

МУНИЦИПАЛЬНОЕ  
БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 35 ГОРОДСКОГО ОКРУГА  
САМАРА



«Утверждаю»  
Директор МБОУ СОШ № 35  
г.о. Самара  
Н.С.Мушкат  
« 1 » сентября 2014 г.

**ИНСТРУКЦИЯ**

пользователя информационной системы персональных данных в МБОУ СОШ № 35

Самара, 2014

## **1. Общие положения**

Настоящая Инструкция разработана для обеспечения защиты персональных данных в МБОУ СОШ № 35

Персональные данные (ПДн) относятся к категории информации ограниченного распространения.

Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с персональными данными строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;
- принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

## **2. Обязанности работников, имеющих доступ к ПДн.**

Работники, получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных данных немедленно информировать руководителя структурного подразделения, специалиста по защите информации.

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Правительства области, полученные в течение срока работы.

Работники при работе с персональными данными обязаны:

Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

Выполнять требования администратора безопасности, касающиеся защиты информации;

Знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

Хранить в тайне свой аудентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;

Использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и т.д.);

Контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности, ответственному за антивирусную защиту автоматизированной системы;

Немедленно ставить в известность руководителя подразделения, специалиста по отделу по защите информации:

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;

- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИСПДн;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн.

В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

Ставить в известность администратора безопасности структурного подразделения при:

- необходимости обновления антивирусных баз;
- обновлении программного обеспечения;
- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;

- необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;

- резервном копировании информации;

- и т.д.

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Вынос ПЭВМ, на которой проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с руководителем подразделения запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

ПЭВМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

**Запрещается:**

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения ограниченного распространения;
- использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;
- накапливать ненужные для работы персональные данные;
- передавать или принимать без расписки документы ограниченного распространения;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера.
- использовать компоненты программного и аппаратного обеспечения ИСПДн подразделения в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить персональные данные на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения, ответственного за техническое и (или) программное обеспечение, администратора безопасности.

### **3. Ответственность**

Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

**С инструкцией ознакомлены:**

Зам. директора по УВР

Зам. директора по ВР

Т.В. Казурова

О.В. Буянова

Зам директора по начальной школе

Зам. директора по НМР и безопасности

Зам. директора по питанию

Зам. директора по дошкольному отделению

Зам. директора по АХЧ

Главный бухгалтер

Секретарь школы

Системный администратор

С.К. Бординова

Т.С. Милоенко

Н.Е. Титова

Е.В. Тринбачёва

Е.Г. Кузнецова

С.В. Ситникова

Н.Ю. Водовских

А. Ю.Ситников