Приложение № 1
к приказу № 86-ТД от 26.10.2015г.

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.

1.1. Данное «Положение об организации и проведении работ в государственном автономном учреждении здравоохранения Свердловской области «Ирбитская стоматологическая поликлиника»
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).

1.2. Положение определяет порядок работы пользователей и администраторов ИСПДн, сотрудников, ответственных за техническое обеспечение, а также администратора информационной безопасности, в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ИСПДн, порядок создания резервных копий ИСПДн, правила хранения и регистрации носителей информации а также порядок обезличивания ПДн.

1.3. При обеспечении безопасности персональных данных в ИСПДн с использованием криптографических средств защиты информации все сотрудники ГАУЗ СО «Ирбитская стоматологическая поликлиника» 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 главным врачом ГАУЗ СО «Ирбитская стоматологическая поликлиника» (далее руководитель), и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем назначается администратор информационной безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности назначается ответственный за обеспечение безопасности персональных данных при их обработке 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;

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 главным врачом ГАУЗ СО «Ирбитская стоматологическая поликлиника» (далее руководитель), и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем назначается администратор информационной безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности назначается ответственный за обеспечение безопасности персональных данных при их обработке 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 (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ;

- 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 «Ирбитская стоматологическая поликлиника».**

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

Ответственный за обеспечение безопасности персональных данных – штатный сотрудник (или подразделение) отвечающий за проведение мероприятий, связанных с защитой ПДн (организационных и технических), а также осуществляющий контроль за соблюдением требований по защите ПДн в подразделениях. Назначается приказом по учреждению.

Администратор информационной безопасности – штатный сотрудник, ответственный за защиту автоматизированной системы (АС) от несанкционированного доступа (НСД) к информации. Назначается приказом по учреждению.

2.10. Администратор информационной безопасности (при его отсутствии ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн) обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

- вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;

- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

- контролировать своевременное (не реже чем один раз в течение 60 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;
- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;
- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;
- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в месяц;
- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации;
- сопровождать подсистемы обеспечения целостности информации в ИСПДн;
- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;
- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях совместно с лицами, ответственными за техническое обеспечение.
- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;
- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;
- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;
- контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

• присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

• вести журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн;

• поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения;

• в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

• докладывать ответственному за обработку персональных данных о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

• вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.11. Администратор информационной безопасности и ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн имеют право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. Порядок обработки персональных данных без использования средств автоматизации.

3.1. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях.

3.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.3. 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.

3.4. 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 или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

3.4.2. 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;

3.4.3. 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;

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

3.5. 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.

4. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации.

4.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.2. 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.

4.3. Резервное копирование должно осуществляться в специально отведенный сетевой каталог на файловом сервере, а так же путем записи на отчуждаемый носитель.

4.4. 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.

4.5. Базы данных и программное обеспечение должны копироваться в разные папки на файловом сервере.

4.6. На файловом сервере, помимо актуального состояния баз данных и программного обеспечения, должны храниться минимум два их исторических состояния.

4.7. Раз в месяц администратор ИСПДн создает резервную копию баз данных и программного обеспечения ИСПДн на отчуждаемый носитель, хранящийся у администратора информационной безопасности в закрывающемся на ключ хранилище.

4.8. К использованию, для создания резервных копии в ИСПДн, допускаются только зарегистрированные в журнале учета носители.

4.9. 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.

4.10. Если программный продукт, на основе которого функционирует ИСПДн, имеет функцию резервного копирования, то администратор ИСПДн создает резервную копию при помощи данной функции.

4.11. Специалист, ответственный за техническое обеспечение учреждения создает резервную копию сетевого каталога, в котором хранятся резервные копии всех ИСПДн не реже чем раз в месяц.

4.12. Специалист, ответственный за техническое обеспечение учреждения, при помощи специализированного программного обеспечения, средств создает образы дисков всех рабочих мест ИСПДн не реже, чем раз в квартал.

4.13. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов либо полного восстановления системы с образа диска.

4.14. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

4.15. 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.

4.16. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

4.17. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств на зарегистрированный носитель.

4.18. Ответственность за проведение резервного копирования ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора ИСПДн.

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

4.20. Мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных организуются и проводятся 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 «Ирбитская стоматологическая поликлиника, 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;