Утверждено приказом
Заведующего МАДОУ ЦРР-детский сад№33
«Золушка» города Ишимбая
Ишимбайский район РБ
_____ Горяйнова А.Н.
Приказ № 07 от 14.01.2021г

Инструкция пользователя автоматизированного рабочего места (АРМ)

Муниципального автономного дошкольного образовательного учреждения центр развития ребенка – детский сад № 33 «Золушка» города Ишимбая муниципального района Ишимбайский район Республики Башкортостан

1. **Общие обязанности сотрудников по обеспечению информационный безопасности при работе на АРМ.**

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации имеющий доступ к аппаратным средством , программному обеспечению и данным автоматизированного рабочего места (АРМ), несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программами и техническими средствами АРМ;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;
- хранить в тайне свой пароль (пароли). В соответствии с "Инструкцией по организации парольной защиты" с установленный периодичность менять свой пароль (пароли);

- выполнять требования «Инструкции по организации антивирусной защиты » в части, касающейся действий пользователей;

- немедленно ставить в известность администратора защиты информации при подозрении компрометации паролей;

- вызывать специалиста организации ** при обнаружени:

- фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к 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 (дисковода, и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств;
- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ в подразделении.

2. ПОЛЬЗОВАТЕЛЯМ КАТЕГОРИЧЕСКИ ЗАПРЕЩАЕТСЯ:

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить информацию (содержащую сведения конфиденциального характера) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от несанкционированного доступа к данным (временную блокировку экрана);
- оставлять без личного присмотра на рабочем месте (или где бы то ни было) машинные носители, распечатки и другие носители, содержащие защищаемую информацию (сведения конфиденциального характера);

- 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 администратора безопасности информации.