Приложение № 2 к Политике информационной безопасности ООО "ЦИФРОВАЯ НЕЗАВИСИМОСТЬ"

# ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ

# Назначение и область действия

* 1. Настоящее Положение об использовании паролей (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности информационных ресурсов ООО "ЦИФРОВАЯ НЕЗАВИСИМОСТЬ" (далее – «Организация») от угроз, связанных с некорректным использованием средств аутентификации (паролей).
  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.

# Основные требования

# 2.1. Пользовательские пароли (для доступа к электронной почте, сети, компьютеру и т.д.) должны содержать не менее шести буквенно-цифровых символов (буквы латинского алфавита, цифры).

# 2.2. Административные пароли (административных учетных записей

# операционных систем, телекоммуникационного оборудования, баз данных,

# информационных систем и т.д.) должны содержать не менее восьми буквенноцифровых символов и спецсимволов, если они поддерживаются программным обеспечением (буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы типа ! @ # $ % ^ & \* \_ = ).

# 2.3. Для простоты запоминания могут быть использованы парольные

# фразы, разделенные спецсимволами и цифрами.

# 2.4. Пароль не должен совпадать с логином пользователя (наименованием учетной записи) и содержать легко угадываемые слова и

# числа (имена, даты рождения, номера документов и т.п.).

# 2.5. Пользователи лично ответственны за выбор пароля, отвечающего заданным критериям сложности, и за его хранение, исключающее ознакомление с ним третьих лиц.

# 2.6. Запрещается передача паролей третьим лицам.

# 2.7. Запрещается запись и хранение паролей в местах, где они могут

# быть легко доступны и прочитаны.

# 2.8. Все пользовательские пароли должны заменяться не реже одного

# раза в год. Рекомендованный интервал – шесть месяцев.

# 2.9. Все административные пароли должны заменяться не реже одного раза в полгода. Рекомендованный интервал – три месяца.

# 2.10. Запрещается отправлять пароли в сообщениях электронной

# почты, SMS или через другие формы электронного обмена информацией,

# кроме специально оговоренных случаев (одноразовые пароли с ограниченным

# сроком действия; пароли, создаваемые самим пользователем при помощи

# средств электронного обмена информацией и т.п.)

# 2.11. В случае компрометации пароля (утраты, хищения и т.п.),

# пользователь должен немедленно сменить пароль. Если пользователь не имеет

# возможности самостоятельно сменить пароль, администратор заменяет его

# пароль новым паролем, который сообщает пользователю.

# 2.12. Учетные записи сотрудников, чьи пароли не соответствуют

# требованиям настоящего Положения, могут быть заблокированы

# ответственными лицами (см. раздел 3.2).

# Роли и ответственность

* 1. Ответственность за соблюдение данного Положения возлагается на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации.
  2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Организации; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы Организации; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.