УТВЕРЖДАЮ
Директор МБУДО ДЮСШ № 2
_____ Нерубенко В.К.
«02» августа 2018 г.
Приказ от «2» августа 2018 г. № 151

Инструкция пользователя информационных систем персональных данных

Обозначения и сокращения

В настоящем документе применяются следующие обозначения и сокращения:

АРМ	- автоматизированное рабочее место
ИСПДн	- информационная система персональных данных
ЛВС	- локальная вычислительная сеть
МЭ	- межсетевой экран
НСД	- несанкционированный доступ
ОС	- операционная система
ПДн	- персональные данные
ПК	- персональный компьютер
ПМВ	- программно-математическое воздействие
ПО	- программное обеспечение
ПЭМИН	- побочные электромагнитные излучения и наводки
РД	- руководящие документы
САЗ	- средства анализа защищенности
СЗИ	- средство защиты информации
СЗПДн	- система защиты персональных данных
СОВ	- система обнаружения вторжений
УБПДн	- угрозы безопасности персональных данных

1. Общие положения

1.1. Пользователь информационной системы персональных данных осуществляет обработку персональных данных.

1.2. Пользователем является каждый сотрудник МБУДО ДЮСШ № 2 (далее - Учреждение), участвующий, в рамках своих функциональных обязанностей, в процессах обработки информации, содержащей персональные данные, и имеющий доступ к аппаратным средствам, программному обеспечению и средствам защиты информации.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, требованиями законодательства Российской Федерации, а также принятыми в Учреждении положениями, инструкциями и приказами.

2. Обязанности пользователя ИСПДн

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, положения о порядке обработки персональных данных и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него должностными обязанностями.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и передаче информации, обеспечению безопасности персональных данных, в соответствии с руководящими и организационно-распорядительными документами.

2.4. Хранить съемные носители персональных данных в сейфах (металлических шкафах), оборудованных внутренним замком и приспособлением для опечатывания замочных скважин или кодовым замком. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов.

2.5. Соблюдать требования парольной политики.

2.6.Располагать экран монитора во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на ним информацией посторонними лицами; шторы на оконных проемах должны быть завешены (жалюзи закрыты) в случае, если есть возможность просмотра экрана монитора через окно.

2.7. В рабочее время помещение закрывать на замок и открывать только для санкционированного прохода.

2.8. Обо всех выявленных нарушениях необходимо сообщать руководителю учреждения.

2.9. Для получения консультаций по вопросам работы и настройки элементов ИСПДн, необходимо обращаться к Администратору ИСПДн.

2.10. Пользователю запрещается:

разглашать защищаемую информацию (отраженную в Перечне защищаемых информационных ресурсов и Перечне обрабатываемых персональных данных) третьим лицам;

- копировать защищаемую информацию на неучтенные внешние носители;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к ресурсам на своем автоматизированном рабочем месте (АРМ);
- подключать к АРМ и корпоративной информационной сети личные внешние носители и устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию, не имеющую отношения к трудовой деятельности и выполнять другие работы, не предусмотренные должностными обязанностями;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- бесконтрольно оставлять, либо передавать посторонним лицам ключи от помещения, в котором располагаются элементы ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с руководителем.

2.11. В случае возникновения внештатных и аварийных ситуаций, необходимо принимать меры по реагированию с целью ликвидации их последствий.

3. Правила работы в сетях общего доступа и (или) международного информационного обмена

3.1. Работа в сетях общего доступа и (или) международного информационного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус, межсетевой экран и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы, не связанные с исполнением служебных обязанностей, либо содержащие вредоносный код;
- запрещается сохранять (скачивать) и открывать вложения из писем электронной почты от неизвестных отправителей. Если отправитель известен, то необходимо уточнить у него факт отправки письма лично, после чего сохранить вложение и перед открытием проверить антивирусом;
- запрещается посещение сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);

запрещается нецелевое использование подключения к Сети.