

Хороший пароль должен содержать **минимум 10 символов**, чтобы его было сложно взломать (посчитайте, сколько символов в вашем пароле к социальной сети?)

Надёжный пароль должен содержать **12 символов и более** (ваш пароль на основную почту должен быть именно таким длинным!).

Сложный пароль должен содержать **три набора символов**: БОЛЬШИЕ и маленькие буквы, цифры, специальные символы [**PochtiSlozhniyParol123%!**]

Пароль должен быть **без общедоступной информации** (имя, фамилия, ник, важные даты, номера телефонов, ИНН, адреса, как свои, так и родственников — это НЕ для пароля! [**MarinaAV1965** – плохой вариант])

Пароль должен быть **без словарных слов** и без простых сочетаний слов (используйте малораспространённые слова или вообще несуществующие слова [**Абырвалг**])

Организация	ООО “Рога и Копыто”
Владелец сертификата	Иванов Иван Иванович
Логин	User1
Пароль	Pass1

Память инструмент не самый надёжный, поэтому лучше использовать один из нескольких проверенных способов надёжного хранения паролей.

Бумажный блокнот — да, даже ведущие специалисты по информационной безопасности признают этот вариант. Вот только храните такой блокнот подальше от любопытных глаз, да и пароли в нём храните в непонятном виде (об этом мы поговорим в следующий раз).

Менеджер паролей — специальная программа, которая помнит пароли за вас, вам лишь нужно помнить один пароль для доступа к остальной базе.

Текстовый документ — не самый удачный вариант хранения паролей, но его тоже можно использовать, если вы сможете хранить документ безопасно: в архиве под паролем, но это уже вариант менеджера паролей