**ГКУСО ВО «Меленковский социально – реабилитационный центр**

**для несовершеннолетних»**

**ПРИКАЗ**

От 27.03.2017 г. № 26/3

*О порядке доступа сотрудников*

*в помещения, в которых*

*обрабатываются персональные данные*

В целях принятия мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», в том числе выполнения требований к защите персональных данных, установленных постановлением Правительства Российской Федерации от 01.09.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и постановлением Правительства Российской Федерации от 15.09.2008г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

**ПРИКАЗЫВАЮ:**

1. Утвердить перечень лиц, ответственных за доступ в помещения, в которых обрабатываются персональные данные (приложение №1).
2. Утвердить порядок доступа работников учреждения в помещения, в которых ведется обработка персональных данных (приложение №2).
3. Утвердить правила организации режима обеспечения безопасности помещений, в котором размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (приложение №3).
4. Контроль за исполнением приказа оставляю за собой.

**Директор\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.И. Кикеева**

**Приложение №1**

**к приказу №26/2 от 27.03.2017г.**

|  |  |  |
| --- | --- | --- |
| Номер кабинета | ФИО ответственного | Должность |
| 2 | Гурьева Елена Ивановна | Заведующий отделением ПБиП |
| 3 | Румянцева Галина Сергеевна | Заведующий стационарным отделением |
| 7 | Горшкова Елена Валерьевна | Специалист по кадрам |

Ознакомлены: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.И. Гурьева

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.С. Румянцева

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.В. Горшкова

**Приложение №2**

**к приказу №26/2 от 27.03.2017г.**

**Порядок доступа работников учреждения в помещения, в которых ведется обработка персональных данных**

1. Доступ работников учреждения в помещения, в которых ведется обработка персональных данных, осуществляется в целях обеспечения безопасности персональных данных.
2. Для помещений, в которых обрабатываются персональные данные, должен обеспечиваться режим безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этом помещении посторонних лиц.
3. Право самостоятельного входа в помещения имеют работники, непосредственно работающие в этих помещениях и лицо, ответственное за организацию обработки персональных данных.
4. Иные лица допускаются в помещения по согласованию с директором учреждения, ответственным за организацию обработки персональных данных, и в сопровождении лиц, работающих в этих помещениях.
5. Помещения по окончании рабочего дня должны закрываться на ключ.
6. Вскрытие и закрытие помещений производится лицами, имеющими право доступа.
7. Уборка помещений должна производиться в присутствии лиц осуществляющих обработку персональных данных.
8. Перед закрытием помещений по окончании рабочего дня, лица, имеющие право доступа в помещения, обязаны:

- убрать материальные носители персональных данных в шкафы, сейфы и закрыть их;

- отключить технический средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

- закрыть окна.

**9**. Перед открытием помещений лица, имеющие право доступа в помещения, обязаны:

- провести внешний осмотр с целью установления целостности двери и замка;

- открыть дверь и осмотреть помещение, где хранятся материальные носители.

**10.** При обнаружении неисправности двери и запирающих устройств необходимо:

- не вскрывая помещение, доложить директору учреждения;

- в присутствии лица, ответственного за организацию обработки персональных данных, и непосредственного директора учреждения, вскрыть помещение и осмотреть его;

- составить акт о выявленных нарушениях.

**11.** Ответственность за соблюдение порядка доступа в помещения возлагается на лицо, ответственное за организацию обработки персональных данных.

Ознакомлены: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.И. Гурьева

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.С. Румянцева

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.В. Горшкова

**Приложение №3**

**к приказу №26/2 от 27.03.2017г.**

**Правила организации режима обеспечения безопасности помещений, в котором размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения**

**1**. Настоящие правила устанавливают требования к организации режима обеспечения безопасности помещений в учреждении, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

**2.** Пропускной режим предусматривает:

- защиту от проникновения посторонних лиц в помещения учреждения, которая обеспечивается организацией режима доступа.

- запрет на внос и вынос за пределы помещения материальных носителей персональных данных;

- определение перечня должностных лиц, имеющих право доступа в помещение.

**3**. Внутриобъектовый режим предусматривает:

- назначение ответственного за помещения;

- помещения, в которых обрабатываются персональные данные с использованием средств автоматизации и без использования таких средств, должны иметь прочные двери, оборудованные механическими замками, а при необходимости, замками с контролем доступа;

- в нерабочее время помещение должно закрываться;

- в случае ухода в рабочее время из помещений работников, необходимо эти помещения закрыть на ключ;

- уборка помещений должна производиться в присутствии лица, ответственного за эти помещения.

- пребывание в помещениях посторонних лиц, не имеющих права доступа в

эти помещения, разрешено только после согласования с директором учреждения или лицом, ответственным за организацию обработки персональных данных, и в сопровождении лица, работающего в этих помещениях.

- контроль за пребыванием в помещениях посторонних лиц, не имеющих

права доступа в эти помещения, осуществляет ответственный за это помещение.

**4.** Защита информационной системы и машинных носителей персональных данных от несанкционированного доступа, повреждения или хищения:

**4.1.** В период эксплуатации информационных систем персональных данных должны быть предусмотрены меры по исключению случаев несанкционированного доступа при проведении ремонтных, профилактических и других видов работ.

**4.2.** В случае необходимости проведения ремонтных работ средств вычислительной техники, входящих в состав информационной системы, с привлечением специализированных ремонтных организаций обеспечивается обязательное гарантированное уничтожение (стирание) персональных данных и другой конфиденциальной информации, записанной на материальном носителе, под контролем лица, ответственного за организацию обработки персональных данных с составлением соответствующего акта.

**4.3.** Хранение съемных машинных носителей персональных данных должно исключать возможность несанкционированного доступа к ним.

Ознакомлены: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.И. Гурьева

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.С. Румянцева

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.В. Горшкова