защиты информации представляет собой совокупность органов и исполнителей, а также используемой ими техники защиты информации и объектов защиты информации, организующая и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

В соответствии с требованиями государственного стандарта[5] система защиты ПДн в органах внутренних дел должна состоять из следующих элементов: 1) персональные данные и носители таких данных; 2) должностные лица, подразделения и сотрудники, ответственные за организацию и проведение работ по защите ПДн; 3) способы, техника и средства защиты ПДн; 4) меры и мероприятия, проводимые в целях защиты ПДн.

Рассмотрим эти элементы и попробуем провести краткий анализ каждого элемента системы.

1. Персональные данные и носители таких данных

Персональные данные, обрабатываемые в органах внутренних дел, определены в ч. 3 ст. 17 Федерального закона РФ «О полиции».

Помимо них в различных подразделениях и службах органов внутренних дел (медицинские учреждения, кадровые, финансово-экономические, тыловые подразделения) обрабатываются ПДн сотрудников, федеральных государственных служащих, работников, стажеров системы МВД России, а также членов их семей.

Кроме этого в органах внутренних дел обрабатываются ПДн, которые являются государственной тайной и, естественно, защита данной категории ПДн осущест-

1 О персональных данных: Федеральный Закон РФ от 27 июля 2006 г. №152-ФЗ // СЗ РФ. 2006. №31. Ст. 3448. Ч. 1.

2 О персональных данных: Федеральный Закон РФ от 27 июля 2006 г. №152-ФЗ // СЗ РФ. 2006. №31. Ст. 3448. Ч. 1.; Об информации, информационных технологиях и защите информации: Федеральный Закон РФ от 27 июля 2006 г. №149-ФЗ // СЗ РФ. 2006. №31. Ст. 3448. Ч. 1.

3 Баглай М. В. Конституционное право Российской Федерации. -М.: Норма, 2011. С. 768.

4 Об утверждении инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации: приказ МВД России от 6 июля 2012 г. №678: в ред. от 15 июля 2013 г. // Рос. газ. №230. 2012.

5 ГОСТ Р 50922–2006. Защита информации. Основные термины и определения: приказ Ростехрегулирования от 27 декабря 2006 г. №373-ст // М., 2008.

вляется в соответствии с нормами и правилами, установленными для сведений, составляющих государственную тайну[6].

Важной задачей является определение полного перечня носителей Пдн, используемых в органах внутренних дел, так как именно вид используемого носителя информации во многом определяет вид и количество угроз безопасности информации и технических каналов утечки информации.

В соответствии с ГОСТ[7], носителями защищаемой информации являются физические лица или материальные объекты (бумажные, магнитные, оптические и др.), в том числе физические поля (акустическое, электромагнитное и др.), в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Наиболее традиционным носителем является бумажный носитель, который и до настоящего времени широко используется для обработки ПДн. К материальным носителям, наиболее часто используемым в органах внутренних дел для обработки ПДн, также относятся магнитные носители, а именно жёсткий диск компьютера, сервера и т. п.

Для целей передачи ПДн в органах внутренних дел широко используется оптический диск (CD-R, DVD-R). Это обусловлено тем фактом, что использование данного носителя требует применения только относительно «дешёвых» режимных (организационных) мер.

Безусловно, использование электромагнитного излучения, электрических и оптических сигналов в качестве носителя информации является крайне актуальным и необходимым, однако требует создания системы криптографической защиты, а также системы электронной подписи, то есть применения специальных и дорогостоящих средств защиты информации.

2. Должностные лица, подразделения и сотрудники, ответственные за организацию и проведение работ по защите ПДн

В соответствии с требованиями приказа МВД России[8] руководители (начальники) территориальных органов МВД России, руководители структурных подразделений территориальных органов МВД России, эксплуатирующие ИСПДн, обеспечивают выполнение правовых, организационных и технических мер, направленных на обеспечение безопасности ПДн, и являются ответственными за соблюдение требований по защите ПДн при их автоматизированной обработке в подчинённом органе внутренних дел.

Кроме указанных выше должностных лиц ответственными за соблюдение требований по защите ПДн являются администраторы ИСПДн, а также пользователи, непосредственно обрабатывающие ПДн в ИСПДн, инженерно-технический персонал, имеющий доступ к элементам ИСПДн.

Координацию и контроль деятельности по защите ПДн, содержащихся в информационных системах органов внутренних дел, осуществляет Департамент информационных технологий связи и защиты информации МВД России (ДИТСиЗИ МВД России), который выполняет функции головного подразделения МВД России по вопросам защиты ПДн при их автоматизированной обработке[9].

В территориальных органах МВД России функции защиты ПДн и контроля за проведением мероприятий по защите ПДн возложены на подразделение информационных технологий, связи и защиты информации или на должностные лица, назначенные ответственными за проведение мероприятий по технической защите информации, а также должностные лица, назначенные ответственными за организацию обработки ПДн[10].

Таким образом, в территориальных органах МВД России за выполнение мероприятий по обеспечению безопасности ПДн отвечает, в первую очередь, руководитель (начальник) данного органа и руководитель структурного подразделения, осуществляющего обработку ПДн и/или эксплуатацию ИСПДн.

Руководитель подразделения технической защиты информации является ответственным за правильность проведения аттестационных мероприятий ИСПДн в соответствии с требованиями нормативно-методических и руководящих документов ФСТЭК России. Однако, как показывает практика, руководители территориальных органов и структурных подразделений далеко не в полной мере обладают необходимыми знаниями, организационными навыками и умениями в данной области. Всё это приводит к тому, что зачастую руководители территориальных органов не умеют организовывать проведение необходимых мероприятий, направленных на создание системы защиты информации в подчинённом органе, не могут грамотно поставить задачи своим подчинённым, организовать проведение аттестации объектов информатизации, имеют слабое представление о данном направлении деятельности органа внутренних дел.

В Академии управления МВД России наработан многолетний опыт, имеется необходимая материально-техническая база для подготовки руководителей органов внутренних дел разного уровня в области информационной безопасности.

3. Способы, методы, техника и средства защиты ПДн

К способам и методам защиты персональных данных в ИСПДн органов внутренних дел относятся:

- способы и методы защиты ПДн обрабатываемой техническими средствами информационной системы от несанкционированного доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование,

6 Об утверждении перечня сведений, отнесенных к государственной тайне: Указ Президента РФ от 30 ноября 1995 г. №1203 (в ред. от 19 марта 2013 г.) // СЗ РФ. 1995. №49. Ст. 4775.

7 ГОСТ Р 50922–2006. Защита информации. Основные термины и определения: приказ Ростехрегулирования от 27 декабря 2006 г. №373 ст // М., 2008.

8 Об утверждении инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации: приказ МВД России от 6 июля 2012 г. №678: в ред. от 15 июля 2013 г. // Рос. газ. №230. 2012.

9 Об утверждения положения о Департаменте информационных технологий, связи и защиты информации МВД России: приказ МВД России от 16 июня 2011 г. №681 // Документ опубликован не был.

10 Об утверждении типового Положения о подразделении информационных технологий, связи и защиты информации территориального органа Министерства внутренних дел Российской Федерации: приказ от 2 июля 2012 г. №660 // Документ опубликован не был.

копирование, распространение персональных данных, а также реализация иных несанкционированных действий (методы и способы защиты информации от несанкционированного доступа);
- способы и методы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей от несанкционированного доступа к ПДн (методы и способы защиты информации от утечки по техническим каналам).

В целях защиты Пдн, обрабатываемых в ИСПДн, от несанкционированного доступа применяются средства: управления и разграничения доступа пользователей к Пдн; обеспечения регистрации и учета действий с информацией; обеспечения целостности данных; антивирусной защиты; межсетевого экранирования; анализа защищенности; обнаружения вторжений; криптографической защиты ПДн при их передаче по каналам связи сетей общего и (или) международного обмена.

В целях защиты Пдн, обрабатываемых в ИСПДн, от утечки по техническим каналам, применяются генераторы активного акустического, виброакустического и электромагнитного маскирующего зашумления, сетевые помехоподавляющие и телефонные фильтры, а также методы экранирования и заземления и др.

Выбор средств защиты информации для построения системы защиты персональных данных, осуществляется в соответствии с нормативными правовыми актами, принятыми ФСТЭК России и ФСБ России, на основе модели угроз и в зависимости от уровня защищённости ИСПДн.

Для обеспечения защиты ПДн, содержащихся в ИСПДн, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации[11].

4. Меры и мероприятия, проводимые в целях защиты ПДн

Законодатель определяет некоторые меры, направленные на обеспечение безопасности ПДн. К основным из них относятся такие меры, как определение угроз безопасности ПДн, применение организационных и технических мер по обеспечению безопасности ПДн, оценка эффективности принимаемых мер по обеспечению безопасности ПДн и другие.

Также законодатель наделил Правительство РФ правом и обязанностью устанавливать уровни защищенности и требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн[12].

Содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения установленных Правительством РФ требований к защите ПДн, устанавливаются ФСБ России и ФСТЭК России в соответствии с их полномочиями.

В соответствии с п. 7 «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[13], утвержденных приказом ФСТЭК России от 18 февраля 2013 г. №21, меры по обеспечению безопасности ПДн при их обработке в государственных информационных системах принимаются в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[14], которые утверждены приказом ФСТЭК России от 11 февраля 2013 г. №17.

Учитывая, что меры по обеспечению безопасности ПДн и порядок их выбора, установленные Составом содержания мер, аналогичны мерам защиты информации и порядку их выбора, установленным Требованиями для обеспечения безопасности ПДн, обрабатываемых в государственных информационных системах достаточно руководствоваться только Требованиями.

Тем не менее для обеспечения безопасности персональных данных при их обработке в государственных информационных системах в дополнение к Требованиям необходимо руководствоваться требованиями, установленными постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119. При этом в соответствии с п. 27 Требований должно быть обеспечено соответствующее соотношение класса защищенности государственной информационной системы с уровнем защищенности ПДн. В случае, если установленный уровень защищенности ПДн выше, чем установленный класс защищенности государственной информационной системы, то осуществляется повышение класса защищенности до значения, обеспечивающего выполнение п. 27 Требований.

Таким образом, в настоящее время меры, мероприятия и порядок организации защиты Пдн, содержащихся в информационных системах органов внутренних дел РФ, установлены приказами ФСТЭК России от 11 февраля 2013 г. №17 и МВД России от 6 июля 2012 г. №678.

Остановимся более подробно на мероприятиях, направленных на обеспечение безопасности ПДн, обрабатываемых в ОВД. Мероприятия, проводимые в органах внутренних дел, условно можно разделить на две группы:

I. Управленческие (или организационно-управленческие). Направлены на создание системы технической защиты ПДн и управления ею. Ответственными за организацию проведения данных мероприятий являются руководитель территориального органа МВД России и руководители структурных подразделений, обрабатывающих ПДн.

II. Организационно-технические (мероприятия по обеспечению безопасности ПДн и аттестация ИСПДн по требованиям защиты информации). Необходимо особо обратить внимание на то, что обработка ПДн в ИСПДн органов внутренних дел должна осуществляется только после завершения работ по созданию системы

11 О техническом регулировании: Федеральный Закон РФ от 27 декабря 2002 г. №184-ФЗ // СЗ РФ. 2002. №52. Ст. 5140. Ч. 1.; Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г. №17 // Рос. газ. №136. 2013.

12 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01 ноября 2012 г. №1119 // СЗ РФ. 2012. №45. Ст. 6257.

13 Далее «Состав и содержание мер».

14 Далее «Требования».

технической защиты ПДн и вводу в эксплуатацию ИСПДн.

Управленческие мероприятия:

I. Получение территориальным органом МВД России на региональном уровне лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Лицензия необходима для проведения аттестации информационных систем, обрабатывающих ПДн по требованиям защиты информации.

В соответствии с п. 1 ст. 17 Федерального закона «О лицензировании отдельных видов деятельности», деятельность по технической защите конфиденциальной информации подлежит лицензированию в Российской Федерации[15].

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет ФСТЭК России. Положение о лицензировании указанного вида деятельности утверждается Правительством РФ[16]. В нём определён и утверждён порядок лицензирования, предоставления документов по вопросам лицензирования, лицензионные требования, исчерпывающие перечни выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности. Лицензия действует бессрочно.

II. Создание комиссии для определения уровня защищённости ИСПДн.

Комиссия создаётся приказом руководителя (начальника) территориального органа МВД России, в состав включаются представители структурных подразделений, эксплуатирующих ИСПДн, а также специалисты подразделения (сотрудники) информационных технологий, связи и защиты информации.

III. Планирование мероприятий, направленных на защиту Пдн, обрабатываемых в информационных системах территориального органа МВД России.

Работы по обеспечению безопасности ПДн включаются в План основных организационных мероприятий территориального органа МВД России отдельным разделом (или планы работы структурных подразделений территориального органа МВД России).

IV. Организация взаимодействия подразделений, обеспечивающих создание и эксплуатацию ИСПДн с подразделением по защите ПДн. То есть взаимодействие структурных подразделений территориального органа МВД России, эксплуатирующих ИСПДн, с подразделением по противодействию техническим разведкам и технической защите информации территориального органа МВД Росси на региональном уровне.

В настоящее время данный аспект является одним из проблемных и сложных в проведении мероприятий по обеспечению безопасности ПДн в органах внутренних дел. Вопрос заключается в том что, в соответствии с положением об аттестации объектов информатизации по требованиям безопасности информации, подготовку объекта к аттестации осуществляет подразделение, эксплуатирующее ИСПДн. В органах внутренних дел наблюдается серьёзная нехватка специально подготовленных сотрудников для проведения работ по защите информации, которые могут квалифицированно организовать и провести необходимые подготовительные мероприятия.

Кроме этого, по этой же причине после проведения аттестационных мероприятий в структурных подразделениях в ряде случаев не соблюдаются организационные и технические меры по защите ПДн, обрабатываемых в информационных системах.

V. Определение должностных обязанностей лиц, ответственных за организацию обработки ПДн и эксплуатацию ИСПДн, с внесением соответствующих положений в должностные регламенты (инструкции) сотрудников.

VI. Планирование и организация занятий по изучению требований нормативных правовых актов и методических документов по вопросам обеспечения безопасности ПДн, а также ежегодной проверки их знаний.

С работниками и сотрудниками ОВД, уполномоченными на обработку ПДн, в целях повышения уровня профессиональной подготовки необходимо организовывать изучение требований законодательства Российской Федерации по вопросам обеспечения безопасности ПДн, а также ежегодную проверку их знаний.

Ведомственное повышение квалификации работников и сотрудников органов внутренних дел в области защиты ПДн осуществляется на базе ФГОКУ ВПО «Воронежский институт МВД России».

VII. Организация и осуществление контроля выполнения установленных требований по обеспечению безопасности ПДн.

Целью такого контроля является соблюдение структурными подразделениями территориального органа МВД России требований по обеспечению безопасности ПДн при их обработке в ИСПДн.

Ведомственный контроль по определению достаточности принятых мер по обеспечению безопасности ПДн проводится не реже одного раза в два года и осуществляется ДИСТиЗИ МВД России и подразделением (сотрудниками) информационных технологий, связи и защиты информации.

Организационно-технические мероприятия (мероприятия по обеспечению безопасности ПДн и аттестация ИСПДн по требованиям защиты информации):

К основным мероприятиям по обеспечению безопасности ПДн в органах внутренних дел относятся мероприятия, направленные на формирование требований к защите ПДн, содержащихся в ИСПДн, разработку и внедрение системы технической защиты ИСПДн, аттестацию информационной системы по требованиям защиты информации и ввод её в действие, обеспечение защиты ПДн в ходе эксплуатации и при выводе из эксплуатации аттестованной ИСПДн. Состав и содержание указанных мероприятий определён приказом ФСТЭК России[17].

15 О лицензировании отдельных видов деятельности: федеральный закон Российской Федерации от 4 мая 2011 №99-ФЗ // СЗ РФ. 2011. №19. Ст. 2716; Об организации лицензирования отдельных видов деятельности: постановление Правительства РФ от 21 ноября 2011 г. №957 // СЗ РФ. 2011. №48. Ст. 6931.

16 О лицензировании деятельности по технической защите конфиденциальной информации: постановление Правительства РФ от 3 февраля 2012 г. №79 // СЗ РФ. 2012. №7. Ст. 863.

17 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г. №17 // Рос. газ. №136. –2013.

Наиболее технически сложным мероприятием являются аттестационные испытания информационной системы требованиям защиты информации. Аттестация ИСПДн проводится до начала обработки ПДн в данной информационной системе. Проведение данного мероприятия, т. е. аттестации ИСПДн, можно разделить на три этапа[18]:

Этап 1. *Подготовка ИСПДн к аттестации на соответствие требованиям защиты информации:*

1. Предпроектное обследование ИСПДн, которое включает в себя ***определение:*** перечня ПДн, обрабатываемых в ИСПДн органа внутренних дел и подлежащих защите; условий расположения ИСПДн относительно границ контролируемой зоны; конфигурации и топологии ИСПДн; перечня технических средств и систем, используемых или, предполагаемых к использованию в ИСПДн; общесистемных и прикладных программных средств, предполагаемых к использованию в ИСПДн; режимов обработки ПДн в ИСПДн; уровня защищённости ИСПДн.
2. Разработка модели угроз безопасности ПДн при их обработке в ИСПДн и перечня актуальных угроз.

Этап 2. *Разработка технического проекта на систему технической защиты ИСПДн.*

Этап 3. *Создание и аттестация ИСПДн по требованиям защиты информации:*

1. Оснащение подразделения сертифицированными техническими, программными и программно-техническими средствами защиты информации.
2. Установка и настройка, ввод в эксплуатацию средств защиты ПДн.
3. Подготовка проекта приказа о допуске сотрудников к работам в ИСПДн.
4. Оформление журналов учёта эксплуатирующего персонала, администраторов защиты, администраторов, пользователей, непосредственно обрабатывающих ПДн в ИСПДн, и инженерно-технического персонала, имеющего доступ к ИСПДн; учёт машинных носителей ПДн и учёт их выдачи; проведение инструктажей по обеспечению безопасности ПДн; проверки исправности технических средств и технического обслуживания.
5. *Разработка*: инструкций сотрудникам, обрабатывающим ПДн в ИСПДн в части обеспечения безопасности ПДн; технического паспорта на ИСПДн; инструкций по эксплуатации средств защиты информации для пользователей, администраторов ИСПДн и сотрудников.
6. Проверка соответствия организационно-технических мер защиты требованиям нормативно-методических и руководящих документов ФСБ России и ФСТЭК России.
7. Проведение специальных исследований и аттестации ИСПДн с оформлением документов по результатам аттестационных испытаний и выдача аттестата соответствия ИСПДн требованиям по безопасности информации.
8. Проведение контроля состояния защиты информации в ИСПДн.

В заключении необходимо обратить внимание на то, что обработка ПДн в ИСПДн органов внутренних дел должна осуществляется только после завершения работ по созданию системы защиты ПДн и вводу в эксплуатацию ИСПДн. Ввод в эксплуатацию ИСПДн осуществляется на основе приказа руководителя (начальника) территориального органа внутренних дел после аттестации ИСПДн по требованиям защиты информации.

18 Положение по аттестации объектов информатизации по требованиям безопасности информации: утв. Гостехкомиссией РФ 25 ноября 1994 г. // Документ опубликован не был.

Список литературы:

1. О персональных данных: Федеральный Закон РФ от 27 июля 2006 г. №152-ФЗ // СЗ РФ. 2006. №31. Ст. 3448. Ч. 1.
2. Об информации, информационных технологиях и защите информации: Федеральный Закон РФ от 27 июля 2006 г. №149-ФЗ // СЗ РФ. 2006. №31. Ст. 3448. Ч. 1.
3. О техническом регулировании: Федеральный Закон РФ от 27 декабря 2002 г. №184-ФЗ // СЗ РФ. 2002. №52. Ст. 5140. Ч. 1.
4. Об утверждении перечня сведений, отнесенных к государственной тайне: Указ Президента РФ от 30 ноября 1995 г. №1203 (в ред. От 19 марта 2013 г.) // СЗ РФ. 1995. №49. Ст. 4775.
5. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01 ноября 2012 г. №1119 // СЗ РФ. 2012. №45. Ст. 6257.
6. О лицензировании отдельных видов деятельности: федеральный закон Российской Федерации от 4 мая 2011 №99-ФЗ // СЗ РФ. 2011. №19. Ст. 2716; Об организации лицензирования отдельных видов деятельности: постановление Правительства РФ от 21 ноября 2011 г. №957 // СЗ РФ. 2011. №48. Ст. 6931.
7. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения: приказ Ростехрегулирования от 27 декабря 2006 г. №373-ст // М., 2008.
8. О лицензировании отдельных видов деятельности: федеральный закон Российской Федерации от 4 мая 2011 №99-ФЗ // СЗ РФ. 2011. №19. Ст. 2716;
9. Об организации лицензирования отдельных видов деятельности: постановление Правительства РФ от 21 ноября 2011 г. №957 // СЗ РФ. 2011. №48. Ст. 6931.
10. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г. №17 // Рос. газ. №136. –2013.