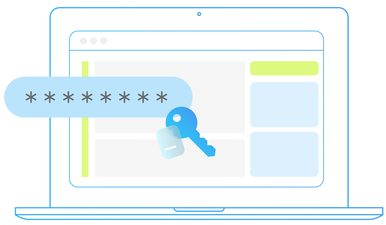
Битрикс24

Рекомендации по созданию и хранению надежного пароля



Правило надежного пароля — чем больше рандома, тем лучше

Пароль считается надежным, если в нем:

Не менее 12 символов
Длинные пароли сложнее взломать с помощью методов перебора (brute force).

Прописные и строчные буквы, цифры и специальные символы (например, !, S, #, %).
Разные типы символов делают пароль сложнее и труднее для взлома

Например:

G7$kL9@wQ2!m
zY8#nT4&bP1^
R3%vJ6*oL7!x

Пароль не должен содержать:

Легко узнаваемую информацию — имена, фамилии, номера телефонов, клички животных, названия организаций, даты рождения и т.д.
Такие данные легко найти или угадать, что делает пароль уязвимым.

Осмысленные слова, словосочетания, общепринятые аббревиатуры (даже набранным в другой раскладке клавиатуры)
Пароли, содержащие осмысленные слова, легче взломать с помощью словарных атак.

Очевидных замен — например, буквы «а» на @ или «о» на 0
Такие замены предсказуемы и не сильно увеличивают сложность пароля.

Например:

}qwerty12345{
P@$sw0rD
Ivanov1985

Не используйте один и тот же пароль для разных сайтов и сервисов. Это увеличивает риск взлома всех учетных записей, если один из сервисов будет скомпрометирован.

Как придумать надежный пароль?

1. Самый простой способ — воспользоваться сервисом для генерации паролей или в менеджере паролей.

2. Кодовые фразы — сочетание слов, не связанных друг с другом и расположенных в бессмысленном порядке.

3. Случайная последовательность символов

Например:

Lthtdj$7!Keyf&9Rjn
- Взяли слова на русскомязыке (Дерево, Луна, Кот)
- Переключили клавиатуру на английскую раскладку
- Написали слова в английской раскладке (Lthtdj, Keyf, Rjn).
- Добавили цифры (7, 9) и спецсимволы ($, !, &)

Например:

g5B#_kL8zQ&n
Можно запомнить, например, с помощью мнемонической фразы: «груши пять бананов решительно подчеркивают и добавляют киви лимон 8 зонтиков квакнули и напомнили».

Как хранить пароли?

• Используйте менеджер паролей, защищённый единым мастер-паролем. Не записывайте пароли на бумажках, в заметках, в легкодоступных файлах.

• Не сообщайте пароли никому: ни коллегам (в т.ч. системным администраторам), ни руководителям

Меняем пароли

Временный (предустановленный) пароль, выданный, например, при устройстве на работу, должен быть изменен незамедлительно при первом входе
Временные пароли могут быть известны другим сотрудникам, поэтому их нужно менять для безопасности.

Пароли должны меняться на периодической основе (не менее 4х раз в год)
Регулярная смена паролей снижает риск их компрометации и повышает общую безопасность системы.

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях
Это предотвращает использование схожих паролей, что делает их менее предсказуемыми и более устойчивыми к атакам.