

УТВЕРЖДЕНА
приказом ГПОУ «УМК»
от 28.09.2016 № 62/а

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных

Оглавление

1. Общие положения.....	3
1.1. Назначение документа	3
1.2. Область действия документа	3
1.3. Вступление в силу документа	3
1.4. Методическое руководство.....	3
1.5. Конфиденциальность	4
2. Работа в ИСПДн.....	4
2.1. Обязанности пользователей ИСПДн	4
2.2. Правила работы в ИСПДн	5
2.3. Ограничение прав пользователей ИСПДн	6
2.4. Информирование руководства	7
3. Обработка ПДн	7
4. Ответственность.....	8

1. Общие положения

1.1. Назначение документа

1.1.1. Инструкция пользователя информационных систем персональных данных определяет права, обязанности и ответственность лиц, допущенных к автоматизированной обработке персональных данных (ПДн) в информационных системах персональных данных (ИСПДн) ГПОУ «УМК» (далее – Учреждение).

1.1.2. Целью настоящей инструкции является определение обязательных требований к лицам, допущенным к автоматизированной обработке ПДн в ИСПДн Учреждения (далее – пользователи ИСПДн), их обязанности и ответственность.

1.2. Область действия документа

1.2.1. Положения настоящей инструкции распространяются на всех пользователей ИСПДн.

1.2.2. Допуск лиц к работе в ИСПДн предоставляется на основании приказа директора Учреждения.

1.2.3. Права доступа пользователей ИСПДн в ИСПДн определяются Перечнями прав доступа к ресурсам ИСПДн.

1.2.4. Все пользователи ИСПДн должны быть ознакомлены с положениями настоящей инструкции под личную подпись.

1.3. Вступление в силу документа

1.3.1. Настоящая инструкция вступает в силу с момента ее утверждения директором Учреждения.

1.3.2. Изменения в настоящую инструкцию вносятся приказом директора Учреждения.

1.4. Методическое руководство

1.4.1. Методическое руководство работой пользователей ИСПДн в вопросах использования программного обеспечения (ПО) и технических средств (ТС) ИСПДн осуществляется администратором ИСПДн.

1.4.2. Методическое руководство работой пользователей ИСПДн в вопросах обработки и защиты ПДн осуществляется постоянно действующей комиссией по защите ПДн (далее – Комиссия).

1.4.3. О всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а также для получения консультаций по вопросам защиты ПДн необходимо обращаться к председателю Комиссии по рабочему телефону или электронной почте.

1.4.4. Для получения консультаций по вопросам использования и настройки элементов ИСПДн необходимо обращаться к администратору ИСПДн по рабочему телефону или электронной почте.

1.5. Конфиденциальность

1.5.1. Пользователи ИСПДн обязаны хранить в тайне ПДн, ставшие им известными в ходе выполнения своих должностных обязанностей или иным путем, и пресекать действия других лиц, которые могут привести к разглашению таких сведений. О таких фактах, а также о других причинах или условиях возможной утечки ПДн пользователи ИСПДн обязаны немедленно информировать руководителя структурного подразделения и председателя Комиссии.

1.5.2. ПДн не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению ПДн.

1.5.3. В случае оставления занимаемой должности работник обязан вернуть все документы, материалы и их носители, относящиеся к деятельности Учреждения, в том числе: отчеты, инструкции, переписку, списки, протоколы, компьютерные программы, машинные носители информации (МНИ), а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Учреждения, полученные в период работы.

1.5.4. Обязательство о неразглашении ПДн действительно в период трудовых (гражданско-правовых или иных не запрещенных законодательством РФ) отношений между работником и Учреждением, и в течение трех лет, после их окончания.

2. Работа в ИСПДн

2.1. Обязанности пользователей ИСПДн

2.1.1. Пользователь ИСПДн отвечает за правильность:

- включения и выключения своего автоматизированного рабочего места (АРМ);
- получения доступа в операционную среду ИСПДн методом ввода имени пользователя (логина) и пароля в окне входа операционной системы (ОС);
- выполнения всех действий, осуществляемых в операционной среде и с элементами ИСПДн (ТС, МНИ и др.).

2.1.2. Пользователь ИСПДн обязан:

- знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, Положения об обработке и защите ПДн и прочих локальных нормативных актов Учреждения, регламентирующих порядок обработки и защиты ПДн;
- перед началом работы с ИСПДн, убедиться в наличии всех необходимых ТС, а также в целостности печати системного блока своего АРМ;
- выполнять на АРМ только те процедуры, которые необходимы для исполнения своих должностных обязанностей;
- знать и соблюдать установленные требования по режиму обработки ПДн, учету, хранению и пересылке МНИ, обеспечению безопасности ПДн, а также

- руководящих и организационно-распорядительных документов, в том числе инструкций;
- соблюдать требования Положения о порядке доступа в выделенные помещения;
 - соблюдать требования Регламента по организации парольной защиты в ИСПДн;
 - соблюдать требования Инструкции по организации антивирусной защиты в ИСПДн;
 - соблюдать требования Инструкции по информационной безопасности в сфере информационного обмена;
 - соблюдать правила работы с МНИ;
 - соблюдать требования Инструкции о порядке обеспечения безопасности ПДн в случае нештатных ситуаций;
 - соблюдать требования Инструкции о порядке предоставления ПДн;
 - соблюдать требования Регламента реагирования на обращения (запросы) субъектов ПДн;
 - выполнять требования Комиссии и администратора ИСПДн, касающиеся защиты и (или) обработки ПДн.

2.2. Правила работы в ИСПДн

2.2.1. Шторы (жалюзи) на оконных проемах во время работы должны быть завешены (закрыты).

2.2.2. Двери во время работы должны быть закрыты, при необходимости – на замок.

2.2.3. Мониторы АРМ должны быть расположены таким образом, чтобы исключалась (либо максимально снижалась) возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами (посетителями или работниками Учреждения, не имеющими соответствующего допуска к ПДн) напрямую, а также через оконные проемы или открытые двери.

2.2.4. На столе должны находиться только документы и материалы, необходимые для выполнения текущих задач (принцип «чистого стола»). Прочие документы и материалы должны быть убраны со стола в места, предусмотренные для их хранения.

2.2.5. Напечатанные документы должны изыматься из принтера (МФУ) сразу после печати.

2.2.6. При отсутствии визуального контроля над АРМ, пользователи ИСПДн обязаны активировать средства защиты от несанкционированного доступа (НСД) нажатием сочетания клавиш <Win>+<L> (или <Ctrl>+<Alt>+ и выбором пункта «Блокировать»).

2.2.7. Не допускается единоличное присутствие в выделенных для обработки ПДн помещениях (выделенных помещениях) лиц, не имеющих права самостоятельного доступа в такие помещения в соответствии со Списками лиц, имеющих право самостоятельного доступа в выделенные помещения.

2.2.8. Вынос АРМ, на котором осуществлялась обработка ПДн, за пределы контролируемой зоны с целью его ремонта, замены и т.п. без согласования с руководителем структурного подразделения запрещен. При принятии решения о выносе АРМ, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет МНИ. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.2.9. По завершению рабочего дня все АРМ ИСПДн, а также иные ТС ИСПДн, должны быть выключены и обесточены.

2.3. Ограничение прав пользователей ИСПДн

2.3.1. Пользователю ИСПДн запрещается:

- допускать кого-либо к работе в ИСПДн под своей учетной записью;
- копировать документы, содержащие ПДн, или делать из них выписки без разрешения руководителя структурного подразделения;
- выносить документы, содержащие ПДн, за пределы выделенных помещений;
- подключать к АРМ ИСПДн личные, неучтенные МНИ и устройства (flash-накопители, телефоны, модемы и др.);
- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие ПДн, а также оставлять незапертыми их хранилища и выделенные помещения;
- оставлять МНИ в доступных местах без присмотра или передавать их на хранение другим работникам (без регистрации этого факта в Журнале учета выдачи и возврата МНИ);
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данным сведениям) лиц;
- передавать или принимать без расписки документы, содержащие ПДн, или предусматривающие их содержание;
- самостоятельно устанавливать, тиражировать, или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, а также вскрывать системные блоки АРМ;
- изменять схему электропитания ТС ИСПДн (например, отключать источник бесперебойного питания без разрешения администратора ИСПДн, если иное не предусмотрено порядком действий в чрезвычайных ситуациях);
- самостоятельно предоставлять общий доступ к папкам или файлам своих АРМ без разрешения Комиссии.
- отключать (блокировать) средства защиты информации (СЗИ);
- обрабатывать ПДн при обнаружении неисправностей в программном или аппаратном обеспечении АРМ или в СЗИ, или при отклонении функционирования АРМ от нормы;
- самостоятельно проводить ремонт ТС ИСПДн или привлекать посторонних лиц для ремонта или настройки АРМ, без предварительного согласования с Комиссией;

- умышленно использовать недокументированные (недекларированные) свойства и ошибки в ПО или в настройках СЗИ, которые могут привести к возникновению нештатной ситуации;
- использовать в выделенных помещениях устройства фото- и видеосъемки.

2.4. Информирование руководства

2.4.1. Пользователи ИСПДн обязаны немедленно ставить в известность руководителя структурного подразделения и Комиссию в случае:

- утери носителя с ПДн;
- подозрения компрометации личных ключей или паролей;
- несанкционированного (произведенного с нарушением установленного порядка) изменения конфигурации программных или аппаратных средств ИСПДн;
- нарушения целостности пломб (наклеек), нарушения или несоответствия номеров печатей на составляющих узлах и блоках АРМ;
- некорректного функционирования СЗИ, установленных на АРМ;
- обнаружения непредусмотренных отводов кабелей или подключенных устройств;
- изменения настроек или параметров СЗИ.

2.4.2. Пользователи ИСПДн должны ставить в известность администратора ИСПДн в случае необходимости:

- обновления антивирусных баз;
- обновления ПО;
- проведения регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;
- вскрытия системных блоков АРМ ИСПДн.

3. Обработка ПДн

3.1. Запрещается разглашать ПДн третьим лицам (в том числе работникам Учреждения, не имеющим соответствующего допуска).

3.2. Запрещается преднамеренно вносить некорректные сведения о субъектах ПДн, а также некорректные изменения в ПДн субъектов ПДн, либо осуществлять несанкционированное удаление ПДн субъектов ПДн.

3.3. Пользователь ИСПДн обязан осуществлять проверку корректности при вводе, изменении или удалении ПДн.

3.4. После распечатки документов, содержащих ПДн субъектов ПДн, необходимо сверить распечатанную информацию со сведениями, содержащимися в первоисточнике ПДн субъекта ПДн (оригинале или копии документа, предоставленного субъектом ПДн), особенно в случаях, если указанные ПДн долго не обновлялись и к ним не осуществлялся доступ.

3.5. Запрещается принимать решения, которые могут иметь последствия для субъектов ПДн на основании ПДн, полученных в результате исключительно автоматизированной обработки.

3.6. Запрещается использовать ПДн субъектов ПДн при подготовке открытых публикаций, докладов, научных работ и т.д., без предварительного получения согласия субъекта ПДн.

4. Ответственность

4.1. Пользователи ИСПДн несут персональную (гражданскую, уголовную, административную, дисциплинарную) ответственность за качество и своевременность выполнения обязанностей и функций, возложенных на них в соответствии с настоящей Инструкцией, а также другими нормативными и регламентирующими документами в области защиты информации.

4.2. За разглашение информации ограниченного распространения (ПДн), а также за нарушение порядка работы с документами или МНИ, содержащими такую информацию, пользователь ИСПДн может быть привлечен к дисциплинарной, гражданско-правовой, уголовной или иной, предусмотренной законодательством РФ ответственности.