Приложение 1
к Приказу №201 от 21.01.2014 г.

УТВЕРЖДАЮ

Главный врач
ММАУ «Городская поликлиника №14»

_____ **Г.А. Костоломова**

«21» января 2014 г.

ТРЕБОВАНИЯ

по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных ММАУ «Городская поликлиника №14»

2014 г.

Содержание

1. Общие положения

1.1. Настоящие Требования разработаны в соответствии с

1) Федеральным Законом РФ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006;
2) Федеральным Законом РФ № 152-ФЗ «О персональных данных» от 27.07.2006;
3) Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
4) «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», (утверждены Постановлением Правительства РФ 01.11.2012 № 1119);
5) «Перечнем мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», (утверждён Постановлением Правительства РФ 21.03.2012 № 211);
6) «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», (утверждено Постановлением Правительства РФ 15.09.2008 № 687);
7) «Требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», (утверждены Постановлением Правительства РФ 06.07.2008 № 512);
8) «Типовыми требованиями 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», утвержденные Руководством 8 Центра ФСБ 21.02.2008 № 149/6/6-622,

в которых установлены методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее – оператор), или лицом, которому на основании договора

оператор поручает обработку персональных данных (далее – уполномоченное лицо).

1.2. К методам и способам защиты информации, применяемым для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных относятся:

- методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе, случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий (далее – методы и способы защиты информации от несанкционированного доступа);
- методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа, результатом которого может стать копирование, распространение информации, а также иных несанкционированных действий (далее – методы и способы защиты информации от утечки по техническим каналам).

1.3. Для выбора и реализации методов и способов защиты информации в информационных системах персональных данных оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных. Для выбора и реализации методов и способов защиты информации в информационных системах персональных данных может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

1.4. Выбор и реализация методов и способов защиты информации в ИСПДн осуществляется на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в зависимости от уровня защищённости персональных данных, обрабатываемых в информационных системах персональных данных, определенного в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», (утверждены Постановлением Правительства РФ 01.11.2012 № 1119).

1.5. Выбранные и реализованные методы и способы защиты информации в информационных системах персональных данных должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах

персональных данных в составе создаваемой оператором (уполномоченным лицом) системы защиты персональных данных.

2. Общие требования по защите информации

2.1. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2) своевременное обнаружение фактов несанкционированного доступа к информации;
3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6) постоянный контроль за обеспечением уровня защищенности информации.

3. Требования к оператору по обеспечению безопасности персональных данных при их сборе и обработке

Обязанности оператора при сборе персональных данных

3.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе следующую информацию:

1) подтверждение факта обработки персональных данных оператором;
2) правовые основания и цели обработки персональных данных;
3) цели и применяемые оператором способы обработки персональных данных;
4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

3.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3.3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных п. 3.4, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

3.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 3.3, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо

научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных п. 3.3, нарушает права и законные интересы третьих лиц.

Обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом «О персональных данных»

3.5. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом «О персональных данных» или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со пп. 3.9-3.19;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

3.6. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3.7. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

3.8. Оператор обязан представить документы и локальные акты, указанные в п. 3.5, и (или) иным образом подтвердить принятие мер, указанных в п. 3.5, по запросу уполномоченного органа по защите прав субъектов персональных данных.

Обеспечение безопасности персональных данных при их обработке

3.9. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.10. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3.11. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

3.12. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с п 3.11 требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

3.13. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

3.14. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с п. 3.13, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

3.15. Проекты нормативных правовых актов, указанных в п. 3.13, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в п. 3.14, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты

информации, об отказе в согласовании проектов решений, указанных в п. 3.14, должно быть мотивированным.

3.16. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящим пунктом, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

3.17. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с данным пунктом, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

3.18. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

3.19. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает

нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

4. Требования к защите персональных данных при их обработке в информационных системах персональных данных

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

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

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

5. Требования к защите персональных данных при их обработке без использования средств автоматизации

5.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

5.2. 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.

5.3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований главы 5.

Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

5.4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

5.5. 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.

5.6. 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).

5.7. 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.

5.8. 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.

5.9. 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, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

5.10. 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).

5.11. Правила, предусмотренные пп. 5.9-5.10, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

5.12. 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.

Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

5.13. 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 либо имеющих к ним доступ.

5.14. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.15. При хранении материальных носителей должны соблюдаться 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, устанавливаются оператором.

6. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных

6.1. Настоящие требования применяются при использовании материальных носителей, на которые осуществляется запись биометрических персональных данных, а также при хранении биометрических персональных данных вне информационных систем персональных данных.

6.2. В настоящих требованиях под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность (далее – материальный носитель).

6.3. Настоящие требования не распространяются на отношения, возникающие при использовании:

в) оператором информационной системы персональных данных (далее – оператор) материальных носителей для организации функционирования информационной системы персональных данных, оператором которой он является;

г) бумажных носителей для записи и хранения биометрических персональных данных.

6.4. Материальный носитель должен обеспечивать:

а) защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;

б) возможность доступа к записанным на материальный носитель биометрическим персональным данным, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством Российской Федерации на работу с

биометрическими персональными данными (далее – уполномоченные лица);

в) возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись;

г) невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе.

6.5. Оператор утверждает порядок передачи материальных носителей уполномоченным лицам.

6.6. Материальный носитель должен использоваться в течение срока, установленного оператором, осуществившим запись биометрических персональных данных на материальный носитель, но не более срока эксплуатации, установленного изготовителем материального носителя.

6.7. Тип материального носителя, который будет использован для обработки биометрических персональных данных, определяет оператор, за исключением случаев, когда нормативными правовыми актами Российской Федерации предписано использование материального носителя определенного типа.

6.8. Оператор обязан:

а) осуществлять учет количества экземпляров материальных носителей;

б) осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

6.9. Технологии хранения биометрических персональных данных вне информационных систем персональных данных должны обеспечивать:

а) доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;

б) применение средств электронной цифровой подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;

в) проверку наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством Российской Федерации в сфере отношений, связанных с обработкой персональных данных.

6.10. В случае если на материальном носителе содержится дополнительная информация, имеющая отношение к записанным биометрическим персональным данным, то такая информация должна быть подписана электронной цифровой подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель.

Использование шифровальных (криптографических) средств защиты информации осуществляется в соответствии с законодательством Российской Федерации.

6.11. При хранении биометрических персональных данных вне информационных систем персональных данных должна обеспечиваться регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

6.12. Оператор вправе установить не противоречащие требованиям законодательства Российской Федерации дополнительные требования к технологиям хранения биометрических персональных данных вне информационных систем персональных данных в зависимости от методов и способов защиты биометрических персональных данных в информационных системах персональных данных этого оператора.

7. Требования по организации и обеспечению безопасности обработки с использованием шифровальных (криптографических) средств персональных данных

7.1. Безопасность обработки персональных данных с использованием криптосредств организуют и обеспечивают операторы, а также лица, которым на основании договора оператор поручает обработку персональных данных и (или) лица, которым на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности обработки в информационной системе персональных данных с использованием криптосредств.

Обеспечение безопасности персональных данных с использованием криптосредств должно осуществляться в соответствии с:

1) Приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005);

2) Постановлением Правительства РФ от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;

3) Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (№ 149/54-144, 2008 г. ФСБ России),

4) Типовыми требованиями 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

7.2. Операторы несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности обработки с использованием криптосредств персональных данных лицензионным требованиям и условиям, эксплуатационной и технической документации к криптосредствам, а также настоящим Требованиям.

При этом операторы должны обеспечивать комплексность защиты персональных данных, в том числе посредством применения некриптографических средств защиты.

7.3. При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе оператор или уполномоченное оператором лицо осуществляет:

1) разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;

2) разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;

3) определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;

4) установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;

5) проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;

6) обучение лиц, использующих криптосредства, работе с ними;

7) поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных;

8) учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств);

9) контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

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

11) описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах, с указанием в частности:

а) индекса, условного наименования и регистрационных номеров используемых криптосредств;

б) соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;

в) соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;

г) выполнения Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Описание принятых мер должно быть включено в уведомление, предусмотренное частью 1 статьи 22 Федерального закона «О персональных данных».

7.4. Пользователи криптосредств допускаются к работе с ними по решению, утверждаемому оператором. При наличии двух и более

пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

7.5. Пользователи криптосредств обязаны:

- не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;
- соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;
- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;
- немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.
- сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

7.6. Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь криптосредств).

Допускается возложение функций ответственного пользователя криптосредств на:

- одного из пользователей криптосредств;
- на структурное подразделение или должностное лицо (работника), ответственных за обеспечение безопасности персональных данных, назначаемых оператором;
- на специальное структурное подразделение по защите государственной тайны, использующее для этого шифровальные средства.

7.7. Ответственные пользователи криптосредств должны иметь функциональные обязанности, разработанные в соответствии с настоящими Требованиями.

7.8. При определении обязанностей пользователя криптосредств необходимо учитывать, что безопасность обработки с использованием криптосредств персональных данных обеспечивается:

- соблюдением пользователями криптосредств конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;
- точным выполнением пользователями криптосредств требований к обеспечению безопасности персональных данных;
- надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;
- обеспечением принятых в соответствии с Требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных мер.
- своевременным выявлением попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;
- немедленным принятием мер по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

7.9. Лица, оформляемые на работу в качестве пользователей (ответственных пользователей) криптосредств, должны быть ознакомлены с настоящими Требованиями и другими документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

7.10. Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на оператора и ответственного пользователя криптосредств в пределах их служебных полномочий.

7.11. Контроль за организацией, обеспечением функционирования и безопасности криптосредств, предназначенных для защиты персональных данных при их обработке в информационных системах персональных

данных, осуществляется в соответствии с действующим законодательством Российской Федерации.

7.12. В случае необходимости взаимодействия операторов информационных систем при использовании криптосредств для обеспечения безопасности обработки персональных данных для организации взаимодействия криптосредств по решению операторов персональных данных выделяется координирующий орган, ответственный за обеспечение безопасности персональных данных, указания которого являются обязательными для всех пользователей криптосредств.

8. Рекомендуемые методы и способы защиты для противодействия актуальным угрозам безопасности персональных данных

В информационных системах персональных данных были выявлены актуальные угрозы информационной безопасности. В Таблице 1 приведены рекомендуемые методы и способы противодействия актуальным угрозам информационной безопасности ПДн.

Таблица 1

Методы и способы противодействия актуальным угрозам безопасности ИСПДн Учреждения

№ угрозы	Наименование угрозы	Мероприятия по снижению вероятности угроз
2	**Физические угрозы**	
2.5	**Непреднамеренные действия внутреннего нарушителя**	
2.5.1	Непреднамеренная утрата носителей информации и ключей доступа	- внедрение учета съемных носителей и Журнала учета съемных носителей, ограничение использования неучтенных съемных носителей; - организация парольной защиты, своевременная смена паролей, соблюдение правил использования паролей и ключей доступа;
2.5.2	Непреднамеренный вывод из строя или изменение режимов работы технических средств ИСПДн	- внедрение Порядка резервного копирования и восстановления работоспособности, соблюдение правил резервного копирования и восстановления работоспособности ТС; - ограничение доступа пользователей к настройкам ТС, инструктаж пользователей по правилам доступа к ПДн и ТС, а так же о действиях в нештатных ситуациях;
3	**Угрозы несанкционированного доступа**	
3.1	**Преднамеренные действия нарушителя**	
3.1.1	Запуск операционной системы с внешнего (сменного) носителя	- внедрение учета съемных носителей и Журнала учета съемных носителей, ограничение использования неучтенных съемных носителей; - организация парольной защиты, своевременная смена паролей, соблюдение правил использования паролей и ключей доступа; - контроль действий пользователя, подключаемых им устройств и носителей;
3.1.2	Внедрение вредоносных программ	- использование сертифицированных средств защиты от вирусов, своевременное их обновление; - внедрение учета съемных носителей и Журнала учета съемных носителей, ограничение использования неучтенных съемных носителей;

3.1.6	Несанкционированное копирование информации на внешние (сменные) носители	- внедрение учета съемных носителей и Журнала учета съемных носителей, ограничение использования неучтенных съемных носителей; - разграничение доступа пользователей к конфиденциальным данным и приложениям, внедрение Положения о разграничении прав доступа к обрабатываемым ПДн, инструктаж пользователей по правилам доступа к ПДн и ТС, а так же о действиях в нештатных ситуациях;
3.1.7	Несанкционированная печать информации, содержащей персональные данные на бумажные носители;	- разграничение доступа пользователей к конфиденциальным данным и приложениям, внедрение Положения о разграничении прав доступа к обрабатываемым ПДн, инструктаж пользователей по правилам доступа к ПДн и ТС, а так же о действиях в нештатных ситуациях; - автоматизированный электронный учет действий пользователей;
3.2	**Непреднамеренные действия нарушителя**	
3.2.1	Непреднамеренный запуск вредоносных программ	- использование сертифицированных средств защиты от вирусов, своевременное их обновление; - внедрение учета съемных носителей и Журнала учета съемных носителей, ограничение использования неучтенных съемных носителей; - ознакомление пользователей с правилами работы с ИСПДн и действиями в нештатных ситуациях;
3.2.2	Непреднамеренная модификация (уничтожение) информации	- разграничение доступа пользователей к конфиденциальным данным и приложениям, внедрение Положения о разграничении прав доступа к обрабатываемым ПДн, инструктаж пользователей по правилам доступа к ПДн и ТС, а так же о действиях в нештатных ситуациях; - внедрение Порядка резервного копирования и восстановления работоспособности, соблюдение правил резервного копирования и восстановления работоспособности ТС;
3.5	**Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия**	
3.5.1	Удаленный сбор информации об операционной системе («отпечатки» протоколов)	-внедрение сертифицированного средства МЭ.
4	**Угрозы персонала**	

4.1	Преднамеренное разглашение конфиденциальной информации	- внедрение Положения об обеспечении информационной безопасности; - ознакомление пользователей с правилами безопасной работы с ПДн, инструктаж по действиям в нештатных ситациях, которые могут возникнуть во время обработки ПДн, донесение вероятных последствий инцидентов ИБ;
4.2	Непреднамеренное разглашение конфиденциальной информации	- внедрение Положения об обеспечении информационной безопасности; - ознакомление пользователей с правилами безопасной работы с ПДн, инструктаж по действиям в нештатных ситациях, которые могут возникнуть во время обработки ПДн, донесение вероятных последствий инцидентов ИБ;

9. Требования по организационной защите персональных данных, обрабатываемых в информационных системах персональных данных

Для эффективного противодействия актуальным угрозам безопасности ПДн необходимо использование организационной защиты ПДн, обрабатываемых в ИСПДн.

Ниже приведён перечень организационно-распорядительной документации, необходимой к принятию/разработке:

Таблица 2

Перечень основных организационно-распорядительных документов

1. Приказ о проведении обследования, в т.ч. приложения:
    - Порядок определения уровня защищённости ПДн, при обработке в ИСПДн
2. Приказ об определении контролируемой зоны, в т.ч. приложение:
    - Положение о доступе сотрудников и посетителей в рабочее и нерабочее время в помещения, в которых обрабатываются ПДн
3. Приказ об определении уровня защищенности ПДн, в т.ч. приложения:
    - Акт определения уровня защищённости персональных данных при их обработке в ИСПДн
    - План мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн
4. Приказ об обеспечении безопасности ПДн, в т.ч. приложения:
    - Концепция информационной безопасности
    - Политика информационной безопасности
    - Политика обработки и защиты ПДн
    - Политика обработки ПДн без использования средств автоматизации
    - Положение об обеспечении безопасности ПДн
    - Положение о применимости базовых мер по обеспечению безопасности ПДн
    - Перечень ИСПДн
    - Перечень общедоступной информации
    - Перечень защищаемых ПДн, обрабатываемых в ИСПДн
    - Перечень сотрудников, допущенных к обработке ПДн

- Перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним
- Положение о разграничении прав доступа к обрабатываемым ПДн в ИСПДн
- Матрица доступа
- Инструкция пользователя ИСПДн
- Положение о порядке работы с электронным журналом обращений пользователей ИСПДн к обрабатываемым ПДн

5. Приказ о назначении ответственных лиц, в т.ч. приложения:
    - Инструкция администратора безопасности ИСПДн
    - Инструкция Администратора ИСПДн
    - Регламент резервного копирования и восстановления работоспособности ТС и ПО, БД и СЗИ в ИСПДн
    - Инструкция пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций
    - Порядок учёта, хранения, обращения и уничтожения носителей ПДн в ИСПДн
    - Порядок реагирования на проведение проверки уполномоченным органом по защите прав субъектов ПДн
6. Приказ об организационно-технических мероприятиях, в т.ч. приложения:
    - Требования по обеспечению защиты информации
    - Положение о парольной защите
    - Положение об антивирусной защите
    - Инструкция по использованию корпоративной сети
    - Инструкция по использованию электронной почты
    - Положение по использованию сети Интернет
    - Частную модель угроз безопасности ПДн при их обработке в ИСПДн
7. Приказ о взаимодействии с субъектами ПДн, в т.ч. приложения:
    - Положение об обработке ПДн
8. Приказ о контрольных мерах, в т.ч. приложения:
    - План внутренних проверок состояния защиты ПДн

- План мероприятий по контролю процессов обработки и состояния защиты ПДн, обрабатываемых в ИСПДн
- Форма Журнала ознакомлений с регламентами обеспечения безопасности ПДн Предприятия
- Форма Журнала учета мероприятий по обеспечению безопасности ПДн Предприятия
- Форма Журнала учета съемных носителей ПДн в ИСПДн Предприятия
- Форма Журнала учета случаев нарушения режима безопасности