

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР БУХГАЛТЕРСКОГО
ОБЕСПЕЧЕНИЯ МУНИЦИПАЛЬНЫХ УЧРЕЖДЕНИЙ ГОРОДА
ПЯТИГОРСКА»

ПРИКАЗ

г.Пятигорск

29 декабря 2017 года

№ 38

Об утверждении инструкции о порядке работы пользователей
информационных систем персональных данных в части обеспечения ПД

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», -

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Инструкцию о порядке работы пользователей информационных систем персональных данных в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных МКУ «ЦБО» согласно приложению.

2. Шельдешовой А.П., ведущему бухгалтеру довести настоящий приказ до сведения сотрудников МКУ «ЦБО».

3. Контроль исполнения приказа оставляю за собой.

Начальник



Н.С.Даниелян

Инструкция
о порядке работы пользователей информационных систем персональных
данных в части обеспечения безопасности персональных данных
при их обработке в информационных системах персональных данных
МКУ «ЦБО» (далее – инструкция)

1. Настоящая инструкция определяет порядок действий пользователей информационных систем персональных данных (далее – ИСПДн) в части обеспечения безопасности персональных данных при их обработке в ИСПДн.

2. Допуск пользователей для работы за автоматизированным рабочим местом (далее – АРМ) осуществляется на основании утверждаемого «Списка сотрудников, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения служебных обязанностей» МКУ «ЦБО».

3. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в «Журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения, транспортировки информации».

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

5. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

6. Запись информации, содержащей персональные данные, может, осуществляться пользователем ИСПДн на съемные машинные носители информации, соответствующим образом учтенные в «Журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения, транспортировки информации».

7. 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.

8. Каждый сотрудник, участвующий в рамках своих служебных 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:

8.1. строго соблюдать установленные соответствующими Инструкциями правила обеспечения безопасности информации ИСПДн;

8.2.знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

8.3.хранить в тайне свой пароль (пароли). Выполнять требования Инструкции по организации парольной защиты в полном объеме;

8.4.хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

8.5.выполнять требования Инструкции по организации антивирусной защиты в полном объеме;

8.6.немедленно известить администратора безопасности информации в ИСПДн в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

8.6.1.нарушений целостности пломб (наклеек, нарушений или несоответствии номеров печатей) на составляющих компонентах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к АРМ;

8.6.2.несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ ИСПДн; 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;

8.6.3.некорректного функционирования установленных на АРМ технических средств защиты; непредусмотренных отводов кабелей и подключенных устройств.

9.Пользователю АРМ категорически запрещается: использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

9.1.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;

9.2.осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

9.3.записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флеш-накопителях и т.п.); оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

9.4.оставлять без личного присмотра на рабочем месте или в ином месте свое персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные;

9.5.умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

9.6. размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.-