Приложение № _2___
к приказу от «_10»_09__2015_ г. № __12-о/д

Инструкция
пользователя информационной системы персональных данных МКОУКШИ «ДКК-1»

I. Общие положения

1. Пользователь информационной системы персональных данных (далее по тексту - ИСПДн) МКОУКШИ «ДКК-1» (далее- Школа) осуществляет обработку персональных данных в ИСПДн.

2. Пользователем является каждый сотрудник Школы, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

3. Пользователь несет персональную ответственность за свои действия.

4. Пользователь в своей работе руководствуется настоящей инструкцией, Концепцией информационной безопасности, Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Оператора.

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

II. Должностные обязанности

1. Пользователь обязан:

- 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.
- 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.
- Соблюдать требования парольной политики. (раздел 3).
- Соблюдать правила при работе в сетях общего - Интернет и других (раздел 4).
- Экран монитора в помещении 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).
- Обо всех выявленных нарушениях, связанных с информационной безопасностью Оператора, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к лицу ответственному за обеспечение информационной безопасности ИСПДн.
- Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2. 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.

3. 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>

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

III. Организация парольной защиты

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

2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

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:
  - 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 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.

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.).

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.
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

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.

IV. Правила работы в сетях общего доступа

1. Работа в сетях общего доступа (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

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.