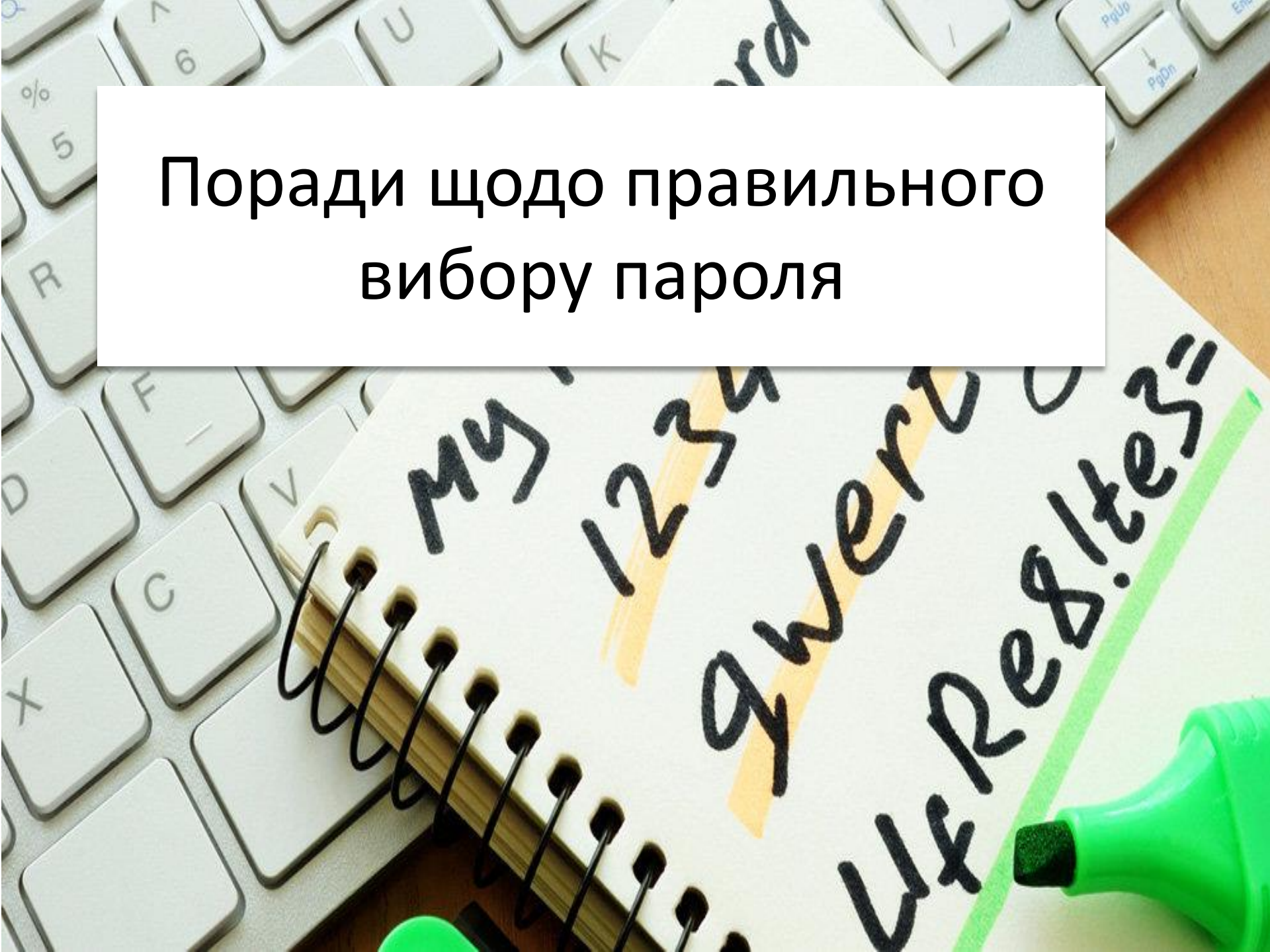
Поради щодо правильного вибору пароля



Пароль - умовне слово або набір знаків, призначений для підтвердження особи або повноважень.

Виходячи з підходів до проведення атаки можна сформулювати критерії стійкості пароля до неї

- Повинен бути довгими.
- Не повинен бути словниковим словом.
- Не повинен складатися тільки з загальнодоступної інформації про користувача.

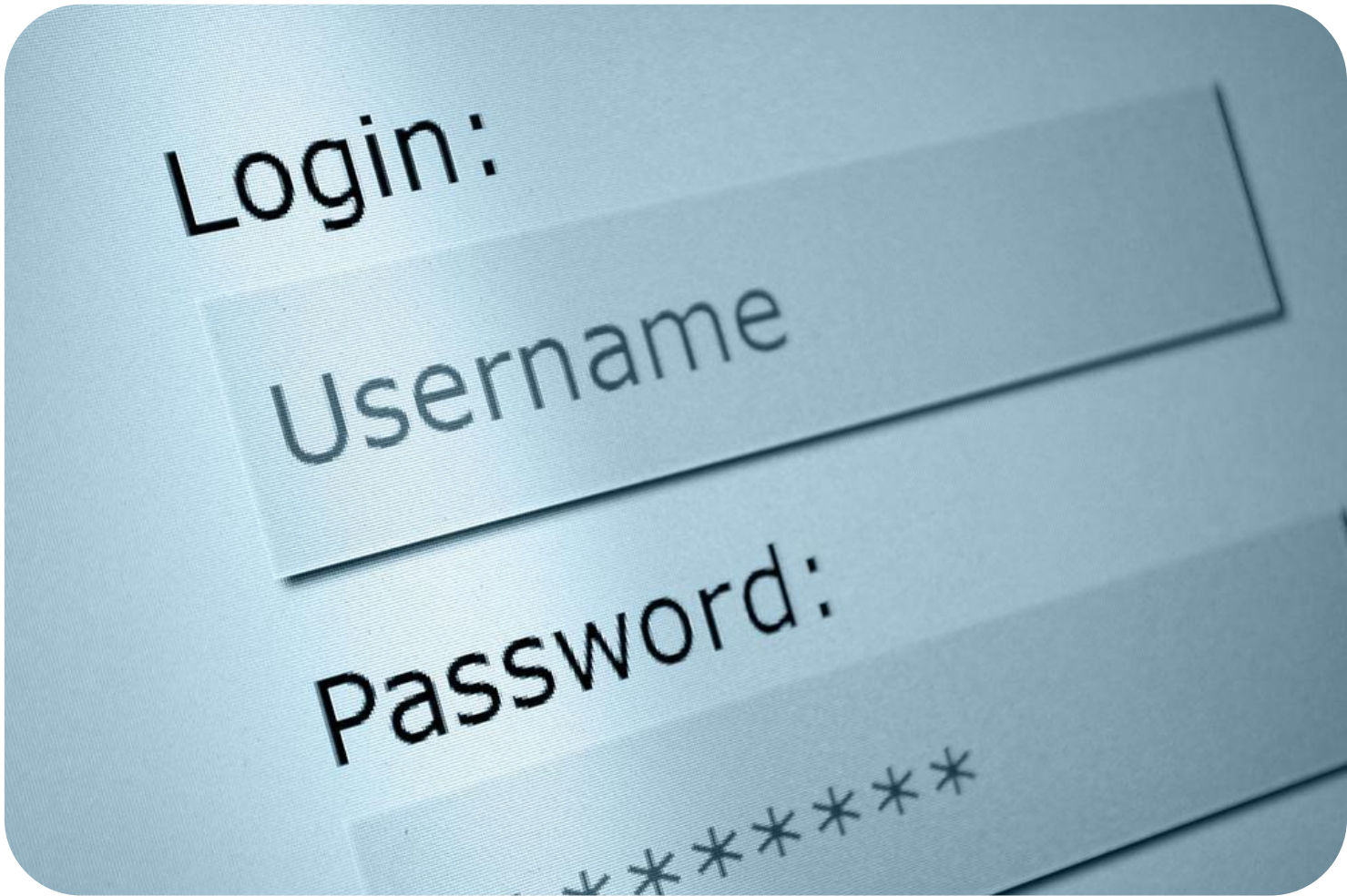
Вимоги до вибору і використання паролів

Вимоги до вибору пароля	Отриманий ефект
Встановлення мінімальної довжини пароля	Ускладнює завдання зловмисника при спробі підглянути пароль або підібрати пароль методом "тотального випробування"
Використання в паролі різних груп символів	Усложняет задачу злоумышленника при попытке подобрать пароль методом "тотального опробования"
Перевірка і відбраковування пароля за словником	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю

Вимоги до вибору пароля	Отриманий ефект
Встановлення максимального терміну дії пароля	Ускладнює завдання зловмисника по підбору паролів методом тотального випробування, в тому числі без безпосереднього звернення до системи захисту
Встановлення мінімального терміну дії пароля	Перешкоджає спробам користувача змінити пароль на старий після його зміни за попереднім вимогу
Ведення журналу історії паролів	Забезпечує додатковий ступінь захисту за попереднім вимогу

Вимоги до вибору пароля	Отриманий ефект
Застосування евристичного алгоритму, блокуючого паролі на підставі даних журналу історії	Ускладнює завдання зловмисника при спробі підібрати пароль за словарб або з використанням еврітічегоского алгоритму
Обмеження кількості спроб введення пароля	Перешкоджає інтерактивного підбору паролів зловмисником
Підтримка режиму примусової зміни пароля користувача	Забезпечує ефективність вимоги, що обмежує максимальним терміном дії пароля

Як популярних рекомендацій до складання пароля можна назвати використання поєднання слів з цифрами і спеціальними символами (#, $, * і т.д)



Перша мета може бути досягнута перевіркою встановлюється пароля на відповідність критеріям складності. Для такої перевірки існують автоматизовані рішення, як, наприклад, cracklib.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth sufficient pam_ldap.so use_first_pass
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so
account [default=die success=ok user_unknown=ignore service_err=ignore authinfo_unavail=ignore]       pam_ldap.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so

password    required     pam_cracklib.so try_first_pass retry=3 minlen=8 ucredit=-1 dcredit=-1 ocredit=-1 lcredit=-1 difok=4
password sufficient pam_ldap.so use_authtok
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
~
~
~
~
~
~
~
~
~
~
~
~
```

Друга мета - запобігання захоплення хеша переданого пароля і захист від багаторазових спроб входу в систему. Зазвичай накладають обмеження на число спроб в одиницю часу (fail2ban)