Приложение 14
к распоряжению Администрации
Кыштымского городского округа
от «24» 10 2018г. № 98р

Инструкция
пользователя информационных систем персональных данных Администрации Кыштымского городского округа

1. Общие положения

1. Настоящая Инструкция пользователя информационных систем персональных данных Администрации Кыштымского городского округа разработана в соответствии с нормативными документами по безопасности информации и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) Администрации Кыштымского городского округа (далее – Администрации).

2. Субъектами доступа к ресурсам ИСПДн являются администратор безопасности (далее – АБ), пользователи и обслуживающий персонал.

3. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

4. Машинные носители информации имеют пометку «ПДн».

5. Пользователи получают свои права на доступ к ресурсам ИСПДн через АБ.

6. Пользователи имеют право письменно вносить предложения по изменению и дополнению данной Инструкции.

7. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

2. Обязанности пользователя

8. Пользователь обязан:

знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации;

выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены технологическим процессом обработки ПДн;

знать и соблюдать установленные требования к обработке ПДн, учету и хранению носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов;

соблюдать требования парольной политики в соответствии с «Инструкцией по организации парольной защиты»;

получить уникальное имя и персональный идентификатор (при его наличии) от АБ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания;

во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Жалюзи на окнах должны быть

закрыты;

при возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ ИСПДн провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения;

9. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения Пользователь обязан:

приостановить обработку данных;

немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБ ИСПДн, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБ ИСПДн).

10. Пользователь обязан немедленно вызывать АБ ИСПДн и поставить в известность руководителя структурного подразделения Администрации при обнаружении:

нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

некорректного функционирования установленных на АРМ технических средств защиты;

непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

11. При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБ.

12. Обо всех выявленных нарушениях, связанных с информационной безопасностью Администрации, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ.

13. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

14. В ИСПДн осуществляется блокирование сеанса доступа пользователя после 20 минут его бездействия (неактивности) в информационной системе.

15. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

16. Пользователям запрещается:

разглашать защищаемую информацию посторонним лицам;

копировать защищаемую информацию на неучтенные внешние носители;

самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;

подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации;

выполнять на АРМ работы, не предусмотренные технологическим процессом обработки ПДн;

сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПДн;

оставлять без присмотра и передавать другим лицам персональный идентификатор;

привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение безопасности ПДн;

оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

3. Порядок работы пользователя с ресурсами ИСПДн

17. Начало работы на ПЭВМ.

При включении ПЭВМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее – СЗИ) и операционной системы (далее – ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ. Для получения доступа к ресурсам ИСПДн пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБ.

18. Завершение работы на ПЭВМ.

По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения ПЭВМ), либо завершить работу ПЭВМ стандартным способом (при этом выключить ПЭВМ).

19. Требования к распечатыванию информации.

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИСПДн, все документы, содержащие ПДн, должны быть недоступны для просмотра и иного их использования.

4. Организация парольной защиты

20. Правила, регламентирующие организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действий паролей, а также контроль действий пользователей при работе с паролями определяются Инструкцией по организации парольной защиты в Администрации, утвержденной распоряжением Администрации.

5. Ответственность

21. Пользователь несет персональную ответственность за:

сохранность носителей информации и содержащейся на них информации (в рабочее время);

соблюдение требований данной Инструкции, неправомерное использование ресурсов ИСПДн и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

22. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Начальник управления информационных технологий
Администрации Кыштымского городского округа С.В. Полев