КОМИТЕТ ПО ЗДРАВООХРАНЕНИЮ ПСКОВСКОЙ ОБЛАСТИ

ПРИКАЗ

от 01.09.2023 № 842

г. ПСКОВ

Об утверждении типовых форм организационно-распорядительной документации по организации обработки и защите информации, в том числе по работе с персональными данными

Во исполнение требований Федеральных законов от 27.07.2006 N 149-ФЗ «Об информационных технологиях и о защите информации» и от 27.07.2006 N 152-ФЗ «О персональных данных», Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»,

ПРИКАЗЫВАЮ:

1. Утвердить типовые формы организационно-распорядительной документации по информационной безопасности и работе с персональными данными.

2. Руководителям медицинских организаций, на основе типовых форм:

2.1. Сформировать и утвердить локальные организационно-распорядительные документы по информационной безопасности и работе с персональными данными по учреждениям.

2.2. Организовать работу по обеспечению обработки и защиты персональных данных в соответствии с нормами, изложенными в прилагаемых документах.

3. Директору ГКУЗ ПО «Медицинский информационно-аналитический центр» А.В. Савину:

3.1 разместить настоящий приказ на сайте Комитета по здравоохранению Псковской области.

4. Приказ вступает в силу со дня, следующего за днем его официального опубликования.

5. Контроль за исполнением настоящего приказа оставляю за собой.

Председатель Комитета М.В.Гаращенко

Бринюк М.В.
8(8112) 29-84-00

Политика

Об обработке персональных данных в <наименование учреждения здравоохранения>

1. Общие положения

1.1. Назначение политики

1.1.1. Настоящая политика в отношении обработки персональных данных в <наименование учреждения здравоохранения> (далее – политика) разработана в соответствии с федеральным законом от 27 июля 2006 г. № 152-фз «о персональных данных».

1.1.2. Политика вступает в силу с момента ее утверждения директором <наименование учреждения здравоохранения>.

1.1.3. Политика подлежит пересмотру в ходе периодического анализа со стороны руководства <наименование учреждения здравоохранения>, а также в случаях изменения законодательства российской федерации в области персональных данных.

1.1.4. Политика подлежит опубликованию на официальном сайте <наименование учреждения здравоохранения>.

1.2. Цели политики

1.2.1. Целью политики является обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных <наименование учреждения здравоохранения>.

1.3. Основные понятия

1.3.1. Для целей политики используются следующие понятия:

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном федеральным законом «о персональных данных»;

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Угрозы безопасности персональных данных – 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;

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

1.4. Область действия

1.4.1. Положения политики распространяются на все отношения, связанные с обработкой персональных данных, осуществляемой <наименование учреждения здравоохранения>:

- с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным;

- без использования средств автоматизации.

1.4.2. Политика применяется ко всем работникам <наименование учреждения здравоохранения>.

2. Цели обработки персональных данных

2.1. Обработка персональных данных осуществляется <наименование учреждения здравоохранения> в следующих целях:

- выполнение требований трудового законодательства российской федерации; ведение бухгалтерского и кадрового учета; оформление договорных отношений в соответствии с законодательством российской федерации;

- анализ деятельности и формирование отчетности для органов управления здравоохранение по всем учреждениям области;

- выполнение требований законодательства российской федерации в сфере здравоохранения;

- обеспечение соблюдения законов и иных нормативных правовых актов в сфере здравоохранения.

3. Правовые основания обработки персональных данных

3.1. Основанием обработки персональных данных в <наименование учреждения здравоохранения> являются следующие нормативные акты и документы:

- конституция российской федерации;

- устав государственного казенного учреждения здравоохранения псковской области «медицинский информационно-аналитический центр»;

- договоры, заключаемые между оператором и субъектом персональных данных;

- согласия субъектов персональных данных на обработку персональных данных;

- трудовой кодекс российской федерации;

- федеральный закон от 21.11.2011 № 323-фз «об основах охраны здоровья граждан в российской федерации»;

- федеральный закон от 29.11.2010 № 326-фз «об обязательном медицинском страховании в российской федерации»;

- федеральный закон от 27.07.2006 № 152-фз «о персональных данных»;

- постановление правительства рф от 05 мая 2018 года № 555 «о единой государственной информационной системе в сфере здравоохранения»;

- приказ минздрава россии от 24 декабря 2018 № 911н «об утверждении требований к государственным информационным системам в сфере здравоохранения субъектов российской федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций»;

- 143-фз «об актах гражданского состояния»;

- приказ минздравсоцразвития россии от 28.04.2011 г. N 364 (ред. От 12.04.2012) «об утверждении концепции создания единой государственной информационной системы в сфере здравоохранения»;

3.2. В случаях, прямо не предусмотренных законодательством российской федерации, но соответствующих полномочиям <наименование учреждения здравоохранения>, обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

3.3. Обработка персональных данных прекращается при реорганизации или ликвидации <наименование учреждения здравоохранения>.

4. Категории субъектов персональных данных

4.1. В соответствии с целями обработки персональных данных, указанными в п. 2 настоящей политики, <наименование учреждения здравоохранения> осуществляется обработка следующих категорий субъектов персональных данных:

– пациенты;

– сотрудники медицинских организаций области;

– пациенты, близкие родственники;

– иностранные граждане;

– сотрудники.

5. Порядок и условия обработки персональных данных

5.1. Принципы обработки персональных данных

Обработка персональных данных осуществляется <наименование учреждения здравоохранения> в соответствии со следующими принципами:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- обработке подлежат только персональные данные, которые отвечают целям их обработки;

- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки;

- обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;

- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;

- <наименование учреждения здравоохранения> принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2. Условия обработки персональных данных

Условия обработки персональных данных, отличные от получения согласия субъекта персональных данных на обработку его персональных данных, являются альтернативными.

5.2.1. Условия обработки специальных категорий персональных данных

Обработка специальных категорий персональных данных осуществляется <наименование учреждения здравоохранения> с соблюдением следующих условий:

- обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством российской федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством российской федерации сохранять врачебную тайну;

- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством российской федерации;

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных.

5.2.2. Условия обработки биометрических персональных данных

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются <наименование учреждения здравоохранения> для установления личности субъекта персональных данных, <наименование учреждения здравоохранения> не обрабатываются.

5.2.3. Условия обработки иных категорий персональных данных

Обработка иных категорий персональных данных осуществляется <наименование учреждения здравоохранения> с соблюдением следующих условий:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором российской федерации или законом, для осуществления и выполнения возложенных законодательством российской федерации на <наименование учреждения здравоохранения> функций, полномочий и обязанностей;

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

5.2.4. Условия обработки персональных данных, разрешённых субъектом персональных данных для распространения

Осуществляется обработка персональных данных, распространение которых необходимо в соответствии с законодательством российской федерации.

Осуществляется обработка персональных данных, разрешённых субъектом персональных данных для распространения.

5.2.5. Поручение обработки персональных данных

5.2.5.1. <наименование учреждения здравоохранения> вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение).

5.2.5.2. Лицо, осуществляющее обработку персональных данных по поручению <наименование учреждения здравоохранения>, соблюдает принципы и правила обработки персональных данных, предусмотренные настоящей политикой. В поручении <наименование учреждения здравоохранения> определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, способы и цели обработки, установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указаны требования к защите обрабатываемых персональных данных.

5.2.5.3. При поручении обработки персональных данных другому лицу ответственность перед субъектом персональных данных за действия указанного лица несет <наименование учреждения здравоохранения>. Лицо, осуществляющее обработку персональных данных по поручению <наименование учреждения здравоохранения>, несет ответственность перед <наименование учреждения здравоохранения>.

5.2.6. Передача персональных данных

5.2.6.1. <наименование учреждения здравоохранения> вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством российской федерации.

5.3. Конфиденциальность персональных данных

5.3.1. Сотрудники <наименование учреждения здравоохранения>, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.4. Общедоступные источники персональных данных

5.4.1. <наименование учреждения здравоохранения> не создает общедоступные источники персональных данных.

5.5. Согласие субъекта персональных данных на обработку его персональных данных

5.5.1. При необходимости обеспечения условий обработки персональных данных субъекта может предоставляться согласие субъекта персональных данных на обработку его персональных данных.

5.5.2. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются <наименование учреждения здравоохранения>.

5.5.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных <наименование учреждения здравоохранения> вправе продолжить обработку

персональных данных без согласия субъекта персональных данных при выполнении альтернативных условий обработки персональных данных.

5.5.4. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство выполнения альтернативных условий обработки персональных данных возлагается на <наименование учреждения здравоохранения>.

5.5.5. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес <наименование учреждения здравоохранения>;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению <наименование учреждения здравоохранения>, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых <наименование учреждения здравоохранения> способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5.5.6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

5.5.7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

5.5.8. Персональные данные могут быть получены <наименование учреждения здравоохранения> от лица, не являющегося субъектом персональных данных, при условии предоставления <наименование учреждения здравоохранения> подтверждения наличия альтернативных условий обработки информации.

5.6. Трансграничная передача персональных данных

5.6.1. Трансграничная передача персональных данных <наименование учреждения здравоохранения> не осуществляется.

5.7. Особенности обработки персональных данных, разрешённых субъектом персональных данных для распространения.

5.7.1. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется на основании соответствующего согласия субъекта персональных данных.

5.7.2. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

5.7.3. Согласие содержит перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

5.7.4. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, предоставляется непосредственно <наименование учреждения здравоохранения>.

5.7.5. Молчание или бездействие субъекта персональных данных не считается согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

5.7.6. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных <наименование учреждения здравоохранения> неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ <наименование учреждения здравоохранения> в установлении субъектом персональных данных запретов и условий, предусмотренных статьей 9 федерального закона «о персональных данных», не допускается.

5.7.7. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством российской федерации.

5.7.8. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

5.7.9. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления <наименование учреждения здравоохранения> соответствующего требования.

5.7.10. Требования, указанные выше, не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством российской федерации на федеральные

органы исполнительной власти, органы исполнительной власти субъектов российской федерации, органы местного самоуправления функций, полномочий и обязанностей.

5.8. Обработка персональных данных, осуществляемая без использования средств автоматизации

5.8.1.общие положения

5.8.1.1. 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.

5.8.2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

5.8.2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются 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).

5.8.2.2. 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 используется отдельный материальный носитель.

5.8.2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники <наименование учреждения здравоохранения> или лица, осуществляющие такую обработку по договору с <наименование учреждения здравоохранения>), проинформированы о факте обработки ими персональных данных, обработка которых осуществляется <наименование учреждения здравоохранения> 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 <наименование учреждения здравоохранения>.

5.8.2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), соблюдаются следующие условия:

А) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес <наименование учреждения здравоохранения>, 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 <наименование учреждения здравоохранения> способов обработки персональных данных;

Б) типовая форма предусматривает 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 составляется 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 исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.8.2.5. 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, принимаются 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.

5.8.2.6. Уничтожение 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). Указанные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

5.8.2.7. 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.

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

5.8.3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

5.8.3.2. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.8.3.3. При хранении материальных носителей соблюдаются 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 <наименование учреждения здравоохранения>.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

6.1. Права субъектов персональных данных

6.1.1. Право субъекта персональных данных на доступ к его персональным данным

6.1.1.1. Субъект персональных данных имеет право на получение информации (далее – запрашиваемая субъектом информация), касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных <наименование учреждения здравоохранения>;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые <наименование учреждения здравоохранения> способы обработки персональных данных;

4) наименование и место нахождения <наименование учреждения здравоохранения>, сведения о лицах (за исключением сотрудников <наименование учреждения здравоохранения>), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с <наименование учреждения здравоохранения> 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 <наименование учреждения здравоохранения>, если обработка поручена или будет поручена такому лицу;

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

6.1.1.2. Субъект персональных данных имеет право на получение запрашиваемой субъектом информации, за исключением следующих случаев:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством российской федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

- обработка персональных данных осуществляется в случаях, предусмотренных законодательством российской федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

6.1.1.3. Субъект персональных данных вправе требовать от <наименование учреждения здравоохранения> уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.1.1.4. Запрашиваемая субъектом информация должна быть предоставлена субъекту персональных данных <наименование учреждения здравоохранения> в доступной форме, и в ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.1.1.5. Запрашиваемая информация предоставляется субъекту персональных данных или его представителю <наименование учреждения здравоохранения> при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с <наименование учреждения здравоохранения> (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных <наименование учреждения здравоохранения>, подпись субъекта персональных данных или его представителя (далее – необходимая для запроса информация). Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством российской федерации.

6.1.1.6. В случае если запрашиваемая субъектом информация, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в <наименование учреждения здравоохранения> или направить повторный запрос в целях получения запрашиваемой субъектом информации и ознакомления с такими персональными данными не ранее чем через тридцать дней (далее – нормированный срок запроса) после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.1.1.7. Субъект персональных данных вправе обратиться повторно в <наименование учреждения здравоохранения> или направить повторный запрос в целях получения запрашиваемой субъектом информации, а также в целях ознакомления с обрабатываемыми персональными данными до истечения нормированного срока запроса, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по

результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимой для запроса информацией должен содержать обоснование направления повторного запроса.

6.1.1.8. <наименование учреждения здравоохранения> вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на <наименование учреждения здравоохранения>.

6.1.2. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

6.1.2.1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации <наименование учреждения здравоохранения> не осуществляется.

6.1.3. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

6.1.3.1. Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, осуществляется:

- в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных (федеральный закон от 21.11.2011 № 323-фз «об основах охраны здоровья граждан в российской федерации»).

6.1.3.2. <наименование учреждения здравоохранения> обязуется разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

6.1.3.3. <наименование учреждения здравоохранения> обязуется рассмотреть возражение, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

6.1.4. Право на обжалование действий или бездействия <наименование учреждения здравоохранения>

6.1.4.1. Если субъект персональных данных считает, что <наименование учреждения здравоохранения> осуществляет обработку его персональных данных с нарушением требований федерального закона «о персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие <наименование учреждения здравоохранения> в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6.1.4.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6.2. Обязанности оператора

6.2.1. Обязанности оператора при сборе персональных данных

6.2.1.1. При сборе персональных данных <наименование учреждения здравоохранения> предоставляет субъекту персональных данных по его просьбе запрашиваемую информацию,

касающуюся обработки его персональных данных в соответствии с частью 7 статьи 14 федерального закона «о персональных данных».

6.2.1.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, <наименование учреждения здравоохранения> разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

6.2.1.3. Если персональные данные получены не от субъекта персональных данных, <наименование учреждения здравоохранения> до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию (далее – информация, сообщаемая при получении персональных данных не от субъекта персональных данных):

1) наименование либо фамилия, имя, отчество и адрес <наименование учреждения здравоохранения> или представителя <наименование учреждения здравоохранения>;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные федеральным законом «о персональных данных» права субъекта персональных данных;

5) источник получения персональных данных.

6.2.1.4. <наименование учреждения здравоохранения> не предоставляет субъекту информацию, сообщаемую при получении персональных данных не от субъекта персональных данных, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных <наименование учреждения здравоохранения>;

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

3) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 федерального закона «о персональных данных»;

4) <наименование учреждения здравоохранения> 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 информации, сообщаемой при получении персональных данных не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

6.2.1.5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «интернет», <наименование учреждения здравоохранения> обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан российской федерации, обрабатываемых в следующих информационных системах:

6.2.1.5.1. Информационная система персональных данных «бухгалтерский и кадровый учет» с использованием баз данных, находящихся на территории следующих стран:

6.2.1.5.1.1. Россия.

6.2.1.5.2. Региональный сегмент единой информационной системы в сфере здравоохранения псковской области с использованием баз данных, находящихся на территории следующих стран:

6.2.1.5.2.1. Россия.

6.2.1.6. Местонахождение центра обработки данных и сведения об организации, ответственной за хранение данных, определены внутренними документами <наименование учреждения здравоохранения>.

6.2.2. Меры, направленные на обеспечение выполнения <наименование учреждения здравоохранения> своих обязанностей

6.2.2.1. <наименование учреждения здравоохранения> принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей. <наименование учреждения здравоохранения> самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, если иное не предусмотрено федеральными законами. К таким мерам, в частности, относятся:

1) назначение ответственного за организацию обработки персональных данных;

2) издание политики, 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;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных, политике, локальным актам <наименование учреждения здравоохранения>;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона «о персональных данных», соотношение указанного вреда и принимаемых <наименование учреждения здравоохранения> мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «о персональных данных»;

6) ознакомление сотрудников <наименование учреждения здравоохранения>, непосредственно осуществляющих обработку персональных данных, с положениями законодательства российской федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, политикой, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

6.2.3. Меры по обеспечению безопасности персональных данных при их обработке

6.2.3.1. <наименование учреждения здравоохранения> при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает 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.

6.2.3.2. 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.

6.2.3.3. 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.

6.2.4. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

6.2.4.1. <наименование учреждения здравоохранения> сообщает в установленном порядке субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

6.2.4.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя <наименование учреждения здравоохранения> дает в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

6.2.4.3. <наименование учреждения здравоохранения> предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, <наименование учреждения здравоохранения> вносит в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для

заявленной цели обработки, <наименование учреждения здравоохранения> уничтожает такие персональные данные. <наименование учреждения здравоохранения> уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

6.2.4.4. <наименование учреждения здравоохранения> сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

6.2.5. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

6.2.5.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных <наименование учреждения здравоохранения> осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению <наименование учреждения здравоохранения>) с момента такого обращения или получения указанного запроса на период проверки.

6.2.5.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных <наименование учреждения здравоохранения> осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению <наименование учреждения здравоохранения>) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.2.5.3. В случае подтверждения факта неточности персональных данных <наименование учреждения здравоохранения> на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению <наименование учреждения здравоохранения>) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.2.5.4. В случае выявления неправомерной обработки персональных данных, осуществляемой <наименование учреждения здравоохранения> или лицом, действующим по поручению <наименование учреждения здравоохранения>, <наименование учреждения здравоохранения> в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению <наименование учреждения здравоохранения>.

6.2.5.5 в случае если обеспечить правомерность обработки персональных данных невозможно, <наименование учреждения здравоохранения> в срок, не превышающий десяти рабочих дней даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных <наименование учреждения здравоохранения> уведомляет

субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.2.5.6. В случае достижения цели обработки персональных данных <наименование учреждения здравоохранения> прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению <наименование учреждения здравоохранения> и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению <наименование учреждения здравоохранения>) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между <наименование учреждения здравоохранения> и субъектом персональных данных либо если <наименование учреждения здравоохранения> не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральным законом «о персональных данных» или другими федеральными законами.

6.2.5.7. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных <наименование учреждения здравоохранения> прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению <наименование учреждения здравоохранения>) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению <наименование учреждения здравоохранения>) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между <наименование учреждения здравоохранения> и субъектом персональных данных либо если <наименование учреждения здравоохранения> не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральным законом «о персональных данных» или другими федеральными законами.

6.2.5.8. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, <наименование учреждения здравоохранения> блокирует такие персональные данные или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению <наименование учреждения здравоохранения>) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.2.6. Уведомление об обработке персональных данных

6.2.6.1. <наименование учреждения здравоохранения>, за исключением случаев, предусмотренных федеральным законом «о персональных данных», до начала обработки персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

6.2.6.2. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление содержит следующие сведения:

1) наименование (фамилия, имя, отчество), адрес <наименование учреждения здравоохранения>;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых <наименование учреждения здравоохранения> способов обработки персональных данных;

7) описание мер, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

8) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

9) дата начала обработки персональных данных;

10) срок или условие прекращения обработки персональных данных;

11) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

12) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан российской федерации;

13) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными правительством российской федерации.

6.2.6.3. В случае изменения указанных сведений, а также в случае прекращения обработки персональных данных <наименование учреждения здравоохранения> уведомляет об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

7. Сферы ответственности

7.1. Лица, ответственные за организацию обработки персональных данных в организациях

7.1.1. <наименование учреждения здравоохранения> назначает лицо, ответственное за организацию обработки персональных данных.

7.1.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

7.1.3. <наименование учреждения здравоохранения> предоставляет лицу, ответственному за организацию обработки персональных данных, необходимые сведения.

7.1.4. Лицо, ответственное за организацию обработки персональных данных, в частности, выполняет следующие функции:

1) осуществляет внутренний контроль за соблюдением <наименование учреждения здравоохранения> и сотрудниками <наименование учреждения здравоохранения> законодательства российской федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводит до сведения сотрудников <наименование учреждения здравоохранения> положения законодательства российской федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

7.2. Ответственность

7.2.1. Лица, виновные в нарушении требований федерального закона «о персональных данных», несут предусмотренную законодательством российской федерации ответственность.

7.2.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральным законом «о персональных данных», а также требований к защите персональных данных, установленных в соответствии с федеральным законом «о персональных данных», подлежит возмещению в соответствии с законодательством российской федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

8. Ключевые результаты

8.1 при достижении целей ожидаются следующие результаты:

– обеспечение защиты прав и свобод субъектов персональных данных при обработке его персональных данных <наименование учреждения здравоохранения>;

– повышение общего уровня информационной безопасности <наименование учреждения здравоохранения>;

– минимизация юридических рисков <наименование учреждения здравоохранения>.

Лист ознакомления с политикой в отношении обработки персональных данных в <наименование учреждения здравоохранения>

№ п/п	Фио	Должность	Дата	Подпись

Приложение № 3
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

Список
лиц, допущенных к обработке персональных данных в РМИС Псковской области

№ п/п	Должность	Фамилия и инициалы
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		

Разработал _____

«___» _____20__г.

Приложение № 4
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

ПРАВИЛА

ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила устанавливают порядок получения, учета, обработки, накопления и хранения документов, содержащих персональные данные, обработка которых необходима для целей, определенных законодательством Российской Федерации.

1.2. Цель настоящих Правил - защита персональных данных граждан от несанкционированного доступа и разглашения. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

1.3. Основанием для разработки настоящих Правил являются Конституция Российской Федерации, Федеральный закон «О персональных данных» №152-ФЗ от 27 июля 2006 года и другие действующие нормативно-правовые акты Российской Федерации.

1.4. Настоящее Правила и изменения к ним утверждаются *<должность руководителя> <наименование учреждения здравоохранения>*, вступают в силу с момента их утверждения и действуют бессрочно, до замены их новыми Правилами. Все изменения в Правила вносятся приказом *<должность руководителя> <наименование учреждения здравоохранения>*. Все сотрудники, допущенные к обработке персональных данных должны быть ознакомлены под роспись с данными Правилами и изменениями к ним.

1.5. В настоящих Правилах используются следующие термины и определения:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.6. Настоящие Правила и изменения к ним подлежат опубликованию на официальном сайте в течение 10 дней после их утверждения.

2. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных допускается в случаях, установленных Федеральным законом «О персональных данных» №152-ФЗ от 27 июля 2006 года.

2.2. В соответствии с Федеральным законом «О персональных данных» №152-ФЗ от 27 июля 2006 года, статья 6, ч.1, п. 4, а также Федеральным законом «Об организации предоставления государственных и муниципальных услуг» №210-ФЗ от 27 июля 2010 года, статья 7, ч.4 не требуется получение согласия заявителя как субъекта персональных данных. Во всех остальные случаях, в соответствии с Федеральным законом «О персональных данных» №152-ФЗ от 27 июля 2006 года, необходимо получение согласия заявителя как субъекта персональных данных.

2.3. Перечень персональных данных, обрабатываемых в *<наименование учреждения здравоохранения>*, утверждается *<должность руководителя> <наименование учреждения здравоохранения>*.

2.4. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.5. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.6. Содержание и объем обрабатываемых персональных данных должны соответствовать целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона №152-ФЗ от 26.07.2006 года «О персональных данных»;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом №152-ФЗ от 27 июля 2006 года «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

– иные сведения, предусмотренные законодательством Российской Федерации.

3.2. Сведения, указанные в пункте 3.1. настоящих Правил, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

3.3. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3.4. Сведения, указанные в 3.1. настоящих Правил, предоставляются субъекту персональных данных или его представителю оператором при обращении, либо при получении письменного запроса субъекта персональных данных или его представителя. Порядок рассмотрения запросов субъектов персональных данных устанавливается «Правилами рассмотрения запросов субъектов персональных данных или их представителей», разработанных в *<наименование учреждения здравоохранения>* на основании требований Федерального закона «О персональных данных» №152-ФЗ от 27 июля 2006 года и иных нормативно-правовых актов.

4. СРОКИ ОБРАБОТКИ И ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки

персональных данных, если срок хранения персональных данных не установлен федеральными законами, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

4.2. Персональные данные подлежат уничтожению, в течение тридцати дней, по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не установлено действующим законодательством.

4.3. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пункте 4.2. настоящих Правил, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более, чем шесть месяцев, если иной срок не установлен федеральными законами.

4.4. Уничтожение бумажных носителей должно осуществляться сотрудниками, допущенными к обработке персональных данных, путем, не допускающим дальнейшую возможность ознакомления с данными документами. Уничтожение информации на автоматизированных рабочих местах должно осуществляется комиссией способами, не позволяющими осуществить восстановление данных.

4.5. При уничтожении данных составляется, в обязательном порядке, акт с указанием, какие именно документы и файлы были уничтожены.

4.6. Решение об уничтожении принимается *<должность руководителя>* *<наименование учреждения здравоохранения>* на основании ходатайства ответственного за обеспечение безопасности персональных данных.

5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1 Доступ к персональным данным имеют лица, согласно «Перечню должностей, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным».

5.2 Сотрудники *<наименование учреждения здравоохранения>*, допущенные к обработке персональных данных, имеют право получать только те персональные данные, которые необходимы им для выполнения своих должностных обязанностей.

5.3 Все лица, допущенные к работе с персональными данными, подписывают обязательство о неразглашении персональных данных, ставших известными им в связи с исполнением должностных обязанностей.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В целях обеспечения сохранности и конфиденциальности персональных данных все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только сотрудниками, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

6.2. Оператор назначает из числа сотрудников ответственного за организацию обработки персональных данных, в обязанности которого, в частности, входит:

– осуществление внутреннего контроля за соблюдением оператором и его сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доведение до сведения сотрудников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений и запросов.

6.3. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений о гражданах.

6.4. Передача информации, содержащей сведения о персональных данных граждан, по телефону, факсу, электронной почте без письменного согласия гражданина запрещается.

6.5. Личные дела и документы, содержащие персональные данные граждан, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

6.6. Средства вычислительной техники (автоматизированные системы), используемые для обработки персональных данных должны быть защищены в соответствии с действующими нормативно-правовыми актами Российской Федерации.

7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ ГРАЖДАНИНА

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных граждан, несут дисциплинарную, административную,

гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Разработал _____

<наименование учреждения здравоохранения>

ПРИКАЗ

«____» _____ 20____года № _____

О контролируемой зоне

В соответствии с требованиями «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденными приказом №282 Гостехкомиссии от 30 августа 2002 года:

ПРИКАЗЫВАЮ:

1. Определить границу контролируемой зоны по периметру территорий, занимаемых *<наименование учреждения здравоохранения>*.

2. Обеспечение контролируемой зоны возлагается на администратора безопасности информации.

3. Контроль исполнения приказа возложить на _____.

<должность руководителя> _____ *<Фамилия И.О.>*

Приложение № 5
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

ТЕХНОЛОГИЧЕСКАЯ ИНСТРУКЦИЯ
ПО РАБОТЕ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности информации (АБ) - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств защиты информации информационных систем *<наименование учреждения здравоохранения>*, предназначенных для обработки информации, содержащей персональные данные.

1.2. АБ в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой в РМИС Псковской области.

1.3. АБ назначается приказом *<должность руководителя> <наименование учреждения здравоохранения>*.

1.4. АБ в своей работе руководствуется положениями нормативно - правовых актов РФ, руководящими документами по безопасности информации, положениями, приказами и нормативными актами министерств и ведомств Российской Федерации и положениями настоящей Инструкции.

2. ОСНОВНЫЕ ОБЯЗАННОСТИ

Основными обязанностями АБ являются:

- управление средствами и системами защиты информации (СЗИ) РМИС Псковской области и поддержание их функционирования;
- восстановление функций программных и технических СЗИ от несанкционированного доступа (НСД) к информации;
- генерация ключей, личных идентификаторов, а так же паролей для пользователей РМИС Псковской области;
- формирование и управление списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;
- назначение прав доступа, полномочий и привилегий пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода (УВВ);
- обеспечение правильной эксплуатации технических и программных СЗИ в РМИС Псковской области;
- контроль целостности эксплуатируемого в РМИС Псковской области программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;
- выявление, анализ и устранение уязвимостей и иных недостатков в программном обеспечении;

– текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации;

– контроль соблюдения пользователями РМИС Псковской области требований инструкций и порядка работы при обработке информации в РМИС Псковской области по вопросам защиты информации от НСД;

– контроль выполнения утвержденной технологии обработки информации в РМИС Псковской области;

– контроль состава технических средств, программного обеспечения и средств зашиты информации;

– контроль за установкой программного обеспечения, запрет установки неразрешённого программного обеспечения (в том числе средств обработки и отладки);

– контроль установки обновлений программного обеспечения;

– обеспечение доступа пользователей (при необходимости) к информации посредствам технологий беспроводного доступа, и контроль за использованием данных технологий;

– контроль за использованием в информационной системе мобильных технических средств;

– выявление подозрительных действий пользователей и попыток НСД к информации, обрабатываемой в РМИС Псковской области, путем анализа системных журналов информационной безопасности при работе в РМИС Псковской области;

– обучение и консультация персонала и пользователей РМИС Псковской области правилам работы с СЗИ от НСД;

– организация антивирусной защиты информации и программных средств в РМИС Псковской области;

– контроль электронного журнала сообщений, и обеспечение доступа к нему лицам которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

– определение событий, относящихся к безопасности персональных данных, и подлежащих регистрации;

– определение состава и содержания информации о событиях, относящихся к безопасности персональных данных и подлежащих регистрации;

– просмотр и анализ результатов регистрации событий, относящихся к безопасности персональных данных, и реагирование на них;

– контроль безотказного функционирования технических средств, принятие мер по восстановлению отказавших средств.

3. ПРАВА

АБ имеет право:

– требовать от пользователей РМИС Псковской области выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности РМИС Псковской области.

– останавливать обработку информации в РМИС Псковской области в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования СЗИ.

4. ОТВЕТСТВЕННОСТЬ

4.1. На АБ возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

4.2. АБ несет ответственность по законодательству РФ за нарушение требований нормативно – методических документов по защите информации и настоящей инструкции.

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 2
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

Перечень
защищаемых ресурсов РМИС Псковской области

№ п/п	Защищаемый ресурс		
	Сведения, содержащиеся в защищаемом ресурсе	**Наименование ресурса (реализация ресурса)**	**Степень конфиденциальности информации, содержащейся в защищаемом ресурсе**
1	Сведения, включенные в «Перечень персональных данных, обрабатываемых в РМИС Псковской области».	Файлы и архивы файлов, расположенные на несъемном жестком магнитном диске АРМ, учтенном в «Журнале учета машинных носителей информации».	Конфиденциально

Разработал _____

«___» _____20__г.

Приложение № 1
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

Перечень
персональных данных, обрабатываемых в РМИС Псковской области

В соответствии с Указом Президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера» в РМИС Псковской области обрабатываются следующие сведения конфиденциального характера:

– сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные, далее - ПДн), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

Обобщенный перечень информации, обрабатываемой в РМИС Псковской области, включает в себя следующие ПДн:

– адрес проживания;
– вид лечения;
– вид транспортировки;
– время и дата выписки (смерти);
– время и дата поступления
– время нахождения в лечебном учреждении;
– выписной эпикриз;
– госпитализация;
– гражданство;
– группа крови
– дата закрытия документа ВН;
– дата направления;
– дата открытия документа ВН;

– дата установки диагноза;
– диагноз направившего учреждения;
– диагнозы;
– информация о состоянии здоровья;
– кем доставлен;
– код врача;
– код первого профильного отделения, код врача первого профильного отделения;
– кратность госпитализации по поводу данного заболевания;
– медицинское заключение;
– наименование кладбища;
– наименование отделения;
– наличие детей младше 16 лет;
– непереносимость лекарств;
– номер истории болезни;
– номер медицинской карты;
– номер палаты;
– номер СНИЛС;
– номера банковских (лицевых) счетов;
– паспортные данные;
– пол;
– признак доставки по экстренным показаниям;
– продолжительность госпитализации, исход и результат госпитализации;
– резус-принадлежности;
– сведения о детях;
– сведения о наличии социальных льгот, гарантированных государством (документы подтверждающие статусы: мать-одиночка, чернобылец, ветеран войны и т.д.);
– сведения о подразделении работы, должность;
– сведения о семейном положении и состав семьи (муж/жена, дети);
– сведения об учреждении и о сотруднике направившего гражданина;
– фамилия, имя, отчество;
– характер заболевания;
– шифр диагноза осложнения (МКБ-10);
– шифр сопутствующего диагноза (МКБ-10).

При этом под обработкой информации понимается любое действие (операция) или совокупность действий (операций) с данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление или уничтожение данных.

Разработал _____

Приложение № 6
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

ИНСТРУКЦИЯ
ОТВЕТСТВЕННОМУ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных <*наименование учреждения здравоохранения*> назначается приказом <*должность руководителя*> <*наименование учреждения здравоохранения*>.

1.2. Методическое руководство работой ответственного за организацию обработки персональных данных осуществляется администратором безопасности информации.

1.3. Ответственный за организацию обработки персональных данных в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК России и ФСБ России по защите информации и организационно-распорядительными документами и несет персональную ответственность за свои действия.

1.4. Техническое обслуживание, уборка помещения и т.п. проводятся под контролем ответственного за организацию обработки персональных данных или другого ответственного лица.

2. ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Осуществляет контроль за целевым использованием РМИС Псковской области, всех периферийных устройств и технических средств, входящих в состав РМИС Псковской области.

2.2. Следит за тем, чтобы в период обработки защищаемой информации в помещении, где размещается РМИС Псковской области, не находились посторонние лица, не допущенные в установленном порядке к обрабатываемой информации.

2.3. Проводит периодический контроль принятых организационных мер, направленных на исключение несанкционированного доступа в помещение.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

3.2. Обеспечивать функционирование РМИС Псковской области в пределах возложенных на него функций.

3.3. В случае нарушения работоспособности (отказа) технических средств и программного обеспечения РМИС Псковской области, в том числе средств защиты информации, немедленно докладывать о случившемся администратору безопасности информации.

3.4. Обеспечивать постоянный контроль выполнения установленного комплекса мероприятий по обеспечению безопасности информации.

3.5. Контролировать целостность печатей (пломб) на устройствах РМИС Псковской области.

3.6. Соблюдать порядок учета, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов, электронных копий документов.

3.7. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств РМИС Псковской области и отправке их в ремонт. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования, с последующей аттестацией РМИС Псковской области по требованиям безопасности информации.

3.8. Присутствовать при выполнении технического обслуживания РМИС Псковской области, при установке (модификации) программного обеспечения.

3.9. Информировать администратора безопасности информации о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам РМИС Псковской области.

3.10. Контролировать соответствие состава технических средств техническому паспорту на РМИС Псковской области (в т.ч. реальной конфигурации информационных связей).

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

<наименование учреждения здравоохранения>

ПРИКАЗ

«____» _____ 20____года № _____

Об организации работ по обеспечению
безопасности информации при
ее обработке в РМИС Псковской области

С целью организации работ по обеспечению безопасности информации при ее обработке в Региональной медицинской информационной системе Псковской области (далее – РМИС Псковской области)

ПРИКАЗЫВАЮ:

1. Для защиты информации в РМИС Псковской области обеспечить соблюдение требований руководящих и нормативно-методических документов ФСТЭК России и ФСБ России всеми сотрудниками <*наименование учреждения здравоохранения*>.

2. Назначить следующих ответственных лиц:

   - за организацию обработки персональных данных -
   _____

   - администратор безопасности информации -
   _____

   - за обеспечение безопасности персональных данных -
   _____

3. Утвердить «Перечень персональных данных, обрабатываемых в РМИС Псковской области» (Приложение №1).

4. Утвердить «Перечень защищаемых ресурсов РМИС Псковской области» (Приложение № 2).

5. Утвердить «Список лиц, допущенных к обработке персональных данных в РМИС Псковской области» (Приложение №3).

6. Утвердить и ввести в действие «Правила обработки персональных данных» (Приложение № 4).

7. Утвердить и ввести в действие «Технологическую инструкцию по работе администратора безопасности информации» (Приложение № 5).

8. Утвердить и ввести в действие «Инструкцию ответственному за организацию обработки персональных данных» (Приложение № 6).

9. Утвердить и ввести в действие «Инструкцию о порядке технического обслуживания, ремонта, модернизации технических средств» (Приложение № 7).

10. Утвердить и ввести в действие «Инструкцию по проведению антивирусного контроля» (Приложение № 8).

11. Утвердить и ввести в действие «Инструкцию по применению парольной защиты и личных идентификаторов» (Приложение № 9).

12. Утвердить и ввести в действие «Инструкцию по работе пользователей» (Приложение № 10).

13. Утвердить и ввести в действие «Инструкцию об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные» (Приложение № 11).

14. Утвердить и ввести в действие «Инструкцию ответственному за обеспечение безопасности персональных данных в информационных системах персональных данных» (Приложение № 12).

15. Утвердить и ввести в действие «Регламент резервного копирования и восстановления информации» (Приложение № 13).

16. Утвердить «Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных» (Приложение № 14).

17. Утвердить «Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным» (Приложение № 15).

18. Утвердить и ввести в действие «Порядок доступа сотрудников в помещения, предназначенные для обработки персональных данных» (Приложение № 16).

19. Утвердить и ввести в действие «Правила проведения внутреннего контроля и проверок соответствия обработки персональных данных требованиям к защите персональных данных» (Приложение 17).

20. Утвердить и ввести в действие «Правила рассмотрения запросов субъектов персональных данных или их представителей» (Приложение № 18).

21. Утвердить «Перечень лиц, имеющих доступ в помещения, где происходит обработка персональных данных» (Приложение № 19).

22. Утвердить и ввести в действие «Правила работы с обезличенными персональными данными» (Приложение № 20).

23. Утвердить и ввести в действие «Типовую форму обязательства о неразглашении конфиденциальной информации (персональных данных)» (Приложение № 21).

24. Утвердить и ввести в действие «Типовую форму согласия на обработку персональных данных» (Приложение № 22).

25. Утвердить и ввести в действие «Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные» (Приложение № 23).

26. С настоящим приказом и его приложениями ознакомить всех сотрудников (под роспись) в части, их касающейся.

27. Контроль исполнения приказа возложить на _____.

<должность руководителя> _____ *<Фамилия И.О.>*

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 10
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

ИНСТРУКЦИЯ
ПО РАБОТЕ ПОЛЬЗОВАТЕЛЕЙ В РЕГИОНАЛЬНОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ПСКОВСКОЙ ОБЛАСТИ

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Пользователями Региональной медицинской информационной системе Псковской области (далее - РМИС Псковской области) <*наименование учреждения здравоохранения*> являются сотрудники <*наименование учреждения здравоохранения*>, допущенные к работе в РМИС Псковской области.

1.2. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в РМИС Псковской области.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. При эксплуатации РМИС Псковской области пользователь обязан:

2.1.1. Руководствоваться требованиями следующих документов:

– «Инструкция по применению парольной защиты и личных идентификаторов», в части их касающейся;

– «Инструкция по проведению антивирусного контроля», в части их касающейся;

– «Инструкция об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные», в части их касающейся;

– настоящей инструкцией.

2.1.2. Помнить личные пароли и идентификаторы.

2.1.3. Соблюдать установленную технологию обработки информации.

2.1.4. Руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники (СВТ) и средств защиты информации (СЗИ).

2.1.5. Размещать устройства вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

2.2. При выходе в течение рабочего дня из помещения, в котором размещается РМИС Псковской области, пользователь обязан:

– блокировать ввод-вывод информации на своем рабочем месте РМИС Псковской области в случаях кратковременного отсутствия (перерыв) или выключать СВТ РМИС Псковской области;

– блокировать вывод информации на монитор ПЭВМ;

2.3. Пользователю **ЗАПРЕЩАЕТСЯ**:

– подключать к ПЭВМ нештатные устройства;

– производить загрузку нештатной операционной системы с внешнего носителя;

– самостоятельно вносить изменения в состав, конфигурацию и размещение РМИС Псковской области;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения (ПО), установленного в РМИС Псковской области;

– устанавливать запрещенное к использованию ПО (средства обработки и отладки);

– самостоятельно вносить изменения в размещение, состав и настройку СЗИ РМИС Псковской области;

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам пароли, передавать личные идентификаторы, ключевые дискеты и другие реквизиты доступа к ресурсам РМИС Псковской области.

3. ПРАВА

Пользователь РМИС Псковской области имеет право:

– обращаться к администратору безопасности информации (АБ) с просьбой об оказании технической и методической помощи по обеспечению безопасности, обрабатываемой в РМИС Псковской области информации, по использованию установленных программных и технических средств РМИС Псковской области, а также по вопросам эксплуатации установленных СЗИ;

– обращаться к ответственному за организацию обработки ПДн по вопросам эксплуатации РМИС Псковской области (выполнение установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности объекта и защиты информации);

– обращаться к ответственному за обеспечение безопасности персональных данных по вопросам выполнения режимных мер при обработке информации.

4. ОТВЕТСТВЕННОСТЬ

Пользователь несет персональную ответственность:

– за соблюдение установленной технологии обработки информации;

– за соблюдение режима конфиденциальности при обработке и хранении в РМИС Псковской области информации;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в РМИС Псковской области;

– за соблюдение требований нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с персональными данными.

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 11
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

ИНСТРУКЦИЯ
об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные

1. Настоящая Инструкция устанавливает организацию учета, хранения и выдачи машинных носителей, содержащих персональные данные *<наименование учреждения здравоохранения>*.

2. Учет, хранение и выдачу машинных носителей, содержащих персональные данные, осуществляют ответственные за организацию обработки персональных данных. Данные сотрудники несут личную ответственность за сохранность персональных данных.

3. Организация учета машинных носителей персональных данных.

Все находящиеся на хранении и в обращении машинные носители, содержащие персональные данные (далее - машинные носители) подлежат учёту. Учет всех видов и типов машинных носителей производится в Журнале учета машинных носителей информации. Форма журнала учета машинных носителей информации приведена в Приложении №1 к настоящей инструкции.

4. Организация выдачи машинных носителей

При получении или возврате машинных носителей ответственным за организацию обработки персональных данных делаются соответствующие записи в Журнале учета машинных носителей информации.

5. Организация хранения машинных носителей

Хранение машинных носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение информации, а также хищение машинных носителей. Машинные носители должны храниться в служебных помещениях, в металлическом хранилище (сейфе) в установленном порядке. Запрещается хранить машинные носители на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

6. В случае утраты машинных носителей либо разглашения, содержащихся в них сведений, ответственный за организацию обработки персональных данных немедленно ставит в известность ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных. При утрате машинных носителей производится служебное расследование. Соответствующие отметки вносятся в Журнале

учета машинных носителей информации.

Для проведения служебного расследования *<должность руководителя> <наименование учреждения здравоохранения>* назначает комиссию, в состав которой входят не заинтересованные в исходе дела компетентные сотрудники *<наименование учреждения здравоохранения>* либо приглашенные специалисты. Комиссия состоит из трех-четырех человек, которые имеют отношение к персональным данным и допущены в соответствующем порядке.

Комиссия по проведению служебного расследования обязана:

– определить обстоятельства, при которых имело место утраты;

– содействовать розыску утраченных машинных носителей;

– выявить всех виновных лиц в утрате машинных носителей;

– выявить причины, которые способствуют утрате машинных носителей;

– выявить условия, при которых имело или может иметь место утрата машинных носителей;

– выработать рекомендации по устранению всех возможных рисков, связанных с потерей машинных носителей.

Членам комиссии при проведении расследования не запрещается:

– проводить досмотр местности, помещений, предметов мебели, канцелярских принадлежностей, где потенциально возможно нахождение машинных носителей;

– проверять все существующие машинные носители;

– вести опрос сотрудников, которые могут иметь возможность или мотивы для утраты машинных носителей, а также все возможных работников, которые могут оказать содействие в установлении обстоятельств утраты машинных носителей.

Служебное расследование необходимо проводить не более месяца. Прекращение розыска утраченных машинных носителей может быть прекращено только в случаях:

– исчерпания всех возможных мер розыска;

– внесена ясность в происшедшее;

– выявлены виновные.

Решение о завершении или приостановлении расследования утверждается *<должность руководителя> <наименование учреждения здравоохранения>*.

По завершению служебного расследования комиссии необходимо представить *<должность руководителя> <наименование учреждения здравоохранения>* следующие документы:

– выводы о результатах проведенного служебного расследования;

– письменные объяснения лиц, которых опрашивали члены комиссии;

– акты проверок наличия машинных носителей, осмотра и проверки служебных помещений, хранилищ и т.п.;

– другие документы, имеющие отношение к служебному расследованию.

7. Машинные носители, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. По результатам уничтожения машинных носителей составляется Акт уничтожения машинных носителей, содержащих персональные данные.

8. При передаче средств вычислительной техники РМИС Псковской области сторонним организациям для проведения ремонтно-восстановительных или иных работ, машинные носители, изымаются из состава средств вычислительной техники.

9. При увольнении ответственного за организацию обработки персональных данных, составляется акт приема-передачи машинных носителей, который утверждается <*должность руководителя*> <*наименование учреждения здравоохранения*>.

10. Ответственность за сохранность машинных носителей, при выполнении непосредственных работ с носителями, несет пользователь РМИС Псковской области.

11. Контроль выполнения пользователями установленных правил учета, хранения и выдачи машинных носителей, содержащих персональных данных, осуществляет ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в рамках своих должностных обязанностей.

Приложение 1
к инструкции об организации учета,
хранения и выдачи машинных
носителей информации

Форма журнала учета, хранения и выдачи машинных носителей информации

№ п/п	Тип машинного носителя информации	Серийный (инвентарный) номер	Учетный номер	Кол-во экз.	Номер экз.	Расписка в получении (дата, ФИО и подпись), отметка об отправке	Расписка в обратном приеме (дата, ФИО и подпись)	Примечание

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 12
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

ИНСТРУКЦИЯ
ОТВЕТСТВЕННОМУ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность лица, назначенного ответственным за обеспечение безопасности персональных данных.

1.2. Ответственный за обеспечение безопасности персональных данных назначается приказом *<должность руководителя> <наименование учреждения здравоохранения>*.

1.3. Ответственный за обеспечение безопасности персональных данных в своей работе руководствуется требованиями руководящих документов по безопасности информации, положениями нормативно-правовых актов РФ, приказами, а также положениями настоящей Инструкции.

1.4. Ответственный за обеспечение безопасности персональных данных является лицом, ответственным за выявление инцидентов в информационной системе и реагирование на них.

2. ОСНОВНЫЕ ОБЯЗАННОСТИ

Основными действиями ответственного за обеспечение безопасности персональных данных при выполнении своих обязанностей являются:

2.1. Проведение инструктажа и консультации пользователей ПЭВМ по соблюдению установленного режима конфиденциальности при обработке персональных данных.

2.2. Взаимодействие с ответственными за организацию обработки персональных данных и администратором безопасности информации (АБ) по вопросам обеспечения защиты информации и прав доступа пользователей к ней.

2.3. Выполнение, учет и контроль изменений, вносимых:

- в списки пользователей;
- в перечень защищаемых информационных ресурсов;

2.4. Организация и проведение периодического и внеочередного контроля работы пользователей.

2.5. Контроль выполнения пользователями установленного режима конфиденциальности при обработке персональных данных, в том числе, соблюдения режима конфиденциальности при обращении с персональными идентификаторами, личными ключевыми дискетами и карточками паролей, со съемными машинными носителями информации, в процессе создания машинных документов, при процедурах «лечения» администратором безопасности информации зараженных файлов.

2.6. Участие в процедурах контроля операций по безопасному удалению личных файлов пользователя при прекращении полномочий учетной записи, по уничтожению (в установленном порядке) старых карточек паролей (при замене АБ паролей пользователям) и созданию новых карточек паролей.

2.7. Организация и участие в служебных расследованиях для выяснения причин утечки или воздействия на обрабатываемую информацию, компрометации паролей с целью выяснения величины нанесенного ущерба безопасности информации и выработки новых или совершенствования принятых технических и организационных мер по защите информации от реализации угрозы в будущем.

2.8. При возникновении необходимости, организация и участие в мероприятиях, связанных с событиями вскрытия, опечатывания, модификации состава, ремонта и т.д. технических средств. Опечатывание корпусов технических средств. Составление актов о вскрытии и опечатывании корпусов технических средств.

2.9. Проведение анализа воздействия изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение безопасности персональных данных.

2.10. Документальное оформление изменений в конфигурации информационной системы и системы защиты персональных данных.

2.11. Анализ инцидентов, в том числе, определение источников и причин возникновения инцидентов, а так же оценка их последствий, принятие мер по устранению последствий инцидентов.

2.12. Планирование и принятие мер по предотвращению повторного возникновения инцидентов.

3. ПРАВА

Ответственный за обеспечение безопасности персональных данных имеет право:

3.1. Требовать от пользователей выполнения положений следующих инструкций по обеспечению информационной безопасности:

– «Инструкцию по работе пользователей»;

– «Инструкцию по применению парольной защиты и личных идентификаторов», в части их касающейся;

– «Инструкцию по проведению антивирусного контроля», в части их касающейся;

– «Инструкцию об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные», в части их касающейся».

3.2. Участвовать в разработке мероприятий по совершенствованию системы защиты информации.

3.3. Вносить изменения в конфигурацию информационной системы и системы защиты персональных данных.

3.4. Обращаться к *<должность руководителя> <наименование учреждения здравоохранения>* с мотивированным предложением по приостановке процесса обработки информации или отстранению от работы пользователя в случаях систематического нарушения режима конфиденциальности, технологии обработки информации.

3.5. Требовать от пользователей и администраторов информационной системы своевременного информирования о возникновении инцидентов в информационной системе.

4. ОТВЕТСТВЕННОСТЬ

На ответственного за обеспечение безопасности персональных данных возлагается персональная ответственность за полноту и качество выполнения своих должностных обязанностей, а также за реализацию адекватных реальным угрозам безопасности информации режимных мер по защите информации и за их своевременное применение.

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 13
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

РЕГЛАМЕНТ

РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся в информационных системах <*наименование учреждения здравоохранения*>, разработан с целью:

– определения порядка резервирования данных для последующего восстановления работоспособности информационных систем <*наименование учреждения здравоохранения*> при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

– определения порядка восстановления информации в случае возникновения такой необходимости;

– упорядочения работы должностных лиц <*наименование учреждения здравоохранения*>, связанной с резервным копированием и восстановлением информации.

1.2. В настоящем документе регламентируются действия при выполнении следующих мероприятий:

– резервное копирование;

– контроль резервного копирования;

– хранение резервных копий;

– полное или частичное восстановление данных и приложений.

1.3. Резервному копированию подлежит информация следующих основных категорий:

– Персональные профили пользователей сети;

– Персональные данные в электронном виде, согласно «Перечню персональных данных, обрабатываемых в ЕГИСЗ Псковской области.

1.4. Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности «Для служебного пользования».

2. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ

2.1. Резервное копирование автоматизированных систем производится на основании следующих данных:

– состав и объем копируемых данных, периодичность проведения резервного копирования;

– максимальный срок хранения резервных копий -1 месяц;

– хранение 3-х следующих архивов:

- архив на 1-е число текущего месяца;

- архив среда-четверг, либо пятница-суббота текущей недели;
- архив, сделанный в текущую ночь.

2.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.

2.3. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за организацию обработки ПДн.

3. МЕТОДИКА РЕЗЕРВНОГО КОПИРОВАНИЯ

3.1. Резервное копирование осуществляется средствами ОС Windows путем копирования информации на несъемный жесткий диск.

4. КОНТРОЛЬ РЕЗУЛЬТАТОВ РЕЗЕРВНОГО КОПИРОВАНИЯ

4.1. Контроль результатов всех процедур резервного копирования осуществляется ответственным за организацию обработки ПДн в срок до 18 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

4.2. В случае обнаружения ошибки ответственный за организацию обработки ПДн сообщает об этом факте ответственному за обеспечение безопасности персональных данных до 18 часов текущего рабочего дня.

4.3. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

5. РОТАЦИЯ НОСИТЕЛЕЙ РЕЗЕРВНОЙ КОПИИ

5.1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

5.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются ответственным за организацию обработки ПДн.

5.3. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

5.4. Персональные данные с носителей, которые перестают использоваться в системе резервного копирования, должны стираться.

6. ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНЫХ КОПИЙ

6.1. В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации, согласованной с ответственным за организацию обработки ПДн в *<наименование учреждения здравоохранения>*.

6.2. После поступления заявки восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

7. МЕТОДИКА РЕЗЕРВНОГО КОПИРОВАНИЯ

7.1. Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы персональных данных или ее компонент, выполняется на основании приказа *<должность руководителя> <наименование учреждения здравоохранения>*.

Разработал _____

«___» _____20__г.

Приложение № 9
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

ИНСТРУКЦИЯ
по применению парольной защиты и личных идентификаторов

1. Настоящая Инструкция определяет порядок использования, генерации, смены и прекращения действия паролей и личных идентификаторов пользователей в РМИС Псковской области *<наименование учреждения здравоохранения>*, а также контроль действий пользователей при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе с паролями возлагается на администратора безопасности информации.

3. Пароли для всех учетных записей пользователей РМИС Псковской области должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);
- максимальное действие пароля - не более чем 90 дней;
- пароль не должен повторяться;
- пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.

4. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

4.1 При первичной регистрации пользователя в системе пароль ему назначает администратор безопасности информации.

4.2 Пользователи РМИС Псковской области обязаны хранить свой личный пароль втайне от других и не передавать любым способом пароль третьим лицам.

4.3. Пользователь РМИС Псковской области лично должен проводить смену пароля учетной записи регулярно не реже одного раза в три месяца.

5. Привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности информации.

5.1 Пользователи РМИС Псковской области получают свой идентификатор у администратора безопасности информации.

5.2 В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности информации.

5.3 Пользователь РМИС Псковской области обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

5.4 Пользователю РМИС Псковской области запрещается передавать свой личный идентификатор.

5.5 В случае утери личного идентификатора, пользователь РМИС Псковской области должен немедленно доложить об этом администратору безопасности информации.

5.6 При необходимости передачи пароля удаленному легальному пользователю РМИС Псковской области администратор безопасности должен обеспечить сохранность передачи данному пользователю пароля путем передачи на электронном носителе в зашифрованном виде, по защищенному каналу связи или путем личной передачи на бумажном носителе в опечатанном конверте. В случае если пользователь не подтвердил факт получения им пароля, администратор безопасности информации должен произвести смену пароля данного пользователя и произвести повторную передачу пароля.

6. При наличии технологической необходимости использования имен и паролей сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), пароли данных сотрудников должны быть незамедлительно изменены администратором безопасности информации.

7. Полная плановая смена паролей пользователей должна проводиться регулярно, но не реже одного раза в год.

8. В случае прекращения полномочий учетной записи пользователя РМИС Псковской области (увольнение, переход на другую работу, в другой отдел или помещение, а также

другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасности информации после окончания последнего сеанса работы данного пользователя в РМИС Псковской области.

9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности информации.

10. В случае компрометации личного пароля или утери личного идентификатора пользователя администратором безопасности информации должны быть немедленно предприняты меры в соответствии с п. 11 настоящей Инструкции.

11. Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

12. Пользователи РМИС Псковской области должны быть ознакомлены под роспись с личными паролями и с требованиями настоящей Инструкции.

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 7
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

ИНСТРУКЦИЯ
О ПОРЯДКЕ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ, РЕМОНТА,
МОДЕРНИЗАЦИИ ТЕХНИЧЕСКИХ СРЕДСТВ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, входящих в состав РМИС Псковской области, защищенных от несанкционированного доступа (НСД) и предназначенных для обработки и хранения персональных данных.

1.2. Данные работы проводятся только с разрешения *<должность руководителя> <наименование учреждения здравоохранения>* или лица, исполняющего его обязанности, после согласования с ответственным за организацию обработки ПДн или администратором безопасности информации.

2. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТ ПО ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ, РЕМОНТУ, МОДЕРНИЗАЦИИ

2.1. В случае, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) технических средств, входящих в состав РМИС Псковской области, ответственный за организацию обработки ПДн представляет служебную записку, в которой:

– указывает название и номер ПЭВМ (технического средства, системы), техническое обслуживание (ремонт, модернизацию) которой необходимо провести и с какой целью;

– обосновывает необходимость технического обслуживания (модернизации);

– указывает планируемые место и сроки работ, режим их проведения;

– перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью недопущения доступа к персональным данным посторонних лиц.

2.2. В случае если для проведения работ необходимо привлекать лиц, не имеющих постоянного допуска к работе на ПЭВМ или в помещение, составляется список сотрудников, который согласовывается с *<должность руководителя> <наименование учреждения здравоохранения>*.

Запрещается выносить технические средства и системы (ТСС), входящие в состав РМИС Псковской области, с территории здания без согласования с ответственным за организацию обработки ПДн и разрешения *<должность руководителя> <наименование учреждения здравоохранения>*.

2.3. Вскрытие печатей на корпусах ПЭВМ или других технических средств (систем) и последующее опечатывание производится комиссионно в присутствии администратора безопасности информации, о чём составляется акт.

В акте указывается:

– номер (название) помещения, в котором проводились работы;

– дата и время начала и окончания работ;

– лица, присутствовавшие при вскрытии и обслуживании (ремонте, модернизации);

– наличие, целостность и места размещения печатей (пломб, специальных защитных знаков) до вскрытия ПЭВМ (технического средства, системы);

– установленные неисправности;

– виды и результаты проведенных работ;

– замененные или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков;

– какими печатями (пломбами и т.д.) и в каких местах ПЭВМ (устройство) опечатано по окончании работ;

– необходимость проведения дополнительной специальной проверки и специальных исследований (сертификации) ПЭВМ (технического средства, системы) или её отдельных узлов;

– иная необходимая для дальнейшей работы и обеспечения безопасности информация.

2.4. Если для ремонта (модернизации) технических средств (системы, узла ПЭВМ в составе РМИС Псковской области) необходимо направить в специализированную организацию, то комиссией составляется заключение.

2.5. Перед отправкой ПЭВМ (другого технического средства, системы, узла ПЭВМ) администратор безопасности информации обязан гарантированно удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, о чем он совместно с ответственным за организацию обработки ПДн составляет акт. По запросу из специализированной организации копия акта передаётся и ей.

2.6. В случае если не имеется возможности гарантированно удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами или произвести обезличивание персональных данных, эти устройства опечатываются и хранятся у ответственного за организацию обработки ПДн с соблюдением требований, предъявляемым к хранению персональных данных.

2.7. Ремонт и замена жесткого диска производится с соблюдением требований п. п. 2.4.-2.6. настоящей Инструкции в присутствии администратора безопасности

информации. При диагностике и ремонте жесткого диска должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 14
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

ПЕРЕЧЕНЬ
должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

№ п/п	Подразделение	Должность
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		

Разработал _____

«___» _____20__г.

Приложение № 8
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

ИНСТРУКЦИЯ
по проведению антивирусного контроля

1. Настоящая Инструкция предназначена для пользователей РМИС Псковской области *<наименование учреждения здравоохранения>*.

2. В целях обеспечения антивирусной защиты в РМИС Псковской области производится антивирусный контроль.

3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации.

4. К применению в РМИС Псковской области допускаются лицензионные антивирусные средства.

5. В РМИС Псковской области запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

6. Пользователи РМИС Псковской области при работе со съемными носителями информации (компакт-дисками (CD- дисками), USB флеш-накопителями) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

7. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.

8. Администратор безопасности информации осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

9. Администратор безопасности информации проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

10. При обнаружении компьютерного вируса пользователь РМИС Псковской области обязан немедленно поставить в известность администратора безопасности информации и прекратить какие-либо действия в РМИС Псковской области.

11. Администратор безопасности информации проводит, в случае необходимости, лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

12. В случае обнаружения на съемных носителях информации нового вируса, не поддающегося лечению, администратор безопасности информации обязан запретить использование данного съемного носителя информации.

13. В случае обнаружения вируса, не поддающегося лечению, администратор безопасности информации обязан поставить в известность ответственного за организацию обработки ПДн, запретить работу в РМИС Псковской области и в возможно короткие сроки обновить пакет антивирусных программ.

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 20
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

ПРАВИЛА
РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными данными в <*наименование учреждения здравоохранения*> разработаны с учетом Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

1.2. Настоящие Правила определяют порядок работы с обезличенными данными в <*наименование учреждения здравоохранения*>.

1.3. Настоящие Правила утверждаются приказом <*должность руководителя*> <*наименование учреждения здравоохранения*>.

1.4. В настоящих Правилах используются следующие термины и определения:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

2.1. Обезличивание персональных данных может быть проведено с целью ведения статистического учета, снижения риска разглашения защищаемых персональных данных, а так же в иных целях, не противоречащих требованиям законодательства о защите персональных данных.

2.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- понижение точности некоторых сведений;
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

2.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

2.4. Для обезличивания персональных данных могут использоваться любые не противоречащие действующему законодательству способы.

2.5. Перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, утверждается приказом <*должность руководителя*> <*наименование учреждения здравоохранения*>:

2.5.1. <*должность руководителя*> <*наименование учреждения здравоохранения*> принимает решение о необходимости обезличивания персональных данных.

2.5.2. Руководители отделов, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

2.5.3. Сотрудники отделов, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

3. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

3.1. Обезличенные данные не подлежат разглашению в случае, когда в результате такого разглашения появляется вероятность определения принадлежности персональных данных конкретному субъекту персональных данных.

3.2. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение положений:

- «Инструкции по применению парольной защиты и личных идентификаторов»;
- «Инструкции по проведению антивирусного контроля»;
- «Инструкции об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные»;
- «Регламента резервного копирования и восстановления информации»;
- «Порядка доступа сотрудников в помещения, предназначенные для обработки персональных данных».

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- «Правил обработки персональных данных»;

– «Порядка доступа сотрудников в помещения, предназначенные для обработки персональных данных».

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 23
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

Типовая форма
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Уважаемый(-ая), *(инициалы субъекта персональных данных)*!

В соответствии с требованиями статьи 18 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» уведомляем Вас, что в целях:

_____

_____

(указать цели, для которых необходима обработка персональных данных)

оператору необходимо получить от Вас следующие персональные данные:

_____

_____

(указать, какие именно персональные данные или документы, их содержащие, должны быть представлены)

Обязанность предоставления Вами указанных персональных данных установлена:

_____

_____

(реквизиты и наименование нормативных правовых актов)

В случае Вашего отказа предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять их обработку, что приведет к следующим для Вас юридическим последствиям:

_____

_____

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных, либо имущественных прав граждан или случаи, иным образом затрагивающие его права, свободы и законные интересы)

_____ _____

(дата) (фамилия, инициалы и подпись сотрудника оператора)

УТВЕРЖДАЮ

<должность руководителя>

<наименование учреждения здравоохранения>

_____ *<Фамилия И.О.>*

«___» _____ 20___ г.

ИНСТРУКЦИЯ
ПО ОБРАЩЕНИЮ С СЕРТИФИЦИРОВАННЫМИ ФСБ РОССИИ СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – (СКЗИ)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция регламентирует порядок обращения со средствами криптографической защиты информации (далее СКЗИ), сертифицированными ФСБ, в процессе получения, доставки, хранения, тестирования, передачи и установки (инсталляции).

1.2. СКЗИ, включая аппаратные средства, инсталляционные дискеты, ключевую документацию, описания и инструкции к СКЗИ, составляют служебную тайну <*наименование учреждения здравоохранения*>.

1.3. Сотрудники допускаются к работе с СКЗИ на основании приказа <*должность руководителя*> <*наименование учреждения здравоохранения*> после прохождения необходимой подготовки.

1.4. Приказом <*должность руководителя*> <*наименование учреждения здравоохранения*> назначаются лица, ответственные за обеспечение безопасности при обращении с СКЗИ.

1.5. Все сотрудники, допущенные к работе с СКЗИ, должны строго выполнять требования настоящей инструкции в части, их касающейся. Указанные сотрудники должны ознакомиться с данной инструкцией под роспись.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ СКЗИ

2.1. Пользователи СКЗИ обязаны:

– не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;

– соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

– сообщать в ответственному пользователю криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– ведение технического (аппаратного) журнала;

– немедленно уведомлять ответственного пользователя криптосредств о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению

защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

3.1. Ответственный пользователь криптосредств обязан:

– контролировать соблюдение пользователями СКЗИ 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 СКЗИ и ключевых документах к ним;

– обеспечивать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

– своевременным выявлением попыток посторонних лиц получать сведения о защищаемой информации, об используемых криптосредствах или ключевых документах к ним;

– принимать меры по предупреждению разглашения защищаемой информации, 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.

– контролировать соблюдение условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ;

– расследовать и составлять заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации; разрабатывать и принимать меры по предотвращению возможных опасных последствий подобных нарушений;

– вести журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

– вести на каждого пользователя СКЗИ лицевой счет.

4. ТРЕБОВАНИЯ ПО РАЗМЕЩЕНИЮ, СПЕЦИАЛЬНОМУ ОБОРУДОВАНИЮ И ОХРАНЕ ПОМЕЩЕНИЙ, В КОТОРЫХ ПРОИЗВОДЯТСЯ РАБОТЫ С СКЗИ

4.1. Размещение, специальное оборудование, охрана и режим в помещениях, в которых производится работа с СКЗИ (далее - помещения), должны обеспечивать безопасность СКЗИ и исключать возможность неконтролируемого доступа к СКЗИ.

4.2. Доступ лиц в эти помещения должен быть ограничен и обеспечиваться в соответствии со служебной необходимостью и приказом *<должность руководителя> <наименование учреждения здравоохранения>*.

4.3. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь прочные входные двери, оборудованные надежными замками.

4.4. Входная дверь должна опечатываться металлической печатью, либо должна быть оборудована кодовым замком, код которого известен только сотрудникам, работающим в этом помещении.

4.5. По окончании рабочего дня ответственный сотрудник обязан закрыть помещение, опечатать помещение личной номерной печатью, сдать помещение под охрану с отметкой в журнале приема-сдачи помещений под охрану. При вскрытии помещений должны проверяться целостность печатей и замков. В случае нарушения целостности печатей или замков ответственный сотрудник обязан немедленно сообщить об этом лицу, ответственному пользователю криптосредств.

4.6. На дверях и оконных стеклах должны быть установлены датчики охранной сигнализации (при нахождении помещения вне крайних этажей допускается установка датчиков объемной сигнализации). В помещении должна быть установлена система пожарной сигнализации.

4.7. Для хранения СКЗИ, инсталляционных дискет, тестовых ключей, нормативной и эксплуатационной документации помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Сейфы должны быть оборудованы приспособлением для их опечатывания, либо специальным защитным замком для замочной скважины. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого *<должность руководителя> <наименование учреждения здравоохранения>*.

5. ПОРЯДОК ОБРАЩЕНИЯ С СКЗИ

5.1. СКЗИ, инсталляционные дискеты, тестовые ключи, нормативную и эксплуатационную документацию получает уполномоченный сотрудник *<наименование учреждения здравоохранения>* непосредственно у производителя СКЗИ. Безопасность в процессе доставки обеспечивается организационными мерами.

5.2. При транспортировке СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть обеспечены условия, исключающие возможность физических повреждений и внешнего воздействия на записанную информацию, а также копирование.

5.3. Все поступающие СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету.

5.4. Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

5.5. В соответствии с контрактом с производителем СКЗИ разрешается сделать одну копию программных СКЗИ (исключая ключевую информацию) для архива или обеспечения продажи, а также сделать одну дополнительную копию каждый раз, когда рабочая копия приходит в негодность и должна быть заменена. При этом ответственный сотрудник должен удостовериться, что каждая произведенная им копия отображает на дисплее авторские права производителя СКЗИ и другие указания в отношении собственности, которые записаны на оригинале.

5.6. Пользователи СКЗИ хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.7. Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов. При вскрытии сейфа должна быть проверена целостность печатей и замков. В случае нарушения целостности печатей или замков ответственный сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

5.8. Хранение инсталляционных дискет СКЗИ и тестовых ключей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами использования СКЗИ применение.

5.9. В случае отсутствия у сотрудника индивидуального хранилища инсталляционные дискеты СКЗИ и тестовые ключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

5.10. В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

5.11. Ответственными сотрудниками периодически должен проводиться контроль сохранности СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов.

5.12. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно - программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

5.13. Ответственный сотрудник <*наименование учреждения здравоохранения*> заносит в Журнал учета СКЗИ дату приема-передачи СКЗИ, фамилию, имя, отчество сотрудника, которому передаются СКЗИ, серийный номера СКЗИ. Все операции по передачи СКЗИ производятся под роспись.

5.14. В каждый экземпляр передаваемого СКЗИ должна быть включена ссылка на авторские права производителя, его товарный знак и другие обозначения в форме, согласованной с производителем. Вся документация на СКЗИ и на продукты, включающие СКЗИ, а также отображаемая на экране при запуске информация о нем должна включать вышеуказанные обозначения.

5.15. Установка (инсталляция) СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

6. ВОССТАНОВЛЕНИЕ СВЯЗИ В СЛУЧАЕ КОМПРОМЕТАЦИИ ДЕЙСТВУЮЩИХ КЛЮЧЕЙ К СКЗИ

6.1. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;

– случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

6.2. В случае возникновения обстоятельств, указанных в п.6.1 настоящей Инструкции, пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и сообщить о факте компрометации ответственному пользователю криптосредств.

6.3. О факте компрометации ключевой информации Пользователями совместно с Ответственным пользователем производится информирование всех заинтересованных участников информационного обмена.

6.4. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

6.5. Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в пункте 7 настоящей Инструкции.

7. УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

7.1. Уничтожение криптоключей производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (уничтожения) криптоключей без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

7.2. Криптоключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт - дисков (CD - ROM), eToken и т.п.). Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ.

7.3. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ.

7.4. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

7.5. Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали.

7.6. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация.

7.7. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под расписку в техническом (аппаратном) журнале.

7.8. Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным пользователем СКЗИ под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом, форма акта представлена в Приложении №1 к данной инструкции. Ответственный пользователь СКЗИ обеспечивает хранение данных актов.

7.9. Пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом ответственного пользователя СКЗИ для списания уничтоженных документов с их лицевых счетов. Не реже одного раза в год пользователи СКЗИ должны направлять ответственному пользователю СКЗИ письменные отчеты об уничтоженных ключевых документах.

7.10. Ответственный пользователь СКЗИ делает соответствующие отметки об уничтожении в журнале поэкземплярного учета СКЗИ.

8. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ИНСТРУКЦИИ

8.1. За нарушение требований настоящей Инструкции виновные в этом лица несут дисциплинарную, либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

Разработал _____

Приложение №1 к Инструкции
по обращению с сертифицированными
ФСБ России средствами криптографической
защиты информации

АКТ №_____
об уничтожении криптографических ключей и ключевых документов

Комиссия в составе:
Председателя:_____,
членов комиссии: _____
_____
_____

произвела уничтожение криптографических ключей и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)	Примечание

Всего уничтожено (_____) криптографических ключей на (_____) ключевых носителях. Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем их стирания в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/
_____ /_____/
_____ /_____/

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

<наименование учреждения здравоохранения>

ТЕХНИЧЕСКИЙ (АППАРАТНЫЙ)
ЖУРНАЛ № ____

Начат: «__»_____ 20__г.

Окончен: «__»_____20__г.

20__г.

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

Приложение № 18
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

Правила рассмотрения запросов
субъектов персональных данных или их представителей

1. При поступлении письменного запроса субъекта персональных данных или их представителей ответственное лицо <*наименование учреждения здравоохранения*> должно зарегистрировать данный запрос в «Журнале учета обращений субъектов персональных данных по вопросам обработки персональных данных».

2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе, содержащей:

– подтверждение факта обработки персональных данных оператором;

– правовые основания и цели обработки персональных данных;

– цели и способы обработки персональных данных, применяемые в <*наименование учреждения здравоохранения*>;

– место нахождения <*наименование учреждения здравоохранения*>, сведения о лицах (за исключением сотрудников), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании федеральных законов;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению <*наименование учреждения здравоохранения*>, если обработка поручена такому лицу;

– иные сведения, предусмотренные действующим законодательством.

3. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных в <наименование учреждения здравоохранения>, подпись субъекта персональных данных

или его представителя (Приложение 1). Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. Сведения по запросу должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

5. В случае, если сведения, указанные в ответе (Приложение 2), были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе повторно обратиться или направить повторный запрос в целях получения сведений и ознакомления с персональными данными не ранее, чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральными законами, принятыми в соответствии с ними нормативными правовыми актами или договорами, стороной которых являются либо выгодоприобретатели, либо поручители.

6. Субъект персональных данных вправе повторно обратиться или направить повторный запрос в целях получения сведений, касающихся обработки его персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 5 настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 5 настоящих правил, должен содержать обоснование направления повторного запроса.

7. <*наименование учреждения здравоохранения*> вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным п.5 и п.6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на <наименование учреждения здравоохранения>.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том случае, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

Разработал _____

Приложение 1 к Правилам рассмотрения запросов субъектов персональных данных или их представителей

<должность руководителя>
<наименование учреждения здравоохранения>

от _____
(ФИО субъекта ПДн)
_____
(адрес регистрации субъекта ПДн)
_____
(паспортные данные субъекта ПДн)
_____
_____

З А П Р О С
(о предоставлении/ изменении / исключении
персональных данных субъекта)

Мною, _____, «____» _____ _____ г.
(ФИО) (дата предоставления ПДн)

в связи с осуществлением_____
_____

в *<наименование учреждения здравоохранения>* были предоставлены следующие персональные данные

_____
_____
_____
_____

(*указать, какие сведения были предоставлены, например: ФИО, паспортные данные, сведения о дате и месте рождения и т.п.*)

Указанные данные были предоставлены мною для_____
_____
_____

(*указать, для проведения какой операции были предоставлены данные*)

В настоящее время сообщаю об *изменении/исключении* следующих моих персональных данных в связи с _____
_____
_____
_____

(*указать какие данные, каким образом поменялись, например: - ФИО изменение Иванова И.И, на Петрова И.И.*)

В срок не позднее 7 (Семи) рабочих дней с даты получения документального подтверждения об изменении персональных данных прошу внести изменение/ исключить персональные данные в связи с_____

_____
_____
_____
(*прекращением отношений с <наименование учреждения здравоохранения>, утратой сведениями достоверности и т.д*).

Уведомить о факте изменения прошу по телефону номер _____.

приложение:
- _____
- _____

_____	_____	_____
(ФИО)	(подпись)	(дата)

Приложение 2 к Правилам рассмотрения запросов субъектов персональных данных или их представителей

ОТВЕТ НА ЗАПРОС
(о предоставлении/ изменении / исключении
персональных данных субъекта)

гр. _____
_____
_____

Уважаемый _____!

В ответ на Ваш запрос № _____ от _____, <*наименование учреждения здравоохранения*> (далее – оператор) сообщает: «___» _____ _____ г. оператор получил
от_____
сведения, содержащие персональные данные:
1. ФИО: _____,
2. паспортные данные: _____
_____
3. дата и место рождения: _____
4. _____
5. _____
6. _____
7._____
8. _____
9. _____
10._____

Указанные данные были получены в целях_____
_____
_____
на что предварительно было получено Ваше письменное согласие (копия прилагается).
В настоящее время, материальные носители, содержащие Ваши персональные данные –
_____,
хранятся в _____
по адресу_____.
Непосредственный доступ к ним имеют следующие лица: _____
_____
_____
_____
_____,

обязанность работы с персональными данными субъектов на них предусмотрена характером выполняемых трудовых обязанностей, а также Приказом № _____ <*наименование учреждения здравоохранения*>.

Необходимость хранения Ваших персональных данных связана с текущим исполнением условий договора и/или не достижением целей обработки персональных данных.

Вы можете безвозмездно ознакомиться с указанными персональными данными в срок не позднее 30 дней с даты подачи заявления на ознакомление с персональными данными по адресу _____.

Приложение № 16
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

Порядок доступа
сотрудников в помещения, предназначенные для обработки персональных данных

1. Настоящая инструкция определяет порядок допуска сотрудников *<наименование учреждения здравоохранения>* и других лиц в помещения, предназначенные для обработки персональных данных.

2. Ответственность за обеспечение исполнения требований настоящей инструкции несет ответственный за обеспечение безопасности персональных данных. Контроль за исполнением требований осуществляет *<должность руководителя>* *<наименование учреждения здравоохранения>*.

3. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

4. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники и должностные лица, получившие доступ к персональным данным.

5. Нахождение в помещениях, в которых ведется обработка персональных данных лиц, не являющихся сотрудниками и должностными лицами, получившими доступ к персональным данным, возможно только в присутствии сотрудников и должностных лиц, получивших доступ к персональным данным на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных функций.

6. Присутствие других лиц в данных помещениях допускается в той мере, в какой этого требуют технологические процессы обработки персональных данных. Доступ в помещения *<наименование учреждения здравоохранения>* осуществляется только в сопровождении сотрудника *<наименование учреждения здравоохранения>*, который

предварительно производит оценку целесообразности и требуемого времени нахождения лица в помещении, а также проверяет документы, удостоверяющие личность.

7. Сотрудники и должностные лица, получившие доступ к персональным данным не должны покидать помещение, в котором ведется обработка персональных данных, оставляя в нем без присмотра посторонних лиц, включая сотрудников, не уполномоченных на обработку персональных данных.

8. Доступ в помещения, в которых осуществляется обработка персональных данных, разрешается только в рабочее время.

9. Доступ в помещения, в которых осуществляется обработка персональных данных, в нерабочее время возможен только по письменной заявке работника, согласованной с его непосредственным руководителем и имеющей разрешающую резолюцию <*должность руководителя*> <*наименование учреждения здравоохранения*>. Данные заявки хранятся у лица, ответственного за организацию обработки персональных данных в <*наименование учреждения здравоохранения*>.

10. В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

11. Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных <*должность руководителя*> <*наименование учреждения здравоохранения*> или его заместителями. Работы проводятся под контролем сотрудников <*наименование учреждения здравоохранения*>.

12. Для исключения несанкционированного доступа к информации, содержащей ПДн, быть организована охрана помещений <*наименование учреждения здравоохранения*>. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

13. Уборка помещения выполняется обслуживающим персоналом под контролем сотрудников <*наименование учреждения здравоохранения*>, имеющих право доступа в данное помещение. Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть выключены все АРМ, на которых хранятся ПДн, носители, содержащие ПДн должны быть убраны в сейф.

14. После окончания рабочего дня дверь каждого помещения закрывается на

ключ, при этом запрещается оставлять ключ в замке помещения.

15. В нерабочее время помещения, в которых ведется обработка персональных данных, хранятся документы, содержащиеся персональные данные, должны закрываться на ключ и сдаваться под охрану.

16. По окончании рабочего дня помещения, в которых ведется обработка ПДн, и установленные в них хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале ответственному за организацию обработки персональных данных или лицу, им уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

17. Ключи от помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службе охраны или дежурному по организации одновременно с передачей под охрану самих помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников <*наименование учреждения здравоохранения*>, ответственных за эти хранилища.

18. При утрате ключа от хранилища или от входной двери в помещение, в котором ведется обработка ПДн, замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за безопасность персональных данных.

19. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за обеспечение безопасности персональных данных. Ответственный за обеспечение безопасности персональных данных должен составить акт и принять, при необходимости, меры к локализации последствий несанкционированного доступа к ПДн.

20. Контроль соблюдения настоящего Порядка осуществляется лицом, ответственным за организацию обработки персональных данных <*наименование учреждения здравоохранения*>.

21. Лицо, ответственное за организацию обработки персональных данных, в случае установления факта нарушения сотрудником <*наименование учреждения здравоохранения*> настоящего Порядка проводит с ним разъяснительную работу, а в

случае неоднократного нарушения – уведомляет руководство *<наименование учреждения здравоохранения>*.

Разработал _____

«___» _____20__г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 19
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

Перечень
лиц, имеющих доступ в помещения, где происходит обработка персональных данных

№ п/п	Должность	Фамилия и инициалы
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		

Разработал _____

«___» _____20__г.

Приложение № 21
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

Типовая форма обязательства
о неразглашении конфиденциальной информации
(персональных данных)

Я, _____,
(ФИО)

Исполняющий(ая) должностные обязанности по замещаемой должности _____

_____,
(должность, наименование структурного подразделения)

предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностным регламентом (должностной инструкцией) мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащей сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доведены (будут доведены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доведены (будут доведены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному начальнику, а также лицу, ответственному за организацию защиты информации в *<наименование учреждения здравоохранения>*.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. После прекращения трудового договора и увольнения прекратить обработку известных мне конфиденциальных сведений.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(Фамилия и инициалы) (подпись)

«____»_____20___г.

<наименование учреждения здравоохранения>

ПРИКАЗ

«____» _____ 20____года № _____

О создании комиссии

В целях осуществления мероприятий по допуску сотрудников к самостоятельной работе со средствами криптографической защиты информации

ПРИКАЗЫВАЮ:

1. Создать комиссию для приема зачетов по самостоятельной работе со средствами криптографической защиты информации в *<наименование учреждения здравоохранения>* информации в составе:
   Председатель комиссии -_____
   Члены комиссии: _____
   _____
   _____
2. Приказ довести до ответственных лиц.
3. Контроль за исполнением приказа возложить на _____.

<должность руководителя> _____ *<Фамилия И.О.>*

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

УТВЕРЖДАЮ

<должность руководителя>

<наименование учреждения здравоохранения>

_____ *<Фамилия И.О.>*

«___» _____ 20___ г.

Инструкция
о порядке допуска сотрудников *<наименование учреждения здравоохранения>* к самостоятельной работе со средствами криптографической защиты информации

1. Настоящая Инструкция разработана в соответствии с законодательством Российской Федерации, нормативными правовыми актами в области защиты информации, а также эксплуатационной документацией на используемые СКЗИ, и определяет порядок допуска сотрудников *<наименование учреждения здравоохранения>* к самостоятельной работе со средствами криптографической защиты информации (СКЗИ).

2. К самостоятельной работе с СКЗИ допускаются лица:

– принятые на работу в соответствии с приказом *<должность руководителя> <наименование учреждения здравоохранения>*;

– назначенные на должности, выполнение обязанностей по которым связано с хранением и использованием СКЗИ;

– прошедшие специальную подготовку (обучение) по программам, утвержденным Директором <наименование учреждения здравоохранения>;

– успешно сдавшие зачет комиссии, назначенной приказом *<должность руководителя> <наименование учреждения здравоохранения>*, на допуск к самостоятельной работе с СКЗИ.

3. Документом, подтверждающим специальную подготовку сотрудников *<наименование учреждения здравоохранения>* и возможность их допуска к самостоятельной работе с СКЗИ, является заключение (Приложение № 1), составленное комиссией на основании принятого зачета по программе подготовки (обучения). Заключения о допуске сотрудников к самостоятельной работе с СКЗИ утверждаются *<должность руководителя> <наименование учреждения здравоохранения>*.

4. Лица, принятые на работу в организацию и назначенные на должности, выполнение обязанностей по которым связано с хранением и использованием СКЗИ, не сдавшие зачет на

допуск к самостоятельной работе с СКЗИ до истечения установленного трудовым законодательством РФ испытательного срока, подлежат увольнению как не выдержавшие испытания.

5. Программы подготовки сотрудников *<наименование учреждения здравоохранения>* к самостоятельной работе с СКЗИ (Приложение № 2) разрабатываются ответственным пользователем криптосредств и утверждаются *<должность руководителя>* *<наименование учреждения здравоохранения>*, и должны включать:

– ознакомление с нормами действующего законодательства Российской Федерации, регулирующими отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации, защите информации, прав субъектов, участвующих в информационных процессах и информатизации, правила применения и использовании электронной цифровой подписи в электронных документах, а также информацию об ответственности за нарушение указанных норм;

– ознакомление с нормативными актами органов государственного управления Российской Федерации, определяющими порядок разработки, производства, реализации, использования СКЗИ, регламентирующими вопросы взаимодействия участников и информационного обмена с использованием СКЗИ;

– изучение должностных инструкций, положений, других локальных нормативных актов *<наименование учреждения здравоохранения>* по вопросам деятельности, связанной с разработкой, производством, хранением, реализацией и использованием СКЗИ;

– изучение эксплуатационно-технической документации на СКЗИ;

– приобретение практических навыков выполнения работ, предусмотренных обязанностями по занимаемой должности.

6. Методика подготовки сотрудников *<наименование учреждения здравоохранения>* к сдаче зачета на допуск к самостоятельной работе со СКЗИ определяется ответственным пользователем криптосредств и должна предусматривать как формы самостоятельного изучения и освоения программного материала сотрудником, так и формы группового и индивидуального обучения с привлечением подготовленных специалистов в качестве преподавателей.

7. Ответственность за полноту и качество подготовки сотрудников *<наименование учреждения здравоохранения>* к сдаче зачета на допуск к самостоятельной работе с СКЗИ возлагается на ответственного пользователя криптосредств.

Разработал _____

Приложение № 1
к «Инструкции о порядке допуска работников *<наименование учреждения здравоохранения>* к самостоятельной работе со средствами криптографической защиты информации»

ЗАКЛЮЧЕНИЕ
о допуске к самостоятельной работе с СКЗИ

Структурное подразделение _____

Должность _____

Фамилия, имя, отчество _____

с «__» _____ 20 __ г. по «__» _____ 20 __ г.

в соответствии с Программой, утвержденной *<должность руководителя>* *<наименование учреждения здравоохранения>* «__» _____20 __ г. прошел(ла) подготовку по специальности или виду работ

_____

количество часов _____ и сдал(а) зачет с общей оценкой_____ .

По решению комиссии _____ допущен(а) к самостоятельной работе со средствами криптографической защиты информации.

Председатель комиссии: _____

Члены комиссии: _____

_____

_____

«__» _____ 20 __ г.

<должность руководителя> _____

Приложение № 2
к «Инструкции о порядке допуска работников <*наименование учреждения здравоохранения*> к самостоятельной работе со средствами криптографической защиты информации»

ПРОГРАММА
подготовки к самостоятельной работе с СКЗИ

_____
(Фамилия и инициалы)

№ п/п	Изучаемые вопросы (темы)	Кол-во часов	Форма (метод) подготовки	Преподаватель
1	Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информатизации и защите информации»	4	Самоподго-товка	
2	Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»	2	Самоподго-товка	
3	Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности»	2	Самоподго-товка	
4	Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»	2	Самоподго-товка	
5	Положение о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (Положение ПКЗ-2005)	4	Лекция	
6	Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченным доступом, не содержащей сведений,	4	Лекция	.

№ п/п	Изучаемые вопросы (темы)	Кол-во часов	Форма (метод) подготовки	Преподаватель
	составляющих государственную тайну (приказ ФАПСИ РФ от 13 июня 2001 г. N 152)			
7	Эксплуатационно-техническая документация на используемые СКЗИ	12	Самоподго-товка	
8	Внутренние нормативные документы <*наименование учреждения здравоохранения*> • Должностные инструкции; • Инструкция по использованию сертифицированных ФСБ (ФАПСИ) СКЗИ в <*наименование учреждения здравоохранения*>; • Инструкция о порядке сдачи под охрану и вскрытия помещения (помещений).	6	Самоподго-товка	
9	Санитарные правила и нормативы «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» СанПиН 2.2.2/2.4.1340-03	4	Самоподго-товка	
10	Постановление Правительства Российской Федерации от 25.04.2012 г. № 390 «Правила противопожарного режима в Российской Федерации»	4	Самоподго-товка	

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

<наименование учреждения здравоохранения>

ПРИКАЗ

«____» _____ 20____года № _____

Об организации работ по обеспечению безопасности информации при ее обработке с использованием средств криптографической защиты информации

С целью определения порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, в соответствии с руководящими документами ФСБ России

ПРИКАЗЫВАЮ:

1. Возложить обязанности ответственного пользователя криптосредств на администратора безопасности *<наименование учреждения здравоохранения>*.
2. Ввести в действие «Инструкцию о порядке учета и выдачи средств криптографической защиты информации, электронной подписи, эксплуатационно - технической документации и ключевых документов».
3. Ввести в действие «Инструкцию о порядке допуска сотрудников *<наименование учреждения здравоохранения>* к самостоятельной работе со средствами криптографической защиты информации».
4. Ввести в действие «Инструкцию по обращению с сертифицированными ФСБ России средствами криптографической защиты информации»
5. Организовать ведение «Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».
6. Организовать ведение «Журнала регистрации пользователей СКЗИ».
7. Организовать ведение «Технического (аппаратного) журнала СКЗИ».
8. С настоящим приказом ознакомить всех сотрудников (под роспись) в части, их касающейся.
9. Контроль за исполнением приказа возложить на _____.

<должность руководителя> _____ *<Фамилия И.О.>*

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

УТВЕРЖДАЮ

<должность руководителя>

<наименование учреждения здравоохранения>

_____ *<Фамилия И.О.>*

«___» _____ 20___ г.

ИНСТРУКЦИЯ
о порядке учета и выдачи средств криптографической защиты информации, электронной подписи, эксплуатационно - технической документации и ключевых документов

1. Учет средств криптографической защиты информации (СКЗИ), сертификатов электронной подписи (ЭП), эксплуатационно - технической документации на СКЗИ и ЭП, ключевых документов и ЭП организуется в соответствии с требованиями нормативной документации ФСБ России, Правилами использования СКЗИ, утвержденными разработчиком СКЗИ.

2. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3. Поэкземплярный учет СКЗИ, поступающих от разработчиков, изготовителей и поставщиков СКЗИ необходимо вести в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

4. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем Журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

5. Ответственные пользователи криптосредств заводят и ведут на каждого пользователя СКЗИ лицевой счет, в котором регистрируют числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы. Типовая форма лицевого счета пользователя СКЗИ представлена в Приложении №1 к данной инструкции.

6. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их

действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем СКЗИ.

7. Учет СКЗИ, средств ЭП, эксплуатационной и технической документации, ключевых документов и информации должен быть организован на бумажных носителях.

8. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ, ответственными пользователями криптосредств под расписку в соответствующих журналах поэкземплярного учета.

9. Учет СКЗИ, средств ЭП, эксплуатационной и технической документации, ключевых документов и информации должен быть организован на бумажных носителях.

10. Ответственным пользователем криптосредств в <*наименование учреждения здравоохранения*> является администратор безопасности информации.

11. Ведение непосредственных операций по учету СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы, в соответствии с функциональными обязанностями и инструкциями, возлагается на администратора безопасности информации.

Разработал _____

«___» _____20__г.

Приложение №1
к Инструкции о порядке учета и выдачи
средств криптографической защиты информации

ЛИЦЕВОЙ СЧЕТ ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

Сотрудник _____

(ФИО, должность)

_____

(структурное подразделение)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов или серийные номера их носителей	Регистрационные номера экземпляров (крипто-графические номера) ключевых документов	Дата и расписка о получении СКЗИ	Дата и расписка возвращения СКЗИ	Примечание

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

Приложение № 22
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

Типовая форма
согласия пациента на обработку персональных данных

Я, нижеподписавшийся _____,

(ФИО субъекта персональных данных)

документ, удостоверяющий личность _____серия_____№_____,

выдан _____20___г., _____,

(дата выдачи) (кем выдан)

проживающий по адресу _____,

(адрес регистрации)

Сведения о законном представителе* _____

(фамилия, имя, отчество)

_____

(почтовый адрес места жительства, пребывания, фактического проживания, телефон, дата рождения,

_____

документ, удостоверяющий личность, документ, подтверждающий полномочия)

*Заполняется в том случае, если заявление заполняет законный представитель гражданина Российской Федерации.

в соответствии с требованиями Федерального закона от 27.07.2006 г. «О персональных данных» № 152-ФЗ подтверждаю (даю) свое согласие на обработку Государственным бюджетным учреждением здравоохранения «_____» моих персональных данных, а именно: фамилия, имя, отчество, пол, дата рождения, адреса места жительства и(или) пребывания, рождения, место работы, данные паспорта (или иного документа, удостоверяющего личность), данные полиса ОМС (или ДМС); страховой номер индивидуального лицевого счета (СНИЛС), контактный телефон, e-mail,сведения о семейном положении и составе семьи, гражданстве, месте работы/учебы, сведения о факте обращения мной за оказанием медицинской помощи, состоянии моего здоровья и диагнозе, иные сведения, полученные при медицинском обследовании и лечении.

Цель обработки персональных данных: в целях установления медицинского диагноза и оказания медицинских услуг формирование государственного информационного ресурса, содержащего сведения о гражданах, необходимые для актуализации документов воинского учета.

Перечень действий с персональными данными, на совершение которых дается согласие: сбор, запись, обработка, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача, обезличивание, блокирование, удаление, уничтожение персональных данных.

Передача персональных данных осуществляется в:
Комитет по здравоохранению Псковской области (далее - Оператор).
Оператор имеет право на передачу моих персональных данных для дальнейшей обработки в региональных медицинских центрах и органах власти, осуществляющих руководство и контроль в области здравоохранения, территориальным фондам обязательного медицинского страхования и медицинским страховым организациям, при условии заключения договоров, защищающих мои права со всеми участниками информационного обмена и соблюдения всеми участниками обмена норм хранения, обработки, ограничения доступа к персональным данным, предусмотренных законодательством РФ.
Государственное бюджетное учреждение здравоохранения «_____» имеет право: при обработке моих персональных данных вносить их в реестры, базы данных автоматизированных информационных систем для формирования отчетных форм и иных сведений, предоставление которых регламентировано договорами или иными документами, определяющими взаимодействие со страховыми медицинскими организациями, медицинскими организациями, органами управления здравоохранения, иными организациями; с целью выполнения своих обязательств, предусмотренных нормативными правовыми актами или договорами, на предоставление, передачу моих

персональных данных иным организациям, при условии, что передача указанных данных будет осуществляться с использованием машинных носителей или по каналам связи с соблюдением мер, обеспечивающих защиту моих персональных данных от несанкционированного доступа, а также при условии, что их прием и обработка будут осуществляться лицом, обязанным сохранять профессиональную тайну.

Государственное бюджетное учреждение здравоохранения «_____» имеет право разглашать: сведения, составляющие врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях (согласно ч.3 ст. 13 Федерального закона от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»);
сведения о факте обращения за психиатрической помощью, состоянии психического здоровья и диагнозе психического расстройства, иные сведения, полученные при оказании психиатрической помощи, составляющие врачебную тайну (согласно статье 9 Закона Российской Федерации от 02.07.1992 N 3185-1 (ред. от 30.12.2021) «О психиатрической помощи и гарантиях прав граждан при ее оказании».

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов.

Я оставляю за собой право отозвать свое согласие полностью или частично по моей инициативе на основании письменного заявления в Государственное бюджетное учреждение здравоохранения «_____», в т.ч. и в случае ставших мне известных фактов нарушения моих прав при обработке персональных данных.

Подтверждаю, что ознакомлен(а) с «Правилами обработки персональных данных», и с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Представитель Оператора	Субъект персональных данных
_____ (_____)	_____(_____)
Подпись расшифровка подписи	Подпись расшифровка подписи
Дата _____	Дата _____

<наименование учреждения здравоохранения>

ПРИКАЗ

«____» _____ 20____года № _____

Об организации ведения журналов

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Организовать ведение следующих журналов:
   - Журнал учета машинных носителей информации;
   - Журнал проведения периодического антивирусного контроля;
   - Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных;
   - Журнал учета документов и изданий с пометкой «Для служебного пользования»;
   - Журнал проведения периодического контроля средств защиты информации от НСД;
   - Журнал регистрации доступа к программному и аппаратному обеспечению;
   - Журнал учета металлических хранилищ и ключей от них;
   - Журнал учета выдачи ключей и печатей;
   - Журнал приема-сдачи помещений под охрану.

2. С настоящим приказом ознакомить всех сотрудников в части их касающейся (под роспись).

3. Контроль исполнения приказа возложить на администратора безопасности информации.

<должность руководителя> _____ *<Фамилия И.О.>*

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

<наименование учреждения здравоохранения>

ЖУРНАЛ №___
учета машинных носителей, содержащих персональные данные

Начат: «__»_____ 20___г.

Окончен: «__»_____20___г.

20___г.

№ п/п	Тип машинного носителя информации	Серийный (инвентарный) номер	Учетный номер	Кол-во экз.	Номер экз.	Расписка в получении (дата, ФИО и подпись), отметка об отправке	Расписка в обратном приеме (дата, ФИО и подпись)	Примечание

<наименование учреждения здравоохранения>

ЖУРНАЛ № __

приема-сдачи помещений под охрану

Начат: «__»_____ 20___г.

Окончен: «__»_____20___г.

20___г.

Сдача под охрану						Снятие с охраны				
№ п/п	№ поме-ще-ния	Дата сдачи	Время сдачи	Фамилия сдающего	Подпись	Дата снятия	Время снятия	Фамилия снимающего	Подпись	Примечание

Приложение № 15
к приказу *<наименование учреждения здравоохранения>*
от _____ №_____

ПЕРЕЧЕНЬ
должностей, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным

№ п/п	Подразделение	Должность
1		
2		
3		
4		
5		
6		
7		
8		
9		

Разработал _____

«___» _____20__г.

<наименование учреждения здравоохранения>

ЖУРНАЛ №___
учета выдачи ключей и печатей

Начат: «__»_____ 20___г.

Окончен: «__»_____20___г.

20___г.

№ п/п	Номер ключа, печати	Кому выдан	Дата	Расписка в получении	Дата изъятия, расписка или номер акта

<наименование учреждения здравоохранения>

ЖУРНАЛ № ____
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов
(для обладателя конфиденциальной информации)

Начат: «__»_____ 20__г.

Окончен: «__»_____20__г.

20__г.

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	

<наименование учреждения здравоохранения>

ЖУРНАЛ № __

учета обращений субъектов персональных данных по вопросам обработки персональных данных

Начат: «__»_____ 20___г.

Окончен: «__»_____20___г.

20___г.

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель получения персональных данных	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи/ отказа в предоставлени и информации	Подпись запраши-вающего лица	Подпись ответствен-ного сотрудника

Приложение № 17
к приказу <*наименование учреждения здравоохранения*>
от _____ №_____

Правила
проведения внутреннего контроля и проверок соответствия обработки персональных данных требованиям к защите персональных данных

1. Настоящими Правилами осуществления внутреннего контроля и проверок соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в <*наименование учреждения здравоохранения*> определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации».

3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. № 152 ФЗ «О персональных данных».

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в <*наименование учреждения здравоохранения*> организовывается проведение периодических проверок условий обработки персональных данных.

5. Проверки осуществляются ответственным за обеспечение безопасности персональных данных <*наименование учреждения здравоохранения*>, либо комиссией, образуемой приказом <*должность руководителя*> <*наименование учреждения здравоохранения*>.

6. Проверки осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

7. В проведении проверки не может участвовать сотрудник, прямо или косвенно заинтересованный в её результатах.

8. Проверки соответствия обработки персональных данных установленным требованиям в *<наименование учреждения здравоохранения>* проводятся на основании утвержденного *<должность руководителя>* *<наименование учреждения здравоохранения>* ежегодного плана мероприятий по организации защиты персональных данных или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

9. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

10. Ответственный за обеспечение безопасности персональных данных в *<наименование учреждения здравоохранения>* (комиссия) имеет право:

- запрашивать у сотрудников *<наименование учреждения здравоохранения>* информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

− принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

− вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

− вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

11. Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении №1 к настоящим Правилам.

12. При выявлении в ходе проверки нарушений, ответственным за обеспечение безопасности персональных данных либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

13. Протоколы хранятся у ответственным за обеспечение безопасности персональных данных либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится ответственным за обеспечение безопасности персональных данных либо комиссией самостоятельно в январе следующего за проверочным годом.

14. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, *<должность руководителя> <наименование учреждения здравоохранения>* докладывает ответственный за обеспечение безопасности персональных данных либо председатель комиссии, в форме письменного заключения.

15. *<должность руководителя> <наименование учреждения здравоохранения>*, назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.

Разработал _____

Приложение №1 к Правилам

Протокол

проведения внутренней проверки условий обработки персональных данных в

<наименование учреждения здравоохранения>

Настоящий Протокол составлен в том, что __.__.201_ ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка _____.

(тема проверки)

Проверка осуществлялась в соответствии с требованиями

_____

_____

_____.

(название документа)

В ходе проверки проверено:

_____

_____

_____

_____

_____

Выявленные нарушения:

_____

_____

_____

_____

_____.

Меры по устранению нарушений:

_____

_____

_____

_____

_____.

Срок устранения нарушений: _____.

Должность ответственного за организацию обработки персональных данных _____ И.О. Фамилия

либо

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Должность руководителя проверяемого подразделения _____ И.О. Фамилия

<наименование учреждения здравоохранения>

ЖУРНАЛ № ____

регистрации доступа к программному и аппаратному обеспечению

Начат: «__»_____ 20__г.

Окончен: «__»_____20__г.

20__ г.

№ п/п	Дата	Серийный (инвентарный) номер системного блока	Причина вскрытия (доступа)	Дата закрытия	Ф.И.О. и подпись администратора безопасности информации	Примечание

<наименование учреждения здравоохранения>

ПРИКАЗ

«____» _____ 20____года № _____

О допуске сотрудников к самостоятельной
работе со СКЗИ

В целях осуществления мероприятий по организации и обеспечению безопасности при обработке и передаче с использованием СКЗИ конфиденциальной информации

ПРИКАЗЫВАЮ:

1. Допустить к самостоятельной работе со СКЗИ следующих сотрудников:

№ п/п	ФИО	Должность

2. Приказ довести до ответственных лиц.

3. Контроль за исполнением приказа возложить на _____.

<должность руководителя> _____ *<Фамилия И.О.>*

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата

<наименование учреждения здравоохранения>

ЖУРНАЛ №___
регистрации пользователей СКЗИ

Начат: «__»_____ 20___г.

Окончен: «__»_____20___г.

20___г.

№ п/п	Должность пользователя	Ф.И.О. пользователя	Номер и дата приказа о допуске	Номер и дата приказа о прекращении допуска	Примечание

<наименование учреждения здравоохранения>

ЖУРНАЛ № ____
учета документов и изданий с пометкой «Для служебного пользования»

Начат: «__»_____ 20__г.

Окончен: «__»_____20__г.

20__ г.

№ п/п	Дата поступления и индекс документа	Дата и исходящий номер документа	Откуда поступил или куда направлен	Вид документа и краткое содержание	Количество листов		Количество и номера экземпляров
					документа	приложения	

<наименование учреждения здравоохранения>

ЖУРНАЛ №___

проведения периодического контроля средств защиты информации от НСД

Начат: «__»_____ 20__г.

Окончен: «__»_____20__г.

20__г.

№ п/п	Дата проведения контроля	Наименование автоматизированной системы	Наименования средства защиты	Тип проверки	Результат проверки	Примечание	Фамилия проверявшего

<наименование учреждения здравоохранения>

ЖУРНАЛ №___
проведения периодического антивирусного контроля

Начат: «__»_____ 20___г.

Окончен: «__»_____20___г.

20___г.

№ п/п	Дата проведения контроля	АРМ	Наименование средств антивирусной защиты	Результат проверки	Примечание	Фамилия проверявшего

<наименование учреждения здравоохранения>

ЖУРНАЛ № __

учета металлических хранилищ и ключей от них

Начат: «__»_____ 20___г.

Окончен: «__»_____20___г.

20___г.

№ п/п	Номер хранилища/ комплекта ключей	Ответственный	Дата	Расписка в получении	Дата изъятия, расписка или номер акта