

УТВЕРЖДАЮ

Директор МБОУ СОШ № 28

_____ / М.М.Кривчук

Приказ № «_____»

от «_____» _____ 20____ г.

ИНСТРУКЦИЯ
пользователя информационной системой
персональных данных
в МБОУ СОШ № 28

1. Общие положения

1.1. Пользователь информационных систем персональных данных (далее - Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник МБОУ СОШ № 28 (далее – МБОУ СОШ №28), 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, руководящими и нормативными документами ФСТЭК России и регламентирующими документами МБОУ СОШ № 28.

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 только те процедуры, которые определены для него.

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

2.4. Соблюдать требования парольной политики.

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

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключить возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью МБОУ СОШ № 28, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться в школу по электронной почте: school28@krsrm.kubannet.ru или по телефону 8(86165) 93-2-44.

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

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 автоматизированном рабочем месте информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системе персональных данных;
- привлекать посторонних лиц для производства ремонта или настройки автоматизированного рабочего места без согласования с директором школы.

3. Организация парольной защиты

3.1. Личные пароли доступа к элементам информационной системы персональных данных создаются пользователями самостоятельно.

3.2. 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:
 - прописные буквы английского алфавита от A до Z
 - строчные буквы английского алфавита от a до z
 - десятичные цифры (от 0 до 9)
 - 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 также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информацию 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.

3.3. Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
- во время ввода пароля необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.4. Правила хранения паролей:

- 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.

3.5. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
- своевременно сообщать ответственному за информационную безопасность об утере, компрометации, несанкционированном изменении паролей.

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 информационной системы персональных данных, 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 шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое программное обеспечение и другие);
- запрещается нецелевое использование подключения к Сети.

5. Права и ответственность пользователей информационной системой персональных данных

5.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам информационной системы персональных данных.

5.2. Пользователи виновные в несоблюдении настоящей инструкции расцениваются как нарушители Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.