**Утверждаю**

**Главный врач**

**ГАУЗ СО "Режевская СП**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.П. Сурганова**

**ПОЛОЖЕНИЕ**

**об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации.**

**1. Общие положения.**

* 1. Данное «Положение об организации и проведении работ в

ГАУЗ СО "Режевская СП" по обеспечению безопасности персональных данных при их автоматизированной обработке и/или без использования средств автоматизации в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

123. При обеспечении безопасности персональных данных в ИСПДн с использованием криптографических средств защиты информации все сотрудники ГАУЗ СО "Режевская СП"обязаны выполнять требования, изложенные в документе «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСБ России, № 149/6/6-622, 2008).

**2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации.**

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается руководителем ГАУЗ СО "Режевская СП" (далее руководитель), и в соответствии со списком лиц, допущенных к работе в ИСПДн.

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам определяются в матрице доступа, которая создается ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн и утверждается руководителем организации. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей.

2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

2.4. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.5. Запись информации, содержащей ПДн, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей.

2.6. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ в помещение, в котором производится обработка ПДн, аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и ***обязан***:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);

- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе, или ящике, закрывающемся на ключ;

- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн и обнаружении:

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на компьютеры технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

2.8. Пользователю категорически ***запрещается***:

- использовать компоненты программного и аппаратного обеспечения персонального компьютера в неслужебных целях;

-  вносить какие-либо изменения в конфигурацию аппаратных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы существовала возможность визуального считывания информации.

2.9. **Лица, ответственные за защиту персональных данных в** ГАУЗ СО "Режевская СП"

**Ответственный за обработку ПДн -** штатный сотрудник определяющий уровень доступа и ответственность лиц участвующих в обработке ПДн. Назначается приказом по учреждению.

**3. Порядок обработки персональных данных без использования средств автоматизации.**

* 1. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях.
  2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.
  3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

* 1. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

3.4.1. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

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

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

* 1. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

1. **Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации.**
   1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.
   2. Резервному копированию подлежат базы данных ПДн, а так же прикладное программное обеспечение, предназначенное для работы с этими базами данных в случае, если оно подвергается модификации со стороны разработчиков ИСПДн.
   3. Резервное копирование должно осуществляться в специально отведенный сетевой каталог на файловом сервере, а так же путем записи на отчуждаемый носитель.
   4. Права доступа к сетевым каталогам должны исключать возможность доступа пользователей к резервным копиям других ИСПДн, хранящихся на сервере, при отсутствии допуска к работе в этих ИСПДн.
   5. Базы данных и программное обеспечение должны копироваться в разные папки на файловом сервере.
   6. На файловом сервере, помимо актуального состояния баз данных и программного обеспечения, должны храниться минимум два их исторических состояния.

4.7. Резервное копирование на файловый сервер должно осуществляться

непосредственно после любого изменения состояния баз данных или программного обеспечении этих баз, но не реже, чем раз в неделю.

4.8. Если программный продукт, на основе которого функционирует ИСПДн, имеет функцию резервного копирования, то создается резервная квопия при помощи данной функции.

4.9. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

4.10. Ответственность за проведение резервного копирования сетевого каталога хранения резервных копий ИСПДн возлагается на специалистов, ответственных за техническое обеспечение учреждения.

4.11. Мероприятия по восстановлению работоспособности технических средств и программного обеспечения баз данных организуются и проводятся с помощью специалистов, ответственных за техническое обеспечение учреждения, привлечением ответственного пользователя той ИСПДн, функционирование которой было нарушено.

**5. Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий.**

5.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

5.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях ГАУЗ СО "Режевская СП",учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

- выявление демаскирующих признаков объектов ИСПДн;

- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

5.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн ГАУЗ СО "Режевская СП"и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

5.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн) мерам, предписанным законодательством РФ и установленным нормативными документами предприятия;

- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- эффективность проведения организационных и технических мероприятий по защите информации;

- устранение ранее выявленных недостатков.

5.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

5.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор информационной безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения.

5.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн проводится расследование.

Для проведения расследования назначается комиссия. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководительпринимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

5.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты.

5.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора информационной безопасности, ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн информации, администратор ИСПДн. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

5.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» (если проводилась аттестация) и (или) требованиям по безопасности персональных данных.

5.11. В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

- соблюдение организационно-технических требований помещений, в которых располагается ИСПДн;

- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем положении;

- выполнение требований по защите информационных систем от несанкционированного доступа;

- выполнение требований по антивирусной защите.

**6. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных.**

6.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

6.2.Пользователи должны продемонстрировать администратору информационной безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор информационной безопасности должен вести журнал учета пользователей, допущенных к информационным системам персональных данных.

6.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.

6.4. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

6.5. К работе в ИСПДн допускаются только сотрудники, прошедшие первичный инструктаж по обеспечению безопасности в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта допуска к работе в ИСПДн.

**7. Правила антивирусной защиты.**

7.1. На каждом компьютере ИСПДн должны быть установлены лицензионные антивирусные средства, сертифицированные ФСТЭК РФ.

7.2. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется специалистами, ответственными за техническое обеспечение информационных систем учреждения.

7.3. Специалисты, ответственные за техническое обеспечение информационных систем учреждения, осуществляют периодическое обновление антивирусных пакетов и контроль их работоспособности.

7.4. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

7.5. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

7.6. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

7.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором информационной безопасности должна быть выполнена антивирусная проверка ИСПДн.

7.8. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

7.9. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно должен провести внеочередной антивирусный контроль компьютера.

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

- приостановить обработку данных в ИСПДн;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

7.10. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на специалистов по техническому обеспечению, и всех пользователей данной ИСПДн.

**8. Управление учетными записями пользователей.**

8.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должна быть создана уникальная учетная запись пользователя.

8.2. Работу в ИСПДн сотрудник должен осуществлять только с использованием своего уникального имени пользователя. Работа в ИСПДн под чужой учетной записью, кроме случаев, описанных в п.9.5, ***запрещена.***

**9. Порядок охраны и допуска посторонних лиц в защищаемые помещения.**

9.1. Данный раздел Положения устанавливает порядок охраны помещений ИСПДн.

9.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.

9.3. При отсутствии сотрудников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа. Комиссией составляется акт вскрытия.

9.4. При закрытии помещений сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убирают для хранения в опечатываемый сейф (металлический шкаф). Закрываемое помещение опечатывается личной печатью сотрудника, ответственного за помещение.

9.5. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт. О происшествии немедленно сообщается руководителю и (или) ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн.

Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

9.6. Руководитель, ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн организует проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

9.7. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн, или руководителю, или администратору информационной безопасности. Помещения вскрывать запрещается.

9.8. Помещения вскрываются ответственным за помещение, или руководителем, или ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн в присутствии сотрудника охраны с составлением акта.

**10. Порядок хранения медицинской документации.**

Под Медицинской документацией в настоящем положении понимается медицинская карта пациента, получающего медицинскую помощь в амбулаторных условиях, другие документы на бумажном носителе, находящиеся на постоянном хранении в медицинской организации.

Основанием для организации порядка хранения медицинской документации в медицинской организации являются Федеральные законы от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», от 27.07.2006 № 152-ФЗ «О персональных данных», приказ Министерства здравоохранения Российской Федерации от 15.12.2014 № 834н «Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях, оказывающих медицинскую помощь в амбулаторных условиях, и порядков по их заполнению», письмо Минздравсоцразвития Российской Федерации от 04.04.2005 № 734/МЗ-14 «О порядке хранения амбулаторной карты».

10.1. На Медицинскую документацию в полной мере распространяются положения настоящего документа об особенностях обработки персональных данных без использования средств автоматизации .

10.2. Пациент, либо его законный представитель, в соответствии с положениями ч. 4 ст. 22 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», имеют право знакомиться с содержанием Медицинской документации в части информации, отражающей состояние здоровья пациента, получать выписки и копии.

10.3. Медицинская документация, выписки и копии из нее, предоставляется лечащим врачом лично пациенту или его законному представителю при наличии документов, подтверждающих его законное представительство.

10.4. Информация, содержащаяся в Медицинской документации или выписки из нее могут предоставляться третьим лицам с письменного согласия пациента. Без согласия пациента информация, содержащая в Медицинской документации, может предоставляться третьим лицам только по основаниям, изложенным в п.4 ст.13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в российской Федерации». Такая информация может предоставляться на основании мотивированного, надлежащим образом оформленного официального запроса соответствующего органа органам дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, органам прокуратуры в связи с осуществлением ими прокурорского надзора, органам уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно и пр.