

## **ИНСТРУКЦИЯ**

### **пользователя информационных систем персональных данных по обеспечению безопасности персональных данных**

#### **1. Общие положения**

1.1. Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в муниципальном бюджетном общеобразовательном учреждении г. Астрахани «СОШ№30» (далее – МБОУ г. Астрахани «СОШ№30»).

1.2. Пользователем является каждый работник – МБОУ г. Астрахани «СОШ№30», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных 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 Федеральной службы по техническому и экспортному контролю(ФСТЭК) России и другими внутренними документами Управления образования по защите информации.

#### **2. Обязанности пользователя**

Пользователь обязан:

2.1. Знать и выполнять требования настоящей Инструкции и других внутренних нормативно–правовых документов, по защите персональных данных.

2.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

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 (Раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и международного обмена – Интернет (Раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью в – МБОУ г. Астрахани «СОШ№30», а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к Администратору информационной системы персональных данных или ответственному за обработку персональных данных.

2.8. Для получения консультаций по вопросам работы и настройке элементов информационной системы персональных данных необходимо обращаться к Администратору информационной системы персональных данных.

2.9. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам;
- Копировать защищаемую информацию на внешние носители без письменного разрешения директора МБОУ г. Астрахани «СОШ№30» или заведующего обособленного подразделения;
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- Несанкционированно открывать общий доступ к ресурсам;
- Запрещено подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;
- Отключать (блокировать) средства защиты информации;
- Обращивать на АРМ 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 АРМ, без согласования с Администратором информационной системы персональных данных.

2.10. 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>

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

### **3. Организация парольной защиты**

3.1. Пароли доступа к элементам информационной системы персональных данных создаются Администратором безопасности информационных систем персональных данных.

3.2. Полная плановая смена паролей в информационной системе персональных данных 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:

- прописные буквы английского алфавита от А до Z;

- строчные буквы английского алфавита от а 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 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 хранения 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 и других руководящих документов по паролированию;

- Своевременно сообщать Администратору информационной системы персональных данных об утере, компрометации, несанкционированном

изменении паролей и несанкционированном изменении сроков действия паролей.

#### **4. Правила работы в сетях общего доступа и (или) международного обмена**

4.1. Работа в сетях общего доступа и международного обмена (сети Интернет) (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 исполняемые файлы (файлы с расширением exe, dll, msi);
- Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие);
- Запрещается нецелевое использование подключения к Сети.

#### **5. Ответственность**

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.