«УТВЕРЖДАЮ»
Заведующий МДОУ № 12 «Полянка»
_____Н.В. Касьянова
«__» _____ 2015 года

Инструкция пользователя ИСПД н

Пользователями ИСПДн (далее - Пользователь) являются сотрудники, ответственные за обработку персональных данных в ИСПДн МДОУ № 12 «Полянка» ТМР, а также сотрудники, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации в ИСПДн, имеющие доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты ИСПДн. Пользователь в своей работе руководствуется настоящей инструкцией, Федеральным законом №152-ФЗ от 27 июля 2006 года «О персональных данных», Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК.

Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных.

1. Обязанности пользователя

1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

1.2. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

1.3. Соблюдать требования парольной политики.

1.4. Соблюдать правила работы в сетях общего доступа и (или) международного обмена - Интернет и других (п.3 данного приложения).

1.5. 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).

1.6. Обо всех выявленных нарушениях, связанных с информационной безопасностью МДОУ № 12 «Полянка» ТМР, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться в _____по электронной почте: или по внутреннему телефону.

1.7. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн по внутреннему телефону

1.8. Пользователям запрещается: .

Разглашать защищаемую информацию третьим лицам.

Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

Несанкционированно открывать общий доступ к папкам на своей рабочей станции. Подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
Отключать (блокировать) средства защиты информации.
Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
1.9. 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> (либо комбинацию <Windows>+<L>).
1.10. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

2. Организация парольной защиты

2.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.
2.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
2.3. Правила формирования пароля:
Пароль не может содержать имя учетной записи пользователя или какую-либо его часть. Пароль должен состоять не менее чем из 8 символов.
В пароле должны присутствовать символы трех категорий из числа следующих четырех:

1) прописные буквы английского алфавита от A до Z;
2) строчные буквы английского алфавита от a до z;
3) десятичные цифры (от 0 до 9);
4) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения свои или родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.); Запрещается выбирать пароли, которые уже использовались ранее.
2.4. 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.).
2.5. Правила хранение 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.
Запрещается регистрироваться в системе под чужой учетной записью.
2.6. Лица, использующие пароли доступа к элементам ИСПДн, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.
своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

3.1. Работа в сетях общего доступа и (или) международного 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 и других). Передавать по Сети защищаемую информацию без использования средств шифрования. Скачивать из Сети программное обеспечение и другие файлы.
Посещать сайты сомнительной репутации (сайты эротического содержания, сайты содержащие нелегально распространяемое ПО, медиаконтент и другие). Использовать подключение к Сети во внеслужебных целях.