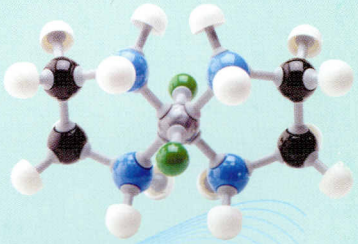
Министерство здравоохранения и социального развития
Самарской области

Организация работ по защите персональных данных

Методические материалы
для медицинских учреждений



Самара
2009

УДК 004.056:61
ББК 32.973+51
О64

О64 **Организация работ по защите персональных данных:** Методические материалы для медицинских учреждений – Самара, 2009. – 131 с.

ISBN 978-5-901294-46-8

В предлагаемом руководстве рассматриваются основные положения защиты персональных данных в медицинских учреждениях и даются рекомендации по их применению.

Руководство содержит список основных терминов защиты персональных данных, нормативных правовых актов, а также примерные формы локальных нормативных актов и рекомендации по их составлению.

Защита персональных данных – это комплекс организационных и технических мероприятий, направленных на обеспечение безопасности и конфиденциальности персональных данных, обрабатываемых как в информационных системах персональных данных, так и вне таких информационных систем.

Предназначено для специалистов медицинских учреждений, осуществляющих обработку персональных данных.

УДК 004.056:61
ББК 32.973+51

Составители: М. А. Никитин, Д. А. Лютов
Рецензент: П. В. Шмелев

ISBN 978-5-901294-46-8

Содержание

Законодательством Российской Федерации ответственность за надлежащую защиту персональных данных возлагается на организации, в которых персональные данные обрабатываются. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является Роскомнадзор.

Роскомнадзор проводит плановые (целевые, комплексные) проверки, а также проверки по жалобам и обращениям физических и юридических лиц. Проверки систем защиты персональных данных могут также осуществляться ФСТЭК России или ФСБ России при проведении контроля систем защиты персональных данных или использования криптосредств. При обнаружении неправомерных действий с персональными данными их обработка должны быть прекращена до устранения выявленных нарушений.

Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Нарушение законодательства о персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (статья 24) влечет за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в

соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года.

Нормативные правовые акты и документы, регламентирующие защиту данных

В целях защиты прав граждан на неприкосновенность частной жизни, личной и семейной тайны в последние годы принят ряд законодательных актов. В настоящее время законодательно-нормативная база по персональным данным включает:

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (14-я глава, с изменениями и дополнениями).

http://pd.rsoc.ru/low/

http://www.consultant.ru/popular/tkrf/

2. Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

http://pd.rsoc.ru/low/

http://www.businesspravo.ru/Docum/DocumShow_DocumID_106723.html

3. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

http://pd.rsoc.ru/low/

http://www.fstec.ru/_razd/_ispo.htm

4. Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

http://www.rg.ru/2007/11/21/personalnye-dannye-dok.html

http://www.garant.ru/hotlaw/doc/106330.htm

5. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных

данных, осуществляемой без использования средств автоматизации».

http://www.rg.ru/2008/09/24/dannye-obrabotka-dok.html

http://www.garant.ru/hotlaw/doc/122316.htm

6. Постановление Правительства Российской Федерации от 6.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

http://www.rg.ru/2008/07/11/trebovaniya-dok.html

http://www.garant.ru/hotlaw/doc/117878.htm

7. Постановление Правительства Российской Федерации от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

http://www.fstec.ru/_razd/_ispo.htm

http://infopravo.by.ru/fed2005/ch01/akt11179.shtm

8. Постановление Правительства Российской Федерации от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

http://www.rsoc.ru/main/about/953.shtml

http://www.rg.ru/2009/03/24/polozhenie-dok.html

9. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

http://www.fstec.ru/_docs/_perech2.htm

http://www.rg.ru/2008/04/12/informaciya-doc.html

10. Приказ Россвязькомнадзора от 17.07.2008 № 08 «Об утверждении образца формы уведомления об обработке персональных данных».

http://pd.rsoc.ru/low/

11. Приказ Россвязькомнадзора от 18.02.2009 № 42 «О внесении изменений в приказ Россвязькомнадзора от 17 июля 2008 г. № 8 «Об утверждении образца формы уведомления об обработке персональных данных».

http://pd.rsoc.ru/low/

12. Методические документы ФСТЭК России:

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

– «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных»;

– «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

http://www.fstec.ru/_razd/_ispo.htm

13. Приказ ФСБ России от 9.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

http://www.businesspravo.ru/Docum/DocumShow_DocumID_97997.html

http://www.rfcmd.ru/sphider/docs/InfoSec/Prikaz_FSB_N_66_ot_09_02_05.htm

14. Постановление Правительства Российской Федерации от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

http://www.fsb.ru/fsb/supplement/contact/lsz/post957.htm

http://www.garant.ru/hotlaw/doc/109485.htm

15. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, от 21.02.2008 № 149/54-144).

http://www.fsb.ru/fsb/science/single.htm!id%3D10434826%40fsbResearchart.html

http://www.mediann.ru/article_6_1_1.html

16. 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 (ФСБ России, от 21.02.2008 № 149/6/6-622).

http://www.fsb.ru/fsb/science/single.htm!id%3D10434826%40fsbResearchart.html

http://www.mediann.ru/article_6_1_1.html

Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе: фамилия, имя, отчество, год, месяц, день и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без наличия таких средств.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

Доступ к информации – возможность получения информации и ее использования.

Трансграничная передача персональных данных – передача персональных данных оператором через государственную границу Российской Федерации.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Под **техническими средствами**, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации, применяемые в информационных системах.

Порядок проведения работ в медицинских учреждениях по обеспечению защиты информационных систем персональных данных и персональных данных, обрабатываемых без использования средств автоматизации

Под защитой персональных данных подразумевается комплекс организационных и технических мероприятий, направленных на обеспечение безопасности и конфиденциальности персональных данных, обрабатываемых как в ИСПДн, так и вне ИСПДн.

Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением следующих случаев:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут

распространяться без согласия в письменной форме субъектов персональных данных;

4) являющихся общедоступными персональными данными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

В соответствии с рекомендациями ФСТЭК России выделяют следующие стадии создания системы защиты персональных данных (СЗПДн):

Первая стадия – предпроектная.

– Предпроектное обследование;

– Разработка примерного плана мероприятий по обеспечению защиты ПДн;

– Разработка технического задания (необходимо для сложных информационных структур).

Вторая стадия – проектирования и реализации.

– Разработка технического проекта (необходим для сложных информационных структур и крупных организаций);

– Внедрение технических средств защиты ПДн;

– Разработка нормативной и регламентирующей документации.

Третья стадия – ввода в действие.

– Опытная эксплуатация системы защиты ПДн;

– Приемо-сдаточные испытания;

– Оценка соответствия требованиям по безопасности информации (может осуществляться как в форме сертификации, так и в форме аттестации. Для медицинских учреждений свойственна и приемлема именно аттестация, а не сертификация);

– Обучение персонала.

Проведение предпроектного обследования

На этапе обследования информационных систем ПДн выполняются следующие работы:

– формируется перечень ПДн, информационных систем и технических средств, используемых для их обработки;

– определяются подразделения и сотрудники, обрабатывающие ПДн;

– определяются категории ПДн;

– разрабатывается описание объекта защиты, включая состав и характеристики средств обработки данных;

– проводится предварительная классификация информационных систем ПДн (пересмотр класса производится на усмотрение оператора в любое время);

– в соответствии с рекомендациями ФСТЭК России и ФСБ России определяются и уточняются типовые модели угроз и соответствующие им типовые требования к системам защиты ПДн;

– осуществляется оценка необходимых мероприятий и затрат по приведению информационных систем ПДн в соответствие с предъявляемыми требованиями.

Результатами работ на этапе обследования являются:

– перечень ПДн и категории ПДн;

– перечни информационных систем и технических средств, используемых для обработки ПДн, и анализ их состояния;

– состав имеющихся в наличии мер и средств защиты ПДн;

– перечень подразделений и сотрудников, обрабатывающих ПДн;

– классификация информационных систем, обрабатывающих ПДн на типовые (1–4-го классов) и специальные;

– акты классификации информационных систем, обрабатывающих ПДн;

– описание объектов защиты;

– уточненные типовые модели угроз и требования к системам защиты ПДн;

– перечень необходимых мероприятий и ориентировочная стоимость работ по приведению информационных систем ПДн в соответствие с предъявляемыми требованиями.

Следует оценить возможность обезличивания или понижения классов информационных систем и провести необходимые работы повторно.

Наиболее эффективным способом приведения ИСПДн в соответствие с предъявляемыми требованиями является их обезличивание. Оно позволяет классифицировать ИСПДн по низшему классу К4 и самостоятельно определить необходимость и способы их защиты.

Если обезличивание невозможно, то понизить требования по защите персональных данных можно путем

сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных автоматизированных рабочих местах (АРМ).

После определения способов понижения требований по защите персональных данных и необходимого повторного обследования оформляются акты классификации ИСПДн, осуществляются определение и анализ типовых моделей угроз и требований, определение необходимых мер и средств защиты ПДн, а также перечень и шаблоны внутренних нормативных документов, регламентирующих порядок обработки и защиты ПДн.

Предпроектное обследование завершается формированием типовых требований к системам защиты ПДн.

Предпроектное обследование является важнейшим этапом работ по обеспечению защиты персональных данных, во многом определяющим состав и эффективность реализации мероприятий и необходимые затраты. Поэтому на данном этапе целесообразно привлекать для анализа результатов обследования и консультаций сертифицированных специалистов в области защиты персональных данных.

Классификация информационных систем персональных данных и определение актуальных угроз их безопасности

Для проведения классификации ИСПДн, определения категорий персональных данных и экспертной оценки угроз их безопасности целесообразно сформировать комиссию с привлечением специалистов в области информационной безопасности, в том числе по защите государственной тайны (лица с высшим профильным

образованием в сфере защиты информации или с повышением квалификации в сфере ЗИ).

Классы типовых ИСПДн определены приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». Классификация ИСПДн осуществляется в зависимости от категории персональных данных (ПДн), не содержащих сведения, относящиеся к государственной тайне:

категория 1 – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 – ПДн, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1;

категория 3 – ПДн, позволяющие идентифицировать субъекта персональных данных;

категория 4 – обезличенные и (или) общедоступные персональные данные.

Целесообразно отдельно определять категории ПДн, обрабатываемых в ИСПДн в электронном и в бумажном виде. В последнем случае следует руководствоваться постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

Типовые ИСПДн, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных, относятся к классу 1 (К1), к негативным последствиям – к классу 2 (К2), к незначительным негативным последствиям – к классу 3 (К3), не приводит к

негативным последствиям для субъектов персональных данных – к классу 4 (К4).

Кроме того, при классификации учитываются объем и территория охвата субъектов персональных данных в порядке, приведенном в приказе ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

ИСПДн, обрабатывающие обезличенные или общедоступные персональные данные класса (категории 4), относятся к классу К4. В этом случае обязательные требования по защите ПДн не устанавливаются.

Постановлением 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» определены необходимые мероприятия по защите персональных данных, обрабатываемых в ИСПДн. В их число входят определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз; разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем, и другие мероприятия.

При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации (прежде всего, регламентирование доступа сотрудников к обработке персональных данных, парольная и антивирусная защита);

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным (прежде всего, регламентирование использования и регулярное обновление антивирусных средств);

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование (охрана и регламентирование использования технических средств);

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (прежде всего, путем хранения резервных копий на съемных маркированных носителях);

д) постоянный контроль за обеспечением уровня защищенности персональных данных (осуществляемый в основном администраторами ИСПДн и иным персоналом).

При этом следует учитывать, что в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» основным обязательным требованием к ИСПДн является обеспечение конфиденциальности. Если право доступа субъекта к своим персональным данным на их изменение, блокирование или отзыв реализуется не самим субъектом непосредственно, а персоналом ИСПДн при обращении или по запросу субъекта, или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, если в ИСПДн не обрабатываются персональные данные 1-й категории и не предусмотрено принятие решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы на основании исключительно автоматизированной обработки персональных данных, то другие требования (кроме конфиденциальности) менее

критичны. Так, в случае выявления неправомерных действий с персональными данными для их устранения законом предусмотрено три рабочих дня с даты такого выявления.

Если система не может быть отнесена к типовой, модель угроз для специальной информационной системы разрабатывается на основе ГОСТ Р 51275-2006 специалистами в области информационной безопасности. Типовые модели угроз приводятся в «Базовой модели угроз безопасности персональных данных».

Определение угроз безопасности персональных данных осуществляется на основе утвержденной ФСТЭК России «Базовой модели угроз безопасности персональных данных». Полный перечень угроз определен ГОСТ Р 51275-2006.

Выбор типовой модели угроз осуществляется в зависимости от того, имеют ли ИСПДн подключение к сетям общего пользования и (или) сетям международного информационного обмена, а также от их структуры (автономные автоматизированные рабочие места, локальные сети, распределенные ИСПДн с удаленным доступом).

Наименьшее количество угроз имеют автоматизированные рабочие места и локальные ИСПДн, не подключенные к сетям общего пользования. Если ИСПДн нераспределенные и соответствуют классу К3, то необходимые мероприятия по защите персональных данных могут быть осуществлены без привлечения специалистов в области информационной безопасности.

Для каждой угрозы, приведенной в типовой модели, следует оценить возможную степень ее реализации. Если она окажется высокой, то это может потребовать применения соответствующих дополнительных технических средств защиты информации.

Возможность реализации угрозы зависит от исходной защищенности ИСПДн и вероятности реализации угрозы.

Вероятность реализации угрозы – определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация конкретной угрозы безопасности ПДн для каждой ИСПДн:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, отсутствует физическое подключение к сети);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, действия персонала оговорены в утвержденном регламенте или имеются средства защиты и инструкции по их применению);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (например, средства защиты имеются, но инструкции по их применению отсутствуют);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Исходная защищенность ИСПДн определяется в соответствии с утвержденной ФСТЭК России «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Расчет исходной защищенности ИСПДн осуществляется по таблице, приведенной в «Методике...», в зависимости от ряда показателей, по которым подразделяются ИСПДн.

В соответствии с «Методикой...» осуществляется расчет возможности реализации угроз и оценка их опасности.

Определяемый на основе опроса экспертов показатель опасности имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных, что соответствует классу К3;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных, что соответствует классу К2;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных, что соответствует классу К1.

Информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных, соответствуют классу К4.

При использовании типовых моделей угроз и соответствующих им требований, приведенных в утвержденных ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», следует учитывать, что в ряде случаев возможности реализации отдельных угроз могут быть более высокими и потребовать дополнительных мер защиты персональных данных. Например, возможность реализации угроз увеличивается, если:

– помещения не запираются;

– при обработке персональных данных используются микрофон и динамики;

– монитор не отвернут от окна и посетителей;

– используются беспроводные устройства, в т. ч. клавиатура и мышь;

– отсутствует парольная защита BIOS;

– используются средства сетевого взаимодействия по электропроводке или беспроводные;

– запуск неразрешенных приложений не контролируется.

Актуальные угрозы определяются по приведенной в «Методике...» таблице в зависимости от их опасности и возможности реализации.

При отсутствии дополнительных опасных факторов (например, перечисленных) для нераспределенных ИСПДн 3-го класса анализ угроз можно провести при окончательном уточнении требований на этапе выбора и реализации системы защиты персональных данных.

Исходя из составленного перечня актуальных угроз и класса ИСПДн на основе утвержденных ФСТЭК России «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные требования по защите ИСПДн и осуществляется выбор программных и технических средств защиты информации.

В случае использования криптосредств в целях защиты персональных данных анализ актуальности угроз и защита персональных данных могут также осуществляться на основании Методических рекомендаций ФСБ России по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Однако для типовых ИСПДн 3-го класса в большинстве случаев это потребует дополнительных затрат.

Если аномально опасные угрозы не выявлены, то для ИСПДн 3-го класса, как правило, можно ограничиться типовыми требованиями к средствам защиты, приведенными в выписке из «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных».

В документе приводятся три варианта требований к ИСПДн 3-го класса:

– при однопользовательском режиме обработки;

– при многопользовательском режиме обработки и равных правах доступа;

– при многопользовательском режиме обработки и разных правах доступа.

В последнем случае при подключении к Интернету нераспределенных ИСПДн класса К3 сертифицированные межсетевые экраны не указаны как обязательные. Это существенно уменьшает затраты на реализацию системы защиты персональных данных, но требует настройки ИСПДн с учетом прав доступа конкретных пользователей.

Определение способов для удовлетворения более низким требованиям по защите персональных данных

По результатам первичной классификации ИСПДн во многих случаях относятся к 1-му или 2-му классам, требующим существенных затрат и обязательной аттестации. Значительно уменьшить обязательные требования и необходимые затраты на защиту персональных данных можно путем обезличивания и сегментирования ИСПДн, отключения сегментов ИСПДн от сетей общего пользования, организации выделенных АРМ и др.

Основная экономия затрат достигается при этом за счет отключения от Интернета, изменения классификации

сегментов ИСПДн на К4 или К3 и замены требований по обязательной аттестации на добровольное декларирование соответствия, а также за счет уменьшения количества защищаемых АРМ в аттестуемых ИСПДн высоких классов К2 и К1.

Наилучшим результатом является обезличивание и обоснование соответствия ИСПДн классу К4, для которого все персональные данные относятся к категории 4 и являются обезличенными или общедоступными.

В этой связи наиболее эффективным является обезличивание ИСПДн путем замены Ф. И. О. субъектов ПДн на их личные коды (табельные номера), используемые для автоматизированного учета в данной организации. Существенным преимуществом этого способа является возможность непосредственной замены всех Ф. И. О. кодами вручную или с помощью встроенных средств в недоступных для самостоятельной модернизации ИСПДн (1С:Бухгалтерия, Парус и др.).

Персональные данные 2-й категории, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (за исключением ПДн, относящихся к категории 1), целесообразно вывести из интегрированных ИСПДн в отдельные локальные системы и отключить от Интернета.

Персональные данные 3-й категории, позволяющие только идентифицировать субъекта персональных данных, в зависимости от объема данных и класса ИСПДн можно обезличивать или обрабатывать в неизменном виде.

Изменение класса информационных систем персональных данных путем обезличивания

Обезличивание ИСПДн позволяет сохранить действующий порядок доступа пользователей, включая удаленный. Единственным отличием является размещение

и использование в обезличенных ИСПДн личных кодов вместо Ф. И. О. субъектов персональных данных. При этом нельзя ограничиться обезличиванием вновь вводимых персональных данных, а ранее накопленные оставить в той же базе данных без изменения. Неиспользуемые персональные данные за предшествующие годы целесообразно скопировать на съемные оптические носители и удалить из действующих ИСПДн.

Обезличивание является наиболее приемлемым способом снижения затрат на защиту персональных данных в интегрированных многофункциональных ИСПДн и распределенных ИСПДн, использующих для обмена данными сети общего пользования.

Обезличивание небольших по объему баз данных может осуществляться вручную. Для обезличивания больших объемов персональных данных целесообразно формировать специальные SQL-запросы.

Наиболее просто обезличить ИСПДн, в которых Ф. И. О. использовались только в качестве логинов или паролей для доступа пользователей к информационным системам. В этом случае достаточно изменить способ формирования идентификационных данных. Функциональность и порядок использования таких обезличенных информационных систем полностью сохраняются.

Возможен также универсальный способ обезличивания и последующей эксплуатации недоступных для самостоятельной модернизации ИСПДн, которые позволяют выводить предназначенные для распечатки бухгалтерские и иные документы в файл в формате MS Excel или MS Word для последующего редактирования. Он заключается в разработке несложной программы или макроса для автоматической обратной замены личных кодов на Ф. И. О. в выгруженных из ИСПДн для распечатки документах. Файлы кодификатора (таблицы

соответствия) Ф. И. О. и личных кодов могут быть легко сформированы путем выгрузки нужной формы из действующей ИСПДн и последующей ручной ее обработки, например, в Excel, с конвертированием в файлы требуемого формата.

Важными достоинствами указанного способа обезличивания ИСПДн, кроме универсальности, являются:

– сохранение функциональности и сервисного сопровождения обезличиваемых действующих ИСПДн без их программной модернизации;

– использование единого кодификатора Ф. И. О., содержащего персональные данные 3-й категории, для распечатки документов, выгружаемых из различных обезличиваемых ИСПДн;

– возможность децентрализованного использования кодификатора Ф. И. О. на отдельных АРМ;

– возможность редактирования и дополнения кодификатора Ф. И. О. средствами MS Office.

Понижение требований по защите персональных данных путем сегментирования информационных систем персональных данных

Сегментирование заключается в разделении сетевой ИСПДн на несколько сегментов для удовлетворения более низким требованиям и упрощения защиты персональных данных. Оно позволяет:

– децентрализовать обработку персональных данных 2-й категории и понизить класс сегментов ИСПДн до К3, если количество субъектов персональных данных превышает 1000 человек, или если они не принадлежат организации-оператору;

– уменьшить количество защищаемых АРМ в распределенных ИСПДн.

Данный способ на практике является одним из основных.

При сегментировании ИСПДн на взаимодействующие по сети подсистемы следует иметь в виду, что класс системы в целом равен наиболее высокому классу ее подсистем (сегментов). Поэтому простое разделение на ИСПДн подсистемы без ограничения их взаимодействия не снижает требования по защите персональных данных.

Простейшим способом ограничения взаимодействия сегментов является их физическое изолирование друг от друга. Альтернативным способом сегментирования является использование сертифицированных ФСТЭК России межсетевых экранов. Однако на практике оба эти способа сопряжены с приобретением дополнительного серверного оборудования и программного обеспечения и повышенными затратами на администрирование и технологическое сопровождение сегментированной ИСПДн. Поэтому наиболее целесообразно сегментировать слабо взаимодействующие подсистемы ИСПДн с обменом данными между ними с помощью съемных носителей.

Более эффективно осуществлять сегментирование до отдельных рабочих мест в сочетании с обезличиванием действующей ИСПДн. При этом затраты на эксплуатацию единой обезличенной ИСПДн не увеличиваются, а хранить кодификаторы Ф. И. О. (или их части) можно непосредственно на тех рабочих станциях, на которых персональные данные визуализируются. Если ИСПДн не является распределенной и не подключена к Интернету, то мероприятия по защите отдельных рабочих мест не потребуют больших затрат.

Наиболее сложной является защита персональных данных в распределенных ИСПДн. Поэтому пересылку персональных данных по сетям общего пользования целесообразно осуществлять только в обезличенном

виде, а обмен кодификаторами Ф. И. О. – курьерским способом. Это позволит избежать классификации и защиты распределенных ИСПДн.

Уменьшение требований к защите информации путем отключения ИСПДн от сетей общего пользования

Подключение ИСПДн к сетям общего пользования, в том числе Интернету, требует дополнительных средств защиты даже в том случае, если передача персональных данных по ним не предусмотрена. Для уменьшения требований и затрат на защиту информации целесообразно изолировать от Интернета все локальные сетевые ИСПДн.

Если персоналу необходим доступ в Интернет, то наиболее просто предусмотреть для этого дополнительные компьютеры (например, устаревшие), не подключая их к ИСПДн.

При невозможности размещения дополнительных рабочих станций требуются дополнительные сертифицированные ФСТЭК России средства защиты подключенных к Интернету персональных компьютеров, если они обрабатывают персональные данные.

Средства защиты информации (сертифицированная операционная система или специализированные средства) не должны разрешать одному и тому же зарегистрированному пользователю обрабатывать персональные данные и выходить в Интернет. Должны быть также разграничены разделы дисковой памяти и сменные носители информации. Выбор и настройка сертифицированных средств защиты информации могут осуществляться системными администраторами медицинских учреждений при консультировании со специалистами в области информационной безопасности. При этом один виртуальный пользователь (со своим логином и паролем) получает возможность выхода в

Интернет, а другой – работать с персональными данными. Этими пользователями может быть одно и тоже физическое лицо. По сравнению с выделенными АРМ, изолированными от Интернета, затраты на защиту персональных данных в нераспределенных ИСПДн 3-го класса для многопользовательских АРМ с разными правами пользователей увеличиваются незначительно.

Для уменьшения требований к защите информации типовые ИСПДн (системы бухгалтерского и кадрового учета 1С, Парус и др.) рекомендуется изолировать от сети Интернет. При обработке персональных данных в пределах организации такие системы, как правило, будут соответствовать нераспределенным ИСПДн класса К3. При этом лицензий ФСТЭК России[1] от оператора персональных данных не требуется, а защита данных осуществляется типовыми широко распространенными средствами.

Загрузку обновленных антивирусных баз данных, а также программ и форм персонифицированного учета и отчетности целесообразно осуществлять на других компьютерах, подключенных к сети Интернет. Безопасный перенос загруженных файлов в изолированные от Интернета локальные ИСПДн может осуществляться с использованием маркированных съемных носителей, в обязательном порядке проверяемых антивирусными средствами перед загрузкой в ИСПДн.

Официально распространяемые территориальными органами ФНС России и Пенсионного фонда России программы при соблюдении требований информационной безопасности в изолированных ИСПДн класса К3 могут использоваться при подготовке данных персонифицированного учета. При этом сформированные данные персонализированного учета должны выгружаться

[1] Лицензия на деятельность по технической защите конфиденциальной информации.

из ИСПДн на съемные маркированные носители. Незащищенная пересылка по сети Интернет данных, содержащих Ф. И. О. физических лиц, недопустима! Исключение могут составлять сведения, идентифицирующие работников только по ИНН, личному коду пенсионного страхования и другим кодам, без передачи Ф. И. О. физических лиц.

Обеспечение обмена персональными данными

Обмен персональными данными с помощью маркированных съемных носителей – не очень удобный, но менее затратный способ защищенного информационного взаимодействия.

Для обеспечения необходимого информационного взаимодействия по сети Интернет (в том числе пересылки электронных платежных документов, данных персонализированного налогового учета и др.) рекомендуется использовать выделенные автоматизированные рабочие места, которые не подключены к локальным сетевым ИСПДн. При этом повышенные требования и необходимость использования дополнительных сертифицированных средств защиты пересылаемых данных распространяются только на соответствующие АРМ.

Перенос персональных данных между взаимодействующими по сети Интернет выделенными АРМ и локальными ИСПДн целесообразно осуществлять с помощью маркированных съемных носителей. Это не очень удобный, но менее затратный способ защищенного информационного взаимодействия. В противном случае необходимо дополнительно использовать дорогостоящие сертифицированные межсетевые экраны.

С целью защиты персональных данных при передаче по каналам связи участниками информационного обмена

применяются средства криптографической защиты информации (СКЗИ), сертифицированные в установленном порядке.

Так, допускается представление сведений по форме № 2-НДФЛ с привлечением специализированных средств и операторов связи, осуществляющих передачу данных по телекоммуникационным каналам связи от налоговых агентов в налоговые органы. При этом налоговый агент и налоговый орган обеспечивают хранение данных в электронном виде в установленном порядке.

Аналогичные возможности предоставляют территориальные органы Пенсионного фонда РФ. При этом необходимо соблюдать «Регламент обеспечения безопасности информации при обмене электронными документами в СЭД ПФР по телекоммуникационным каналам связи».

При этом также могут использоваться средства специализированных провайдеров (Контур-Экстерн, Такском и др.), которые позволяют отправлять юридически значимые электронные документы по установленным формам в налоговые органы и ПФР, а также в органы государственной статистики.

После определения способов понижения класса ИСПДн уполномоченная руководителем учреждения (оператора) комиссия оформляет акты классификации информационных систем персональных данных.[2]

Подготовка к проверкам законности обработки персональных данных

Роскомнадзор, ФСТЭК России и ФСБ России в рамках своей компетенции осуществляют плановые и внеплановые проверки законности и порядка обработки

[2] Форма акта приведена в разделе «Примерные формы локальных нормативных актов и документации».

персональных данных. Это предусмотрено регламентом проведения проверок при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных (плановые проверки Роскомназора можно посмотреть по адресу: http://rsoc.ru/plan-and-reports/contolplan/).

Проверка осуществляется в отношении операторов – государственных органов, муниципальных органов, юридических или физических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных.

О проведении плановой проверки оператор уведомляется не позднее чем в течение трех рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Роскомнадзора или ее территориального органа с уведомлением о вручении или иным доступным способом.

Внеплановые проверки проводятся по следующим основаниям:

– истечение срока исполнения оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных;

– поступление в Роскомнадзор или его территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:

– возникновение угрозы причинения вреда жизни, здоровью граждан;

– причинение вреда жизни, здоровью граждан;

– нарушение прав и законных интересов граждан действиями (бездействием) операторов при обработке их персональных данных;

– нарушение операторами требований законодательства о персональных данных и иных нормативных правовых актов в области персональных данных, а также о несоответствии сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

О проведении внеплановой выездной проверки оператор уведомляется Роскомнадзором или его территориальным органом не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом.

Должностные лица Роскомнадзора или его территориального органа в качестве приглашенных специалистов могут принимать участие в проверках ФСБ России, ФСТЭК России, правоохранительных органов и органов прокуратуры.

В ходе проведения проверки Роскомнадзор или его территориальный орган осуществляют следующие **мероприятия по контролю**:

а) рассмотрение документов оператора, включающих сведения:

– содержащиеся в уведомлении об обработке персональных данных, поступивших от оператора, и фактической деятельности оператора;

– о фактах, содержащих признаки нарушения законодательства Российской Федерации в области персональных данных, изложенных в обращениях граждан, и информации, поступившей в Роскомнадзор или его территориальный орган;

– о выполнении оператором предписаний об устранении ранее выявленных нарушений законодательства Российской Федерации в области

персональных данных. Данная проверка проводится в виде внеплановой проверки;

– о наличии у оператора письменного согласия субъекта персональных данных на обработку его персональных данных;

– о соблюдении требований законодательства Российской Федерации при обработке специальных категорий и биометрических персональных данных;

– о порядке и условиях трансграничной передачи персональных данных;

– о порядке обработки персональных данных, осуществляемой без использования средств автоматизации;

– о соблюдении требований конфиденциальности при обработке персональных данных;

– о фактах уничтожения оператором персональных данных субъектов персональных данных по достижении цели обработки;

– локальные акты оператора, регламентирующие порядок и условия обработки персональных данных;

– об иной деятельности, связанной с обработкой персональных данных.

б) исследование (обследование) информационной системы персональных данных в части, касающейся персональных данных субъектов персональных данных, обрабатываемых в ней.

Должностные лица Роскомнадзора или его территориального органа при проведении проверок вправе в пределах своей компетенции:

– выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области персональных данных;

– составлять протоколы об административном правонарушении или направлять в органы прокуратуры, другие правоохранительные органы материалы для

решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подследственностью;

– обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;

– использовать необходимую технику и оборудование, принадлежащие Роскомнадзору или его территориальному органу;

– запрашивать и получать необходимые документы (сведения) для достижения целей проведения мероприятия по контролю (надзору);

– получать доступ к информационным системам персональных данных;

– направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности предусмотрен запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства Российской Федерации в области персональных данных;

– требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

Примерный **перечень запрашиваемых документов**:

– учредительные документы оператора;

– копия уведомления об обработке персональных данных;

– положение о порядке обработки персональных данных;

– положение о подразделении, осуществляющем функции по организации защиты персональных данных;

– должностные регламенты лиц, имеющих доступ и (или) осуществляющих обработку персональных данных;

– план мероприятий по защите персональных данных;

– план внутренних проверок состояния защиты персональных данных;

– приказ о назначении ответственных лиц по работе с персональными данными;

– типовые формы документов, предполагающие или допускающие содержание персональных данных;

– журналы, реестры, книги, содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

– договоры с субъектами персональных данных, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных;

– выписки из ЕГРЮЛ, содержащие актуальные данные на момент проведения проверки;

– приказы об утверждении мест хранения материальных носителей персональных данных;

– письменное согласие субъектов персональных данных на обработку их персональных данных (типовая форма);

– распечатки электронных шаблонов полей, содержащие персональные данные;

– справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка персональных данных;

– заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке (проверяется только наличие данных документов);

– приказ о создании комиссии и акты проведения классификации информационных систем персональных данных (проверяется только наличие данных документов);

– журналы (книги) учета обращений граждан (субъектов персональных данных);

– акт об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения цели обработки);

– иные документы, отражающие исполнение оператором требований законодательства Российской Федерации в области персональных данных.

Акт по результатам проверки может содержать одно из следующих заключений:

– об отсутствии нарушений требований законодательства Российской Федерации в области персональных данных;

– о выявленных нарушениях требований законодательства Российской Федерации в области персональных данных, с указанием конкретных статей и (или) пунктов нормативных правовых актов.

Наличие и соблюдение персоналом требуемых распорядительных документов и инструкций является необходимым условием для обеспечения информационной безопасности и конфиденциальности персональных данных.

Порядок обработки персональных данных, осуществляемой без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с законодательством Российской Федерации и «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687 (ТРЕБОВАНИЯ ПОСТАНОВЛЕНИЯ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 17.11.2007 № 781 НЕ ПРИМЕНЯЮТСЯ).

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

– определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

– обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

– соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливается оператором в соответствии с требованиями, предъявляемыми указанными правовыми актами.

Порядок проведения аттестационных (сертификационных) испытаний

Аттестационные (сертификационные) испытания проводятся организациями, имеющими необходимые лицензии ФСТЭК России. При этом под аттестацией понимают комплекс мер, позволяющих привести информационную систему в соответствие с требованиями по безопасности информации к заявленному классу, изложенными в нормативных методических документах ФСТЭК России.

Аттестационные (сертификационные) испытания содержат в себе анализ уже имеющихся на объекте информационных систем персональных данных, а также вновь принятых решений по обеспечению безопасности информации и включают проверку:

– организационно-режимных мероприятий по обеспечению защиты информации;

– защищенности информации от утечек по техническим каналам (ПЭМИН);

– защищенности информации от несанкционированного доступа.

По результатам аттестационных испытаний принимается решение о выдаче «Аттестата соответствия» информационной системы заявленному классу по требованиям безопасности информации. Аттестат выдается сроком на 3 года.

Перечень локальных нормативных актов организации, организационно-распорядительных документов, необходимых для обеспечения исполнения требований по обработке и защите персональных данных в информационных системах персональных данных[3]

Локальные нормативные акты

– Положение о персональных данных в организации. Утверждается приказом руководителя организации.

– Перечень информационных систем персональных данных. Может включать в себя (в виде полей таблиц) перечень категорий ПДн и перечень категорий субъектов ПДн. Утверждается приказом. Может указывать ИСПДн, обрабатываемые с использованием и без использования средств автоматизации. Перечень ПДн, обрабатываемых без использования средств автоматизации, может являться отдельным документом.

– Перечень категорий ПДн и перечень категорий субъектов ПДн (при отсутствии в перечне ИСПДн) для каждой ИСПДн.

– Акт классификации ИСПДн для каждой ИСПДн. Составляется и утверждается в порядке и по форме, утвержденной совместным приказом ФСТЭК, ФСБ и Мининформсвязи № 55/86/20 от 13.02.2008 г.

[3] Список локальных нормативных актов и документов может различаться в зависимости от видов обработки ПДн, объемов ПДн, размера организации и т. д.

– Уведомление уполномоченного органа по защите прав субъекта ПДн (РСОК). Направляется в РСОК до начала обработки.

– Должностные инструкции администратора безопасности. Должность может называться по-другому. Утверждаются приказом руководителя организации.

– Приказ с поименным списком лиц, утвержденный руководителем организации, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей.

– Журнал учета допуска к работе в ИСПДн (учет логинов).

– Инструкция по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

– Регламент «О порядке действий организации при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных». Утверждается приказом руководителя организации. К данному регламенту могут быть разработаны формы: уведомления субъекта ПДн об уничтожении ПДн, уведомления субъекта о блокировании ПДн, уведомления субъекта ПДн о прекращении обработки ПДн, уведомления в РОСК об устранении нарушений. Утверждаются приказом руководителя организации.

– Форма заявления согласия субъекта ПД на обработку ПДн. в случаях, определенных законом. Может быть как в виде самостоятельного документа, так и в виде части договора. Утверждается приказом руководителя организации.

– Порядок взаимодействия с третьими лицами при передаче ПДн для обработки. Основан на ч. 4 ст. 6 ФЗ152 и ст. 10 ПП РФ № 781. Заключается в введении существенного условия договора. Исполнение обязательно (наличие желательно).

– Регламент получения согласия субъекта на обработку ПДн субъекта. Может быть закреплено в положении либо в иных документах (наличие желательно).

– Регламент направления (приказ об утверждении форм) уведомления субъекта ПДн об уничтожении ПДн, уведомления субъекта о блокировании ПДн, уведомления субъекта ПДн о прекращении обработки ПДн. Может быть закреплено в положении либо в иных документах (наличие желательно).

– Раздел по конфиденциальности ПДн в трудовом договоре.

– Раздел по конфиденциальности ПДн в гражданско-правовом договоре.

– Должностные инструкции ответственного за ИБ организации.

– Должностные инструкции администратора информационной системы ПДн.

– Раздел в должностных инструкциях работников, осуществляющих обработку ПДн (пользователи ИСПДн).

– Регламент расследования инцидентов безопасности персональных данных.

– Регламент присвоения прав доступа к ИСПДн.

Организационно-распорядительные, технические и иные документы

– Инструкция по организации антивирусной защиты (составляется самостоятельно).

– Инструкция по организации парольной защиты (составляется самостоятельно).

– Акт обследования ИСПДн органом по аттестации.

– Технический паспорт на каждую ИСПДн. Включает в себя перечень ОТСС, ВТСС, структуру, топологию и размещение ОТСС, схему электропитания и заземления, перечень СЗИ, перечень программных средств, сведения об аттестации, результаты периодического контроля).

– Частная модель угроз на каждую ИСПДн (составляется самостоятельно).

– Сертификаты на используемые технические и программные средства защиты.

– Техническое задание на внедрение СЗ ИСПДн (не является обязательным).

– Акт приемки-сдачи системы защиты (СЗ) ИСПДн. Подписывается лицензиатом ФСТЭК (организацией, осуществлявшей работы по внедрению СЗ ИСПДн) и оператором.

– Акт о вводе в эксплуатацию (СЗ) ИСПДн.

– Аттестат соответствия требованиям по безопасности информации.

РЕКОМЕНДАЦИИ
по подготовке некоторых документов, регламентирующих обработку персональных данных в медицинских учреждениях

Приказ о создании комиссии по защите персональных данных с наделением ее полномочиями по проведению мероприятий, касающихся организации защиты персональных данных

В комиссию рекомендуется включать руководителей или полномочных представителей всех структурных подразделений учреждения, обрабатывающих персональные данные. Председателем комиссии целесообразно назначить заместителя руководителя учреждения. При необходимости вместо создания отдельной комиссии по защите персональных данных могут быть расширены состав и полномочия комиссии по защите сведений, составляющих государственную тайну.

Приказ об утверждении Положения об обработке и защите персональных данных

В Положении рекомендуется отразить следующее.

1. **Общие положения**, в том числе:

– предмет Положения (например, порядок получения, обработки и гарантии конфиденциальности персональных данных физических лиц, необходимых для осуществления деятельности в соответствии с Федеральным законом Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных», нормативными правовыми актами Российской Федерации в области трудовых отношений и здравоохранения, нормативными и распорядительными документами Минздравсоцразвития);

– цель и задачи обработки персональных данных учреждения в области защиты персональных данных (например, обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных работников, пациентов ЛПУ, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных);

– понятие и состав персональных данных (персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, профессия, доходы, другая информация, определяемая нормативными правовыми актами Российской Федерации в области трудовых отношений и здравоохранения, нормативными и распорядительными документами Минздравсоцразвития, Положением об обработке и защите персональных данных и приказами *(Наименование организации)*;

– кто является оператором персональных данных (например, *(Наименование организации*; Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений);

2. **Порядок получения и обработки персональных данных**, в том числе:

– как происходит получение персональных данных (получение персональных данных осуществляется в соответствии с нормативными правовыми актами Российской Федерации в области трудовых отношений и здравоохранения, нормативными и распорядительными документами Минздравсоцразвития, Положением об

обработке и защите персональных данных и приказами учреждения на основе согласия субъектов на обработку их персональных данных. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц. Согласия субъекта персональных данных, предусмотренного частью 1 настоящей статьи, не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением следующих случаев:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные являются общедоступными;

3) персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской

деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима в связи с осуществлением правосудия;

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации,

– как они обрабатываются и используются (обработка и использование персональных данных осуществляется только в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативными правовыми актами Российской Федерации. Не допускается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы. В случае увольнения субъекта персональных данных или иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, оператор обязан незамедлительно прекратить обработку персональных

данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями оператора);

– в каких структурных подразделениях и на каких носителях (бумажных, электронных) накапливаются и хранятся эти данные (персональные данные могут храниться в бумажном и (или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативными правовыми актами Российской Федерации мер по защите персональных данных. Право на обработку персональных данных предоставляется работникам структурных подразделений и (или) должностным лицам, определенным Положением об обработке и защите персональных данных, распорядительными документами и иными письменными указаниями оператора. Также целесообразно привести в приложении к приказу об утверждении Положения укрупненный перечень персональных данных и перечень структурных подразделений и (или) отдельных должностей, имеющих право на их обработку).

3. Права, обязанности и ответственность субъекта персональных данных и оператора при обработке персональных данных, в том числе:

– Права субъекта персональных данных в целях обеспечения защиты своих персональных данных (в целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных» за исключением случаев,

предусмотренных данным Федеральным законом, имеет право:

- на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;
- требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;
- на обжалование действий или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке).

– Обязанности оператора при сборе персональных данных:

- оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту

персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы;

– в случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя;
– в случае отзыва субъектом персональных данных согласия на обработку своих

персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

– Права оператора на передачу персональных данных третьим лицам (оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации).

– Ответственность оператора за разглашение персональных данных (оператор, а также должностные лица, виновные в нарушении требований законодательства РФ, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц оператора, обрабатывающих персональные данные).

Типовой раздел по конфиденциальности ПДн в гражданско-правовом договоре

1. В случае если исполнение обязательств по настоящему договору сопряжено с необходимостью

передачи сторонами друг другу каких-либо сведений, содержащих персональных данные физических лиц, являющихся полномочными представителями сторон, то сторона, получившая такие сведения обязана:

– соблюдать требования федеральных законов и иных нормативных правовых актов в сфере обеспечения конфиденциальности и безопасности персональных данных физических лиц;

– не использовать полученные персональные данные в целях, не связанных с исполнением обязательств по настоящему договору.

2. За нарушение условий пункта 1 стороны несут ответственность в соответствии с федеральным законодательством РФ.

Типовой раздел по конфиденциальности ПДн в трудовом договоре

1.1. Работник обязуется:

1.1.1. Соблюдать требования федеральных законов, иных нормативных правовых актов, Положения об организации работы с персональными данными в МИАЦ и прочих локальных нормативных актов работодателя в сфере обеспечения конфиденциальности и безопасности персональных данных физических лиц.

1.1.2. Не допускать распространения в устной или письменной форме персональных данных физических лиц, в том числе работников работодателя, доступ к которым будет получен работником в связи с исполнением им своих должностных обязанностей.

1.1.3. Сообщать своему непосредственному руководителю и лицу, ответственному за информационную безопасность у работодателя, обо всех ставших известными работнику фактах получения третьими лицами несанкционированного доступа либо

попытки получения доступа к персональным данным работников либо иных физических лиц, персональные данные которые обрабатываются у работодателя.

1.1.4. Использовать информацию о персональных данных физических лиц, ставшую известной работнику в силу трудовой деятельности у работодателя, исключительно для целей, связанных с выполнением своих трудовых функций у работодателя.

1.1.5. При прекращении действия данного договора все носители информации, содержащие персональные данные физических лиц (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении работника в связи с выполнением должностных обязанностей, передать лицу, ответственному за информационную безопасность у работодателя и/или непосредственному руководителю (в зависимости от организационной структуры работодателя).

1.1.6. Об утрате или недостаче носителей информации, содержащей персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений немедленно сообщать лицу, ответственному за информационную безопасность у работодателя и/или непосредственному руководителю (в зависимости от организационной структуры работодателя).

1.1.7. Использовать переданные ему работодателем и установленные на рабочем месте технические средства обработки и передачи информации исключительно для выполнения обязанностей, предусмотренных настоящим договором.

1.2. Работодатель предоставляет работнику необходимые условия для выполнения требований по обеспечению конфиденциальности и безопасности

персональных данных, к которым допускается работник: знакомит работника под роспись с требованиями Положения об организации работы с персональными данными в МИАЦ, должностной инструкции и прочих локальных нормативных актов работодателя в сфере обеспечения конфиденциальности и безопасности персональных данных, предоставляет хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т. п.), обучает правилам эксплуатации средств защиты информации и др., определяемых обязанностями, выполняемыми работником.

1.3. Работодатель оставляет за собой право, но не принимает каких-либо обязательств контролировать надлежащие использование работником технических средств обработки и хранения информации, соблюдение им мер по обеспечению конфиденциальности.

1.4. Работник подтверждает, что не имеет никаких обязательств перед какими-либо физическими или юридическими лицами, которые входят в противоречие с настоящим договором или которые ограничивают его трудовую деятельность в соответствии с настоящим договором.

1.5. Работнику известно, что разглашение информации о персональных данных физических лиц, ставшей ему известной в период действия настоящего договора, использование такой информации иными способами в нарушение требований федеральных законов, иных нормативных правовых актов, в т. ч. локальных нормативных актов работодателя, может повлечь дисциплинарную, материальную, административную, гражданско-правовую и уголовную ответственность в порядке, установленном федеральными законами.

1.6. Отсутствие контроля со стороны работодателя за надлежащим использованием работником своих обязанностей в области обеспечения конфиденциальности

и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной федеральным законодательством и настоящим договором ответственности.

Приказ(ы) о возложении персональной ответственности за защиту персональных данных

В приказе рекомендуется привести список должностных лиц, ответственных за защиту информационных систем и групп обрабатываемых в учреждении персональных данных.

Разрешительные документы о допуске конкретных сотрудников к обработке персональных данных

Приказы или иные утвержденные руководством учреждения разрешительные документы должны включать списки сотрудников оператора и временно привлекаемых лиц, допущенных к обработке укрупненных групп персональных данных. Работа с персональными данными лиц, не включенных в разрешительные документы, не допускается.

Уведомление об обработке персональных данных

В соответствии со статьей 22 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказами Роскомнадзора и утвержденной формой уведомления, размещенными на его официальном сайте *www.rsoc.ru*, уведомление об обработке персональных данных до начала обработки должно быть направлено в соответствующее территориальное подразделение Роскомнадзора.

В соответствии с приведенными законодательными и нормативными актами уведомление должно содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных.

Если обработка персональных данных смешанная, то в уведомлении описание мер и средств обеспечения безопасности персональных данных рекомендуется осуществлять для автоматизированного и неавтоматизированного способов обработки с указанием соответствующих категорий персональных данных.

В случае изменений оператор обязан уведомить соответствующее территориальное подразделение Роскомнадзора в течение десяти рабочих дней с даты возникновения изменений.

Без уведомления оператор вправе осуществлять обработку персональных данных:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующим общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

4) являющихся общедоступными персональными данными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской

Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Должностные инструкции сотрудников, имеющих отношение к обработке персональных данных

Должностные инструкции сотрудников учреждения, дополненные положениями о необходимости соблюдения утвержденного положения об обработке и защите персональных данных и инструкции о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

Журнал обращений по ознакомлению с персональными данными

Журнал рекомендуется вести в каждом структурном подразделении в произвольной форме. В журнале необходимо фиксировать все обращения субъектов персональных данных (дата, Ф. И. О., адрес) по ознакомлению с их персональными данными, дату направления запрашиваемых данных почтовой связью или предоставления лично заявителю. В случае отзыва данных субъектом персональных данных или выявления их несоответствия, в журнале должны быть сделаны соответствующие записи. По каждому обращению необходимо указывать, когда и каким образом на него отреагировали. Хранение журналов должно исключать несанкционированный доступ к ним.

Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

В инструкции рекомендуется отразить следующее.

1. **Общие положения**, в том числе:

– предмет инструкции (например, обязательные для всех структурных подразделений учреждения требования по обеспечению конфиденциальности документов, содержащих персональные данные);

– определение персональных данных (персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, день и место рождения, адрес, семейное, социальное, имущественное положение, профессия, доходы, другая информация).

– когда обеспечение конфиденциальности персональных данных не требуется (в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных);

– необходимость согласия субъекта персональных данных или наличие иного законного основания на их обработку.

Согласие субъекта персональных данных не требуется на обработку данных:

- в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;

- адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
- данных, включающих в себя только фамилии, имена и отчества;
- в целях однократного пропуска на территорию или в иных аналогичных целях;

– порядок ведения перечней персональных данных (например, в структурных подразделениях учреждения формируются и ведутся перечни конфиденциальных данных с указанием регламентирующих документов, мест хранения и ответственных за хранение и обработку данных. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается);

– нормативные документы, определяющие основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных и использования средств автоматизации *(основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями 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» и от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее);*

– общие правила хранения и передачи персональных данных (например, запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных. Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается. Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках);

– ответственность за защиту обрабатываемых персональных данных (например, сотрудники подразделений «учреждения», сотрудники организаций-операторов или лица, осуществляющие такую обработку по договору с оператором, а также иные лица, осуществляющие обработку или хранение конфиденциальных данных в учреждении, несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами);

– порядок ознакомления с инструкцией (например, сотрудники подразделений учреждения и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей инструкцией).

2. **Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации**, в том числе:

– условия хранения персональных данных (например, обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним

доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающему одновременное копирование иных персональных данных, не подлежащих распространению и использованию).

– использование типовых форм документов и журналов учета (при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и

журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации,

запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор);

– порядок уничтожения или обезличивания персональных данных (уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными).

3. Порядок обеспечения безопасности при обработке и хранении персональных данных,

осуществляемыми с использованием средств автоматизации, в том числе:

– правила доступа, хранения и пересылки персональных данных (например, безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в помещениях, где осуществляется обработка персональных данных, посторонних лиц. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа или под чужими или общими (одинаковыми) паролями запрещается. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернету, запрещается).

– общие требования по защите персональных данных в автоматизированных системах (например, технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим

защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание системы защиты персональных данных),

– специфические требования по защите персональных данных в отдельных автоматизированных системах (например, специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации).

4. Порядок учета, хранения и обращения со съемными носителями персональных данных, «твердыми» копиями и их уничтожении, в том числе:

– организация учета носителей персональных данных (например, все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учету. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер. Учет и выдачу съемных носителей персональных данных по форме осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Сотрудники учреждения получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета;

– правила использования съемных носителей персональных данных (например*, запрещается:*

– хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах либо

оставлять их без присмотра или передавать на хранение другим лицам;

– выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения).

– порядок действий при утрате или уничтожении съемных носителей персональных данных (например, о фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт[4]).

[4] Форма акта приведена в разделе «Примерные формы локальных нормативных актов и документации».

При осуществлении обработки персональных данных с использованием средств автоматизации для каждой информационной системы персональных данных должен быть назначен администратор, а для системы высоких классов – также администратор системы безопасности. Инструкции для этого должностного лица составляются отдельно. Для технического обслуживания оборудования должен быть предусмотрен соответствующий обслуживающий персонал.

В зависимости от класса системы и ее характеристик инструкции обслуживающего персонала (включая администраторов систем) и пользователей будут существенно различаться. Применительно к нераспределенным информационным системам класса К3 в инструкции пользователя и инструкции администратора по обеспечению мониторинга защиты информации и антивирусного контроля рекомендуется отразить следующее.

Инструкция пользователя при обработке персональных данных на объектах вычислительной техники (характерна для ИСПДн 3-го нераспределенного класса)

В инструкции рекомендуется отразить следующее.

1. **Общие положения**, в том числе:

– предмет инструкции (например, основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) учреждения);

– общие требования к пользователю (например, пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ. Пользователь при выполнении

работ в пределах своих функциональных обязанностей обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ, и несет персональную ответственность за соблюдение требований руководящих документов по защите информации).

2. **Обязанности пользователя**, например:

– выполнять общие требования по обеспечению режима конфиденциальности персональных данных, установленные в настоящей инструкции;

– при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами;

– соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

– после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня произвести стирание остаточной информации с жесткого диска ПЭВМ;

– оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

– не допускать «загрязнение» ПЭВМ посторонними программными средствами;

– знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий;

– помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

– знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;

– при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов;

– при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции;

– в случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

3. **Запрещаемые действия**, например**:**

– записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

– удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

– самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

– самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

– осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

– сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

– отключать (блокировать) средства защиты информации;

– производить какие-либо изменения в подключении и размещении технических средств;

– производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;

– оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

4. **Права пользователя ПЭВМ**, например:

– обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;

– обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации;

5. **Ответственность пользователей ПЭВМ**, например, за:

– надлежащее выполнение требований настоящей инструкции;

– соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

– сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;

– сохранность персональных данных.

Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных

В инструкции рекомендуется отразить следующее.

1. **Общие положения**, определяющие предмет инструкции, например:

Порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации учреждения.

2. **Мониторинг аппаратного обеспечения**, например:

Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих

персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

3. **Мониторинг парольной защиты**, например:

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

– установление сроков действия паролей (не более 3 месяцев);

– периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

4. **Мониторинг целостности**, например:

Мониторинг целостности программного обеспечения включает следующие действия:

– проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;

– обнаружение дубликатов идентификаторов пользователей;

– восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. **Мониторинг попыток несанкционированного доступа**, например:

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с

использованием средств операционной системы и специальных программных средств и предусматривает:

– фиксацию неудачных попыток входа в систему в системном журнале;

– протоколирование работы сетевых сервисов;

– выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

6. **Мониторинг производительности**, например:

Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

7. **Системный аудит**, например:

Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующем специально составленному списку для проверки.

Обзоры безопасности должны включать:

– отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля,

неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;

– проверку содержимого файлов конфигурации на соответствие списку для проверки;

– обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

– проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

– проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

– проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, которого касается изменение; выслушиванием претензий в случае, если это изменение причинило кому-нибудь вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

8. **Антивирусный контроль**, например:

Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

– резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

– утилиты для обнаружения и анализа новых вирусов.

К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно

после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т. п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

– осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;

– проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

– отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;

– немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т. д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

9. **Анализ инцидентов**, например:

Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

– факт попытки несанкционированного доступа (НСД);

– продолжается ли НСД в настоящий момент;

– кто является источником НСД;

– что является объектом НСД;

– когда происходила попытка НСД;

– как и при каких обстоятельствах была предпринята попытка НСД;

– точка входа нарушителя в систему;

– была ли попытка НСД успешной;

– определить системные ресурсы, безопасность которых была нарушена;

– какова мотивация попытки НСД.

Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

При анализе системных журналов администратору необходимо произвести следующие действия:

– проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;

– проверить не уничтожен ли системный журнал и нет ли в нем пробелов;

– просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;

– проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;

– проверить наличие мест в журналах, которые выглядят необычно;

– выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;

– выявить наличие неудачных попыток входа в систему.

В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

– проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;

– проверить не уничтожен ли системный журнал и нет ли в нем пробелов;

– проверить наличие мест в журналах, которые выглядят необычно;

– выявить попытки изменения таблиц маршрутизации и адресных таблиц;

– проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

– составить базовую схему того, как обычно выглядит система;

– провести поиск подозрительных файлов, скрытых файлов, имен файлов и каталогов, которые обычно используются злоумышленниками;

– проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;

– проверить целостность системных программ;

– проверить систему аутентификации и авторизации.

В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и разработка частной модели угроз[5]

Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) разработана ФСТЭК России на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, с учетом действующих нормативных документов ФСТЭК России по защите информации.

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В соответствии со статьей 19 Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных

[5] Основана на МЕТОДИКЕ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ, утвержденной заместителем директора ФСТЭК России 14 февраля 2008 г. http://www.fstec.ru/_razd/_ispo.htm

действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн либо потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Рекомендуемый подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 1.

Таблица 1

Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
распределенная ИСПДн,	-	-	+

которая охватывает несколько областей, краев, округов или государство в целом;			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	-	-	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	-	+	-
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	-	+	-
локальная ИСПДн, развернутая в пределах одного здания	+	-	-
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	-	-	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	-	+	-
ИСПДн, физически отделенная от сети общего пользования	+	-	-
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	-	-
запись, удаление, сортировка;	-	+	-
модификация, передача	-	-	+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеет	-	+	-

доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн; ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн; ИСПДн с открытым доступом	- -	- -	+ +
5. По наличию соединений с другими базами ПДн иных ИСПДн: интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн); ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	- +	- -	+ -
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т. д.);	+	-	-
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	-	+	-

ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т. е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	-	-	+
7.По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю БД с ПДн;	-	-	+
ИСПДн, предоставляющая часть ПДн;	-	+	-
ИСПДн, не предоставляющая никакой информации	+	-	-

Исходная степень защищенности определяется следующим образом:

– ИСПДн имеет ***высокий*** уровень исходной защищенности, если не менее 70 % характеристик ИСПДн соответствуют высокому уровню (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

– ИСПДн имеет ***средний*** уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70 % характеристик ИСПДн соответствуют уровню не ниже среднего (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

– ИСПДн имеет ***низкую*** степень исходной

защищенности, если не выполняется условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением:

$$Y = (Y_1 + Y_2) / 20.$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0 < Y < 0{,}3$, то возможность реализации угрозы признается низкой;

если $0{,}3 < Y < 0{,}6$, то возможность реализации угрозы признается средней;

если $0{,}6 < Y < 0{,}8$, то возможность реализации угрозы признается высокой;

если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, показанными в таблице 2.

Таблица 2

Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Таблица 3

Форма таблицы частной модели угроз

Наименование угрозы	Вероятность реализац	Возможность	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе

	ии угрозы (Y_2)	реализации угрозы (Y)			Технич ес-кие	Органи за-ционные

Для классификации и защиты информационных систем персональных данных медицинские учреждения, не располагающие необходимыми специалистами и лицензиями, могут обратиться на договорных условиях за методической и консультационной поддержкой в организации, имеющие соответствующие лицензии.

Государственный реестр сертифицированных средств защиты информации и реестр лицензиатов по ТЗКИ размещены на сайте ФСТЭК России www.fstec.ru.

Специализированным организациям могут быть поручены:

1) Методическая поддержка и консультирование при проведении сегментирования интегрированных информационных систем, определении состава и классификации информационных систем, обрабатывающих персональные данные.

2) Консультирование и помощь в формировании перечня организационно-технических мероприятий, необходимых для создания системы защиты информационных систем, обрабатывающих персональные данные.

3) Консультирование при подготовке декларации соответствия для систем класса К3.

4) Аудит информационных систем персональных данных, подбор и установка необходимых технических средств защиты информации для систем классов К2 и К1, а также распределенных информационных систем класса К3.

5) Подготовка, проведение аттестационных испытаний информационных систем классов К2 и К1 с выдачей аттестата соответствия.

При использовании перечисленных нормативных методических документов по защите персональных данных необходимо иметь в виду, что регулирующими органами могут вноситься уточнения и разъяснения, которые должны приниматься к исполнению всеми операторами информационных систем, обрабатывающими персональные данные.

Примерные формы локальных нормативных актов и документации

ИНСТРУКЦИЯ

Администратора *(ответственного за...)* информационной безопасности (эта должность может быть названа по-другому. Ее смысл – ответственный за ИБ в масштабах всей организации, и его обязанности шире, чем администратора вычислительной сети)

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ администратора информационной безопасности дата _____ № _____	УТВЕРЖДАЮ Директор _____ наименование организации _____Ф. И. О. _____дата

I. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности организации.

1.2. Администратор информационной безопасности является штатным сотрудником службы обеспечения информационной безопасности (либо СБ, если таковая отсутствует, ее не обязательно создавать, и нахождение в штате именно СБ не критично; важно, чтобы такой человек был персонально закреплен. В противном случае эти обязанности и ответственность возлагаются на первого руководителя).

1.3. Администратор информационной безопасности назначается приказом руководителя *(Наименование организации)* по представлению руководителя службы обеспечения информационной *безопасности (службы*

безопасности по представлению курирующего заместителя), согласованному с отделом автоматизации.

1.4. Прямыми служебными обязанности администратора информационной безопасности являются организация и реализация комплекса мер по обеспечению информационной безопасности в *(Наименование организации)* в объемах и в порядке, определенными федеральными законами, иными нормативными правовыми документами, регулирующими защиту конфиденциальной информации, безопасность и конфиденциальность персональных данных.

1.5. Администратор информационной безопасности обладает правами доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты.

1.6 Администратор несет ответственность за реализацию принятой в *(Наименование организации)* политики безопасности, закрепленной в концепции обеспечения информационной безопасности АС и планах защиты подсистем АС *(перечень этих документов может быть расширен либо сокращен в зависимости от принятой системы управления, однако он, безусловно, должен включать весь перечень документов, регулирующих защиту КИ и ПД в организации, включая и те документы, которые будут созданы на стадиях предпроектного обследования и внедрения системы защиты персональных данных).*

Примечание. Для данной единицы целесообразно предусмотреть совмещение обязанностей не только в части защиты ПДн, но и конфиденциальной информации в целом, если таковая (помимо ПДн) существует в организации.

II. Обязанности администратора информационной безопасности

2.1. Знать перечень установленных в подразделениях *(Наименование организации)* рабочих станций (автоматизированных систем) и перечень задач, решаемых с их использованием.

2.2. Знать схемы информационных потоков, циркулирующих в организации. Представлять топологию и архитектуру сети, взаимосвязь и степень участия в процессе обработки данных всех субъектов информационного обмена.

2.3. Знать перечень ИСПДн и баз данных, содержащих ПДн и обрабатываемых (находящихся в эксплуатации, находящихся в ведении) *(Наименование организации)*.

2.4. Своевременно подготавливать и представлять для утверждения руководителем *(Наименование организации)* акты классификации ИСПДн, обрабатываемых *(Наименование организации)*, а при изменении параметров, влияющих на класс ИСПДн, – проводить пересмотр класса ИСПДн.

2.5. До начала обработки ИСПДн подготавливать для утверждения руководителем *(Наименование организации)* уведомления в уполномоченный орган по защите прав субъектов персональных данных. При изменении правовых оснований обработки, категорий обрабатываемых ПДн, категорий субъектов обрабатываемых ПДн, способов обработки обязан в срок, не превышающий трех рабочих дней, пересматривать содержание соответствующих разделов уведомления.

2.6. Организовывать и обеспечивать:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

2.7. Организовывать реализацию следующих мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

2.8. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на РС АС *(Наименование организации)* технических средств защиты от НСД.

2.9. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных РС и серверов, устанавливать и осуществлять настройку средств защиты РС.

2.10. Периодически проверять состояние используемых СЗИ НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

2.11. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных РС.

2.12. Периодически проверять содержание электронного журнала обращений запросов пользователей информационной системы на получение персональных

данных, а также факты предоставления персональных данных по этим запросам.

2.13. Докладывать руководству службы обеспечения информационной безопасности *(руководителю службы безопасности, руководителю организации – в зависимости от принятой системы управления в организации)* об имевших место попытках несанкционированного доступа к информации и техническим средствам ПЭВМ.

2.14. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты от НСД, установленных на РС АС.

2.15. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

2.16. Участвовать в работе комиссий по пересмотру планов защиты.

Необходимо помнить, что непосредственно администратор вправе выполнять лишь те функции (действия) которые не являются частью деятельности, подлежащей обязательному лицензированию.

Поэтому в п. 2.7 обязанностей администратора внесена именно организация и реализация этих мероприятий законным способом, в т. ч. с привлечением к таким работам лицензиатов ФСТЭК и ФСБ в пределах их компетенции.

III. Права администратора информационной безопасности

3.1. Требовать от сотрудников, эксплуатирующих систему управления информационной безопасности, сотрудников, эксплуатирующих ИСПДн, выполнения инструкций по обеспечению безопасности и защите информации в АС.

3.2. Инициировать и проводить служебные проверки по фактам нарушения установленных требований

обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АС.

3.3. Обращаться непосредственно к руководителям технологических подразделений с требованием прекращения работы в АС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.4. Вносить руководству *(Наименование организации)* свои предложения по совершенствованию мер защиты информации, развитию системы управления информационной безопасностью.

IV. Ответственность главного администратора информационной безопасности

4.1. На администратора информационной безопасности возлагается персональная ответственность за бесперебойное функционирование программно-технических и криптографических средств защиты информации, средств вычислительной техники, информационно-вычислительных комплексов, сетей и автоматизированных систем обработки информации. Указанная ответственность закрепляется за ним приказом руководителя *(Наименование организации)*. (*При необходимости эта ответственность может выражаться в частичной и полной материальной ответственности с заключением соответствующего договора)*.

4.2. На администратора информационной безопасности возлагается персональная ответственность за качество, своевременность, эффективность и соответствие нормативным правовым документам в сфере защиты информации проводимых в *(Наименование организации)* работ по обеспечению защиты информации.

4.2. Администратор информационной безопасности несет дисциплинарную, административную, головную,

гражданско-правовую ответственность в соответствии с действующим законодательством за разглашение сведений, составляющих конфиденциальную информацию и ставших известными ему по роду работы.

Наименование должности _____ _____
дата Ф. И. О.

СОГЛАСОВАНО:
Сотрудник юридического отдела _____ _____
дата Ф. И. О.

С инструкцией ознакомлен: _____ _____
дата Ф. И. О.

Утверждено
Приказом
№___ от «__»_____20__г.

_____
Наименование должности

_____
Наименование организации

_____
Ф. И. О.

РЕГЛАМЕНТ
О порядке действий *(Наименование организации)* при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Настоящий регламент разработан на основании и во исполнение Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ, Федерального закона РФ «О порядке рассмотрения обращений граждан РФ» от 02.05.2006 № 59-ФЗ, а также положения «Об организации работы с персональными данными в *(Наименование организации)*, утвержденного приказом директора *(Наименование организации)* № ___ от _____г.

Целью настоящего регламента является:

– обеспечение прав субъектов персональных данных на доступ к их персональным данным, обрабатываемым *(Наименование организации)*;

– обеспечение прав уполномоченного органа по защите прав субъектов персональных данных на получение информации, необходимой ему для реализации полномочий по защите прав субъектов персональных данных;

– упорядочение действий сотрудников

(Наименование организации) при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

Настоящий регламент распространяется на должностных лиц и специалистов *(Наименование организации)*, которые в рамках исполнения своих должностных обязанностей осуществляют прием и регистрацию обращений (запросов) субъектов персональных данных, а также уполномоченного органа по защите прав субъектов персональных данных, ведут личный прием граждан, осуществляют рассмотрение обращений (запросов), подготовку и направление ответов на них.

Настоящий регламент подлежит применению исключительно в случаях обращений либо при получении запросов субъектов персональных данных или их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в рамках Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ.

1. Общие положения

1.1. Настоящий регламент использует следующие сокращения:

ПДн – персональные данные

ИСПДн – информационная система персональных данных

1.2. Субъект ПДн – это физическое лицо, определенное или определяемое на основании любой относящейся к нему информации.

1.3. Законный представитель субъекта ПДн – это гражданин, который в силу закона выступает во всех учреждениях и организациях от имени и в защиту личных и имущественных прав и законных интересов недееспособных, ограниченно дееспособных граждан либо

дееспособных, но в силу своего физического состояния (по старости, болезни и т. п.) не могущих лично осуществлять свои права и выполнять свои обязанности. В качестве законных представителей выступают родители, усыновители, опекуны и попечители.

1.4. Далее по тексту настоящего регламента под субъектом ПДн будет подразумеваться также законный представитель субъекта ПДн.

1.5. В соответствии со ст. 14 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ субъект ПДн имеет право:

– на получение сведений о *(Наименование организации)* как операторе ПДн, в т. ч. о месте ее нахождения;

– на получение сведений о наличии у *(Наименование организации)* как у оператора ПДн, относящихся к соответствующему субъекту ПДн;

– на ознакомление с такими ПДн;

– требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– на получение при обращении или при получении запроса информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки персональных данных *(Наименование организации)*, а также цель такой обработки;
- способы обработки персональных данных, применяемые *(Наименование организации)*;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных

данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

1.6. В соответствии со ст. 9 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ субъект ПДн имеет право отозвать свое согласие на обработку ПДн.

В соответствии со ст. 14, 20 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ *(Наименование организации)* как оператор ПДн в случае поступления соответствующего запроса от субъекта ПД обязан:

– Предоставить субъекту ПДн в доступной форме сведения о наличии его ПДн (при этом указанные сведения не должны содержать ПДн, относящиеся к другим субъектам ПДн).

– Сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, и другие сведения, право на получение которых субъектом ПДн предусмотрено ст. 14 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ.

– Предоставить возможность ознакомления с ПДн без взимания платы за это.

– Внести в ПДн необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет *(Наименование организации)*, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для

заявленной цели обработки, а также прекратить обработку ПДн и уничтожить их в случае отзыва субъектом ПДн согласия на обработку своих ПДн. О внесенных изменениях и предпринятых мерах *(Наименование организации)* обязан уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы; об уничтожении ПДн *(Наименование организации)* обязан уведомить субъекта ПДн.

1.8. В соответствии с п. 3 ч. 5 ст. 14 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ право субъекта ПДн на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц.

1.9. В целях реагирования на соответствующие запросы в сроки, предусмотренные федеральными законами, в *(Наименование организации)* используется автоматизированный механизм поиска и представления информации, необходимой для подготовки ответов субъектам ПДн и уполномоченному по защите прав субъектов ПДн органу. При этом запросы пользователей ИСПДн на получение ПДн, а также факты предоставления ПДн по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) *(Наименование организации)*.

2. Действия *(Наименование организации)* **при обращении субъекта ПДн.**

2.1. Для целей обеспечения исполнения *(Наименование организации)* своих обязанностей при обращении субъекта ПДн в *(Наименование организации)* устанавливаются следующие дни и часы для личного приема граждан: _____ _____.

2.2. Должностными лицами *(Наименование организации)*, осуществляющими личный прием граждан, являются: (указать соответствующие должности лиц руководящего состава, например:

– директор *(Наименование организации)*;

– заместитель директора *(Наименование организации)*

2.3. В соответствии с Федеральным законом РФ «О порядке рассмотрения обращений граждан РФ» от 02.05.2006 № 59-ФЗ при личном приеме гражданин предъявляет документ, удостоверяющий его личность.

2.4. В случае если при личном приеме от имени субъекта ПДн действует его законный представитель, должностное лицо *(Наименование организации)* обязано удостовериться в наличии у такого лица законных полномочий.

2.5. Содержание устного обращения заносится в карточку личного приема гражданина. Ответ на обращение с согласия гражданина может быть дан устно в ходе личного приема, а также гражданину предоставляется возможность ознакомления с его ПДн, о чем делается запись в карточке личного приема гражданина. При отсутствии возможности ознакомления субъекта с его ПДн немедленно при его личном обращении такая возможность должна быть предоставлена субъекту ПДн в течение десяти рабочих дней с даты обращения.

2.6. В том случае, когда при личном приеме гражданин изъявил желание получить ответ в письменной форме, должностное лицо, ведущее прием, предлагает гражданину оформить письменный запрос и сообщает ему о сроках, в течение которых *(Наименование организации)* обязан дать ответ на такой запрос в соответствии с федеральным законом (см. п. 3.11. настоящего регламента).

2.7. При наличии к тому волеизъявления гражданина письменный запрос может быть оформлен

непосредственно в ходе личного приема путем заполнения Формы 1 (приложение № 1 к настоящему регламенту).

2.8. Если при обращении субъекта ПДн будет установлено, что предоставление ПДн нарушает конституционные права и свободы других лиц, должностное лицо, осуществляющее личный прием гражданина, сообщает ему об отказе в предоставлении информации о ПДн либо таких ПДн, о чем делается запись в карточке личного приема гражданина. Также в срок, не превышающий семи рабочих дней со дня обращения, *(Наименование организации)* обязан направить в адрес субъекта ПДн мотивированный ответ в письменной форме, содержащий ссылку на положение п. 3 ч. 5 ст. 14 Федерального закона РФ «О персональных данных» от 27.07.2006 г. № 152-ФЗ.

3. Действия *(Наименование организации)* **при получении запроса субъекта ПДн.**

3.1. В соответствии с ч. 3 ст. 14 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя.

3.2. Прием и регистрация запросов субъектов ПДн, а также регистрация ответов, направляемых субъектам ПДн, ведутся в *(Наименование организации)* отдельно от приема и регистрации иной входящей и исходящей корреспонденции, в т. ч. запросов и требований органов, уполномоченных на осуществление государственного контроля (надзора) и муниципального контроля, и ответов на них.

3.3. В целях регистрации запросов субъектов ПДн и ответов на такие запросы в *(Наименование организации)*

осуществляется ведение журнала регистрации запросов субъектов ПДн.

3.4. Специалистами *(Наименование организации)*, осуществляющими прием и регистрацию запросов субъектов ПДн, а также регистрацию и направление ответов на такие запросы, являются: указать соответствующие должности лиц, например:

– секретарь;

– начальник канцелярии.

3.5. Должностными лицами *(Наименование организации)*, осуществляющими рассмотрение запросов субъектов ПДн и подготовку ответов на них, являются: указать соответствующие должности лиц руководящего состава, например:

– директор *(Наименование организации);*

– заместитель директора *(Наименование организации).*

3.6. При получении запроса (обращения) физического лица, специалист *(Наименование организации)*, ответственный за прием и регистрацию входящей корреспонденции в *(Наименование организации)*, непосредственно в день получения устанавливает:

3.6.1. отвечает ли такой запрос (обращение) обязательным требованиям к письменному обращению гражданина, установленным ст. 7 Федерального закона РФ «О порядке рассмотрения обращений граждан РФ» от 02.05.2006 № 59-ФЗ, а именно:

– адресован ли запрос в *(Наименование организации)* (содержит ли наименование адресата);

– содержит ли фамилию, имя, отчество (последнее при его наличии) гражданина;

– содержит ли почтовый адрес, по которому должен быть направлен ответ;

– имеется ли личная подпись и дата.

3.6.2. отвечает ли такой запрос (обращение) дополнительным требованиям, установленным ст. 14

Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ, к запросу субъекта ПДн, а именно:

– содержит ли он номер основного документа, удостоверяющего личность гражданина или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

– является ли содержанием запроса (обращения) требование о предоставлении гражданину информации или о выполнении *(Наименование организации)* действий, перечисленных в п. 1.5, 1.6. настоящего регламента.

3.7. В случае если при приеме запроса (обращения) физического лица будет установлено, что он содержит в себе все сведения, перечисленные в п. 3.6. настоящего регламента, следует сделать вывод о том, что такой запрос (обращение) является запросом субъекта ПДн. Такой запрос подлежит приему и регистрации в журнале регистрации запросов субъектов ПДн в тот же день.

3.8. В случае если при приеме запроса (обращения) физического лица будет установлено, что он не содержит в себе сведений, перечисленных в п. 3.6.2. настоящего регламента, следует сделать вывод о том, что такой запрос (обращение) не является запросом субъекта ПДн. Такой запрос подлежит приему и регистрации в порядке, предусмотренном *(Наименование организации)* для приема и регистрации прочей входящей корреспонденции.

3.9. В случае если при приеме запроса (обращения) физического лица будет установлено, что он не содержит в себе сведений, перечисленных в п. 3.6.1. настоящего регламента, такой запрос следует считать запросом субъекта ПДн; он подлежит приему и регистрации в журнале регистрации запросов субъектов ПДн в тот же день, однако в соответствии с ч. 1 ст. 11 Федерального закона РФ «О порядке рассмотрения обращений граждан РФ» от 02.05.2006 № 59-ФЗ ответ на такой запрос не

дается, о чем делается отметка в журнале регистрации запросов субъекта ПДн.

3.10. Запросы субъектов ПДн, зарегистрированные в соответствии с п. 3.7., 3.9. настоящего регламента, в день регистрации подлежат передаче должностному лицу *(Наименование организации)*, указанному в п. 3.5. настоящего регламента.

3.11. Должностные лица *(Наименование организации)*, указанные в п. 3.5. настоящего регламента, обязаны рассмотреть запрос субъекта ПДн и подготовить ответ на него в письменной форме в течение десяти рабочих дней с даты получения *(Наименование организации)* указанного запроса.

3.12. В случае если в запросе субъект ПДн изъявил желание ознакомиться со своими ПДн, возможность такого ознакомления должна быть предоставлена субъекту ПДн в течение десяти рабочих дней с даты получения *(Наименование организации)* указанного запроса.

3.13. Письменный ответ на запрос субъекта ПДн должен быть направлен в его адрес заказным письмом с уведомлением о вручении с соблюдением сроков, предусмотренных п. 3.11, 3.12. настоящего регламента.

3.14. Если при рассмотрении запроса субъекта ПДн будет установлено, что предоставление ПДн нарушает конституционные права и свободы других лиц, *(Наименование организации)* сообщает ему об отказе в предоставлении информации о ПДн либо таких ПДн, о чем в срок, не превышающий семи рабочих дней со дня получения запроса субъекта ПДн, в адрес субъекта ПДн направляется мотивированный ответ в письменной форме, содержащий ссылку на положение п. 3 ч. 5 ст. 14 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ.

3.15. Для обработки персональных данных, содержащихся в обращении в письменной форме субъекта ПД, дополнительного согласия не требуется.

4. Действия *(Наименование организации)* **при получении запроса уполномоченного органа по защите прав субъектов ПДн.**

4.1. Прием и регистрация запросов уполномоченного органа по защите прав субъектов ПДн осуществляется *(Наименование организации)* в порядке, установленном для приема и регистрации входящей корреспонденции.

4.2. При получении запроса уполномоченного органа по защите прав субъектов ПДн специалисты *(Наименование организации)*, ответственные за прием и регистрацию входящей корреспонденции, в тот же день осуществляют регистрацию такого запроса и передают его должностному лицу, указанному в п. 3.5. настоящего регламента.

4.3. *(Наименование организации)*, в лице своих должностных лиц, указанных в п. 3.5. настоящего регламента, сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, а также направляет требуемые им документы в течение семи рабочих дней с даты получения такого запроса.

4.4. В случае выявления уполномоченным органом по защите прав субъектов ПДн фактов недостоверности ПДн или неправомерных действий с ними, уточнение, блокирование или уничтожение таких ПДн осуществляется в порядке и сроки, предусмотренные п. 5.5.–5.9. настоящего регламента для соответствующих действий (операций) в отношении ПДн.

5. Действия *(Наименование организации)* **при получении требования субъекта ПДн об уточнении своих ПДн, их блокировании или уничтожении; в случае выявления при обращении или по запросу субъекта ПДн фактов недостоверности ПДн или**

неправомерных действий с ними; в случае отзыва субъектом ПДн согласия на их обработку.

5.1. При получении требований субъектов ПДн об уточнении своих ПДн, их блокировании, уничтожении прием и регистрация таких требований осуществляется в порядке, предусмотренном п. 3.6.–3.9. настоящего регламента.

5.2. Требования субъектов ПДн в тот же день передаются должностным лицам *(Наименование организации)*, указанным в п. 3.5.

5.3. Полномочные должностные лица *(Наименование организации)* вносят в ПДн субъекта необходимые изменения, уничтожают или блокируют соответствующие ПДн по предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет *(Наименование организации)*, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.4. О внесенных изменениях и предпринятых мерах *(Наименование организации)* обязан уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы.

5.5. В случае если факт недостоверности ПДн или неправомерных действий с ними будет выявлен при обращении или по запросу субъекта ПДн, *(Наименование организации)* обязан осуществить блокирование ПДн, относящихся к соответствующему субъекту ПДн, с момента такого обращения или получения такого запроса на период проверки.

5.6. В случае подтверждения факта недостоверности ПДн *(Наименование организации)* на основании документов, представленных субъектом ПДн,

или иных необходимых документов обязан уточнить ПДн и снять их блокирование.

5.7. В случае выявления неправомерных действий с ПДн *(Наименование организации)* в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения.

5.8. В случае невозможности устранения допущенных нарушений *(Наименование организации)* в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, обязан уничтожить ПДн.

5.9. Об устранении допущенных нарушений или об уничтожении ПДн *(Наименование организации)* обязан уведомить субъекта ПДн.

5.10. В случае отзыва субъектом ПДн согласия на обработку своих ПДн *(Наименование организации)* обязан прекратить обработку ПДн и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между *(Наименование организации)* и субъектом ПДн. Об уничтожении ПДн *(Наименование организации)* обязан уведомить субъекта ПДн.

Утверждаю
(Наименование должности руководителя)
(Наименование организации)
Ф. И. О.
«___» _____20__ г.

А К Т
проверки наличия носителей сведений конфиденциального характера за 20__ год

Комиссия в составе председателя – _____, и членов: _____ – произвела проверку носителей сведений конфиденциального характера, учтенных и находящихся в делопроизводстве *(Наименование организации)* за 20__ год.

Проверкой установлено, что все поступившие, разработанные и учтенные в специальном делопроизводстве носители сведений конфиденциального характера, другие материалы имеются в наличии, а именно:

– Дела с грифом «Коммерческая тайна» в соответствии с номенклатурами прошлых лет;

– Дела, книги и журналы учета в соответствии с номенклатурой дел на 20__ год от __.__.20__ № _____ с № _____ по _____;

– Входящие документы в соответствии с журналом регистрации документов № _____ с № 1 по № _____;

– Исходящие документы в соответствии с журналом регистрации документов № _____ с № 1 по № _____;

– Печати и штампы в соответствии с журналом учета № _____;

– Магнитные носители информации в соответствии с журналом учета № _____

Замечаний и нарушений по ведению делопроизводства нет.

Председатель комиссии

Члены комиссии:

Руководителю
(курирующему заместителю, уполномоченному лицу)
Наименование организации

ЗАЯВКА
на предоставление пользователю прав доступа
к ресурсу ИСПДн

_____

(наименование ресурса – ИСПДн, базы данных, справочной системы и т. п.)

№ п/п	Фамилия, имя, отчество	Должность	Имя ПК в домене	Права доступа		Время	
				Только чтение	Редактирование	Дни	Часы
1	2	3	4	5	6	7	8
1							

Руководитель структурного подразделения
Иванов И. И.
(фамилия, инициалы)

___.___.20__ № ____

«Разрешаю»
Руководитель
(курирующий заместитель, уполномоченное лицо)
Наименование организации
Петров П. П.

___.___.20___

«Согласовано»
Администратор службы ИБ

Сидоров С. С.

___.___.20___

Утверждаю

_____

«____»_____ _____ г.

АКТ
классификации информационной системы, обрабатывающей персональные данные

_____

наименование информационной системы

Комиссия в соответствии с приказом от ___ _____ ____ № _____ в составе:

Председатель:
Члены комиссии:

провела классификацию информационной системы *(наименование информационной системы)*, обрабатывающей персональные данные, и установила:

Выявленные определяющие признаки классификации типовой информационной системы:

– наивысшая категория обрабатываемых персональных данных (1, 2, 3);

– наличие сведений, составляющих государственную или служебную тайну;

– количество обрабатываемых субъектов персональных данных (диапазон);

– структура системы (автономная, локальная, распределенная);

– наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;

– режим обработки персональных данных (однопользовательский или многопользовательский);

– режим разграничения прав доступа пользователей информационной системы (без разграничения прав доступа или с разграничением прав);

– местонахождение технических средств информационной системы (в пределах Российской Федерации, частично или целиком за пределами Российской Федерации).

Комиссия на основании определяющих признаков классификации и в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных», а также с рекомендациями ФСТЭК России

РЕШИЛА:

присвоить информационной системе *наименование информационной системы,* обрабатывающей персональные данные, класс *К1, или К2, или К3, или специальный.*

Председатель

Члены комиссии

Пример формы учета
персональных данных

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых
в структурных подразделениях

_____

наименование учреждения

_____

наименование структурного подразделения

№ п/п	Наименование (вид, типовая форма) документов с персональными данными	Регламентирующие документы (Наименование, дата, номер)	Наименование информационной системы / без использования средств автоматизации	Отдел	Место хранения (комната)	Ф. И. О. ответственных за обработку и хранение
1						
2						
3						

_____ _____

Должность и Ф. И. О. начальника структурного подразделения — Подпись

_____ _____

Должность и Ф. И. О. ответственного за защиту персональных данных в структурном подразделении — Подпись

Пример формы журнала
учета съемных носителей

ЖУРНАЛ

учета съемных носителей персональных данных

наименование структурного подразделения

Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.
На _____ листах

_____ _____
Должность и Ф. И. О. ответственного за хранение Подпись

№ п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи инфор-мации	Подпись испол-нителя	Примечание*
1						
2						
3						
4						
5						

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными).

Пример акта

«УТВЕРЖДАЮ»

_____ _____

«___» _____ 20__ г.

АКТ
уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом _____ от __ _____ 20__ г. № __, в составе: *(должности, Ф. И. О.)* провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
1	2	3	4

Всего съемных носителей _____
(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т. п.).

Перечисленные съемные носители уничтожены

_____

путем (разрезания, демонтажа и т. п.),

_____

измельчены и сданы для уничтожения предприятию по утилизации вторичного сырья

_____ _____
Наименование предприятия Дата

Председатель комиссии _____ _____
Подпись Дата

Члены комиссии (Ф. И. О.) _____ _____
Подпись Дата

Зарегистрировано в Минюсте РФ 3 апреля 2008 г. № 11462

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ № 55

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ № 86

МИНИСТЕРСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ № 20

ПРИКАЗ от 13 февраля 2008 года

ОБ УТВЕРЖДЕНИИ ПОРЯДКА ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с пунктом 6 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением 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, часть II, ст. 6001), приказываем:

Утвердить
прилагаемый Порядок проведения
классификации информационных систем
персональных данных

Директор Федеральной службы
по техническому и экспортному контролю
С. И. ГРИГОРОВ

Директор Федеральной службы безопасности
Российской Федерации
Н. П. ПАТРУШЕВ

Министр информационных технологий и связи
Российской Федерации
Л. Д. РЕЙМАН

Утвержден
Приказом ФСТЭК России, ФСБ России,
Мининформсвязи России
от 13 февраля 2008 г. № 55/86/20

ПОРЯДОК ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящий порядок определяет проведение классификации информационных систем персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее – информационные системы) <*>.

<*> Абзац первый пункта 1 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 (Собрание законодательства Российской Федерации, 2007, № 48, часть II, ст. 6001) (далее – Положение).

2. Классификация информационных систем проводится государственными органами, муниципальными органами, юридическими и физическими лицами,

организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее – оператор) <*>.

<*> Абзац первый пункта 6 Положения.

3. Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

4. Проведение классификации информационных систем включает в себя следующие этапы:

– сбор и анализ исходных данных по информационной системе;

– присвоение информационной системе соответствующего класса и его документальное оформление.

При проведении классификации информационной системы учитываются следующие исходные данные:

– категория обрабатываемых в информационной системе персональных данных – Х пд;

– объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) – Х нпд;

– заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;

– структура информационной системы;

– наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;

– режим обработки персональных данных;

– режим разграничения прав доступа пользователей информационной системы;

– местонахождение технических средств информационной системы.

6. Определяются следующие категории обрабатываемых в информационной системе персональных данных (Х пд):

категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;

категория 4 – обезличенные и (или) общедоступные персональные данные.

7. Х нпд может принимать следующие значения:

1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 – в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов

персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

8. По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

– информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

– информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

9. По структуре информационные системы подразделяются:

– на автономные (не подключенные к иным информационным системам) комплексы технических и

программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);

– на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

– на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

10. По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

11. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

12. По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

13. Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

14. По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

15. Класс типовой информационной системы определяется в соответствии с таблицей.

Х пд \ Х нпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

16. По результатам анализа исходных данных класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 Постановления 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, часть II, ст. 6001.

17. В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

18. Результаты классификации информационных систем оформляются соответствующим актом оператора.

19. Класс информационной системы может быть пересмотрен:

– по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

– по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Список источников

1. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

2. Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

3. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

4. Методические документы ФСТЭК России;

5. Письмо Федерального агентства по образованию от 29.07.2009 № 17-110;

6. Письмо Федерального агентства по образованию от 22.10.2009 № 17-187;

7. Аналитическая справка от 30.09.09 о законности обработки ПДн МИАЦ и соответствии организационно-правовых мер по обеспечению безопасности ПДн и локальных нормативных актов МИАЦ требованиям Закона «О персональных данных», подготовленная ООО «НИЦ «ФОРС».

Нормативное производственно-практическое издание

Составители:
Никитин Максим Александрович
Лютов Дмитрий Анатольевич

Организация работ по защите персональных данных

Методические материалы для медицинских учреждений

Рецензент: Шмелев П. В.

Ответственный редактор Л. А. Молякова
Корректор Н. С. Глинская
Компьютерная верстка Л. М. Баева, Н. П. Селифонова

Подписано в печать 21.12.2009. Формат 60x84/16.
Бумага офсетная. Печать офсетная. Усл.-печ. л. 8,19
Тираж 500 экз. Заказ № ____
Отпечатано в типографии ООО «ДСМ Принт»
443070, г. Самара, ул. Верхне-Карьерная, 3а