УТВЕРЖДАЮ
Главный врач
ГАУЗ ТО
«Городская поликлиника №4»
_____ Н.В.Шанаурина
«21» 08 2023 г.

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных
ГАУЗ ТО «ГОРОДСКАЯ ПОЛИКЛИНИКА №4»
«Медицинская информационная система»

Тюмень- 2023

Содержание

1. Общие положения

1.1. Требования по обеспечению безопасности конфиденциальной информации (далее - Требования), обрабатываемой в информационных системах ГАУЗ ТО «ГОРОДСКАЯ ПОЛИКЛИНИКА №4» определяют совокупный набор организационных и технических мер, которые необходимо реализовать в Учреждении в целях организации и обеспечения безопасной обработки конфиденциальной информации в соответствии с актуальными требованиями законодательства РФ в области защиты информации.

1.2. Настоящие Требования разработаны в соответствии со следующими нормативными правовыми актами и нормативно-методическими документами:

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 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4) Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5) «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», (утверждены Постановлением Правительства РФ 01.11.2012 № 1119).

6) «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).

7) «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», (утверждено Постановлением Правительства РФ 15.09.2008 № 687).

В настоящих документах 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).

1.3. 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).

1.4. Для выбора и реализации методов и способов защиты информации в информационных системах персональных данных оператором или уполномоченным лицом необходимо организовать 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.

1.5. Выбор и реализация методов и способов защиты информации в ИС осуществляется на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в соответствии с перечнем мер, изложенных в нормативных документах ФСТЭК России в области защиты конфиденциальной информации, подбор которых (мер) осуществляется по результатам классификации ИС, 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).

1.6. Выбранные и реализованные методы и способы защиты информации в ИС должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах персональных данных в составе создаваемой оператором (уполномоченным лицом) системы защиты информации (далее - СЗИ).

2. Общие требования по защите информации

2.1. На основании статьи 16 Федерального закона № 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации» приведены следующие требования к защите информации.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) Соблюдение конфиденциальности информации ограниченного доступа;
3) Реализацию права на доступ к информации.

2.2. 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. Область действия требований

3.1. Настоящие Требования распространяются на информационные системы ГАУЗ ТО «ГОРОДСКАЯ ПОЛИКЛИНИКА №4», обрабатывающие конфиденциальную информацию. Кроме того, настоящие Требования предусматривают принятие мер по предотвращению нарушений конфиденциальности и целостности КИ, потенциально реализуемых в процессе ее неавтоматизированной обработки.

3.2. Настоящие Требования являются ключевым документом, содержащим сведения, необходимые для проектирования Системы защиты информации (далее СЗИ) ГАУЗ ТО «ГОРОДСКАЯ ПОЛИКЛИНИКА №4».

3.3. Требования распространяются на информационную систему, представленную ниже (список систем может быть дополнен системами, в отношении которых было принято решение по их защите от НСД, а также от прерываний работы и утрачивания целостности обрабатываемых данных):

- **«МИС»**

3.4. Общие требования к защите ПДн в ИС, а также требования по ведению неавтоматизированной обработки КИ, сформулированы в основной части настоящего документа.

Развернутые требования для каждой частной ИС изложены в Приложениях к настоящему документу, в которых обосновывается применимость базового набора мер (на основании нормативных актов ФСТЭК России) по обеспечению безопасности для каждой из ИС.

4. Общие требования к средствам защиты информации ГАУЗ ТО «ГОРОДСКАЯ ПОЛИКЛИНИКА №4»

4.1. Базовый набор требований по защите конфиденциальной информации напрямую связан с выполнением Постановления Правительства РФ № 1119 от 01 ноября 2012 г. «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

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 (далее – персональные данные), 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.

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, осуществляемых 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.

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

6.1. 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.

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

6.3. 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.

7. Меры по обеспечению безопасности персональных данных при их обработке

7.1 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.

7.2 Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 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;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним
- 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;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

7.3 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:

- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

7.4 Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 6.3 настоящей статьи 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.

7.5 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.

7.6 Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 6.5 настоящей статьи, 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.

7.7 Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, 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.

7.8 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.

7.9 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.

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

8.1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.

8.2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующие актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

8.3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

8.4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных"

8.5. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

8.6. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн **«МИС»** в ГАУЗ ТО «ГОРОДСКАЯ ПОЛИКЛИНИКА №4» актуальны **угрозы 3-го типа (угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе).**

8.7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

8.8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

8.9. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

8.10. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

8.11. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

8.12. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

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

а) 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;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) 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.

8.14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 6.13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

8.15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 6.14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

8.16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 6.15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

8.17. 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).

8.18. Для ИСПДн **«МИС»** необходимо обеспечить 2 уровень защищённости (для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных).

В соответствии с пунктом 15 Требований к защите персональных данных **для обеспечения 2 уровня защищенности персональных данных** при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктами 5 и 16 настоящего документа (приказа ФСБ России от 10 июля 2014г. № 378), необходимо выполнение требования о том, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Для выполнения требования, указанного в пункте 7.18 настоящего документа, необходимо:

а) утверждение руководителем оператора списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии;

б) обеспечение информационной системы автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений;

в) обеспечение информационной системы автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений;

г) обеспечение периодического контроля работоспособности указанных в подпунктах "б" и "в" настоящего пункта автоматизированных средств (не реже 1 раза в полгода).

Для выполнения требования, указанного в подпункте "г" пункта 7.18 настоящего документа, необходимо вместо мер, предусмотренных подпунктом "в" использовать для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе:

СКЗИ класса КА в случаях, когда для информационной системы актуальны угрозы 1 типа;

СКЗИ класса КВ и выше в случаях, когда для информационной системы актуальны угрозы 2 типа;

СКЗИ класса КС1 и выше в случаях, когда для информационной системы актуальны угрозы 3 типа.

9. 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

№ угрозы	Наименование угрозы	Мероприятия по снижению вероятности угроз
2	**Угрозы несанкционированного доступа**	
2.1	**Угрозы уничтожения, хищения аппаратных средств**	
2.1.1	Кража, вывод из строя узлов ПЭВМ	- внедрение Порядка резервного копирования и восстановления работоспособности, соблюдение правил резервного копирования и восстановления работоспособности технических средств (далее – ТС); - ограничение доступа пользователей к настройкам ТС, инструктаж пользователей по правилам доступа к ПДн и ТС, а также о действиях в нештатных ситуациях
2.1.2	Кража и вывод из строя носителей информации	- введение учета носителей информации; - организация пропускного режима
2.5	**Угрозы непреднамеренных действий пользователя**	
2.5.2	Непреднамеренная модификация, удаление 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 также о действиях в нештатных ситуациях; - внедрение Порядка резервного копирования и восстановления работоспособности, соблюдение правил резервного копирования и восстановления работоспособности ТС
2.7	**Угрозы преднамеренных действий**	
2.7.2	Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	- внедрение Положения об обеспечении информационной безопасности; - ознакомление пользователей с правилами безопасной работы с ПДн, инструктаж по действиям в нештатных ситуациях, которые могут возникнуть во время обработки ПДн, донесение вероятных последствий инцидентов ИБ; - сбор согласия о неразглашении информации с пользователей.

10. 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.

С целью организационной защиты ПДн в учреждении должен иметься следующий перечень организационно-распорядительной документации:

- Приказ о назначении ответственных лиц за обеспечение безопасности ПДн
- Инструкция администратора безопасности ИСПДн
- Инструкция Администратора ИСПДн;
- Порядок 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;
- Политика оператора при обработке и обеспечении безопасности персональных данных в информационной системе персональных данных
- Приказ об определении уровня защищенности ПДн;
- Приказ о постоянно действующей комиссии по определению уровня защищённости ИСПДн
- Акт определения уровня защищённости персональных данных при обработке в ИСПДн;
- Перечень ИСПДн;
- Перечень ПДн, обрабатываемых в ИСПДн;
- Положение о разграничении прав доступа к ПДн;
- Матрица доступа;
- Перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- Инструкция пользователя ИСПДн;
- Требования по обеспечению защиты информации;
- Положение о парольной защите;
- Положение об антивирусной защите;
- Положение по использованию сети Интернет;
- Частную модель угроз безопасности ПДн при их обработке в ИСПДн;
- Приказ об установлении границ контролируемой зоны;
- Акт установки средств защиты информации в ИСПДн;
- Описание технологического процесса обработки информации в ИСПДн;
- Инструкция о пропускном и внутри объектовом режимах;
- Приказ об утверждении форм согласий на обработку ПДн;
- Приказ об утверждении форм обязательства о неразглашении информации.

Дополнительно необходимо реализовывать следующие меры:

- Производить идентификацию и аутентификацию пользователей являющейся работниками оператора;
- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей;
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя;
- Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени;
- Реализация антивирусной защиты;
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- Контроль состава технических средств, программного обеспечения и средств защиты информации;
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;
- Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.