

Чек-лист: пароли и доступы сайта

Как создавать надёжные пароли, настроить многофакторную защиту, защитить доступы магазина и построить форму входа по современным рекомендациям. 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: длина, уникальность, менеджер паролей и двухфакторная защита. Рекомендации Роскачества даны по пересказам, цифры расходятся. Расчёты стойкости верны только для полностью случайных паролей. Разработку формы входа доверьте специалисту по безопасности.

1. Основа: что считается надёжным

- | | | |
|--------------------------|---|-----------|
| ☐ | Понятно, что длина важнее сложности: по NIST пароль как единственный фактор не короче 15 символов, как часть MFA не короче 8
<small>NIST SP 800-63B</small> | P1 |
| ☐ | Понятно, что обязательные правила состава и плановая смена паролей по NIST запрещены; смена нужна при признаках компрометации
<small>NIST и OWASP</small> | P1 |
| ☐ | Известно, что рекомендации Роскачества в публикациях называют 16–17 символов; цифры в источниках расходятся
<small>Сверьте с публикацией Роскачества</small> | P2 |
| ☐ | Принято, что пароль не защищает от фишинга; нужна многофакторная защита
<small>NIST</small> | P3 |

2. Создание паролей

- | | | |
|--------------------------|--|-----------|
| ☐ | Пароли длинные (16 символов и больше), случайные и уникальны для каждого сервиса
<small>Менеджер паролей</small> | P1 |
| ☐ | В паролях нет личных данных: имён, дат, кличек, названия сайта и логина
<small>Контекстные слова входят в запрещаемые</small> | P1 |
| ☐ | Для главного пароля (менеджер, почта, устройство) используется парольная фраза из случайных слов (от 5–6)
<small>Слова выбирает генератор или кубик</small> | P2 |
| ☐ | Пароль не придумывается по схеме с заменой букв и номерами «Пароль1, Пароль2»
<small>Человеческие схемы предсказуемы</small> | P2 |
| ☐ | Новый пароль проверен по базе утёкших паролей безопасным способом (k-anonymity)
<small>Не вводите действующие пароли в непроверенные сервисы</small> | P3 |

3. Генератор и хранение

☐	Генератор паролей работает в браузере и использует <code>crypto.getRandomValues</code> , а не <code>Math.random</code> Проверьте вкладку Network	P1
☐	Пароли хранятся в менеджере паролей, а не в заметках, таблицах и мессенджерах Генератор паролей на tools.cetto.ru	P1
☐	Резервный доступ к менеджеру продуман: главный пароль помнится, есть защита второго фактора Риск потери доступа	P2
☐	Для общих доступов используется общее хранилище менеджера или временные доступы, а не пересылка паролей Подрядчики и сотрудники	P3

4. Многофакторная защита

☐	Включена двухфакторная защита на почте домена, регистраторе, хостинге, админке CMS, вебмастерах и рекламных кабинетах Почта защищается сильнее всего	P1
☐	Для критичных аккаунтов используется приложение-аутентификатор или физический ключ, а не только SMS NIST: один вариант должен быть устойчив к фишингу	P2
☐	Резервные коды восстановления сохранены безопасно Иначе потеря доступа	P2
☐	Для Госуслуг и банковских сервисов включена двухфакторная защита Рекомендации Роскачества	P3

5. Доступы сайта и команды

☐	У каждого сотрудника и подрядчика отдельная учётная запись с минимальными правами; общих учёток нет Админка CMS, FTP, SSH	P1
☐	При увольнении и окончании работ подрядчика доступы отзываются в тот же день Контрольный список	P1
☐	Доступы к вебмастерам, аналитике и рекламе выданы только нужным людям Проверяйте раз в квартал	P2
☐	Домен и хостинг оформлены на компанию, а не на личный аккаунт сотрудника; срок оплаты отслеживается Whois на tools.cetto.ru	P2
☐	Установлено оповещение о входах и уведомления о подозрительных действиях Если поддерживается	P3

6. Если вы делаете форму входа

☐	Система принимает пароли не менее 64 символов, любые печатные символы, пробелы и Unicode; не обрезает пароль молча NIST и OWASP	P1
☐	Нет обязательных сочетаний регистров, цифр и спецсимволов; нет принудительной смены по расписанию Запрещено NIST	P1

- | | | |
|--------------------------|--|-----------|
| ☐ | Новые пароли сверяются со списками утёртых, словарных и контекстных слов; пользователю объясняется причина отказа
Pwned Passwords или локальная копия | P1 |
| ☐ | Пароли хранятся в солёном виде подходящей функцией хеширования и передаются только по защищённому каналу
Соль не менее 32 бит по NIST | P1 |
| ☐ | Разрешены менеджеры паролей, автозаполнение и вставка; есть опция «показать пароль»
Рекомендации NIST | P2 |
| ☐ | Ограничено число неудачных попыток; верхняя граница не более 100, предпочтительно строже
NIST | P2 |
| ☐ | Предложена многофакторная аутентификация, один из вариантов устойчив к фишингу
Реализацию доверьте специалисту по безопасности | P3 |

Подсчёт результата

Всего пунктов: 29, из них P1: 13. Запишите, сколько выполнено: P1 _____ из 13; P2 _____; P3 _____.
Если не выполнен раздел 4 про многофакторную защиту, начните с него: почта домена и админка — главные точки взлома.

Хотите проверить сайт на признаки взлома и технические риски?

В рамках SEO-аудита проверю признаки взлома и нарушений, HTTPS, служебные страницы, robots.txt и noindex, уведомления вебмастеров и дам рекомендации по доступам. PDF-отчёт на 30–50 страниц, задания для программистов и созвон. От 30 000 Р, 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/nadezhnyy-parol/. Чек-лист распространяется бесплатно, при цитировании указывайте источник.