

- административные – каждые 60 дней;
- пользовательские – каждые 90 дней.

2.6. Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (*локальная вычислительная сеть, интернет, электронная почта*).

2.7. Пароли нельзя записывать на бумагу, в память телефона и т.д. Нельзя сообщать, передавать кому-либо пароль.

2.8 В ходе внутреннего аудита администратором информационной безопасности не реже двух раз в год возможна проверка соответствия пароля требованиям данной инструкции в присутствии пользователя: пользователь называет свой пароль, а проверяющий осуществляет ввод пароля и его проверку. После такой проверки требуется обязательная и немедленная смена пароля.

2.9. Пароли сервисных идентификаторов должны входить в процедуру управления паролями, включающую хранение их в защищенном месте периодическую смену (*1 раз в год*).

3. Ответственность.

3.1 Виновные в нарушении условий настоящей инструкции несут ответственность в соответствии с законодательством Российской Федерации, трудовым договором, должностной инструкцией.