|  |  |
| --- | --- |
|  | Приложение № 19 утверждена |
|  | распоряжением администрации городского поселения р.п.Средняя Ахтуба от 29 мая 2019г. № 136-р |
|  |  |  |

**ИНСТРУКЦИЯ**

**по организации парольной защиты информационных систем**

**персональных данных в Администрации городского поселения р.п.Средняя Ахтуба Среднеахтубинского муниципального района**

**Волгоградской области**

# Общие положения

## Настоящая Инструкция предназначена для организации парольной защиты информационных систем персональных данных в Администрации городского поселения р.п.Средняя Ахтуба Среднеахтубинского муниципального района Волгоградской области (далее – Администрация).

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

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

# Организация парольной защиты

## Пароли доступа к элементам информационной системы персональных данных создаются Администратором безопасности информационной системы персональных данных.

## Правила смены личных паролей:

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

## Внеплановая смена (удаление) личного 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.

## Администратор безопасности информационной системы персональных данных оказывает необходимую помощь пользователям в процессе смены пароля.

## 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.

## 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.).

## 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.

## 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.

## 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

# Ответственность

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

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

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

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