

Чек-лист: ошибки в паролях и как их исправить

Какие ошибки в паролях встречаются чаще всего (даты, имена, шаблоны, повторы), как их исправить и как защитить аккаунты сайта и команды. Версия от октября 2026 г. Автор: Владимир Родионов, tools.cetto.ru.

P1 критично	исправить в первую очередь
P2 важно	заметно влияет на результат, делать после P1
P3 желательно	улучшения по мере возможностей

Как пользоваться: проходите разделы по порядку и начинайте с P1. Главное правило: длинные случайные уникальные пароли в менеджере плюс двухфакторная защита. Цифры исследований приведены по пересказам и расходятся между изданиями; расчёты автора условные. Это не консультация по информационной безопасности.

1. Основа: как подбирают пароли

- ☐ Понятно, что подборщики сначала пробуют предсказуемые пароли: даты, имена, слова с цифрами на конце, клавиатурные цепочки и уже утёкшие **P1**
Исследования утёкших паролей
- ☐ Известно, что скорость подбора зависит от способа хранения пароля на сайте и условий атаки; онлайн-вход с ограничением попыток подбирается медленнее **P2**
Не путать с утёкшей базой хешей
- ☐ Принято, что придуманный человеком пароль почти всегда уступает случайному **P2**
Генератор паролей на tools.cetto.ru
- ☐ Цифры исследований Касперского и NordPass используются как ориентиры, источники и годы расходятся **P3**
Сверяйте с первоисточником

2. Содержимое пароля

- ☐ В пароле нет значимых дат (рождение, свадьба, годы) и их фрагментов **P1**
NCSC
- ☐ В пароле нет имён, кличек, команд, названия магазина, домена и логина **P1**
NIST: контекстные слова
- ☐ Нет шаблона Слово1! и замен букв на цифры и символы **P1**
Замены известны подборщикам
- ☐ Нет клавиатурных цепочек и последовательностей (qwerty, йцукен, 1234) **P1**
Частые пароли утечек
- ☐ Длина не меньше 16 символов для обычных аккаунтов; для пароля как единственного фактора не меньше 15 **P2**
NIST

3. Уникальность и хранение

☐	Каждый сервис имеет собственный пароль; повторов и «почти таких же» нет Подстановка учётных данных	P1
☐	Пароли хранятся в менеджере, а не в таблице, чате или заметках Менеджер паролей	P1
☐	Главный пароль менеджера — случайная фраза из 6 и более слов Выбирайте слова генератором или кубиком	P2
☐	Пароли не отправляются в мессенджерах и письмах открытым текстом; для передачи используется менеджер или одноразовая ссылка Пароль подрядчику	P2
☐	Бумажная запись хранится только в безопасном месте NCSC допускает	P3

4. Защита аккаунтов сайта

☐	Двухфакторная защита включена на домене, хостинге, CMS, почте, вебмастерах и рекламных кабинетах OWASP: основная мера	P1
☐	Пароли по умолчанию (admin, admin123, из инструкции хостинга) заменены у всех админов и сервисов Частые пароли мира	P1
☐	Для восстановления используются защищённые способы; контрольные вопросы с публичными ответами не применяются Данные для сброса тоже уязвимы	P2
☐	Почта для восстановления доступов защищена надёжнее остальных аккаунтов Ключ ко всему	P2
☐	Список аккаунтов с ответственными ведётся в одном документе Домен, хостинг, CMS, кабинеты	P3

5. Команда и подрядчики

☐	У каждого сотрудника и подрядчика своя учётная запись; общих паролей нет Можно отозвать и понять, кто что сделал	P1
☐	При уходе сотрудника или подрядчика доступы отозваны в тот же день, пароли общих сервисов заменены Регламент ухода	P1
☐	Права выданы по задачам и на срок работы Минимально необходимые	P2
☐	Правила паролей изложены в одной странице регламента и известны команде Повторяйте раз в квартал	P3

6. Свой сайт и проверка

- | | | |
|--------------------------|--|-----------|
| ☐ | Если на сайте есть личные кабинеты, пароли пользователей сверяются со списком утёкших, словарными словами и названием сервиса
NIST | P1 |
| ☐ | Сайт разрешает длинные пароли, пробелы и вставку из менеджера; обязательные правила состава не навязываются
NIST и OWASP | P2 |
| ☐ | Смена пароля выполняется при подозрении на утечку или простом пароле, а не по календарю
NIST и OWASP | P2 |
| ☐ | Раз в квартал пересматривается список доступов и срок домена и хостинга
Whois домена на tools.cetto.ru | P3 |

Подсчёт результата

Всего пунктов: 27, из них P1: 12. Запишите, сколько выполнено: P1 _____ из 12; P2 _____; P3 _____.
Если не выполнен раздел 4 про защиту аккаунтов, начните с него: без двухфакторной защиты на почте, домене и хостинге взлом одного пароля открывает всё.

Сомневаетесь, что доступы к сайту защищены?

В рамках SEO-аудита проверю доступы к CMS, хостингу, домену и кабинетам, двухфакторную защиту, открытые админки и признаки взлома и дам план исправлений. PDF-отчёт на 30–50 страниц, задания для программистов и созвон. От 30 000 ₽, 3–5 рабочих дней для небольшого сайта.

Подробнее об услуге: cetto.ru/services/seo-audit

Написать в Telegram

t.me/cettomarketing

Пояснения к пунктам и разбор типичных ошибок: tools.cetto.ru/blog/oshibki-parolej/. Чек-лист распространяется бесплатно, при цитировании указывайте источник.