

УТВЕРЖДАЮ

Директор МБОУ гимназии №23

МЕНТОВ О.Ф. Позднякова

« 13 » сентября 2011 г.

Инструкция пользователя при обработке персональных данных на объектах вычислительной техники

1. Общие положения

1.1. Данная Инструкция определяет основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) школы

1.2. Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации).

2. Основные обязанности пользователя

2.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции.

2.2. При работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами.

2.3. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке.

2.4. Оповещать инженера, а также директора обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ.

2.6. Не допускать "загрязнение" ПЭВМ посторонними программными средствами.

2.7. Знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий.

2.8. Знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

2.9. Помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе.

2.10. Знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов.

2.11. При применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

3. Требования к антивирусной безопасности

3.1. 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.

3.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;

- оценить необходимость дальнейшего использования файлов, зараженных вирусом;

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

4. Пользователю запрещается

4.1. Записывать и хранить персональные данные на неуценных установленном порядке машинных носителях информации.

4.2. Удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности.

4.3. Самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ.

4.4. Самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей.

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

4.6. сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ.

4.7. отключать (блокировать) средства защиты информации.

4.8. Производить какие-либо изменения в подключении и размещении технических средств.

4.9. Производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

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

5. Права пользователя ПЭВМ

5.1. Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

5.2. Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

6. Пользователи ПЭВМ несут ответственность за

6.1. Ненадлежащее выполнение требований настоящей инструкции.

6.2. Соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов.

6.3. Сохранность и работоспособное состояние средств вычислительной техники ПЭВМ.

6.4. Сохранность персональных данных.