СОГЛАСОВАНО
Председатель профкома
Муниципального автономного дошкольного образовательного учреждения «Детский сад общеразвивающего вида № 49» НМР РТ
_____ А.Ф. Шакирянова
«05» 09 2018 г.

УТВЕРЖДАЮ
Заведующий МАДОУ «Детский сад общеразвивающего вида № 49" НМР РТ
_____ Р.Г.Хайдарова
«05» 09 2018 г.
Приказ № 82 от 23.09.2019

Руководство пользователя по обеспечению безопасности ИСПДн
МАДОУ «Детский сад общеразвивающего вида №49»
Нижнекамского муниципального района
Республики Татарстан

Г. Нижнекамск

Руководство пользователя по обеспечению безопасности ИСПДн
МАДОУ «Детский сад общеразвивающего вида №49»
Нижнекамского муниципального района
Республики Татарстан

1.Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
1.2. Пользователем является сотрудник ДОУ, 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. Пользователь несет персональную ответственность за свои действия.
1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Политикой информационной безопасности в ДОУ, руководящими и нормативными документами ФСТЭК России и регламентирующими документами.
1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2.Должностные обязанности

Пользователь обязан:
2.1. 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.
2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.
2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационнораспорядительных документов.
2.4. Соблюдать требования парольной политики (раздел 3).
2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).
2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.
2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью в ДОУ, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться руководителю.
2.8. 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.
- Запрещено 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.

2.9. 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>.

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

3.Организация парольной защиты

3.1. Пароли доступа к элементам ИСПДн имеются только у ответственного лица.

3.2. Смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- Пароль не может содержать имя учетной записи пользователя или какуюлибо его часть.
- Пароль должен состоять не менее чем из 8 символов.
- В пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) 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 своей личности и своих 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.

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 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.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

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

4.1. Работа в сетях общего доступа и (или) международного 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 и других).
- Передавать по Сети защищаемую информацию без использования средств защиты каналов связи.
- Запрещается скачивать из Сети программное обеспечение и другие файлы.
- Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).
- Запрещается нецелевое использование подключения к сети.

ЛИСТ ОЗНАКОМЛЕНИЯ

Руководство пользователя по обеспечению безопасности ИСПДн

№	ФИО	Дата ознакомления	Роспись
1.	Ахмадуллина Э.Х.		
2.	Калимуллина Э.С		
3.	Хайдарова Р.Г.		
4.	Шарафутдинова И.В		
5.	Калимуллина Г.К.		
6.			
7			
8			
9			
10			
11			
12			
13			
14			