МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
НАЧАЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 7
ГОРОДА ЮЖНО-САХАЛИНСКА

693007, г. Южно-Сахалинск, ул. им. Антона Буюклы, 14,
Тел.: (4242) 22-54-75, (4242) 22-54-76, факс: (4242) 22-54-76 Email: school7@yuzhno-sakh.ru

УТВЕРЖДЕНА
приказом директора
Муниципального автономного
общеобразовательного учреждения
начальная общеобразовательная
школа №7 города Южно-Сахалинска
от 16.05.2016 № 120 – ОД

Инструкция пользователя информационных систем персональных данных

1. Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является сотрудник Муниципального автономного общеобразовательного учреждения начальная общеобразовательная школа №7 (далее ОУ), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Сведения, содержащиеся в электронных документах и базах данных ОУ, должны использоваться только в служебных целях в рамках полномочий сотрудника, работающего с соответствующими материалами.

1.4. Пользователь несет персональную ответственность за свои действия.

2. Функциональные обязанности

Пользователь обязан:

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

2.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее АРМ).

2.3. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.4. Соблюдать правила работы с паролем своей учётной записи.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.8. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

2.9. Немедленно вызвать администратора безопасности ИСПДн и поставить в известность ответственного за организацию и осуществление мероприятий по защите конфиденциальной информации в ОУ:

2.9.1. Нарушений целостности наклеек, нарушении или несоответствии номеров учёта на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ.

2.9.2. Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ.

2.9.3. 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.

2.9.4. Некорректного функционирования установленных на АРМ технических средств защиты.

2.9.5. Непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

2.10. Работа в информационно-телекоммуникационной сети Интернет на элементах ИСПДн, должна проводиться только при служебной необходимости.

3. Запрещается

Всем сотрудникам ОУ, являющимся пользователями ИСПДн, запрещается:

3.2. Использовать компоненты программного и аппаратного обеспечения ИСПДн ОУ в неслужебных целях.

3.3. Самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за обеспечение безопасности персональных данных.

3.4. Оставлять без присмотра своё АРМ не активизировав блокировки доступа или оставлять своё АРМ включенным по окончании работы.

3.5. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

3.6. Привлекать посторонних лиц для производства ремонта или настройки АРМ.

3.7. Копировать защищаемую информацию на внешние носители.

3.8. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

4.8. При работе в информационно-телекоммуникационной сети Интернет запрещается:

– осуществлять работу при отключенных средствах защиты (антивирус и других);

– передавать защищаемую информацию без использования средств шифрования;

– запрещается скачивать программное обеспечение и другие файлы, которые могут привести к нарушению работы ПО;

– запрещается посещение сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);

– запрещается нецелевое использование подключения к Сети.

4. Ответственность пользователей ИСПДн

4.1. Каждый пользователь ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

4.2. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, сотрудники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

4.3. Распространение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ОУ, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ОУ, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ОУ (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

4.4. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.