



Инструкция
пользователям по обеспечению информационной безопасности
при работе с информационными ресурсами в
МАУ ДО «ДЮСШ №2» г. Стерлитамак РБ

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным автоматизированной системы (далее-АС) автоматизированного рабочего места (далее-АРМ) — персональный электронно-вычислительной машины (далее ПЭВМ), несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте;
- хранить в тайне свой пароль (пароли). В соответствии с «Инструкцией по организации парольной защиты...» с установленной периодичностью менять свой пароль (пароли);
- выполнять требования «Инструкции по организации антивирусной защиты...» в части касающейся действий пользователей;
- немедленно вызывать и ставить в известность администратора безопасности информации при подозрении компрометации паролей, а также при обнаружении:
- фактов совершения в его отсутствие попыток несанкционированного доступа к АРМ;
- несанкционированных изменений в конфигурации программных или аппаратных 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;
- непредусмотренных отводов кабелей и подключённых устройств;
- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию АС АРМ.

Сотрудникам запрещается:

- использовать компоненты программного и аппаратного обеспечения АС 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 информации (содержащую ограниченного распространения) на неучтенных носителях информации (флэшки);
- оставлять включенной без присмотра свою ПЭВМ, не активизировав средства защиты от несанкционированного доступа (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 ограниченного распространения);
- 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.