

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА С УГЛУБЛЕННЫМ  
ИЗУЧЕНИЕМ ОТДЕЛЬНЫХ ПРЕДМЕТОВ №32» города Кирова**

УТВЕРЖДАЮ:  
Директор

\_\_\_\_\_  
С.Ю.Старостина

**Инструкция  
пользователя при автоматизированной обработке персональных  
данных**

**1. Общие положения**

**1.1.** Данная Инструкция определяет основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации школы

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

**1.3.** Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в образовательном учреждении, 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 расположено автоматизированное рабочее место учителя (далее АРМ), 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.** после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации;

**2.5.** оповещать заместителя директора, курирующего вопросы защиты персональных данных обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой оператором;

**2.6.** не допускать "загрязнение" ПК 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;

**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 .

**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 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 неучтенных установленным порядком носителях информации;

**4.2.** удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

**4.3.** самостоятельно подключать к ПК какие-либо устройства и вносить изменения в состав, конфигурацию, размещение АРМ;

**4.4.** самостоятельно устанавливать и/или запускать (выполнять) на ПК 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 ПК;

**4.6.** сообщать кому-либо устно или письменно личные атрибуты доступа к базам данных;

**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 ПК с загруженными персональными данными, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

### **5. Права пользователя:**

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

**5.2.** Обращаться к информационному совету школы с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, а также со средствами защиты информации.

### **6. Пользователи несут ответственность за:**

**6.1.** надлежащее 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 технических средств;

**6.4.** сохранность персональных данных.