БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ АЛТАЙ
«КОШ-АГАЧСКАЯ РАЙОННАЯ
БОЛЬНИЦА»

АЛТАЙ РЕСПУБЛИКАНЫН СУ-КАДЫК
КОРЫЫР БЮДЖЕТ ТӦЗӦМИ
«КОШ-АГАШ АЙМАКТЫН ЭМЧИЛИГИ»

ПРИКАЗ

«18 » сентября 2017г № 181

с.Кош-Агач

Об организации мероприятий по защите персональных данных

Во исполнение Конституции Российской Трудового Кодекса Российской Федерации, ст.57,65,81,86-88,90,192 Кодекса Российской Федерации об административных правонарушениях, ст. 5.27,5.39,13.11 Гражданского Кодекса Российской Федерации, Федерального закона от 27.07.2006 года №149-ФЗ «Об информации , информационных технологиях и о защите информации», Федерального закона от 27.07.2006 года №152 ФЗ «О персональных данных», Указа президента Российской Федерации от 06.03.1997 года №188 «О перечне сведений конфиденциального характера», **приказываю**:

1. Осуществлять режим защиты персональных данных в отношении данных перечисленных в Перечне персональных данных с учетом ведомственной специфики БУЗ РА «Кош-Агачская РБ» (приложения №1)
2. Назначить системного администратора Шохорова Олег Александровича администратором безопасности информационных систем персональных данных и администратором антивирусной защиты персональных данных.
3. Ввести в действие в БУЗ РА «Кош-Агачская РБ» документы регламентирующие порядок работы с персональными данными.

Утвердить:

1) Инструкцию администратора безопасности информационных системах персональных данных (приложения №2)
2) Инструкцию по организации антивирусной зашиты (приложение №3)
3) Форму журнала учета обращений субъектов персональных данных о выполнений их законных прав (приложение №4), журнал хранит и ведет руководитель структурного подразделения, в котором осуществляется обработка персональных данных;
4) Инструкцию по организации парольной защиты (приложение №5)
5) Инструкцию оператора информационных систем персональных данных (приложение №6)
6) Порядок резервирования и восстановления работоспособности технических систем и программного обеспечения, бах данных и средств защиты информации (приложение №7)
7) Перечень по учету применяемых средств защиты информации эксплуатационной и технической документации к ним (приложение №8), перечень хранит и ведет системный администратор;

8) Инструкцию пользователя ИСПДн (оператора ИСПДн, администратора ИСПДн, администратора безопасности ИСПДн, техника ИСПДн) по обеспечению безопасности обработки персональных данных, при возникновений внештатных ситуаций (приложение №9)

9) Инструкцию администратора информационных систем персональных данных (приложение №10)

4. Главному специалисту по кадрам Коккезевой А.К.:

- при приеме на работу новых сотрудников организовать проведение инструктажа по режиму обработки персональных данных в БУЗ РА «Кош-Агачская РБ» у ответственного по организации работ по защите персональных данных – системного администратора.

- внести в должностные инструкции сотрудников, имеющих доступ к персональным данным, пункт следующего содержания: «Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта персональных данных, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с действующим законодательством»

5. Контроль за исполнением данного приказа оставляю за собой.

6. Приказ №170 от 07 июня 2011года «Об организации мероприятий по защите персональных данных» считать утратившим в силу.

Главный врач
БУЗ РА «Кош-Агачская РБ» Макин А.А.

С приказом ознакомлены: Шонхоров О.А «18» 09 2017г.
Коккезева А.К. «18» 09 2017г.

Приложение №1
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Перечень персональных данных с учетом ведомственной специфики БУЗ РА «Кош-Агачская РБ»

№ п.п.	Наименований сведений	Типы документов, где возможно появление сведений конфиденциального характера
1	Сведения о Ф.И.О., месте жительства, месте работы или учебы, иные данные граждан, обратившихся в БУЗ РА «Кош-Агачская РБ» за исключением сведений, подлежащих распространению в средствах массовой информации в соответствии с законодательством	Письменные обращения граждан, с приложениями.
2	Сведения, содержащиеся в личных делах сотрудников БУЗ РА «Кош-Агачская РБ» в том числе сведения о фактах, событиях и обстоятельствах частной жизни сотрудников.	Личные дела, база данных.
3	Сведения о лицах, имеющих социально-значимые заболевания на территории Кош-Агачского района	Медицинские карты пациентов, базы данных, регистры
4	Информация о факте обращения за медицинской помощью, о состоянии здоровья гражданина, диагнозе его заболевания, иные сведения, полученные при его обследовании и лечении, в том числе сведения о фактах, событиях и обстоятельствах частной жизни больного.	Медицинские карты пациентов, базы данных, регистры, истории болезни.
5	Сведения о начисленной заработной плате, доходе, налоговых и других отчислениях сотрудников	Документы расчетной группы бухгалтерии

Приложение №2
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Инструкция администратора безопасности информационных систем персональных данных (ИСПДн)

1. Общие положения

1.1. Администратор безопасности ИСПДн (далее – Администратор) назначается приказом главного врача БУЗ РА «Кош-Агачская РБ».
1.2. Администратор подчиняется главному врачу.
1.3. Администратор в своей работе руководствуется настоящей инструкцией, требованиями законов и иных нормативных актов Российской Федерации по вопросам защиты персональных данных, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами БУЗ РА «Кош-Агачская РБ».
1.4. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.
1.5. Администратор безопасности является ответственным должностным лицом БУЗ РА «Кош-Агачская РБ», уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.
1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании БУЗ РА «Кош-Агачская РБ» так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.
1.7. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а также средствами контроля за техническими средствами защиты.
1.8 Администратор безопасности осуществляет методическое руководство Операторов ИСПДн и Администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.
1.9. Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.
1.7. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. Должностные обязанности

Администратор безопасности обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий

по защите информации.
2.2. Осуществлять установку, настройку и сопровождение технических средств защиты.
2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.
2.4. Участвовать в приемке новых программных средств.
2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.
2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.
2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.
2.8. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.
2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.
2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
2.11. Контролировать физическую сохранность средств и оборудования ИСПДн.
2.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.
2.13. Контролировать исполнение пользователями парольной политики.
2.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.
2.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.
2.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.
2.17. Не допускать к работе на элементах ИСПДн посторонних лиц.
2.18. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.
2.19. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.
2.20. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.
2.21. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
2.22. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

Приложение №3
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Инструкция по организации антивирусной защиты в информационных системах персональных данных БУЗ РА «Кош-Агачская РБ»

1. Общие требования

1.1. Настоящая инструкция определяет требования к организации защиты информационных систем персональных данных (далее - ИСПДн) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность работников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все ИСПДн, существующие и вновь создаваемые в БУЗ РА «Кош-Агачская РБ». Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности их работы.

1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства. В ИСПДн рекомендуется использовать антивирусные средства, имеющие сертификат системы сертификации средств защиты информации по требованиям безопасности

1.3. Установка и настройка средств антивирусного контроля на компьютерах (серверах) осуществляется специально назначенным лицом администратор (далее – администратор антивирусной защиты), в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных машинных носителях (накопителях информации типа flash, магнитных и CD/DVD-дисках) передкопированием в ИСПДн.

2.2. Полную проверку всех файлов ИСПДн средствами антивирусных программ на наличие вирусов проводит администратор антивирусной защиты не реже одного раза в месяц.

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

2.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений системных ошибках и т.п.) работник подразделения самостоятельно или вместе с администратором антивирусном защиты должен провести н антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора антивирусной защиты;
- провести анализ необходимости дальнейшего использования зараженных файлов;
- провести лечение или уничтожение зараженных файлов.

2.5. Администратор антивирусной защиты обязан **не реже одного** раза в месяц обновлять информационные базы антивирусных программ.

3. Ответственность

3.1. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкцией возлогается на администратора антивирусной защиты.

3.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями ИСПДн

3.3. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется администратором антивирусной защиты.

Приложение №4
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Журнал учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в информационных системах персональных данных

«_____»

№	Ф.И.О.	дата	цель

Пример цели: информирование, прекращение обработки, уточнение ПДн

Приложение №5
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Инструкция по организации парольной защиты информационных систем персональных данных БУЗ РА «Кош-Агачская РБ»

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (ИСПДн) БУЗ РА «Кош-Агачская РБ» , а также контроль за действиями пользователей и обслуживающего персонала системы при работе с идентификаторами и с личными паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей и контроль за действиями пользователей при работе с паролями возлагается на администратора безопасности информации.

2. Личные пароли должны генерируются, распределяются и выдаются пользователем администратором ИСПДн с учетом следующих требований: т

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присуствовать буквы в верхнем или нижнем регистрах, цифры, специальные символы (@,#,$,&,*,% и.т.п.);
- символы паролей должны вводится в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего.

3. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

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

5. Внеплановая смена личного пароля или удаление учетной записи пользователя, в случае прекращения его полномочий (увольнение, переход на другую работу, в другое подразделение организации и т.п.) должно немедленно производиться стирание администратором безопасности информации о пользователе после окончания последнего сеанса работы данного пользователя в информационной системе.

6. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора безопасности информации.

7. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п.4 или п.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

8. Хранение пользователем зарегистрированных идентификаторов и значений своих паролей на бумажном носителе допускается только в сейфе у администратора безопасности информации.

9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности информации.

Приложение №6
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Инструкция оператора информационной системы персональных данных БУЗ РА «Кош-Агачская РБ»

1. Общие положения

1.1. Оператор информационной системы персональных данных (далее по тексту - ИСПДн) осуществляет обработку персональных данных в ИСПДн.
1.2. Оператором является сотрудник БУЗ РА «Кош-Агачская РБ» участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
1.3. Оператор несет персональную ответственность за свои действия.
1.4. Оператор в своей работе руководствуется настоящей инструкцией, Концепцией информационной безопасности, Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами БУЗ РА «Кош-Агачская РБ»
1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Оператор обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.
2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопас- ности ПДн, а также руководящих и организационно-распорядительных документов.
2.4. Соблюдать требования парольной политики (Инструкция по парольной защите).
2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других.
2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них ин- формацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты). 2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Оператора, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к лицу ответственному за обеспечение информационной безопасности ИСПДн.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.
2.9. Операторам запрещается:
- Разглашать защищаемую информацию третьим лицам.
- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
- Отключать (блокировать) средства защиты информации.
- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован.
2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.
3.2. При работе в Сети запрещается:
- Осуществлять работу при отключенных средствах защиты (антивирус и других).
- Передавать по Сети защищаемую информацию без использования средств шифрования.
- Запрещается скачивать из Сети программное обеспечение и другие файлы.
- Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).
- Запрещается нецелевое использование подключения к Сети

Приложение №7
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Порядок резервирования и восстановления работоспособности технических систем и программного обеспечения, баз данных и средств защиты информации

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Инструкция), связанные с функционированием ИСПДн БУЗ РА «Кош-Агачская РБ», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех сотрудников БУЗ РА «Кош-Агачская РБ» , имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор ИСПДн.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности.

2. Порядок реагирования на инцидент

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

Происшествие, вызывающее инцидент, может произойти:

- В результате непреднамеренных действий пользователей.
- В результате преднамеренных действий пользователей и третьих лиц.
- В результате нарушения правил эксплуатации технических средств ИСПДн.
- В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения (Администратор безопасности, Администратор и Оператор ИСПДн), сотрудниками предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3 Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1 Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения БУЗ РА «Кош-Агачская РБ» (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2 Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

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

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

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

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

4. Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности.

Приложение №8
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним

Информационная система персональных данных
БУЗ РА «Кош-Агачская РБ»
Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации

Техническое средство	Эксплуатационная информация	Техническая документация

Приложение №9
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Инструкция пользователя ИСПДн по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций

1. Назначение и область действия

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн БУЗ РА «Кош-Агачская РБ» , меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуации, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;

Системы резервного копирования и хранения данных;

- системы контроля физического доступа;

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

2. Порядок реагирования на аварийную ситуацию

2.1. Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в таблице «Источники угроз»

Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	сбои общественного транспорта

7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	сильные морозы
12	Просадка грунта с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействия подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телекомуникационные и ИТ угрозы	
17	Сбой системы кондиционирования
18	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физически разрыв внешних каналов связи

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения сотрудниками (Администратор безопасности, Администратор и Оператор ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

- Уровень 1 – **Незначительный инцидент**. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

- Уровень 2 – **Авария**. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

1. Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- сбоя системы кондиционирования.

2. Отсутствие Администратора безопасности более чем на сутки из-за:
   - химического выброса в атмосферу;
   - сбоев общественного транспорта;
   - эпидемии;
   - массового отравления персонала;
   - сильного снегопада;
   - торнадо;
   - сильных морозов.

- Уровень 3 – **Катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости от Объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения БУЗ РА «Кош-Агачская РБ» (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Порядке резервирования и восстановления работоспособности технический систем и программного обеспечения, баз данных и средств защиты информации.

3.2. Организационные меры.

Ответственные за реагирование сотрудники ознакомляют всех сотрудников БУЗ РА «Кош-Агачская РБ» , находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового сотрудника на работу. По окончанию ознакомления сотрудник расписывается в листе ознакомления. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц БУЗ РА «Кош-Агачская РБ», имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Администраторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

Приложение № 10
к приказу главного врача
БУЗ РА «Кош-Агачская РБ»
от «18» сентября 2017г. №181

Инструкцию администратора информационных систем персональных данных

1. Общие данные

1.1. Администратор ИСПДн (далее – Администратор) назначается приказом главного врача БУЗ РА «Кош-Агачская РБ», на основании Положение о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется главному врачу.

1.3. Администратор в своей работе руководствуется настоящей инструкцией и Положением о защите персональных данных, руководящими и нормативными документами ФСТЭК России и другими регламентирующими документами БУЗ РА «Кош-Агачская РБ».

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Администратор обязан:

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

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения автоматизированных рабочих мест (далее – АРМ) и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов 2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственного за приведение ИСПДн в соответствие нормативным требованиям о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.