УТВЕРЖДАЮ
Директор МОУ
«СОШ №57»
Г.Н.Жербанова
01 сентября 2013

Инструкция пользователей
и технология обработки информации, содержащей персональные данные, на объекте вычислительной техники

1. Объекты вычислительной техники (ОВТ) разрешается использовать для обработки персональных данных при соблюдении следующих условий:

1.1. Право работы на ОВТ предоставляется сотрудникам школы: заместителю директора по УВР, заместителю директора по ВР, секретарю школы, преподавателю информатики, классным руководителям

1.2. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ОВТ, несет персональную ответственность за свои действия.

2. Обязанности пользователя ОВТ.

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 обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

2.5. Не допускать "загрязнение" ПЭВМ посторонними программными средствами;

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

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

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

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

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

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.

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).

2.11. Пользователям ОВТ запрещается:

- записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;
- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- 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, загружаемые по сети Интернет или с внешних носителей;
- 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 атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.
- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

3. Организация парольной защиты при работе на объектах информатизации.

3.1 Личные пароли доступа к объекту информатизации, системе защиты от НСД, выдаются пользователям Администратором информационной безопасности, и при этом необходимо руководствоваться следующими требованиями:

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- не использовать ранее использованные пароли.

3.2. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

- своевременно сообщать о всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

3.3. При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;

- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

3.4. Удаление личного пароля любого пользователя ОВТ должна производиться в следующих случаях:

- в случае подозрения на дискредитацию пароля;
- в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) пользователя после окончания последнего сеанса работы с системой;
- по указанию администратора.

4. Технология обработки персональных данных.

4.1. При первичном допуске к работе на ОВТ Пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает инструкцию пользователя и получает личный текущий пароль у Администратора.

4.2. В процессе работы пользователь производит обработку персональных данных на ОВТ с применением программного обеспечения Microsoft Office, 1 С бухгалтерия.

4.3. При необходимости вывод персональных данных осуществляется следующим образом:

- копированием персональных данных на учтенные носители;
- печать на принтере
- передача персональных данных по защищенным каналам связи.