Муниципальное автономное учреждение дополнительного образования
«Межшкольный учебный комбинат»

ДАЙДЖЕСТ №238

30.01.2026

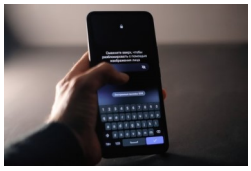
НОВОСТИ IT-ТЕХНОЛОГИЙ

Nord Clan обновила платформу ML Sense

Компания Nord Clan представила обновление платформы машинного зрения ML Sense. Основным вектором развития стало смещение фокуса с разработки узкоспециализированных систем контроля качества на создание модульной платформы, позволяющей решать комплекс задач по безопасности, операционной логистике и управлению эффективностью на базе единого цифрового контура. Обновление отражает растущий рыночный запрос, когда промышленные предприятия рассматривают технологии компьютерного зрения и анализа данных не как точечный инструмент, а как компонент для системного повышения устойчивости производственных процессов. ML Sense подтверждает статус ведущего отраслевого решения, став победителем ключевых рейтингов 2025 года.

Источник: https://www.itweek.ru

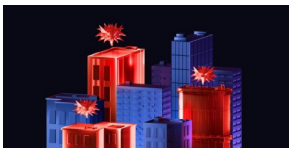
Назван самый популярный пароль 2025 года



Самым популярным паролем 2025 года в интернете стала числовая последовательность 123456, соответствующий рейтинг опубликован Институтом Хассо Платтнера. Рейтинг базируется на анализе баз учетных записей, распространяющихся в даркнете. Кроме 123456, в числе самых популярных паролей 123456789, 565656 и 12345678. В десятку также вошли комбинации с простыми словами, включая qwerty, hallo123, kaffeetasse, passwort и lol123. Эксперты рекомендуют пользователям применять менеджеры паролей, использовать уникальные комбинации длиной более 15 символов для каждого сервиса и включать двухфакторную аутентификацию.

Источник: https://info.sibnet.ru

Хакеры Vortex Werewolf маскируются под Telegram



Вредоносная кампания длилась с декабря 2025 года по январь 2026 года. Злоумышленники присылали жертвам фишинговые ссылки, замаскированные под файловое хранилище Telegram. Пользователю приходило сообщение со ссылкой на якобы важные рабочие документы. Ссылка выглядела как файловое хранилище Telegram. При этом злоумышленники могли отправлять такие сообщения напрямую в мессенджере или через электронную почту. Если жертва переходила по ссылке, начинался процесс «восстановления доступа» к аккаунту Telegram. У пользователя запрашивали код подтверждения с другого устройства, а при включенной двухфакторной аутентификации — еще и облачный пароль. Якобы для того, чтобы документ мог отобразиться полностью. На самом же деле атакующие получали доступ к активной сессии мессенджера жертвы со всей перепиской и контактами.

Источник: https://xakep.ru

https://vk.com/maudomuk

НЕМНОГО КОМПЬЮТЕРНОЙ ГРАМОТНОСТИ

Уязвимость нулевого дня, 0-day (англ. zero day) — термин, обозначающий неустранённые уязвимости, а также вредоносные программы, против которых ещё не разработаны защитные механизмы. Сам термин означает, что у разработчиков было 0 дней на исправление дефекта: уязвимость или атака становится публично известна до момента выпуска производителем ПО исправлений ошибки (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от неё). В этой связи более верным был бы перевод «уязвимость нуля дней».

Источник: https://ru.wikipedia.org