Муниципальное бюджетное дошкольное образовательное учреждение «Детский сад №22 «Журавлик» города Сафоново Смоленской области
(МБДОУ д/с №22)

УТВЕРЖДАЮ:
Заведующий МБДОУ д/с №22
_____ С.В. Зыбина
Приказ № 109
от «26» сентября 2023 г.

ИНСТРУКЦИЯ
Пользователя информационных систем персональных данных в Муниципальном бюджетном дошкольном образовательном учреждении «Детский сад №22 «Журавлик» города Сафоново Смоленской области (МБДОУ д/с №22)

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 бюджетного дошкольного образовательного учреждения «Детский сад №22 «Журавлик» города Сафоново Смоленской области (далее - МБДОУ).

1.2. Пользователь информационных систем персональных данных (ИС ПД) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

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

1.4. Машинные носители информации имеют пометку «ПД».

1.5. Пользователем является каждый сотрудник муниципального бюджетного дошкольного образовательного учреждения «Детский сад №22 «Журавлик» города Сафоново Смоленской области (далее — учреждение), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.6. Пользователь несёт персональную ответственность за свои действия.

1.7. Пользователь в своей работе руководствуется настоящей инструкцией и регламентирующими документами учреждения.

1.8. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Обязанности пользователя

2.1. Пользователь обязан соблюдать порядок обеспечения конфиденциальности при обращении с информацией, содержащей ПДн, ставшей ему известной (или доступной для обработки) в процессе работы.

2.2. Пользователь обязан знать и выполнять требования действующих нормативных и руководящих документов в области защиты ПДн, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите сведений, отнесённых к категории «Персональные данные».

2.3. Пользователь должен выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в должностной инструкции.

2.4. Пользователь должен 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.

2.5. Пользователь должен соблюдать требования парольной политики в соответствии с Инструкцией по организации парольной защиты в информационных системах персональных данных в МБДОУ.

2.6. Экран монитора в помещении Пользователя, где обрабатываются ПДн, Пользователь должен 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 ПДн, обрабатываемых в ИСПДн, а также для получения консультаций по вопросам безопасности ПДн Пользователь должен обращаться к ответственному за обеспечение защиты ПД.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИС ПДн необходимо обращаться к Администратору системы.

2.9. 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;
- оставлять без присмотра и передавать другим лицам персональный идентификатор;
- 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;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
- принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Организация парольной защиты

3.1 . Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2 . Полная плановая смена паролей в ИСПД проводится не реже одного раза в 6 месяцев.

3.3. 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 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.

3.4. 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 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 своей учетной записью.

3.6. Лица, использующие паролирование, 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.

4. Порядок работы пользователя с ресурсами ИСПД

4.1. 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.

4.2. 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).

4.3. 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.

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

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

5.2. При работе в Сети запрещается:

- осуществлять работу при отключённых средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- 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.

6. Права и ответственность пользователей ИСПДн

6.1. 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.