

**МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 1»
АРСЕНЬЕВСКОГО ГОРОДСКОГО ОКРУГА**

П Р И К А З

05 мая 2025 года

г. Арсеньев

№ 67-а

О внесении изменений в приказ МОБУ «СОШ № 1» от 10.02.2023 № 21-а «Об утверждении Положения о защите персональных данных обучающихся Муниципального общеобразовательного бюджетного учреждения «Средняя общеобразовательная школа № 1» Арсеньевского городского округа»

Во исполнение представления прокуратуры г. Арсеньева от 11.04.2025 № Прдр-20050009-272-25/20050009, в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и в целях приведения Положения о защите персональных данных обучающихся Муниципального общеобразовательного бюджетного учреждения «Средняя общеобразовательная школа № 1» Арсеньевского городского округа», утвержденного приказом МОБУ «СОШ № 1» от 10.02.2023 № 21-а, в соответствии с законодательством Российской Федерации о защите персональных данных

ПРИКАЗЫВАЮ:

1. Внести в приказ МОБУ «СОШ № 1» от 10.02.2023 № 21-а «Об утверждении Положения о защите персональных данных обучающихся Муниципального общеобразовательного бюджетного учреждения «Средняя общеобразовательная школа № 1» Арсеньевского городского округа следующие изменения:

1.1. В раздел 7 «Передача персональных данных обучающегося» внести пункт 7.2. следующего содержания:

«7.2. Защита персональных данных.

7.2.1. Оператор при обработке персональных данных обязано принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования,

копирования, распространения персональных данных, а также от иных неправомерных действий.

7.2.2. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, используемых в процессе деятельности Учреждения.

7.2.3. Основными организационными мерами по защите персональных данных оператора являются:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое, избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- обеспечение знания работником требований нормативно-методических документов по защите информации и сохранении тайны;
- обеспечение наличия необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- грамотная организация процесса уничтожения информации;
- организация регулярной воспитательной и разъяснительной работы с работниками оператора по предупреждению утраты и утечки сведений при работе с конфиденциальными документами, содержащими персональные данные;
- разработка комплекта внутренних документов оператора, регламентирующих процессы обработки персональных данных.

7.2.4. В качестве дополнительных организационных мер защиты персональных данных оператором создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ к персональным данным с целью овладения ценными сведениями и их использования, а также их искажения, уничтожения, подмены, фальсификации содержания реквизитов документа и т.д.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности оператора: клиенты, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов, содержащих персональные данные.

Для защиты персональных данных от несанкционированного доступа оператором необходимо обеспечить:

- охрану в дневное время в помещении оператора (в контролируемую зону),
- постоянную работоспособность пожарной и охранной сигнализации.

7.2.5. В качестве технических мер защиты персональных данных оператором должны применяться:

- антивирусная защита;
- межсетевые экраны;
- разграничение прав доступа (пароли);
- специализированные средства защиты информации от несанкционированного доступа.

7.2.6. После установки (обновления) программного обеспечения, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам ПЭВМ и проверить работоспособность программного обеспечения и правильность его настройки.

7.2.7. Администратор безопасности должен проводить периодическое тестирование технических и программных средств защиты.

7.2.8. В целях организации контроля за обеспечением безопасности персональных данных в Учреждении приказом создается постоянно действующая Комиссия по обеспечению безопасности персональных данных (далее Комиссия).

7.2.9. Комиссия является совещательным органом при руководителе Учреждения.

Основными задачами Комиссии являются:

- Организация и проведение экспертизы ценности документов на стадии делопроизводства при составлении номенклатуры дел и формировании дел.
- Организация и проведение экспертизы ценности документов на стадии подготовки их к архивному хранению.
- Организация и проведение отбора и подготовки документов к передаче на государственное хранение, в том числе научно-технической, аудиовизуальной и другой специальной документации.
- Организация и приведение документооборота оператора в соответствии с актуальными требованиями законодательства о персональных данных.».

2. Контроль исполнения настоящего приказа оставляю за собой.

Директор МОБУ «СОШ № 1»



М.В. Захарьяшева