Приложение 16
к приказу МБДОУ «Детство» «ЦРР» г. Калуги
от 30.08.2022г. № 398-од

Руководство
пользователя информационной системы персональных данных
МБДОУ «Детство» «ЦРР» г. Калуги

1. Общие положения

Пользователь информационной системы персональных данных МБДОУ «Детство» «ЦРР» г. Калуги (далее - ИСПДн, пользователь) при выполнении работ в пределах своих функциональных обязанностей обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ИСПДн, и несет персональную ответственность за соблюдение требований настоящего Руководства.

2. При осуществлении обработки персональных данных пользователь обязан:

- не допускать обработку персональных данных в присутствии лиц, не допущенных к обрабатываемой информации, располагать экран видеомонитора во время работы так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами;
- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при их обработке;
- оповещать должностное лицо, ответственное за обеспечение безопасности персональных данных в информационных системах, администратора ИСПДн обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в персональной электронно-вычислительной машине (далее - ПЭВМ);
- помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;
- при применении съемных машинных носителей информации перед началом работы, в случае если локальная сеть не обеспечена средствами технической защиты, исключающими утечку персональных данных, отключить ПЭВМ от локальной сети, провести их проверку на предмет наличия компьютерных вирусов;
- по окончании работы съемные машинные носители информации хранить в местах, исключающих посторонний доступ к ним (столы, шкафы, сейфы и другие предметы, запираемые на ключ);
- использовать машинные носители данных исключительно для выполнения своих служебных обязанностей;
- извещать должностное лицо (работника), ответственное за обеспечение безопасности персональных данных в информационных системах, о фактах утраты (кражи) машинных носителей данных;
- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции и немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за организацию обработки персональных данных;
- блокировать доступ к ПЭВМ при отсутствии за ним визуального контроля.

3. При осуществлении обработки персональных данных пользователю запрещается:

- записывать и хранить персональные данные на не учтенных установленным порядком машинных носителях данных;

- подключать к ПЭВМ не учтенные в установленном порядке машинные носители данных, личные внешние носители и мобильные устройства;

- использовать машинные носители данных в личных целях;

- передавать машинные носители данных другим лицам, за исключением должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационных системах;

- оставлять машинные носители с персональными данными на рабочих столах, оставлять их без присмотра или передавать на хранение другим лицам, не имеющим доступа к ИСПДн;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на ПЭВМ, не входящих в состав информационной системы персональных данных МБДОУ «Детство» «ЦРР» г. Калуги;

- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

- самостоятельно устанавливать и (или) запускать (выполнять) на ПЭВМ любые системные или прикладные программы, в том числе загружаемые в автоматическом режиме по сети Интернет;

- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

- сообщать кому-либо устно или письменно личные информацию о доступе к ресурсам ПЭВМ;

- записывать и хранить пароли либо персональные идентификаторы в доступном месте, а также пересылать пароли открытым текстом в электронных сообщениях;

- отключать (блокировать) средства защиты информации;

- производить иные действия, на исполнение которых предусмотрены ограничения, утвержденные регламентами и инструкциями;

- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.