Приложение №3 к приказу
МАОУ СОШ №9
от 05.04.2023 №41-О

Правила
доступа к персональным данным, обрабатываемым в информационных системах, используемых в МАОУ СОШ №9

1. Общие положения

1.1. Настоящие Правила определяют порядок доступа к персональным данным, обрабатываемым в информационных системах МАОУ СОШ №9 (далее – информационные системы), действия пользователей информационных систем в части обеспечения безопасности персональных данных при их обработке в информационных системах.

1.2. Настоящие правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.4. Перечень персональных данных, обрабатываемых в информационных системах, а также перечень информационных систем утверждаются приказом руководителя МАОУ СОШ №9 (далее – Учреждение).

1.5. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

2. Организация доступа к персональным данным
в информационных системах

2.1. Допуск для работы за автоматизированным рабочим местом (далее - АРМ) в информационной системе предоставляется лицам, включенным в перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей, утвержденный приказом руководителя Учреждения (далее – пользователь информационной системы).

2.2. Право доступа к персональным данным в информационных системах имеют должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, которым доступ к такой информации предусмотрен Федеральными законами.

2.3. Право доступа к персональным данным имеют должностные лица оператора информационных систем, которым доступ к такой информации предусмотрен законодательством и (или) локальными актами оператора информационных систем.

2.4. Доступ к персональным данным субъектов персональных данных осуществляется на основании направленного оператору информационных систем запроса.

2.5. Порядок учета (регистрации), рассмотрения запросов осуществляется в соответствии с утвержденными оператором информационных систем Правилами рассмотрения запросов субъектов персональных данных или их представителей.

2.6. Пользователь информационной системы имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам информационной системе. При этом для хранения информации, содержащей персональные данные, разрешается использовать только учтенные машинные носители информации.

2.7. Пользователь информационной системы несет ответственность за правильность включения и выключения АРМ, входа в информационную систему и все действия при работе в информационной системе.

2.8. Вход пользователя информационной системы в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.9. Запись информации, содержащей персональные данные, может осуществляться пользователем информационной системы на учтенные съемные машинные носители информации.

2.10. Использование неучтенных машинных носителей информации для обработки, хранения, транспортировки персональных данных запрещается.

Использование машинных носителей информации допускается исключительно для выполнения своих служебных обязанностей.

Передача машинных носителей информации третьим лицам или использование их в личных целях запрещается.

2.11. При работе с машинными носителями информации пользователь информационной системы каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь информационной системы обязан немедленно прекратить их использование и действовать в соответствии с требованиями, установленными в Учреждении, Порядком организации антивирусной защиты в информационных системах.

2.12. В случае утраты или уничтожения машинных носителей информации либо разглашении содержащихся в них сведений, об этом немедленно ставится в известность администратор информационной безопасности. По факту утраты машинного носителя информации составляется акт. Соответствующие отметки вносятся в журнал учета машинных носителей информации.

2.13. Машинные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей информации осуществляется уполномоченной комиссией, состав которой утверждается приказом руководителя Учреждения. По результатам уничтожения машинных носителей информации составляется акт об уничтожении.

3. Обязанности пользователей информационных систем

3.1. Сотрудник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в информационных системах и имеющий доступ к АРМ, программному обеспечению и данным информационной системы, обязан:

1) строго соблюдать установленные правила обеспечения безопасности информации в информационных системах;

2) знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

3) хранить в тайне свой пароль (пароли). Выполнять установленный в Учреждении порядок организации парольной защиты в информационных системах;

4) хранить свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

5) выполнять установленный в Учреждении порядок организации антивирусной защиты в ИС;

6) немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (токена, смарт-карты, ключа авторизации) или при подозрении компрометации паролей, а также при обнаружении:

нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих компонентах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к АРМ;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ информационной системы;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

некорректного функционирования установленных на АРМ технических средств защиты;

непредусмотренных отводов кабелей и подключенных устройств.

3.2. Пользователю АРМ категорически запрещается:

1) использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

2) самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств информационной системы или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

3) осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

4) записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флеш-накопителях и т.п.);

5) оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

6) оставлять без личного присмотра на рабочем месте или в ином месте свое персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные;

7) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

8) размещать средства информационной системы так, чтобы с них существовала возможность визуального считывания информации.

3.3. Лица, виновные в нарушении требований настоящих Правил и иных документов, регламентирующих вопросы защиты персональных данных, несут ответственность в соответствии с действующим законодательством Российской Федерации.