Приложение № 2
УТВЕРЖДЕНА
приказом директора МБОУ «НОШ № 5»
_____ Ким Н.А.
от 14.03.2014 № 17/1

Инструкция пользователя информационных систем

1. Общие требования по обеспечению безопасности обработки информации

1.1. К защищаемой информации, обрабатываемой в информационных системах МБОУ «НОШ № 5» (далее – Учреждение), относятся персональные данные.

1.2. Ответственность за организацию защиты информации в Учреждении и выполнение установленных условий ее функционирования возлагается на ответственного за функционирование информационной системы Учреждения. Ответственность за выполнение мероприятий по обеспечению безопасности информации возлагается на работника, производящего ее обработку (пользователя).

1.3. Допуск пользователей к работе в информационных системах Учреждения осуществляется в соответствии со списком лиц, доступ которых к конфиденциальной информации, обрабатываемой в информационных системах, необходим для выполнения должностных обязанностей.

1.4. К самостоятельной работе на автоматизированных рабочих местах, входящих в состав информационной системе Учреждения, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации автоматизированных рабочих мест и технических средств защиты.

1.5. По фактам и попыткам несанкционированного доступа к защищаемой информации, а также в случаях ее утечки и (или) модификации (уничтожения) проводятся служебные расследования.

2. Обязанности пользователя

2.1. При первичном допуске к работе в информационной системе Учреждения пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию.

2.2. Каждый работник Учреждения, участвующий в рамках своих должностных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и базам данным информационных систем Учреждения, несет персональную ответственность за свои действия и обязан:

2.2.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами.

2.2.2. Знать и строго выполнять правила работы со средствами защиты информации.

2.2.3. Выполнять требования по антивирусной защите в части, касающейся действий пользователей.

2.2.4. Немедленно ставить в известность ответственного за функционирование информационной системы Учреждения в следующих случаях:

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию информационной системы инфраструктуры Администрации, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных средств защиты;
- обнаружения непредусмотренных отводов кабелей и подключенных устройств;
- обнаружения фактов и попыток несанкционированного доступа и случаев нарушения установленного порядка обработки защищаемой информации.

2.3. Пользователю категорически запрещается:

2.3.1. Использовать компоненты программного и аппаратного обеспечения информационной системы Учреждения в неслужебных целях.

2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства.

2.3.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.3.4. Записывать и хранить защищаемую информацию на неучтенных машинных носителях информации.

2.3.5. Оставлять без личного присмотра на рабочих местах (АРМ) или где бы то ни было свои персональные реквизиты доступа (пароли, ключи доступа), электронные машинные носители и распечатки, содержащие защищаемую информацию.

2.3.6. Производить перемещения технических средств автоматизированных рабочих мест без согласования с администратором безопасности.

2.3.7. Вскрывать корпусы технических средств автоматизированных рабочих мест и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с администратором безопасности.

2.3.8. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств автоматизированных рабочих станций.