

УТВЕРЖДАЮ

Директор РГБУ «СШ «Армспорт»

Алипов Р.З.

25 марта 2020 г.



ПОЛОЖЕНИЕ

о режиме обеспечения безопасности помещений, в которых размещена информационная система, препятствующем возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

1. Общие положения

- 1.1. Настоящий документ определяет порядок обеспечения безопасности помещений РГБУ «СШ «Армспорт» (далее – Учреждение), в которых размещены компоненты информационных систем персональных данных, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.
- 1.2. Настоящий документ не определяет задачи пропускного и внутриобъектового режима, поскольку пропускной и внутриобъектовый режим в Учреждении установлен соответствующим приказом директора Учреждения.
- 1.3. Пропускной и внутриобъектовый режим обеспечивает исключение несанкционированного прохода спортсменов, их законных представителей, работников и посетителей на территорию и в здания Учреждения, ввоза (вывоза), вноса (выноса) ими материальных ценностей.
- 1.4. Все работники, принимаемые в структурные подразделения Учреждения, знакомятся под подпись с настоящим положением.

2. Размещение компонентов информационных систем

- 2.1. Все компоненты информационных систем – автоматизированные рабочие места, серверы, сетевое оборудование – должны находиться в служебных помещениях 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.

3. Организация доступа в помещения

3.1. В отношении каждого служебного помещения Учреждения должен быть определен перечень лиц (должностей), имеющих к ним доступ.

3.2. Лица, не имеющие доступа к помещениям, не должны иметь возможности самостоятельного доступа без сопровождения в помещения, в которых размещаются компоненты информационных систем, а также носители информации.

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. Служебные помещения открываются и закрываются самими работниками.

Должна быть реализована процедура контроля и учета ключей:

- ключи и журнал учета ключей должны храниться на посту охраны;
- 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.

3.6. 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.