Утверждаю
директор МОКУ «С(К)Ш
_____ Книга Е.И
Приказ №17
«01» сентября 2016

Инструкция
по работе пользователей в информационной системе персональных данных
МОКУ С(К)Ш, защищенной от несанкционированного доступа

Настоящая инструкция определяет общие положения работы пользователей в защищенной от несанкционированного доступа ИСПДн при обработке (наборе,редактировании и печати) персональных данных.

1.Допуск пользователей для работы в ИСПДн осуществляется в соответствии со списком лиц допущенных к работе в ИСПДн.

2.Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера, присвоенными данному пользователю. При этом для хранения файлов, содержащих персональные данные, разрешается использовать только специально выделенные каталоги на жестком магнитном диске, а также соответствующим образом учтенные съемные носители.

3. Пользователь отвечает за правильность включения и выключения ПЭВМ, входа в систему и все действия при работе на ПЭВМ.

4. Вход пользователя в систему осуществляется на основе ввода (по запросу системы) имени, присвоенного при первичной регистрации и ввода персонального пароля, длинной не менее 8 символов ,определяемого конкретным пользователем.

5. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в 3 месяца) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем самостоятельно под контролем администратора.

6.Печать какой- либо обрабатываемой информации осуществляется пользователем только на соответствующим образом оформленных листах (бланках школы) и регистрируются в книге учета документов у секретаря.

7.Резервное копирование, уничтожение и восстановление информации осуществляются пользователем в рамках выделенных полномочий. Пользователь осуществляет резервное копирование информации в процессе, либо по окончании работы на соответствующим образом учтенные съемные носители информации (СНИ).

8. При работе с СНИ пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием штатных антивирусных программ, установленных на ПЭВМ, в соответствии с «Инструкцией по проведению антивирусного контроля ». В случае обнаружения вирусов на СНИ пользователь обязан немедленно сообщить об этом специально назначенному лицу.

9. По окончании работы пользователь обязан провести уничтожение остаточной информации на ЖМД.

10. В процессе работы пользователю запрещается:

- использовать для постоянного хранения и обработки персональных данных каталоги ЖМД, за исключением каталогов, выделенных специально назначенным лицом;
- осуществлять попытки несанкционированного доступа к ресурсам системы и других пользователей;
- покидать помещение с включенной ПЭВМ без блокировки до окончания работы.