



НОВОСТИ IT-ТЕХНОЛОГИЙ

ДАЙДЖЕСТ № 21

ЭКСПЕРТЫ СОСТАВИЛИ РЕЙТИНГ САМЫХ НЕНАДЕЖНЫХ ПАРОЛЕЙ 2017

Эксперты аналитической компании SplashData составили рейтинг самых ненадежных паролей 2017 года. Проанализировав более 5 млн паролей, взломанных в текущем году, специалисты установили, что самым ненадежным паролем в очередной раз стал пароль «123456». Вторую строчку рейтинга ненадежных паролей заняла комбинация «password», третью — «12345678». Далее следуют пароли «qwerty» и «12345». Помимо вариантов цифровых комбинаций, рейтинг ненадежных паролей представлен следующими паролями: «football», «admin», «welcome», «login», «abc123», «dragon», «password» и «master». «Новичками» среди худших паролей года также стали пароли «letmein», «iloveyou», «monkey», «starwars», «hello», «freedom», «whatever», «qazwsx» и «trustno1». **Источник:** <https://iz.ru>



РАДИУС ДЕЙСТВИЯ BLUETOOTH 5 ДОСТИГАЕТ 800 МЕТРОВ.

Стандарт Bluetooth 4.0 был запущен в массовое использование еще в 2010 году, и сейчас его уже считают устаревшим, поскольку на смену ему приходит более современное поколение беспроводной связи. Увеличения радиуса действия до 800 метров удалось добиться посредством перехода к новой технологии, которая включает наработки Wi-Fi. Разработчики отмечают, что радиус активности Bluetooth 5 может сокращаться в случае наличия помех.



Для «умного дома» Bluetooth 5 станет незаменимой технологией, ведь с его помощью можно наладить взаимодействие всех имеющихся в доме устройств. В новом стандарте возросла также и скорость передачи данных, а также их объем. Это позволит управляющему приборам блоку оперативно реагировать на любые изменения.

Источник: <http://actualnews.org>

GOOGLE CHROME ЗАБЛОКИРУЕТ АВТОМАТИЧЕСКОЕ ВОСПРОИЗВЕДЕНИЕ

С новой функцией браузера пользователей не будет беспокоить внезапно включившийся видеоролик. Google готовит масштабное обновление браузера Chrome. Одним из нововведений будет запрет автоматического воспроизведения видео. Об этом сообщает компания в официальном блоге. Такая функция впервые появилась у Apple в macOS High Sierra. Она предотвратит воспроизведение видеоролика на открытом сайте. Активировать её можно будет в настройках. Единственный минус — включать её надо будет на каждом сайте отдельно, а не сразу на всех. Кроме того, Google усовершенствует защиту от всплывающих окон. Ранее некоторые пользователи жаловались, что действующая защита не работает с некоторыми сайтами. Сейчас компания тестирует обновления в бета-версии Chrome 64. Ожидается, что обновление выйдет в ближайшие выходные.



Источник: <https://life.ru>



<https://vk.com/maudomuk>



https://www.instagram.com/maudomuk_kirishi/

Немного компьютерной грамотности - рекомендации по составлению надежных паролей

При составлении паролей рекомендуется придерживаться следующих правил:

1. Пароль должен содержать не менее шести символов.
2. В состав пароля могут входить цифры, латинские буквы, пробелы и специальные символы («», «>», «?», «!», «<», «>», «*» и др.).
3. Рекомендуется составлять пароль из смешанного набора цифровых и буквенных (прописных и строчных) символов.

Не используйте в качестве пароля:

1. Общеупотребительные слова и устойчивые словосочетания.
2. Наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, такие как: **qwerty**, **123456789**, **qazxsw** и т. п.
3. Персональные данные: **имена и фамилии, адреса, номера паспортов, страховых свидетельств** и т. п., пароли, созданные для доступа к другим программам (электронная почта, базы данных и пр.).

Источник: <https://support.kaspersky.ru/viruses/general/3730>

Пример алгоритма создания паролей №1

1. Сделайте начало (сердину или конец) всех паролей одинаковым, например, **18N!p1n**.
2. К нему добавьте части, которые ассоциируются с конкретным сервисом, для которого этот пароль предназначен, например, для почты — **mail**. В результате получим **18N!p1nmail**.
3. Однако при хищении паролей злоумышленником алгоритм может быть легко определен. Поэтому для регистрации на подозрительных сервисах используйте любую другую отвлеченную комбинацию символов.

Пример алгоритма создания паролей №2

Петров Иван Сергеевич 18 апреля 1982 года рождения для регистрации на сайте **superpochta.ru** может задать следующую последовательность:

1. Последние четыре символа адреса прописными буквами (**superpochta.ru = A.RU**).
2. Сумма даты и месяца рождения с количеством согласных букв в адресе сайта (**18+4+7=29**).
3. Предпоследние три буквы отчества, набранные транслитом (**Сергеевич = evi**).
4. В результате получается пароль **A.RU29evi**.

Используя подобные алгоритмы, можно генерировать огромное количество сложных паролей.