Экз. № 1

УТВЕРЖДАЮ
Главный врач ГБУЗ РМ «МРКБ»

_____ В.Г. Крылов
«___» _____ 2012 г.

ПОЛОЖЕНИЕ

по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБУЗ РМ «Мордовская республиканская клиническая больница»

СОГЛАСОВАНО
Начальник отдела вычислительной техники в структуре ОКЭОЭР ГБУЗ РМ «МРКБ»
_____ В.А. Киржиманов
«25» декабря 2012 г.

СОГЛАСОВАНО
Заместитель главного врача по организационно-методической работе ГБУЗ РМ «МРКБ»
_____ А.Е. Иванов
«25» декабря 2012 г.

2012 г.

рег. № 948

Оглавление

Принятые сокращения

АРМ	автоматизированное рабочее место
АС	автоматизированная система
ЖМД	жесткий магнитный диск
ИСПДн	информационная система персональных данных
КЗ	контролируемая зона
ЛВС	локальная вычислительная сеть
ЛОО	лицо, ответственное за организацию обработки персональных данных
МНИ	машинные носители информации
НЖМД	носитель на жестком магнитном диске
НСД	несанкционированный доступ
ОС	операционная система
ПДн	персональные данные
ПО	программное обеспечение
ПЭВМ	персональная электронно-вычислительная машина
ПЭМИН	побочные электромагнитные излучения и наводки
СЗИ	средства защиты информации
СЗПДн	система защиты персональных данных
СКЗИ	средство криптографической защиты информации
ТЗ	техническое задание
ТС	технические средства
ФСТЭК	Федеральная служба по техническому и экспортному контролю

1 Общие положения

1.1 Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБУЗ РМ «Мордовская республиканская клиническая больница» (далее Положение) разработано в соответствии с Законами РФ «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27.07.2006, «О персональных данных» от 27.07.06 г. №152-ФЗ, постановлениями Правительства Российской Федерации от 17.11.07 № 781 и от 24.09.2008 № 687.

1.2 Настоящее Положение определяет порядок организации обеспечения безопасности персональных данных в ГБУЗ РМ «МРКБ».

1.3 Настоящее Положение и все дополнения и изменения к нему утверждаются главным врачом ГБУЗ РМ «МРКБ».

1.4 Работники ГБУЗ РМ «МРКБ» должны быть ознакомлены с отдельными разделами Положения и приложениями к нему, другими организационно-распорядительными или эксплуатационными документами в необходимом и достаточном объеме для выполнения своих должностных обязанностей.

2 Подразделения, должностные лица, ответственные за обеспечение безопасности ПДн

Обеспечение безопасности ПДн в ГБУЗ РМ «МРКБ» возложено на следующие подразделения (должностные лица):

2.1 Главный врач ГБУЗ РМ «МРКБ»

2.1.1 Главный врач ГБУЗ РМ «МРКБ» осуществляет следующие основные функции по обеспечению безопасности ПДн:

2.1.1.1 Организация обработки ПДн, а так же определение целей обработки ПДн и действий, совершаемых с ними;

2.1.1.2 Определение порядка обработки ПДн;

2.1.1.3 Организация работ по обеспечению безопасности ПДн и контроль за их проведением;

2.1.1.4 Назначение должностных лиц, ответственных за обеспечение безопасности;

2.1.1.5 Утверждение перечня обрабатываемых ПДн;

2.1.1.6 Утверждение актов классификации ИСПДн ГБУЗ РМ «МРКБ»;

2.1.1.7 Утверждение правил доступа к ПДн, обрабатываемых в ИСПДн;

2.1.1.8 Утверждение списков лиц допущенных к работе с ПДн в информационной системе;

2.1.1.9 Утверждение списков лиц допущенных в помещения, где размещены ТС ИСПДн и (или) осуществляется обработка ПДн;

2.1.1.10 Утверждение документов, определяющих политику ГБУЗ РМ «МРКБ» в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

2.1.1.11 Утверждение документов, регламентирующих организацию обеспечения безопасности ПДн;

2.1.1.12 Принятие мер по результатам расследования инцидентов безопасности информации;

2.1.1.13 Принятие решения о приостановлении предоставления ПДн при обнаружении нарушений порядка их предоставления;

2.1.1.14 Отдача распоряжения о возобновлении предоставления ПДн после устранения нарушения порядка предоставления ПДн;

2.1.2 Главный врач ГБУЗ РМ «МРКБ» осуществляет контроль за:

2.1.2.1 соответствием процесса обработки персональных данных ФЗ-152 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, требованиями к защите персональных данных, политикой ГБУЗ РМ «МРКБ» в отношении обработки персональных данных и локальными актами;

2.1.2.2 доведением до сведений всех работников ГБУЗ РМ «МРКБ» положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки ПДн и требований к защите ПДн, а также их права и обязанности в этой области.

2.1.2.3 ознакомлением работников ГБУЗ РМ «МРКБ», непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ГБУЗ РМ «МРКБ» в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2.1.2.4 соблюдением прав субъектов ПДн;

2.1.2.5 проведением мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачей их лицам, не имеющим права доступа к такой информации;

2.1.2.6 неконтролируемым проникновением или пребыванием посторонних лиц в помещениях, в которых расположены ТС ИСПДн;

2.1.2.7 соблюдением ГБУЗ РМ «МРКБ» и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2.1.2.8 принимаемыми мерами по обеспечению безопасности персональных данных уровня защищенности информационных систем персональных данных;

2.1.2.9 разбирательством и составлением заключений по фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, разработкой и принятием мер по предотвращению возможных опасных последствий подобных нарушений.

2.2 Руководитель подразделения или отдела

2.2.1 Руководитель подразделения или отдела осуществляет следующие основные функции по обеспечению безопасности ПДн:

2.2.1.1 Проводит учет пользователей, допущенных к работе с ПДн в ИСПДн, в своем отделе;

2.2.1.2 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;

2.2.1.3 Обеспечивает сохранность технических средств, носителей ПДн и средств защиты информации;

2.2.1.4 Исключает возможность неконтролируемого проникновения или пребывания посторонних лиц в помещениях, в которых расположены технические средства ИСПДн и (или) осуществляется обработка ПДн;

2.2.1.5 Ограничивает доступ пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а так же хранятся носители информации;

2.2.1.6 Контролирует содержание и обьем обрабатываемых персональных данных. ПДн должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

2.2.1.7 Контролирует передачу ПДн третьим лицам;

2.2.1.8 Контролирует процесс блокирования неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных;

2.2.1.9 Контролирует процесс прекращения обработки ПДн при отзыве субъектом ПДн согласия на обработку ПДн;

2.2.1.10 Контролирует проведение работ по исключению акустического и визуального каналов утечки конфиденциальной информации;

2.2.1.11 Осуществляет контроль за соблюдением запрета записи ПДн на незарегистрированные носители информации.

2.3 Лицо, ответственное за организацию обработки ПДн

2.3.1 В соответствии с ч.1 ст. 22.1 Федерального закона «О персональных данных» от 27.07.06 г. № 152-ФЗ в ГБУЗ РМ «МРКБ» должно быть назначено лицо, ответственное за организацию обработки ПДн. Лицо, ответственное за организацию обработки ПДн подчиняется Главному врачу ГБУЗ РМ «МРКБ».

2.4 Администратор безопасности информации

2.4.1 Предназначение, полномочия, обязанности администратора безопасности информации определены в документе «Инструкция администратора безопасности информации информационных систем персональных данных ГБУЗ РМ «Мордовская республиканская клиническая больница».

2.5 Пользователь ИСПДн

2.5.1 Обязанности пользователей определены в документе «Инструкция пользователя по работе на АРМ информационных систем персональных данных ГБУЗ РМ «Мордовская республиканская клиническая больница».

3 Порядок организации и проведения работ по защите ПДн

3.1 Общие положения

3.1.1 Организация работ по защите информации возлагается на главного врача ГБУЗ РМ «МРКБ», методическое руководство и контроль за эффективностью предусмотренных мер защиты информации — на лицо, ответственное за организацию обработки ПДн.

3.1.2 Основанием для проведения работ по защите ПДн могут являться:

3.1.2.1 первоначальное приведение ИСПДн в соответствие с требованиями законодательства;

3.1.2.2 создание новых ИСПДн;

3.1.2.3 модернизация существующих ИСПДн, затрагивающая технологический процесс обработки информации;

3.1.2.4 изменение угроз безопасности персональным данным;

3.1.2.5 изменение класса ИСПДн;

3.1.2.6 инциденты безопасности;

3.1.2.7 изменение нормативной базы, регулирующей порядок защиты ПДн;

3.1.2.8 предписания регуляторов.

3.1.3 Решение о необходимости проведения работ по защите ПДн принимается ЛОО.

3.2 Порядок определения защищаемой информации

3.2.1 С целью дифференциального подхода к организации защиты ПДн в ГБУЗ РМ «МРКБ» производится выделение отдельных ИСПДн. Перечень ИСПДн с указанием названия, класса ИСПДн (для автоматизированных систем) приведен в документе «Перечень информационных систем, используемых для обработки персональных данных ГБУЗ РМ «Мордовская республиканская клиническая больница»».

3.2.2 С целью классификации ИСПДн, в которых осуществляется обработка, составляется и утверждается главным врачом ГБУЗ РМ «МРКБ» «Перечень обрабатываемых персональных данных в информационных системах персональных данных ГБУЗ РМ «Мордовская республиканская клиническая больница». Документ должен содержать список обрабатываемых ПДн, наименование ИСПДн, в которой обрабатываются данные, способ обработки, категорию субъектов ПДн.

3.2.3 На часть АРМ пользователей установлено программное обеспечение (СКБ «Контур-экстерн», Клиент-банк «SFT Bank+Client Module»), позволяющее создавать файлы выгрузок с отчетностью в сторонние государственные и негосударственные организации (ФНС, ПФР, ФСС, Банк). С точки зрения выполнения функций передачи отчетности, данные АРМ являются клиентской частью ИСПДн других операторов ПДн. В этом случае, порядок защиты ПДн, в том числе и при использовании СКЗИ, определяется другими операторами.

3.2.4 Первоначальное выделение ИСПДн и определение обрабатываемых ПДн может быть осуществлено по результатам комплексного обследования, проводимого ЛОО как самостоятельно, так и с привлечением специализированных организаций — лицензиатов ФСТЭК. В ходе обследования определяется:

3.2.4.1 Для автоматизированных ИСПДн:

3.2.4.1.1 Цель обработки персональных данных;

3.2.4.1.2 Назначение ИСПДн;

3.2.4.1.3 Статус организации;

3.2.4.1.4 Субъекты ПДн и их ПДн, обрабатываемые в ИСПДн:

3.2.4.1.4.1 Перечень обрабатываемых ПДн;

3.2.4.1.5 Категория обрабатываемых ПДн;

3.2.4.1.6 Объем обрабатываемых ПДн;

3.2.4.1.7 Структура ИСПДн:

3.2.4.1.7.1 Параметры ИСПДн;

3.2.4.1.7.2 Пользователи ИСПДн;

3.2.4.1.7.3 Состав технических средств;

3.2.4.1.7.4 Расположение технических средств;

3.2.4.1.7.5 Описание информационных технологий;

3.2.4.1.7.6 Логическая структура;

3.2.4.1.7.7 Физическая структура;

3.2.4.1.7.8 Расположение ИСПДн относительно границ КЗ;

3.2.4.1.7.9 Используемое программное обеспечение;

3.2.4.1.8 Структура обработки ПДн:

3.2.4.1.8.1 Первоначальный ввод данных;

3.2.4.1.8.2 Внутренний обмен информацией;

3.2.4.1.8.3 Обслуживание ИСПДн;

3.2.4.1.8.4 Объекты, создающие условия для появления угроз персональным данным;

3.2.4.1.8.5 Формы представления персональных данных на различных этапах обработки;

3.2.4.1.8.6 Режим обработки ПДн;

3.2.4.1.8.7 Существующие меры защиты:

3.2.4.1.8.7.1 Технические меры защиты;

3.2.4.1.8.7.2 Организационные меры защиты;

3.2.4.1.9 Передача ПДн третьим лицам;

3.2.5 При изменении технологического процесса обработки информации, документы, указанные в пп. 3.2.1 , 3.2.2 пересматриваются постоянно-действующей комиссией по защите ПДн.

3.3 Порядок определения методов и способов защиты ПДн

3.3.1 Выбор и реализация методов и способов защиты информации в ИСПДн осуществляется на основе модели угроз безопасности ПДн и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 г., регистрационный № 11462). Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781.

3.3.2 Для экспертной оценки состояния исходной защищенности ИСПДн, вероятности реализации угроз и их опасности приказом главного врача ГБУЗ РМ «МРКБ» назначается комиссия по классификации в составе которой должны быть эксперты по безопасно-

ти информации. В качестве экспертов на договорной основе могут привлекаться специалисты специализированных организаций.

3.3.3 Выбранные и реализованные методы и способы защиты информации в системе защиты персональных данных должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в ИСПДн.

3.4 Порядок взаимодействия при разработке и вводе в действие СЗПДн

3.4.1 Устанавливаются следующие стадии создания системы защиты информации:

3.4.1.1 предпроектная стадия, включающая предпроектное обследование информационных систем, разработку аналитического обоснования необходимости создания СЗПДн и технического (частного технического) задания на ее создание;

3.4.1.2 стадия проектирования (разработки проектов) и реализации СЗПДн;

3.4.1.3 стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия СЗПДн по требованиям безопасности информации.

3.4.2 Стадии проектирования и ввода в действие СЗПДн могут быть объеденные в рамках одного договора с Лицензиатом.

3.4.3 **На предпроектной стадии** по обследованию информационных систем выполняются мероприятия, указанные в п. 3.2 .

3.4.4 По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗПДн. Аналитическое обоснование необходимости создания СЗПДн должно содержать:

3.4.4.1 информационную характеристику и организационную структуру ИСПДн;

3.4.4.2 характеристику комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;

3.4.4.3 возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;

3.4.4.4 перечень предлагаемых к использованию сертифицированных средств защиты информации;

3.4.5 Аналитическое обоснование подписывается руководителем предпроектного обследования, согласовывается с заместителем генерального директора по развитию ГБУЗ РМ «МРКБ», начальником управления по техническому развитию ГБУЗ РМ «МРКБ», начальником отдела информационных технологий ГБУЗ РМ «МРКБ», начальником управле-

ния по работе с персоналом ГБУЗ РМ «МРКБ» и утверждается главным врачом ГБУЗ РМ «МРКБ».

3.4.6 На основе действующих нормативных правовых актов и методических документов по защите ПДн, в порядке, определенном в п. 3.3 задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗПДн.

3.4.7 Техническое (частное техническое) задание на разработку СЗИ должно содержать:

3.4.7.1 Общие сведения;

3.4.7.2 Назначение и цели создания системы защиты;

3.4.7.3 Описание информационных систем персональных данных:

3.4.7.3.1 Назначение ИСПДн;

3.4.7.3.2 Цель обработки персональных данных;

3.4.7.3.3 Состав технических средств;

3.4.7.3.4 Расположение ИСПДн;

3.4.7.3.5 Описание информационных технологий;

3.4.7.3.6 Характеристика ИСПДн;

3.4.7.4 Описание неавтоматизированных информационных систем персональных данных:

3.4.7.4.1 Назначение ИСПДн;

3.4.7.4.2 Цели обработки персональных данных;

3.4.7.4.3 Расположение ИСПДн;

3.4.7.4.4 Описание мест хранения ПДн (материальных носителей ПДн)

3.4.7.5 Требования к исполнителю работ:

3.4.7.5.1 Наличие лицензий;

3.4.7.5.2 Требования по обеспечению режима конфиденциальности при выполнении работ

3.4.7.6 Требования к системе защиты информации:

3.4.7.6.1 Требования к системе защиты информации в целом;

3.4.7.6.2 Требования к реализации подсистем, реализующих функции СЗПДн;

3.4.7.6.3 Требования к системе защиты информации от НСД;

3.4.7.6.4 Требования к средствам криптографической защиты;

3.4.7.6.5 Перечень предполагаемых к использованию сертифицированных средств защиты информации:

3.4.7.6.6 Требования к численности и квалификации персонала, режиму его работы;

3.4.7.6.7 Показатели назначения;

3.4.7.6.8 Требования к надежности;

3.4.7.6.9 Требования безопасности;

3.4.7.6.10 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн;

3.4.7.6.11 Требования по сохранности информации при авариях;

3.4.7.6.12 Требования к средствам защиты от внешних воздействий;

3.4.7.6.13 Требования по стандартизации и унификации;

3.4.7.6.14 Требования к программному обеспечению объекта информатизации;

3.4.7.6.15 Требования к организационно–режимным мерам;

3.4.7.6.16 Рекомендации по защите от утечки информации за счет ПЭМИН;

3.4.7.7 Требования к защите персональных данных при обработке персональных данных без использования средств автоматизации:

3.4.7.7.1 Требования к защите персональных данных при их обработке без использования средств автоматизации в целом;

3.4.7.7.2 Организационные требования к защите ПДн при их обработке без использования средств автоматизации;

3.4.7.7.3 Требования к местам хранения персональных данных;

3.4.7.8 Состав и содержание работ по созданию СЗПДн;

3.4.7.8.1 Работы по созданию СЗПДн осуществляются по стадиям и этапам;

3.4.7.9 Требования к документированию;

3.4.7.10 Источники разработки;

3.4.7.11 Порядок внесения изменений в техническом задании.

3.4.8 Техническое (частное техническое) задание на разработку СЗПДн утверждается руководителем предприятия-разработчиком ТЗ и главным врачом ГБУЗ РМ «МРКБ», подписывается разработчиком ТЗ, согласовывается с лицом, ответственным за организацию обработки ПДн и администратором безопасности информации.

3.4.9 **На стадии проектирования и создания СЗПДн** на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

3.4.9.1 разработка технического проекта СЗПДн;

3.4.9.2 разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;

3.4.9.3 закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, либо их сертификация;

3.4.9.4 закупка сертифицированных технических, программных и программно-технических (в т.ч. криптографических) средств защиты информации и их установка;

3.4.9.5 разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;

3.4.9.6 организация охраны и физической защиты помещений объекта информатизации, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;

3.4.9.7 разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;

3.4.9.8 определение подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;

3.4.9.9 выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

3.4.9.10 разработка эксплуатационной документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов).

3.4.10 На стадии проектирования и создания объекта информатизации оформляются также эксплуатационная документация СЗПДн, состав которой приведен в п. 5.2.1 .

3.4.11 **На стадии ввода в действие СЗПДн** осуществляются:

3.4.11.1 опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки технологического процесса обработки (передачи) информации;

3.4.11.2 приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта;

3.4.11.3 оценка соответствия по требованиям безопасности информации.

3.4.12 На этой стадии оформляются:

3.4.12.1 акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний;

3.4.12.2 заключение по результатам испытаний.

3.4.13 Эксплуатация объекта информатизации осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в настоящем документе.

3.5 Порядок привлечения исполнителей работ по защите информации

3.5.1 Для выбора и реализации методов и способов защиты информации в информационной системе может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации (далее Лицензиат).

3.5.2 В случае привлечения Лицензиата главным врачом ГБУЗ РМ «МРКБ» назначается ответственный за организацию и проведение мероприятий по защите информации и за взаимодействием с лицензиатом. Ответственным за организацию и проведение мероприятий по защите информации и за взаимодействием с лицензиатом в ГБУЗ РМ «МРКБ» является лицо, ответственное за организацию обработки ПДн.

3.5.3 Договор с организацией, привлекаемой для выбора и реализации методов и способов защиты информации в информационной системе, должен содержать положения об ответственности сторон в соответствии с действующим законодательством РФ за разглашение сведений ограниченного распространения, а так же других охраняемых законом сведений, которые могут стать известны им в ходе совместной деятельности.

4 Допуск к обработке ПДн

4.1 К работе в ИСПДн должны допускаться сотрудники, имеющие уверенные навыки работы со средствами вычислительной техники.

4.2 Допуск должностных лиц к ПДн, необходимым для выполнения своих должностных обязанностей, осуществляется на основе пофамильных «Перечня лиц, допущенных к обработке ПДн» и «Перечня лиц, допущенных в помещение ...», в соответствии с «Разрешительной системой доступа ...» ИСПДн, утвержденными главным врачом ГБУЗ РМ «МРКБ».

4.3 «Перечень лиц, допущенных к обработке ПДн» должен содержать наименование ИСПДн, к которой предоставляется допуск, Ф.И.О. лица, которому предоставлен доступ к персональным данным и должность лица, допущенного к персональным данным.

4.4 Ответственный за подготовку (корректировку) документов «Перечень лиц, допущенных к обработке ПДн» и «Перечень лиц, допущенных в помещение ...» — заместитель главного врача по организационно-методической работе.

4.5 Порядок допуска сотрудника к обработке ПДн:

4.5.1 Издание приказа о назначении на должность и на допуск к обработке ПДн.

4.5.2 Внесение изменений в документы, перечисленные в п. 4.4 .

4.5.3 Ознакомление под роспись с «Перечнем защищаемых персональных данных» и внутренними документами, устанавливающими порядок обработки ПДн, а также их права и обязанности в этой области.

4.5.4 Предоставление технического доступа в ИСПДн:

4.5.4.1 Создание и передача необходимых атрибутов доступа к информационной системе и данным.

4.5.4.2 Проведение инструктажа по правилам эксплуатации СЗИ и в объеме инструкции пользователя ИСПДн.

4.6 Прекращение доступа сотрудника к ПДн.

4.6.1 Доступ сотрудника к ПДн должен быть прекращен в связи с его увольнением или переводом на другую должность.

4.6.2 При прекращении доступа сотрудников к ПДн должны быть выполнены следующие мероприятия:

4.6.2.1 Издание приказа об увольнении или переводе на другую должность.

4.6.2.2 Прекращение предоставления технического доступа в ИСПДн (удаление или блокирование учетных записей сотрудника, смена паролей для ресурсов, доступ к которым предоставляется без использования учетных записей или по совместно используемым учетным записям).

4.6.2.3 Прием выданных увольняемому (переводимому) сотруднику материальных атрибутов доступа, машинных носителей информации.

4.6.2.4 Внесение соответствующих изменений в документы, перечисленные в п. 4.4 .

4.7 Документ «Разрешительная система доступа ... » содержит перечни субъектов и объектов доступа и матрицу доступа для каждой автоматизированной ИСПДн. В качестве субъектов доступа перечисляет группы пользователей, имеющих одинаковые права доступа в системе. Объектами доступа могут быть информационные ресурсы, аппаратные ресурсы, полномочия на выполнения отдельных действий, а так же сетевые службы.

4.8 «Разрешительная система доступа ...» подготавливается ЛОО и утверждается главным врачом ГБУЗ РМ «МРКБ».

4.9 «Разрешительная система доступа ...» требует уточнения в случае изменения технологического процесса обработки информации. Решение о необходимости изменения принимает ЛОО.

4.10 Реализация изменений разрешительной системы производится в следующем порядке:

4.10.1 подготовка, согласование и утверждение изменений «Разрешительной системы доступа ...» или новой версии этого документа;

4.10.2 приостановка эксплуатации фрагмента информационной системы, которую затрагивают изменения;

4.10.3 изменение настроек СЗИ;

4.10.4 проведение испытаний правильности настроек СЗИ и соответствия их «Разрешительной системе ...»

4.10.5 возобновление эксплуатации фрагмента информационной системы.

5 Защита ПДн в процессе эксплуатации информационной системы

5.1 Перечень применяемых мер по обеспечению безопасности ПДн

5.1.1 Для обеспечения безопасности ПДн применяются следующие основные меры:

5.1.1.1 реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

5.1.1.2 ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также, хранятся носители информации;

5.1.1.3 разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

5.1.1.4 регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

5.1.1.5 учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

5.1.1.6 резервирование технических средств, дублирование массивов и носителей информации;

5.1.1.7 использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

5.1.1.8 использование защищенных каналов связи;

5.1.1.9 размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

5.1.1.10 организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

5.1.1.11 предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

5.2 Эксплуатационная документация системы защиты персональных данных

5.2.1 Информационные системы персональных данных должны иметь комплект эксплуатационной документации, включающий в себя следующие документы:

5.2.1.1 описания технического, программного, информационного обеспечения и технологии обработки (передачи) информации;

5.2.1.2 инструкции и руководства по эксплуатации технических и программных средств защиты для пользователей, администраторов системы, а также для работников службы защиты информации;

5.2.1.3 технические паспорта;

5.2.1.4 журналы учета МНИ, выдачи МНИ, регистрации инцидентов безопасности, учета криптосредств.

5.2.2 Обязанности должностных лиц, в части касающийся обеспечения безопасности ПДн, изложены в документах:

5.2.2.1 «Инструкция администратора безопасности информации информационных систем персональных данных ГБУЗ РМ «Мордовская республиканская клиническая больница»;

5.2.2.2 «Инструкция пользователя по работе на АРМ информационных систем персональных данных ГБУЗ РМ «Мордовская республиканская клиническая больница».

5.2.3 Первоначально инструкции могут быть разработаны Лицензиатом, в рамках договора на создание СЗПДн. В случае изменения технологического процесса обработки информации, либо по результатам расследования инцидентов безопасности в инструкции могут быть внесены изменения. Изменения разрабатываются (согласовываются) с лицом, ответственным за организацию обработки ПДн и главным врачом ГБУЗ РМ «МРКБ»

5.2.4 Технический паспорт должен иметь форму, приведенную в Приложении В «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)». При необходимости, могут быть разработаны технические паспорта отдельных АРМ ИСПДн.

5.2.5 Технический паспорт используется, в том числе, для учета применяемых средств защиты информации.

5.3 Порядок работы с носителями персональных данных

5.3.1 Информация из ИСПДн может отчуждаться либо на бумажные, либо на машинные носители информации (USB-накопители, оптические диски, магнитные дискеты). Право на отчуждение информации определяется «Разрешительной системой доступа ...».

5.3.2 При выводе персональных данных на бумажные носители необходимо исключить просмотр выводимой информации лицами, недопущенными к обработке ПДн.

5.3.3 Выводимые на печать ПДн должны обособляться от иной, не относящейся к ПДн, информации.

5.3.4 Места хранения носителей персональных данных (комната, инв. номер шкафа (сейфа)), должностные лица, ответственные за их сохранность, вид носителя персональных данных определяются в документе «Перечень мест хранения носителей ПДн», разрабатываемом ЛОО.

5.4 Порядок учета машинных носителей информации

5.4.1 В качестве машинных носителей информации (МНИ) в ИСПДн могут использоваться накопители на ЖМД, USB-накопители, накопители на оптических дисках, дискеты.

5.4.2 Все машинные носители информации, включая НЖМД входящие в состав системных блоков ЭВМ, должны быть зарегистрированы в «Журнале учета машинных носителей информации». Ответственный за регистрацию, хранение и выдачу МНИ — администратор безопасности информации.

5.4.3 При регистрации на МНИ любым доступным способом наносятся: гриф «ПДн», регистрационный номер, дата регистрации и подпись лица, ответственного за регистрацию.

5.4.4 Зарегистрированные МНИ выдаются пользователям под роспись в «Журнале учета выдачи машинных носителей информации».

5.4.5 Запрещается запись информации, содержащей ПДн, на незарегистрированные носители информации.

5.4.6 Уничтожение МНИ осуществляется по акту, способом, исключающим возможность восстановления информации.

5.5 Порядок резервирования технических средств, дублирования массивов и носителей информации

5.5.1 Резервное копирование должно осуществлять на периодической основе:

5.5.1.1 для обрабатываемых персональных данных – не реже раза в неделю;

5.5.1.2 для технологической информации – не реже раза в месяц;

5.5.1.3 эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДи – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

5.5.2 Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

5.5.3 Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

5.5.4 Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

5.5.5 Носители должны храниться не менее года, для возможности восстановления данных.

6 Контроль за обеспечением уровня защищенности ПДн

В целях обеспечения заданных характеристик безопасности ИСПДи должен осуществляться контроль состояния и эффективности защиты информации.

Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

Контроль может быть повседневным, периодическим и внеплановым.

Повседневный контроль, с целью своевременного обнаружения фактов НСД, проводится:

непосредственно пользователями автоматизированных рабочих мест перед началом и в ходе работы с защищаемой информацией;

администратором безопасности с выделенного рабочего места с использованием встроенных средств мониторинга СЗИ и средствами обнаружения вторжений.

Периодический, с целью тестирования функций системы защиты персональных данных с помощью тест-программ, имитирующих попытки несанкционированного доступа. Вы-

полняется администратором безопасности информации или Лицензиатом по отдельному договору.

Периодичность контроля определяется ЛОО и отражается в плане работ по защите информации.

Внеплановый контроль выполняется в случаях изменения разрешительной системы, подозрения на НСД, распространения вирусных эпидемий и др. случаях.

О проведениях периодического и внепланового контролей делается отметка в техническом паспорте ИСПДн.

7 Реагирование на инциденты нарушения информационной безопасности и сбои

7.1 В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

7.2 Происшествие, вызывающее инцидент, может произойти:

7.2.1 В результате непреднамеренных действий пользователей.

7.2.2 В результате преднамеренных действий пользователей и третьих лиц.

7.2.3 В результате нарушения правил эксплуатации технических средств ИСПДн.

7.2.4 В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

7.3 Пользователи ИСПДн должны быть проинформированы о необходимости обращать внимание и сообщать о любых замечаниях или предполагаемых недостатках или угрозах в области безопасности. При наличии такой информации пользователи должны сообщать ее администратору безопасности информации. Пользователи ни при каких обстоятельствах не должны самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности, так как это может быть интерпретировано как неправомочное использование системы.

7.3.1 Инцидентами нарушения информационной безопасности являются компрометация ключевой и (или) парольной информации (утеря или оставление без присмотра носителей ключевой и (или) парольной информации, разглашение пароля, ввод пароля в присутствии посторонних лиц), получение предупредительных сообщений от средств защиты информации, странное поведение системы, подозрения в НСД, отсутствие (повреждение, недоступность информационных ресурсов), нарушение физической целостности технических средств или их печатей (пломб) и т.п.

7.3.2 При возникновении (подозрении) инцидентов нарушения информационной безопасности пользователи информационной системы должны:

7.3.2.1 зафиксировать симптомы инцидента (появляющиеся сообщения);

7.3.2.2 физически отключить АРМ от ЛВС, прекратить обработку ПДн;

7.3.2.3 не допускать использования МНИ на других АРМ;

7.3.2.4 незамедлительно информировать любыми доступными средствами своего непосредственного руководителя и администратора безопасности информации.

7.3.3 Администратор безопасности информации при получении информации о возникновении (подозрении) инцидента безопасности информации должен:

7.3.3.1 Принимать меры к сбору информации для расследования инцидента. При этом, копирование информации с носителей и оперативной памяти следует выполнять таким образом, чтобы обеспечить их доступность. Журнал всех действий, выполненных в течение процесса копирования необходимо сохранять, а сам процесс копирования необходимо документировать. Одну копию и журнал необходимо хранить безопасным способом.

7.3.3.2 В случае предполагаемых судебных разбирательств на ранней стадии привлекать юриста или полицию для консультации относительно требуемых свидетельств.

7.3.3.3 Принимать меры к смене утерянных (скомпрометированных) атрибутов доступа и ключей.

7.3.3.4 Принимать меры к восстановлению системы. При нарушении целостности системы должна быть выполнена переустановка ПО и СЗИ с оригинальных дистрибутивов.

7.3.3.5 Регистрировать информацию об инцидентах нарушения информационной безопасности в специальном журнале.

7.3.3.6 Докладывать лицу, ответственному за организацию обработки ПДн, о инцидентах безопасности информации.

7.3.3.7 Периодически, совместно с ЛОО, проводить анализ зарегистрированных инцидентов с целью совершенствования существующих или внедрения дополнительных мероприятий по обеспечению безопасности ПДн.

7.3.3.8 Использовать информацию об инцидентах с целью повышения информированности пользователей.

7.3.4 По фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, лицо, ответственное за организацию обработки ПДн, назначает разбирательство. По результатам разбирательства разрабатываются

меры по предотвращению возможных опасных последствий подобных нарушений и вся информация докладывается Главному врачу ГБУЗ РМ «МРКБ».

7.3.5 При обнаружении нарушений порядка предоставления ПДн пользователям информационной системы Главный врач ГБУЗ РМ «МРКБ» отдает распоряжение о приостановке предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

РАЗРАБОТАЛИ

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата
ООО «Поволжский экспертно-аттестационный центр «ЮРАТЭКС»	Инженер-системотехник ООО «ЮРАТЭКС»	Е.В. Остриков		23.12.11

ег. № 948