

Министерство здравоохранения Свердловской области  
государственное бюджетное учреждение здравоохранения Свердловской области  
**«ДЕМИДОВСКАЯ ГОРОДСКАЯ БОЛЬНИЦА»**  
(ГБУЗ СО «Демидовская ГБ»)  
ул. Горошникова, 37 г. Нижний Тагил, Свердловская область, Россия, 622034  
Телефон/факс: (3435) 41-21-55, эл. адрес: [dcgb@inbox.ru](mailto:dcgb@inbox.ru)  
ИНН 6623097055 КПП 662301001

### ПРИКАЗ

« 12 » 02 \_\_\_\_\_ 2018 г.

№ 90-1 \_\_\_\_\_

***Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ СО «Демидовской ГБ».***

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

#### ПРИКАЗЫВАЮ:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ СО «Демидовской ГБ» (Приложение №1)
2. Утвердить План внутренних проверок данных ГБУЗ СО «Демидовской ГБ» (Приложение № 2).
3. Ответственному за обработку персональных данных начальнику отдела ИТ Игравову Н.С. в срок до 12.02.2018 ознакомить под роспись сотрудников, допущенных к обработке персональных данных с Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ СО «Демидовской ГБ».
4. Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач



С.В. Овсянников

**ПРАВИЛА**  
**осуществления внутреннего контроля соответствия обработки персональных**  
**данных требованиям к защите персональных данных ГБУЗ СО «Демидовской**  
**ГБ»**

1. ОБЩИЕ ПОЛОЖЕНИЯ
  - 1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных ГБУЗ СО «Демидовской ГБ» разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и действуют постоянно.
2. ТЕМАТИКА ВНУТРЕННЕГО КОНТРОЛЯ.
  - 2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:
    - 2.1.1. соответствие полномочий пользователя матрице доступа;
    - 2.1.2. соблюдение пользователями информационных систем персональных данных ГБУЗ СО «Демидовской ГБ» парольной политики;
    - 2.1.3. соблюдение пользователями информационных систем персональных данных ГБУЗ СО «Демидовской ГБ» антивирусной политики;
    - 2.1.4. соблюдение пользователями информационных систем персональных данных ГБУЗ СО «Демидовской ГБ» правил работы со съемными носителями персональных данных;
    - 2.1.5. соблюдение ответственными за криптографические средства защиты информации правил работы с ними;
    - 2.1.6. соблюдение порядка доступа в помещения ГБУЗ СО «Демидовской ГБ», в которых расположены элементы информационных систем персональных данных;
    - 2.1.7. соблюдение порядка резервирования баз данных и хранения резервных копий;
    - 2.1.8. соблюдение порядка работы со средствами защиты информации;
    - 2.1.9. знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.
  - 2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:
    - 2.2.1. соблюдение порядка хранения бумажных носителей с персональными данными;
    - 2.2.2. соблюдение порядка доступа к бумажным носителям персональных данных;
    - 2.2.3. соблюдение порядка доступа в помещения, в которых обрабатываются и хранятся бумажные носители с персональными данными.
3. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК.
  - 3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям ГБУЗ СО «Демидовской ГБ» организует проведение периодических проверок условий обработки персональных данных.
  - 3.2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее Ответственный) либо комиссией, образуемой руководителем ГБУЗ СО «Демидовской ГБ».
  - 3.3. Внутренние проверки проводятся по необходимости в соответствии с поручением руководителя ГБУЗ СО «Демидовской ГБ».
  - 3.4. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

- 3.5. По итогам каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 3 к настоящему Приказу.
- 3.6. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
- 3.7. Протоколы хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится Ответственным, либо комиссией самостоятельно в январе следующего за проверочным годом.
- 3.8. О результатах проверки и мерах, необходимых для устранения нарушений, руководителю ГБУЗ СО «Демидовской ГБ» докладывает Ответственный либо Председатель комиссии.

План внутренних проверок условий обработки персональных данных  
ГБУЗ СО «Демидовской ГБ»

№	Тема проверки	Нормативный документ, предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие полномочий пользователя матрице доступа	Разрешительная система (матрица) доступа Политика ГБУЗ СО «Демидовской ГБ» в отношении обработки персональных данных		
2.	Соблюдение пользователями информационных систем персональных данных парольной политики	Положение по защите персональных данных		
3.	Соблюдение пользователями информационных систем персональных данных антивирусной политики	ГБУЗ СО «Демидовская ГБ» обрабатываемых в ИСПДн		
4.	Соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных	Положение по защите персональных данных, обрабатываемых в ИСПДн ГБУЗ СО «Демидовской ГБ» Политика ГБУЗ СО «Демидовской ГБ» в отношении обработки персональных данных		
5.	Соблюдение ответственными за криптографические средства защиты информации правил работы с ними	Положение по защите персональных данных, обрабатываемых в ИСПДн ГБУЗ СО «Демидовской ГБ»		
6.	Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных	Список помещений ГБУЗ СО «Демидовской ГБ» в которых обрабатываются ПД		

7.	Соблюдение порядка резервирования баз данных и хранения резервных копий	Положение по защите персональных данных, обрабатываемых в ИСПДн ГБУЗ СО «Демидовской ГБ»		
8.	Соблюдение порядка работы со средствами защиты информации			
9.	Знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях			
10.	Хранение бумажных носителей с персональными данными	Положение по защите персональных данных ГБУЗ СО «Демидовской ГБ»		
11.	Доступ к бумажным носителям с персональными данными			
12.	Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными	Положение по защите персональных данных ГБУЗ СО «Демидовской ГБ» Список помещений		

**Форма протокола проведения внутренней проверки  
ГБУЗ СО «Демидовской ГБ»**

Настоящий Протокол составлен в том, что \_\_\_\_\_ .201\_ ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка

\_\_\_\_\_  
*Тема проверки*

Проверка осуществлялась в соответствии с требованиями

\_\_\_\_\_  
*Название документа*

В ходе проверки проверено: \_\_\_\_\_  
\_\_\_\_\_

Выявленные нарушения: \_\_\_\_\_  
\_\_\_\_\_

Меры по устранению нарушений: \_\_\_\_\_  
\_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_

Должность Ответственного \_\_\_\_\_ Ф.И.О.

Либо

Председатель комиссии: \_\_\_\_\_

*Должность, Ф.И.О.*

Членный комиссии \_\_\_\_\_

*Должность, Ф.И.О.*

\_\_\_\_\_  
*Должность, Ф.И.О.*

Руководитель проверяемого подразделения \_\_\_\_\_ Ф.И.О.