ИНСТРУКЦИЯ

пользователя информационных систем муниципального бюджетного общеобразовательного учреждения города Кургана «Средней общеобразовательной школы № 56»

1 Общие сведения

1.1 Настоящая Инструкция определяет общие права и обязанности сотрудников, допущенных к обработке защищаемой информации на средствах вычислительной техники в информационных системах (далее - ИС) муниципального бюджетного общеобразовательного учреждения города Кургана «Средней общеобразовательной школы № 56» (далее - Учреждение).

1.2 Настоящая инструкция разработана на основе:

- методического документа «Меры защиты информации в государственных информационных системах», утвержденного Федеральной службой технического и экспортного контроля России 11 февраля 2014 года;
- Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3 Настоящая Инструкция предназначена для руководителей подразделений, администратора информационной безопасности (далее - администратор ИБ) и пользователей, осуществляющих обработку защищаемой информации в ИС.

2 Общие права и обязанности сотрудников при работе в ИС

2.1 Каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС, несет персональную ответственность за свои действия и имеет право доступа к ИС в соответствие с матрицей доступа, а также обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;
- знать и строго выполнять правила работы со средствами защиты информации, установленными в ИС;
- хранить в тайне свои пароли. Выполнять требования «Правила идентификации и аутентификации пользователей ИС»;
- передавать для хранения установленным порядком свои реквизиты разграничения доступа только руководителю своего подразделения или ответственному за информационную безопасность в подразделении;
- выполнять требования «Правила по организации антивирусной защиты» в части, касающейся действий пользователей;
- немедленно вызывать администратора ИБ и ставить в известность руководителя подразделения в случае утери личных реквизитов доступа или при подозрении компрометации личных паролей, а также при обнаружении:

1) нарушений целостности пломб (наклеек) на аппаратных средствах ИС или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к техническим средствам ИС;

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

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

4) некорректного функционирования установленных на ИС технических средств защиты;

5) непредусмотренных техническим паспортом ИС отводов кабелей и подключенных устройств;

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ в подразделении;
- контролировать вывод информации на съемные носители информации. Пометка на носителе должна быть не ниже пометки записываемой информации.

2.2 Сотрудникам категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные техническим паспортом ИС;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие конфиденциальную 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 ИБ и руководителя своего

подразделения.

2.3 Действия пользователей до идентификации и аутентификации в системе.

Пользователям разрешается:

производить включение, выключение, перезагрузку технических средств и систем ИС;

предъявлять личный идентификатор и вводить пароль для авторизации в системе.

Пользователям запрещается:

входить в настройки базовой системы ввода-вывода технических средств и систем ИС;

- осуществлять загрузку нештатных операционных систем со сторонних носителей информации.

i