УТВЕРЖДАЮ
Директор МАОУ СОШ № 31
_____ Е.В. Иванова
«_4_» _____2023г.

Инструкция
пользователя информационной системы персональных данных
муниципального автономного общеобразовательного учреждения города Калининграда
средняя общеобразовательная школа № 31
(МАОУ СОШ № 31)

1 Общие положения

1.1 Пользователем является каждый сотрудник информационной системы персональных данных муниципального автономного общеобразовательного учреждения города Калининграда средней общеобразовательной школы № 31 (далее - МАОУ СОШ № 31), участвующий в рамках своих функциональных обязанностей в процессах смешанной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты, используемых в информационной системе персональных данных (далее – ИСПДн).

1.2 Пользователь несет персональную ответственность за свои действия.

1.3 Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСБ РФ и ФСТЭК РФ и регламентирующими документами, разработанными и утвержденными в МАОУ СОШ № 31.

1.4 Методическое руководство работой пользователей осуществляется ответственным за обеспечение безопасности персональных данных.

2 Должностные обязанности

Пользователь обязан:

2.1 Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, регламентирующих порядок действий при работе с персональными данными (далее – ПДн).

2.2 Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры, которые определены для него функциональными обязанностями.

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 организационно-распорядительных документов.

2.4 Соблюдать требования парольной политики (раздел 3 настоящей инструкции).

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

2.6 Экран АРМ монитора в помещении, где ведется обработка ПДн, 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).

2.7 Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к администратору информационной безопасности.

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 над рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован.

2.10 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 ИСПДн выдаются пользователям Администратором информационной безопасности.

3.2 Полная плановая 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 какую-либо 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;
- своевременно сообщать об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей Администратору информационной безопасности.

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 в случае 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 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.