ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ БАШКОРТОСТАН ИШИМБАЙСКАЯ ЦЕНТРАЛЬНАЯ РАЙОННАЯ БОЛЬНИЦА

ПРИКАЗ

№ 20/1 «11» 01 2023г.

Об организации работ по обеспечению безопасности персональных данных

С целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных государственного бюджетного учреждения здравоохранения Республики Башкортостан Ишимбайская центральная районная больница (далее – ГБУЗ РБ Ишимбайская ЦРБ) в соответствии с требованиями Федерального Закона РФ «О персональных данных» от 27.07.2006 №152-ФЗ

ПРИКАЗЫВАЮ:

1. Назначить ответственных лиц:

- за организацию обработки персональных данных в ГБУЗ РБ Ишимбайская ЦРБ специалиста по защите информации Кузьминых О.П.
- за выполнение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (администратором безопасности информационной системы персональных данных) Кузьминых О.П.
- за выполнение работ по технической защите персональных данных (администратором информационной безопасности) в ГБУЗ РБ Ишимбайская ЦРБ программиста Кононова А.С.

2. Утвердить инструкции:

- ответственного лица за организацию обработки персональных данных в ГБУЗ РБ Ишимбайская ЦРБ (Приложение № 1),
- администратора безопасности информационной системы персональных данных (Приложение №2),
- администратора информационной безопасности (Приложение №3),
- учета машинных носителей информации, содержащих персональные данные и иную конфиденциальную информацию (Приложение №4).

3. Руководителям структурных подразделений представить ответственному лицу за организацию обработки персональных данных должности сотрудников, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей.

4. Ответственному лицу за организацию обработки персональных данных представить на утверждение «Список должностей, доступ которых к персональным данным необходим для выполнения служебных обязанностей».

5. Ответственному лицу за организацию обработки персональных данных представить на утверждение «Перечень персональных данных, обрабатываемых в ГБУЗ РБ Ишимбайская ЦРБ» для выполнения служебных обязанностей сотрудниками ГБУЗ РБ Ишимбайская ЦРБ, допущенных к обработке персональных данных.

6. Работы по обеспечению безопасности персональных данных проводить в соответствии с «Планом мероприятий по защите персональных данных» (Приложение 4).

7. Приказ довести до всех сотрудников ГБУЗ РБ Ишимбайская ЦРБ.

8. Контроль за выполнением требований настоящего приказа оставляю за собой.

Приложения:

1. «Инструкция ответственного за организацию обработки персональных данных» на 1 л. в 1 экз.

2. «Инструкция администратора безопасности информационной системы» на 2 л. в 1 экз.

3. «Инструкция администратора по информационной безопасности» на 2 л. в 1экз.

4. «План мероприятий по защите персональных данных» на 2 л. в 1 экз.

5. Лист ознакомления с «Приказом об организации работ по обеспечению безопасности персональных данных» на 1 л. в 1 экз.

Главный врач А.Р. Янышев

Приложение №1
к приказу главного врача
ГБУЗ РБ Ишимбайская ЦРБ
от «11» 01 2023г. №2011

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБУЗ РБ ИШИМБАЙСКАЯ ЦРБ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая должностная инструкция определяет права, ответственность и обязанности ответственного (далее - Ответственный) за организацию обработки персональных данных (далее - ПДн) в ГБУЗ РБ Ишимбайская ЦРБ.

2. Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также иными локальными нормативными актами организации, регламентирующими вопросы обработки персональных данных.

3. Методическое руководство и контроль работы должностных лиц в ГБУЗ РБ Ишимбайская ЦРБ осуществляет ответственный за организацию обработки персональных данных.

4. Ответственный за организацию обработки персональных данных относится к категории специалистов и непосредственно подчиняется главному врачу ГБУЗ РБ Ишимбайская ЦРБ.

2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Должностное лицо, ответственное за организацию обработки ПДн в ГБУЗ РБ Ишимбайская ЦРБ, обязано:

- знать и выполнять требования действующего законодательства РФ, а также внутренних инструкций и положений, регламентирующих деятельность по обработке и защите ПДн;
- отслеживать изменения действующего законодательства РФ по вопросам защиты и обработки ПДн;
- участвовать в проведении служебных расследований по фактам нарушения функционирования информационной системы персональных данных, а также других случаев нарушения правил обработки и защиты ПДн;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- организовать ведение журнала учета обращений субъектов ПДн;
- разрабатывать или участвовать в разработке внутренних документов по вопросам защиты личных данных.

3. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Должностное лицо, ответственное за организацию обработки ПДн в ГБУЗ РБ Ишимбайская ЦРБ имеет право:

- требовать от должностных лиц, уполномоченных на обработку персональных данных, безусловного соблюдения установленных правил обработки и защиты ПДн;
- требовать от должностных лиц, уполномоченных на обработку персональных данных прекращения обработки ПДн, в случаях их неправомерного использования и нарушения установленного порядка обработки;
- осуществлять взаимодействие с руководителями структурных служб организации, получать информацию и документы, необходимые для выполнения своих должностных обязанностей;
- доступа во все помещения соответствующего структурного подразделения, где осуществляется обработка ПДн;
- в пределах своей компетенции сообщать главному врачу о недостатках, выявленных в процессе исполнения должностных обязанностей, и вносить предложения по их устранению;
- требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав;
- подписывать и визировать документы в пределах своей компетенции.

4. ОТВЕТСТВЕННОСТЬ

Должностное лицо, ответственное за организацию обработки ПДн в ГБУЗ Ишимбайская ЦРБ несет ответственность:

- за качество и полноту проводимых им работ по организации обработки ПДн в соответствии с функциональными обязанностями, определенными настоящей Инструкцией;
- за сохранность сведений ограниченного распространения в соответствии с требованиями законодательства в области защиты ПДн,
- организовывать публикацию документов, определяющих политику в отношении обработки персональных данных, на официальном сайте учреждения;
- доводить до сведения работников организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

С инструкцией ознакомлен _____ О.П.Кузьминых

«11» 01 2023 г.

Приложение №2
к приказу главного врача
ГБУЗ РБ Ишимбайская ЦРБ
от «11» 01 2023г. №10/1

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция разработана на основании:

- Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации №781 от 17 ноября 2007г.;
- Приказа №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного ФСТЭК России от 05.02.2010 г.;
- Положения «О разрешительной системе допуска пользователей к обрабатываемой в ИСПДн информации», утвержденного главным врачом ГБУЗ РБ Ишимбайская ЦРБ.

1.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственность Администратора безопасности информационной системы персональных данных (далее - ИСПДн) Государственного бюджетного учреждения Республики Башкортостан Ишимбайская центральная районная больница» (далее – ГБУЗ РБ Ишимбайская ЦРБ).

1.3. Администратор безопасности ИСПДн (далее - Администратор) назначается приказом главного врача и является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники ИСПДн ГБУЗ РБ Ишимбайская ЦРБ, в пределах своей зоны ответственности.

1.4. Закрепление функциональных обязанностей и разделение зон ответственности производится приказом главного врача ГБУЗ РБ Ишимбайская ЦРБ.

1.5. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, общегосударственных, ведомственных, а также внутренних нормативных документов по вопросам защиты информации и обеспечивает их выполнение пользователями ИСПДн.

1.6. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. ЗАДАЧИ И ФУНКЦИИ АДМИНИСТРАТОРА

2.1. Основными задачами Администратора являются:

- сопровождение средств защиты информации (в т.ч. криптографических, шифровальных) от несанкционированного доступа (далее - СЗИ) и основных технических средств и систем (далее - ОТСС);

- организация разграничения доступа;

- контроль эффективности защиты информации.

2.2. Для выполнения поставленных задач на Администратора возлагаются следующие функции:

2.2.1. Допуск пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам ИСПДн в соответствии с требованиями «Положения о разрешительной системе допуска пользователей к обрабатываемой в ИСПДн информации» на всех стадиях жизненного цикла ИСПДн.

2.2.2. Участие на стадии проектирования (внедрения) ИСПДн в разработке технологии обработки информации конфиденциального характера (далее - Информации) по вопросам:

- организации порядка учета, хранения и обращения с документами и носителями информации;

- подготовки инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей ИСПДн по вопросам защиты информации;

- сопровождение СЗИ, в том числе средств криптографической защиты информации, на стадии эксплуатации ИСПДн, включая ведение служебной информации СЗИ (управление ключевой системой, сопровождение правил разграничения доступа), оперативный контроль за функционированием СЗИ;

- контроль выполнения требований действующих нормативных документов по вопросам защиты информации при обработке информации в ИСПДн;

- контроль соответствия общесистемной программной среды эталону (контроль целостности программного обеспечения) и проверка включаемых в ИСПДн новых программных средств.

3.ОБЯЗАННОСТИ АДМИНИСТРАТОРА

3.1. Для реализации поставленных задач и возложенных функций **Администратор ОБЯЗАН:**

3.1.1. Сопровождать СЗИ и ОТСС:

- вести учет (по вопросам обеспечения безопасности информации) и знать перечень установленных в подразделениях НГГУ СЗИ и перечень задач, решаемых с их использованием;

- вести журнал учета эксплуатационной и технической документации СЗИ ИСПДн;

- вести журнал учета машинных носителей персональных данных;

- осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на автоматизированных рабочих местах (далее - АРМ) специальных программных и программно-аппаратных СЗИ;

- присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств, защищенных АРМ и серверов, осуществлять

проверку работоспособности системы защиты после установки (обновления) программных средств ИСПДн;

- периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование);
- контролировать соответствие технического паспорта ИСПДн фактическому составу (комплектности) ИСПДн и вести учет изменений аппаратно¬программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИСПДн);
- периодически контролировать целостность печатей (пломб, наклеек) на устройствах, защищенных АРМ;
- вести журнал учета внештатных ситуаций, фактов вскрытия и опечатывания АРМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИСПДн;
- проводить периодический инструктаж сотрудников подразделения (пользователей ИСПДн) по правилам работы с используемыми средствами и системами зашиты информации.

3.1.2. Организовывать разграничения доступа:

3.1.2.1.Участвовать в разработке и знать перечень защищаемых информационных ресурсов.

3.1.2.2.Разрабатывать для ИСПДн решения по:

- составу доменов сети, системы доверительных отношений между ними;
- составу групп (локальных и глобальных) каждого домена;
- приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;
- определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;
- вести учет заявок пользователей на допуск к информационным ресурсам ИСПДн;
- осуществлению контроля за наличием активных компьютеров сети, состоянием активных пользователей, использованием разделяемых ресурсов, процессом печати на общих принтерах;
- разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, проектированию системы почтовых ящиков, использованию СЗИ при передаче закрытых документов);
- разработке порядка выхода пользователей в сети связи общего пользования (далее - Сети) и использованию встроенных СЗИ в сервисных программах;
- определению режимов использования СЗИ: защита паролей, защита в протоколах передачи данных, кодирование файлов, подключение дополнительных алгоритмов криптографической защиты;
- разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита;
- осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ ИСПДн;
- контролировать и требовать соблюдения установленных правил по организации парольной защиты в ИСПДн НГГУ;
- осуществлять оперативный контроль за работой пользователей, защищенных АРМ, анализировать содержимое журналов событий операционных систем (далее -

ОС), систем управления базами данных (далее - СУБД), пакетов прикладных программ (далее - ППП) и СЗИ всех АРМ и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование журналов событий АРМ и надлежащий режим хранения данных архивов;

- принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию серверов и АРМ ИСПДн;

- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АРМ и отправке их в ремонт (контролировать стирание информации на съемных носителях);

- организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль за правильностью их использования;

- осуществлять периодический контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных;

- по указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ, установленных на АРМ ИСПДн;

- требовать от пользователей стирания остаточной информации на несъёмных носителях (жестких дисках) установленным порядком, а в оперативной памяти по окончании обработки информации путем перезагрузки АРМ;

- контролировать обеспечение защиты конфиденциальной информации при взаимодействии абонентов с информационными сетями связи общего пользования.

3.1.3. Контролировать эффективность защиты информации:

- проводить работу по выявлению возможности вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам АРМ;

- докладывать ответственному по обеспечению безопасности о выявленных угрозах безопасности информации, обрабатываемой в ИСПДн, об имевших место попытках НСД к информации и техническим средствам АРМ;

- проводить занятия с пользователями ИСПДн по правилам работы на АРМ, оснащенных СЗИ, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности защиты информации;

- участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в ИСПДн.

3.2. Администратору ЗАПРЕЩАЕТСЯ:

3.2.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации.

3.2.2. Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.

3.2.3. Самостоятельно (без согласования с подразделением автоматизации) вносить изменения в настройки серверной части ИСПДн.

3.2.4. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, предоставлять такую возможность другим.

3.2.5. Выключать СЗИ без письменной санкции руководства.

3.2.6. Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки.

3.2.7. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИСПДн, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей.

3.2.8. Нарушать правила эксплуатации оборудования ИСПДн.

3.2.9. Корректировать, удалять, подменять журналы аудита.

4. ПРАВА И ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА

4.1. **Администратор имеет право**:

- получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и АРМ пользователей;
- требовать от пользователей ИСПДн выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;
- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн;
- осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности;
- производить анализ защищенности ИСПДн путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИСПДн. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением сотрудников подразделений автоматизации и обеспечение безопасности информации;
- вносить свои предложения по совершенствованию мер защиты в ИСПДн.

4.2. **Администратор несет** ответственность за:

- реализацию принятой в НГГУ политики информационной безопасности;
- программно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и ИСПДн обработки информации, закрепленные за ним приказом главного врача ГБУЗ РБ Ишимбайская ЦРБ, а также за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями;
- разглашение сведений, конфиденциального характера, ставших известными ему по роду работы;
- качество и последствия проводимых им работ по контролю действий пользователей при работе в ИСПДн.

С инструкцией ознакомлен _____ О.П. Кузьминых
(подпись) (Ф.И.О.)

«11» 01 2023 г.

Приложение №3
к приказу главного врача
ГБУЗ РБ Ишимбайская ЦРБ
от «11» 01 2023г. №2011

ИНСТРУКЦИЯ АДМИНИСТРАТОРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящая инструкция определяет общие функции, права и обязанности администратора безопасности по вопросам обеспечения информационной безопасности при подготовке и обработки персональных данных на ПЭВМ, входящих в состав информационной системы персональных данных (далее по тексту – ИСПДн).

Администратор безопасности информации назначается из числа сотрудников ГБУЗ РБ Ишимбайская РБ и обеспечивает правильное использование и функционирование установленных средств защиты информации (далее по тексту – СЗИ) от несанкционированного доступа (далее по тексту – НСД).

Настоящая инструкция разработана на основании действующих документов по защите персональных данных.

1.ОСНОВНЫЕ ФУНКЦИИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

1.1. Контроль за выполнением требований действующих нормативных и руководящих по защите персональных данных, при проведении работ на ПЭВМ.

1.2. Работа с учетными записями пользователей ИСПДн (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа пользователей к защищаемым ресурсам ИСПДн согласно разрешительной системе доступа.

1.3. Своевременная корректировка разрешительной системы доступа:

- изменение списка постоянных пользователей ИСПДн (ввод или удаление пользователя из ИСПДн);
- изменение прав доступа к защищаемым программным ресурсам или портам ввода – вывода ИСПДн.

1.4. Корректировка разрешительной системы доступа осуществляется на основании служебной записки пользователя, согласованной с ответственным за эксплуатацию объекта и утвержденной главным врачом ГБУЗ РБ Ишимбайская ЦРБ.

1.5. Контроль доступа пользователей к работе на ПЭВМ (в соответствии со списком допущенных сотрудников), выдача внешних носителей информации и соблюдения пользователями требований нормативных и руководящих документов (в том числе путем просмотра системного журнала).

1.6. Контроль за ежеквартальным проведением пользователями ИСПДн смены их личных паролей для доступа к ПЭВМ.

1.7. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе на ПЭВМ, в том числе и в части периодического контроля за печатью файлов пользователей на принтере и соблюдением установленных

правил и параметров регистрации и учета документов, бумажных и машинных носителей.

1.8. Сопровождение подсистемы обеспечения целостности информации на ПЭВМ:

- периодический контроль за отсутствием на жестком магнитном диске ПЭВМ остаточной информации по окончании работы пользователей;
- поддержание установленного порядка и правил антивирусной защиты информации, обрабатываемой на ПЭВМ.
- контроль за соблюдением пользователями инструкции по антивирусному контролю. Программирование, выдача и учет выдачи пользователям электронных ключей от СЗИ НСД (при их наличии).

1.9. Контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусе ПЭВМ и устройств.

1.10. Контроль за вскрытием и ремонтом (модернизацией) ПЭВМ, недопущением доступа посторонних лиц к конфиденциальной информации во время вскрытия, ремонта, модернизации ПЭВМ или устройств, последующим опечатыванием ПХВМ (устройств), составлением соответствующих актов.

1.11. Контроль срока действия сертификатов соответствия ФСТЭК России на средства защиты от несанкционированного доступа, установленных на ИСПДн.

2. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности имеет право:

2.1. Требовать от сотрудников ГБУЗ РБ Ишимбайская ЦРБ соблюдения установленной технологии обработки конфиденциальной информации и исполнении настоящей инструкции;

2.2. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследования фактов (попыток) несанкционированного доступа;

2.3. Требовать от пользователя прекращения обработки информации в ИСПДн в случае:

- нарушения установленного порядка работ;
- нарушения работоспособности средств и систем защиты информации или окончания срока действия сертификатов соответствия ФСТЭК России;
- получение информации о возможном проведении технической разведки в отношении ИСПДН.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратора безопасности обязан:

3.1. Обеспечивать правильное функционирование и поддерживать работоспособность и СЗИ от НСД в пределах, возложенных на него функции;

3.2. В случае отказа СЗИ от НСД принимать меры по их восстановлению;

3.3. Проводить инструктаж пользователей по правилам работы на ПЭВМ с установленной СЗИ от НСД.

3.4. Немедленно докладывать (по подчиненности) ответственному за эксплуатацию ИСПДн, главному врачу ГБУЗ РБ Ишимбайская ЦРБ или лицу,

исполняющему его обязанности, о фактах и попытках несанкционированного доступа к персональным данным, о неправомерных действиях пользователей и иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности ИСПДн.

3.5. Вносить изменения в документацию ИСПДн в соответствии с требованиями нормативных документов в части, касающейся СЗИ от НСД;

3.6. Проводить работу по выявлению возможных каналов утечки конфиденциальной информации, вести их учет и принимать меры к их устранению;

3.7. Осуществлять не реже одного раза в неделю обновление антивирусных баз на ПЭВМ и ИСПДн;

3.8. Контролировать целостность (неизменность, сохранность) программного обеспечения, разрешительной системы доступа, а при обнаружении фактов изменения проверяемых параметров немедленно докладывать по подчиненности;

3.9. Вводить полномочия работников в разрешительную систему доступа, обеспечивать их своевременную корректировку;

3.10. Регистрировать факты выдачи внешних носителей в журнале учета выдачи внешних носителей.

3.11. Требовать от пользователей прекращения обработки информации ИСПДН при появлении информации о возможном проведении технической разведки в отношении ИСПДН.

3.12. Заблокировать учетные записи пользователей на ПЭВМ в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИСПДн, до момента его продления. В случае не продления сертификата соответствия ФСТЭК России на СЗИ он обязан поставить в известность орган по аттестации, проводивший аттестацию ИСПДн, для принятия совместного решения.

3.13. Контролировать действия пользователей по правильности затирания информации на внешних носителях информации.

С инструкцией ознакомлен _____ А.С.Кононов
(подпись) (Ф.И.О.)

«11» 01 2023 г.

Приложение №5
к приказу главного врача
ГБУЗ РБ Ишимбайская ЦРБ
от «11» 01 2023г. №20/1

ЛИСТ ОЗНАКОМЛЕНИЯ
с «Приказом об организации работ по обеспечению безопасности персональных данных»

Дата ознакомления	ФИО сотрудника, ознакомившегося с документом	Должность сотрудника, ознакомившегося с документом	Подпись сотрудника, ознакомившегося с документом
1	2	3	4
11.01.23	О.П. Кузьминых	Спец. по защите информ.	
11.01.23	А.С. Кононов	программист	