МЕСТНАЯ АДМИНИСТРАЦИЯ
ВНУТРИГОРОДСКОГО МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ГОРОДА СЕВАСТОПОЛЯ
ГАГАРИНСКИЙ МУНИЦИПАЛЬНЫЙ ОКРУГ

РАСПОРЯЖЕНИЕ

«10» октября 2018 г. № 187

Об утверждении положения об 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 местной администрации внутригородского муниципального образования города Севастополя Гагаринского муниципального округа в помещения, в которых ведется обработка персональных данных

В соответствии с федеральными законами от 06 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 09 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», Законом города Севастополя от 30 декабря 2014 г. № 102-ЗС «О местном самоуправлении в городе Севастополе», Уставом внутригородского муниципального образования города Севастополя Гагаринский муниципальный округ, принятым решением Совета Гагаринского муниципального округа от 01 апреля 2015 г. № 17 «О принятии Устава внутригородского муниципального образования города Севастополя Гагаринский муниципальный округ», постановлением местной администрации от 25 июля 2017 г. № 64-ПМА «Об утверждении Положения о персональных данных муниципальных служащих, лиц, замещающих муниципальные должности и лиц, замещающих должности, не отнесенные к должностям муниципальной службы местной администрации внутригородского муниципального образования города Севастополя Гагаринский муниципальный округ и граждан, претендующих на замещение должностей муниципальной службы»

1. Утвердить положение об 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 согласно приложению.

2. Контроль за исполнением распоряжения оставляю за собой.

Глава внутригородского муниципального образования,
исполняющий полномочия председателя Совета,
Глава местной администрации А. Ю. Ярусов

Приложение
к распоряжению местной
администрации
внутригородского округа
муниципального образования
города Севастополя
Гагаринский муниципальный
округ
от «___» _____ 2018 г. № _____

Положение об 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 местной администрации внутригородского муниципального образования города Севастополя Гагаринского муниципального округа

1. Общие положения

1.1. Настоящий документ определяет порядок обеспечения безопасности помещений в местной администрации внутригородского муниципального образования города Севастополя Гагаринский муниципальный округ (далее – местная администрация), 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 образовательной организации установлен соответствующим приказом директора образовательной организации.

1.3. Пропускной и внутриобъектовый режим обеспечивает исключение несанкционированного прохода обучающихся, законных представителей обучающихся, работников и посетителей на территорию и в здания образовательной организации, ввоза (вывоза), вноса (выноса) ими материальных ценностей.

1.4. Все работники, принимаемые в структурные подразделения образовательной организации, ознакамливаются под подпись с настоящим положением.

2. Размещение компонентов информационных систем

2.1. Все компоненты информационных систем – автоматизированные рабочие места, серверы, сетевое оборудование – должны находится 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 подключения 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 образовательной программы 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, сопровождающих 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 производится в присутствии ответственного работника с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

Глава внутригородского муниципального образования,
исполняющий полномочия председателя Совета,
Глава местной администрации А. Ю. Ярусов