Приложение №19
к приказу
от 02.09.2025г. № 01.09-0209-4

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации парольной защиты информационных систем персональных данных в муниципальном бюджетном общеобразовательном учреждении г. Астрахани «СОШ№30».

1.2. Действие настоящей Инструкции распространяется на всех пользователей информационных систем персональных данных (далее – Пользователь).

1.3. Пользователем является каждый работник школы, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

2. Организация парольной защиты

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

2.2. Правила смены паролей:

– Полная плановая смена паролей в информационной системе персональных данных проводится не реже одного раза в 3 месяца.

– Внеплановая смена (удаление) пароля любого пользователя информационных систем персональных данных в случае прекращения его полномочий (увольнение, либо переход на другую работу внутри банка) должна производится немедленно после окончания последнего сеанса работы данного пользователя системы.

– Внеплановая полная смена всех паролей должна производится в случае прекращения полномочий (увольнение, переход на другую должность и другие обстоятельства) администраторов информационных систем персональных данных и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты информации данной системы, а значит, кроме личного пароля им могут быть известны пароли других пользователей системы.

2.3. 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 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.

2.4. Правила ввода пароля:

– Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан и с учётом текущей раскладки клавиатуры.

– Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

2.5. 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.

2.6. Действия в случае утери и компрометации пароля:

– В случае утери пароля сотрудник получает у Администратора безопасности информационной системы персональных данных новый пароль.

– В случае компрометации пароля (подсматривание кем-либо, разглашение пароля и др.) пароль необходимо сменить в соответствии с вышеуказанными требованиями.

2.7. Лица, использующие паролирование, обязаны:

– Четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию.

– Своевременно сообщать Администратору безопасности информационной системы персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

– По первому требованию Администратора безопасности информационной системы персональных данных предъявлять значения действующего личного пароля для контроля соответствия установленным требованиям, а после проверки провести немедленную его смену

3. Ответственность

3.1. Ответственность за организацию парольной защиты в подразделении возлагается на Администратора безопасности информационной системы персональных данных.

3.2. Периодический контроль за соблюдением требований данной инструкции возлагается на Администратора безопасности информационной системы персональных данных.

3.3. Владельцы паролей должны под расписку быть ознакомлены с данной инструкцией.

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