

Порядок
доступа работников МБОУ ДО ЦРТ «Сокол» г.Липецка в помещения,
в которых ведется обработка персональных данных
(утвержден приказом МБОУ ДО ЦРТ «Сокол» г.Липецка от 18.08.2022 № 77)

1. Доступ работников МБОУ ДО ЦРТ «Сокол» г.Липецка (далее – Организация) в помещения, в которых ведется обработка персональных данных, осуществляется в целях обеспечения безопасности персональных данных.

2. Для помещений, в которых обрабатываются персональные данные (далее – Помещения), 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 Организации или лицом, 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 или сейфы и закрыть их;

– отключить технические 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 непосредственному руководителю;

– в присутствии лица, ответственного за организацию обработки персональных данных, и непосредственного руководителя, вскрыть Помещение и осмотреть его;

– составить акт о выявленных нарушениях и передать его директору Организации для проведения служебного расследования.

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

12. Работники Организации, должны ознакомиться с настоящим порядком доступа в помещения, в которых ведется обработка персональных данных, под подпись.

Правила организации режима обеспечения безопасности помещений, в которых 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 МБОУ ДО ЦРТ «Сокол» г.Липецка (далее – Организация), 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 Организации, 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 Организации 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.

5. Работники Организации должны ознакомиться с настоящими Правилами под подпись.

Лист ознакомлений
с порядком доступа сотрудников в помещения, в котором ведется обработка
персональных данных

№ п/п	Фамилия, имя, отчество	Дата ознакомления	Подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			

Лист ознакомлений
с правилами организации режима обеспечения безопасности помещений, в которых
размещена информационная система, препятствующего возможности
неконтролируемого проникновения или пребывания в это помещения лиц, не имеющих
права доступа в эти помещения

№ п/п	Фамилия, имя, отчество	Наименование подразделения, отдела	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				