**ПРИМЕР СТРУКТУРЫ И ОФОРМЛЕНИЯ ПРИЛОЖЕНИЯ № 2**

Приложение № 2 к Политике информационной безопасности ООО АТОМОРС

# ПОЛОЖЕНИЕ

**ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ**

# Назначение и область действия

* 1. Настоящее Положение о использовании паролей(далее – «Положение») определяет основные правила и требования по использованию паролей в ООО АТОМОРС (далее – «Организация»).
  2. Соответствует требованиям Политики информационной безопасности Организации.
  3. Распространяется на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации. Является обязательным для исполнения.

# Организация парольной защиты

* 1. Личные пароли должны создаваться Пользователями самостоятельно.
  2. В случае формирования личных паролей Пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного и Администратора в ИСПДн и на АРМ Пользователей соответственно.
  3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
  4. Внеплановая смена личного пароля Пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение, переход на другую должность в ИСПДн и т.п.) должна производиться Администратором и Ответственным немедленно после окончания последнего сеанса работы Пользователя в АРМ и в ИСПДн соответственно.
  5. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.Назначение прав доступа соответствует принципу «Запрещено все, что явно не разрешено» и определяется, исходя из служебных обязанностей пользователя.
  6. Разблокирование учетной записи осуществляется Администратором и Ответственный для учетных записей Пользователя для АРМ и для ИСПДн соответственно.
  7. После 15 минут бездействия (неактивности) Пользователя в АРМ или ИСПДн происходит автоматическое блокирование сеанса доступа в АРМ и ИСПДн соответственно.

# Требования к формированию паролей

* 1. Длина пароля должна быть не менее 8 символов.
  2. В пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих:

- буквы в верхнем регистре;

- буквы в нижнем регистре;

-специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $, &, \*, % и т.п.).

* 1. Пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть.
  2. Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.
  3. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).
  4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

# Ответственность

* 1. Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к АРМ и к ИСПДн.