

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 МБДОУ д/с №49 (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.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение безопасности персональных данных.

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 (раздел 3).

2.6. Соблюдать правила при работе в сетях общего доступа и (или) международного информационного обмена – Интернет и других (раздел 4).

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

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

2.9. Обо всех выявленных нарушениях необходимо сообщать ответственному за обеспечение безопасности персональных данных.

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

2.11. 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 ответственным за обеспечение безопасности персональных данных.

2.12. При отсутствии визуального контроля за АРМ доступ к компьютеру должен быть немедленно заблокирован (например, для ОС Windows необходимо нажать комбинацию клавиш Ctrl+Alt+Del и выбрать опцию Блокировка).

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

3. Организация парольной защиты

3.1. Пароли доступа к ИСПДн выдаются пользователям ответственным за обеспечение безопасности персональных данных или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- пароль не должен содержать имя учетной записи пользователя или его часть;
- пароль должен состоять не менее, чем из 6 символов;
- в пароле должны присутствовать прописные и строчные буквы английского алфавита, цифры и специальные символы;
- запрещается использовать в качестве пароля простые пароли типа «123456», «qwerty» и т.д., а также свои имена и даты рождения, клички домашних животных, номера телефонов и другие пароли, которые можно подобрать, основываясь на информации о пользователе;
- запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по парольной защите;
- своевременно сообщать лицу, ответственному за обеспечение безопасности персональных данных об утере, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

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

4.2. 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.