

**Правила работы лиц,
доступ которых к персональным данным,
в том числе обрабатываемым в информационных системах
персональных данных,
необходим для выполнения ими должностных обязанностей**

Допуск для работы на автоматизированных рабочих местах (далее – АРМ) состоящих в составе информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных обязанностей (далее – Пользователи ИСПДн).

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее – ПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

Каждый работник, участвующий в рамках своих должностных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

1. Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн.
2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ.
3. Хранить в тайне свой пароль (пароли), выполнять требования инструкции по организации парольной защиты в полном объеме.

4. Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу).

5. Выполнять требования инструкции по организации антивирусной защиты в полном объеме.

6. Немедленно известить ответственного за обеспечение безопасности персональных данных в информационной системе в ГБПОУ КК «КМТ» в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении: несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ; отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения; некорректного функционирования установленных на АРМ технических средств защиты; непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

1. Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

3. Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);

4. Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

5. Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

6. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;

7. Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

Юрисконсульт
Техник по обслуживанию
вычислительной техники

Ведущий специалист по кадрам

О.П.Галюк

А.А. Попов

Т.В. Миллер