

**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,**  
**в Муниципальном бюджетном образовательном учреждении**  
**дополнительного образования**  
**Центра развития творчества «Сокол» г.Липецка**  
(утверждена приказом МБОУ ДО ЦРТ «Сокол» г.Липецка от 18.08.2022 № 80)

1. Настоящие правила устанавливают требования к организации режима обеспечения безопасности помещений Муниципального бюджетного образовательного учреждения дополнительного образования Центра развития творчества «Сокол» г.Липецка (далее – ЦРТ), 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 ЦРТ, 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 руководителем ЦРТ 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 ЦРТ, должны ознакомиться с настоящими Правилами под роспись.