**УТВЕРЖДЕНА**

Приказ директора МОУ «Лицей ЭБ»

от "08" ноября 2018 года № 244

**ПОРЯДОК**

**ДОСТУПА В ПОМЕЩЕНИЯ МАОУ «ЛИЦЕЙ ЭБ»**

**С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**I. Общие положения**

**1.1.** Настоящий Порядок «доступа в помещения МАОУ «Лицей ЭБ» с информационной системой персональных данных» (далее Порядок) определяет условия обеспечения безопасности помещений МАОУ «Лицей ЭБ» (далее Лицей), в которых размещены компоненты информационных систем персональных данных, препятствующие возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

**1.2.** Для помещений, в которых обрабатываются персональные данные, должен обеспечиваться режим безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этом помещении посторонних лиц.

**1.3.** Настоящее Положение не определяет задачи пропускного и внутриобъектового режима.

**II. Размещение компонентов информационных систем**

**2.1.** Все компоненты информационных систем – автоматизированные рабочие места, серверы, сетевое оборудование – должны находиться в служебных помещениях (учебные и административные кабинеты) Лицея на максимально возможном отдалении от границ контролируемой зоны.

**2.2.** Силовые и телекоммуникационные кабели должны быть защищены от помех или повреждений с помощью размещения в защищенных боксах, изолированных каналах.

**2.3.** Мониторы и другие средства отображения информации должны располагаться таким образом, чтобы исключить несанкционированный просмотр третьими лицами.

**2.4.** Оконные проемы помещений, в которых находятся компоненты информационных систем, должны быть закрыты жалюзи.

**2.5.** Автоматизированные рабочие места, сетевое оборудование, серверы и специализированные шкафы для оборудования должны быть опечатаны.

**2.6.** Должно блокироваться несанкционированное подключение устройств и съемных носителей информации к компонентам информационных систем путем отключения или блокирования разъемов на серверном оборудовании и программного блокирования на автоматизированных рабочих местах.

**III. Организация доступа в помещения**

**3.1.** Право самостоятельного входа в помещения, в которых размещены компоненты информационных систем персональных данных, имеют работники, непосредственно работающие в этих помещениях и лицо, ответственное за организацию обработки персональных данных.

**3.2.** Иные лица допускаются в помещения по согласованию с руководителем Лицея или лицом, ответственным за организацию обработки персональных данных, и в сопровождении лиц, работающих в этих помещениях.

**3.3.** Работник, сопровождающий посетителей, должен постоянно контролировать действия посетителей.

**3.4.** Служебное помещение в отсутствие работника, имеющего к нему доступ, должно быть закрыто на механический замок.

**3.5.** Вскрытие и закрытие помещений производится лицами, имеющими право доступа.

**3.6.** Перед закрытием помещений по окончании рабочего дня, лица, имеющие право доступа в помещения, в которых размещены компоненты информационных систем персональных данных, 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.

**3.7.** 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.

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

- не вскрывая помещение, доложить непосредственному руководителю;

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

- составить акт о выявленных нарушениях и передать его руководителю Лицея для проведения служебного расследования.

**3.9.** Должна быть реализована процедура контроля и учета ключей от данных помещений:

- ключи и журнал учета ключей должны храниться на вахте Лицея;

- ключи должны выдаваться в соответствии со списками лиц, имеющих доступ в защищаемые помещения, и под личную подпись;

- должен фиксироваться работник, которому были выданы ключи, дата и время выдачи, а также отметки о сдаче ключей.

**3.10.** Уборка или иные работы в помещениях, в которых размещаются компоненты информационных систем, должны производиться в присутствии ответственного работника с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

**3.11.** Работники Лицея, должны ознакомиться с настоящим Порядком доступа в помещения, в которых ведется обработка персональных данных, под подпись.