Утверждаю :
Заведующий МБДОУ
д/с №11 «Радость»
Р.В.Чернецова
"01" 09 2016 год

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных
МБДОУ д/С №11 «Радость»

1 Общие сведения

1.1 Настоящая Инструкция определяет общие права и обязанности сотрудников, допущенных к обработке персональных данных на средствах вычислительной техники в информационных системах персональных данных МБДОУ д/с №11 «Радость» (далее – МБДОУ д/С №11 «Радость»)

1.2 Настоящая Инструкция предназначена для руководителей подразделений, администратора информационной безопасности (далее – ИБ) и пользователей, осуществляющих обработку персональных данных в информационных системах персональных данных (далее – ИСПДн).

2 Общие права и обязанности сотрудников при работе в ИСПДн

2.1 Каждый сотрудник МБДОУ д/с №11 «Радость», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и имеет право доступа к ИСПДн в соответствие с матрицей доступа, а также обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

– знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн;

– хранить в тайне свои пароли. Выполнять требования «Инструкции по организации парольной защиты информационных систем персональных данных»;

– передавать для хранения установленным порядком свои реквизиты разграничения доступа только руководителю своего подразделения или ответственному за информационную безопасность в подразделении;

– выполнять требования «Инструкции по организации антивирусной защиты в ИСПДн» 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 ИСПДн или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к техническим средствам ИСПДн;

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

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

4) некорректного функционирования установленных на ИСПДн технических средств защиты;

5) непредусмотренных техническим паспортом ИСПДн 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 ИСПДн в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные техническим паспортом ИСПДн;

– 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 ИСПДн;

– предъявлять личный идентификатор и вводить пароль для авторизации в системе.

Пользователям запрещается:

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

– осуществлять загрузку нештатных операционных систем со сторонних носителей информации.