УТВЕРЖДЕНО
Приказом МДОУ ДС «Морошка»
№ 23-ОД от 18.11.2022г

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных в Муниципальном дошкольном образовательном учреждение детский сад «Морошка»

Приложение к приказу **№ 23-ОД** от 18.11.2022

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных в Муниципальном дошкольном образовательном учреждение детский сад «Морошка»

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее - ИСПД) Муниципального дошкольного образовательного учреждения детский сад «Морошка» (далее - МДОУ).

1.2. Субъектами доступа к ресурсам ИСПД являются пользователи ИСПД.

1.3. Обрабатываемая в ИСПД информация относится к сведениям, составляющим персональные данные (далее- ПД).

1.4. Машинные носители информации имеют пометку «ПД».

1.5. Пользователи получают свои права на доступ к ресурсам ИСПД от администратора безопасности информации МДОУ (далее - АБИ).

1.6. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

2. Обязанности пользователя ИСПД

2.1. Знать и выполнять требования действующих нормативных документов, а также внутренних инструкций и приказов, руководства пользователя, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры, которые определены технологическим процессом обработки персональных данных.

2.3. Знать и соблюдать установленные требования к обработке персональных данных, учету и хранению носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики в соответствии с Инструкцией по организации парольной защиты в информационных системах персональных данных в МДОУ.

2.5. Получать уникальное имя и персональный идентификатор (при его наличии) от АБИ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания.

2.6. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации.

2.7. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажение данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБИ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля-уведомить о результатах АБИ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

2.8. В случае появления информационного окна средства антивирусной защиты, сигнализирующего об обнаружении вредоносного программного обеспечения:

2.1.1. приостановить обработку данных;

2.1.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБИ владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

2.1.3. совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

2.1.4. произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБИ).

2.2. Немедленно вызвать АБИ и поставить в известность руководителя структурного подразделения МДОУ при обнаружении:

– фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

– 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;

– некорректного функционирования установленных на АРМ технических средств защиты;

– непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

2.3. При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБИ.

2.4. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБИ.

2.5. 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>.

2.6. Принимать меры по реагированию в случае возникновения внештатных ситуаций и

аварийных ситуаций с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.7. Пользователям запрещается:

– разглашать защищаемую информацию посторонним лицам;

– копировать защищаемую информацию на неучтенные внешние носители;

– самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;

– подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– выполнять на АРМ работы, не предусмотренные технологическим процессом обработки ПД сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПД;

– оставлять без присмотра и передавать другим лицам персональный идентификатор;

– привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным по защите информации;

– оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

3. Порядок работы пользователя с ресурсами ИСПД

3.1. Начало работы на АРМ.

При включении АРМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее-СЗИ) и операционной системы (далее-ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ. Для получения доступа к ресурсам ИСПД пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБИ.

3.2. Завершение работы на АРМ.

По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения АРМ), либо завершить работу АРМ стандартным способом (при этом выключить АРМ).

3.3. Требования к распечатыванию информации.

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИСПД, все документы, содержащие ПД, должны быть недоступны для просмотра и иного их использования.

4. Организация парольной защиты

4.1. Личные пароли доступа к элементам ИСПД выдаются пользователям АБИ или создаются самостоятельно.

4.2. Полная плановая смена паролей в ИСПД проводится не реже одного раза в 12 месяцев.

4.3. Правила формирования пароля:

– пароль должен состоять не менее чем из 8 символов;

–в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от A до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например,!,$,#, %).;

–пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания

символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, 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.

4.4. Правила ввода пароля:

– ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

– во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

4.5. Правила хранения пароля:

– запрещается записывать пароли на бумаге, в файле и других носителях информации, втом числе на предметах;

– запрещается сообщать другим пользователям личный пароль и/или регистрировать их всистеме под своей учетной записью.

4.6. Лица, использующие пародирование, обязаны:

– четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

– своевременно сообщать АБИ об утере, компрометации, несанкционированном измененииипаролей и несанкционированном изменении сроков действия паролей.

5. Ответственность

5.1. Пользователь несет персональную ответственность за:

– сохранность носителей информации и содержащейся на них информации (в рабочее время)

– соблюдение требований данной Инструкции, неправомерное использование ресурсов ИСПД и за все действия, совершенные от имени его учетной записи в ИСПД, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

5.2. За разглашение ПД и нарушение порядка работы со средствами ИСПД, содержащими персональные данные, пользователи могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

5 Ответственность (в рем я)