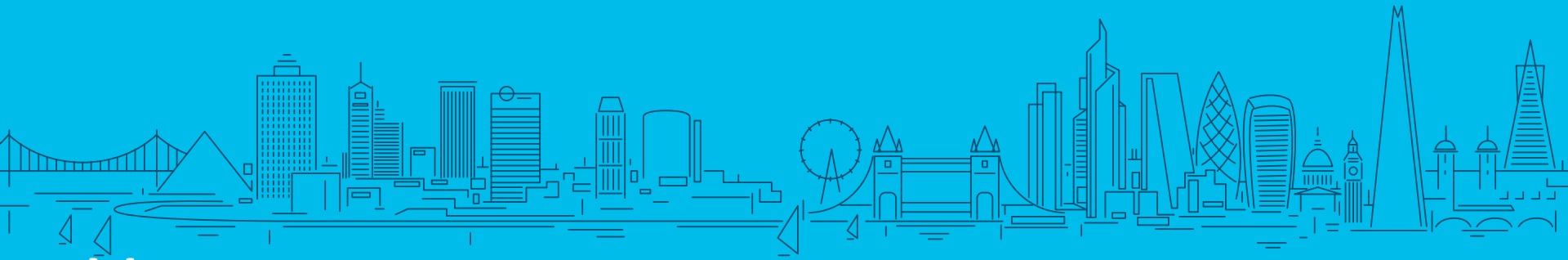


Угрозы завтрашнего дня, ваше место в истории кибератак

Big Data, блокчейн, AI, роботы, квантовые вычисления, биометрия, IoT и вот это вот всё…

Назим Латыпаев

Пожелания на день

- Расслабьтесь
- Пожалуйста, переведите мобильные телефоны в режим виброзвонка.
- Шампанское после танго, можно пить только вместе с нами.
- Активно учувствуйте в дискуссиях.
- Задавайте острые вопросы. Используйте блокноты для анонимных вопросов
- Пожалуйста, заполните анкеты.
- Учувствуйте в розыгрыше.

„У тебя не может быть лучшего завтра, если ты все время думаешь о вчерашнем дне.“

Чарльз Франклин Кеттеринг
(186!!!)

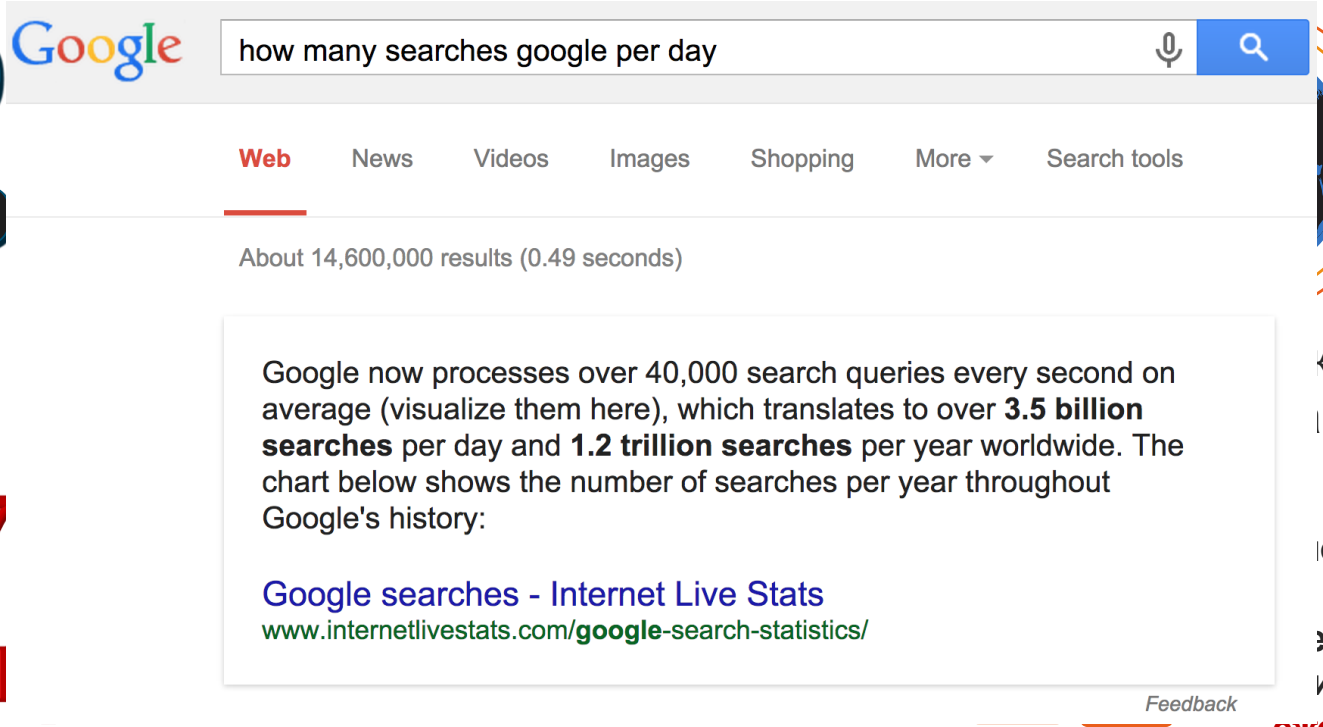
Оцените масштаб проблемы

19

угр

7

уг



кивает

человек

о 3-х угроз

каждого

еля Земли

иходится

ежедневно

Самые распространенные киберугрозы

Шифровальщики

Самая »денежная» угроза у злоумышленников, приносящая им около 1 миллиарда долларов в год

Утечки данных

Утечки персональных данных пациентов, тарифов на услуги, результатов исследований больно бьют не только по карману, но и по репутации

Фишинг

Самая популярная угроза, реализуемая через e-mail (и Web), с которой начинается 95% всех инцидентов безопасности

На самом деле угроз гораздо больше ☹

Угрозы или риски?

Примеры рисков цифровой экосистемы

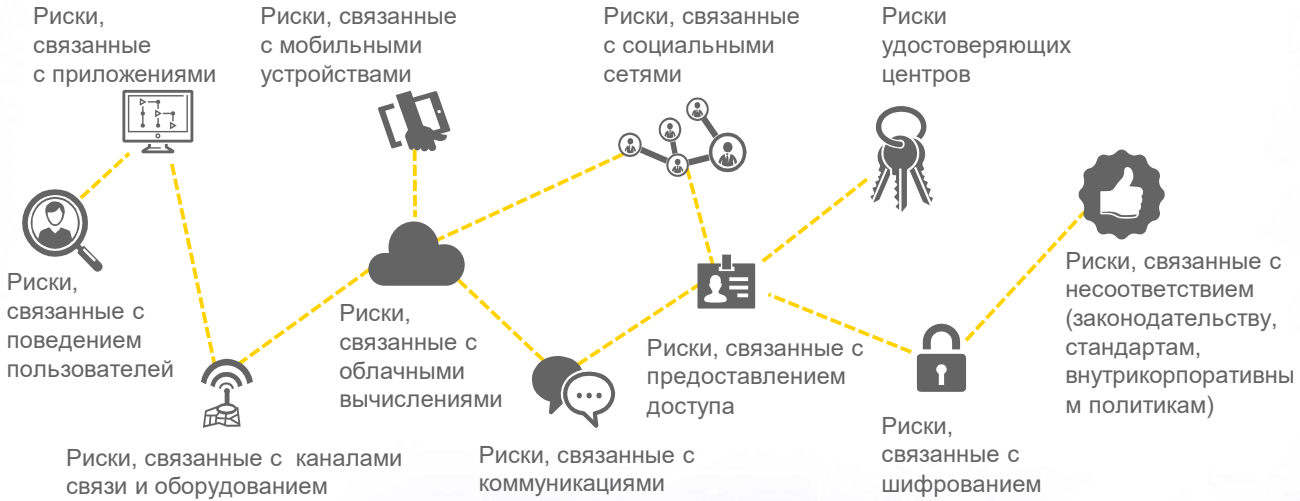
Digital-стратегия бизнеса

Digital-инкубаторы и инновации

Трансформация и применение опыта Digital

Цифровая цепочка поставок и операционная эффективность

Цифровое доверие



Цифровое доверие — свод практик для управления рисками в цифровой экосистеме.

В домене затрагиваются как организационные механизмы, так и технические средства / инструменты, позволяющие снизить уровень негативного воздействия в случае реализации риска

Уверенность в Digital

Отличие инноватора / CDO от безопасника / хакера

	Исследователь	Безопасник / хакер
Основной фокус	Что произойдет в случае нормальных входных данных?	Что произойдет в случае аномальных входных данных?
Отказ в редких условиях и сочетаниях	Что-то, что я смогу игнорировать или чем я могу **пренебречь**	Что-то, что я смогу использовать для **нарушения**

Internet of Things

Интернет-вещей уязвим к атакам больше, чем кто бы то ни был

Кардиостимуляторы

Принтеры

Автомобили

Умные часы

Газовые котлы загородных домов

Двери

Сантехника

Стельки

Секс-роботы

Холодильники…

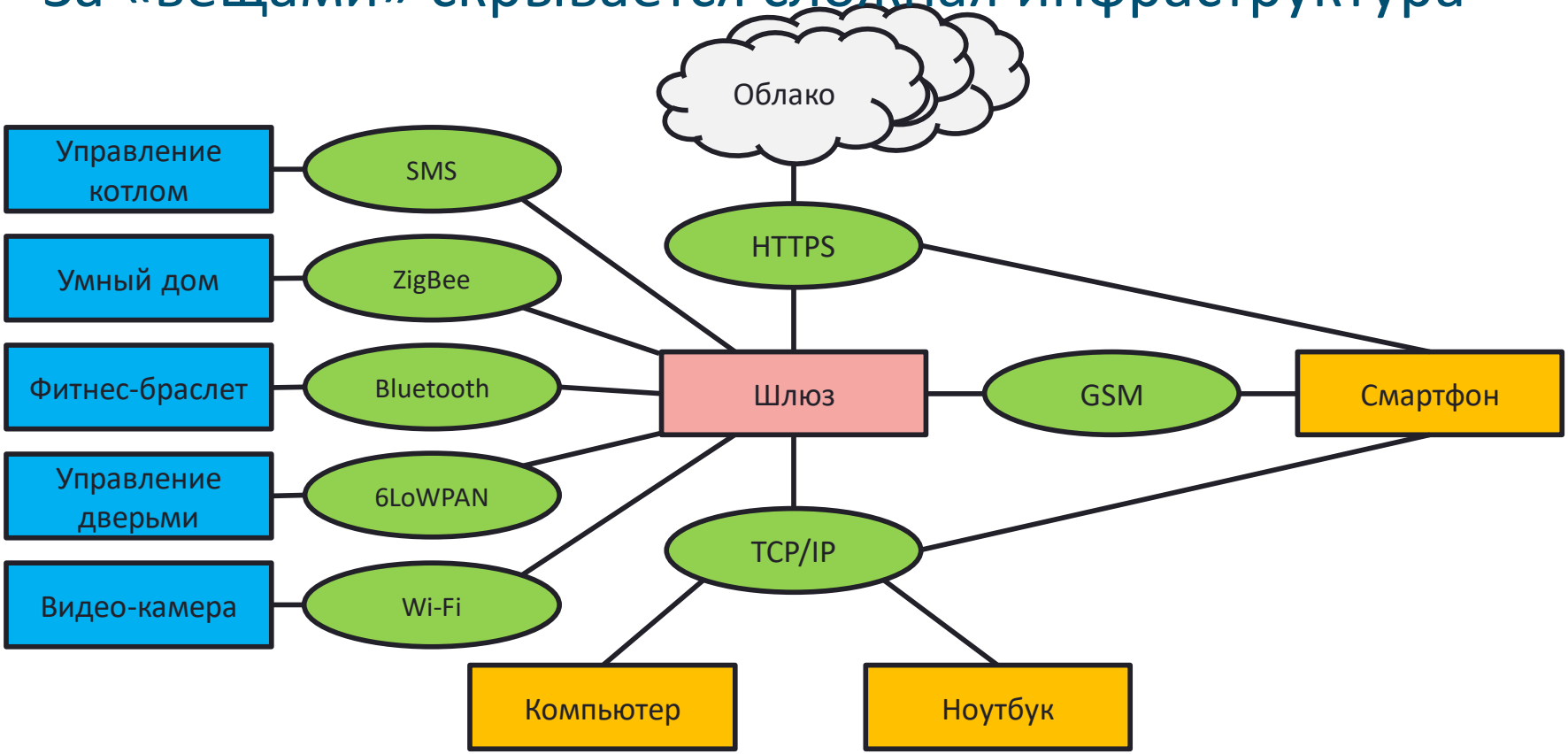
Новости от 29 мая

Исследование Лаборатории Касперского

На фитнес-трекер или умные часы можно загрузить вредоносный код, который будет не только отслеживать перемещение владельца, но и «красть» логины/пароли (точность 96%) и PIN-коды (точность 87%)

Фитнес-браслет

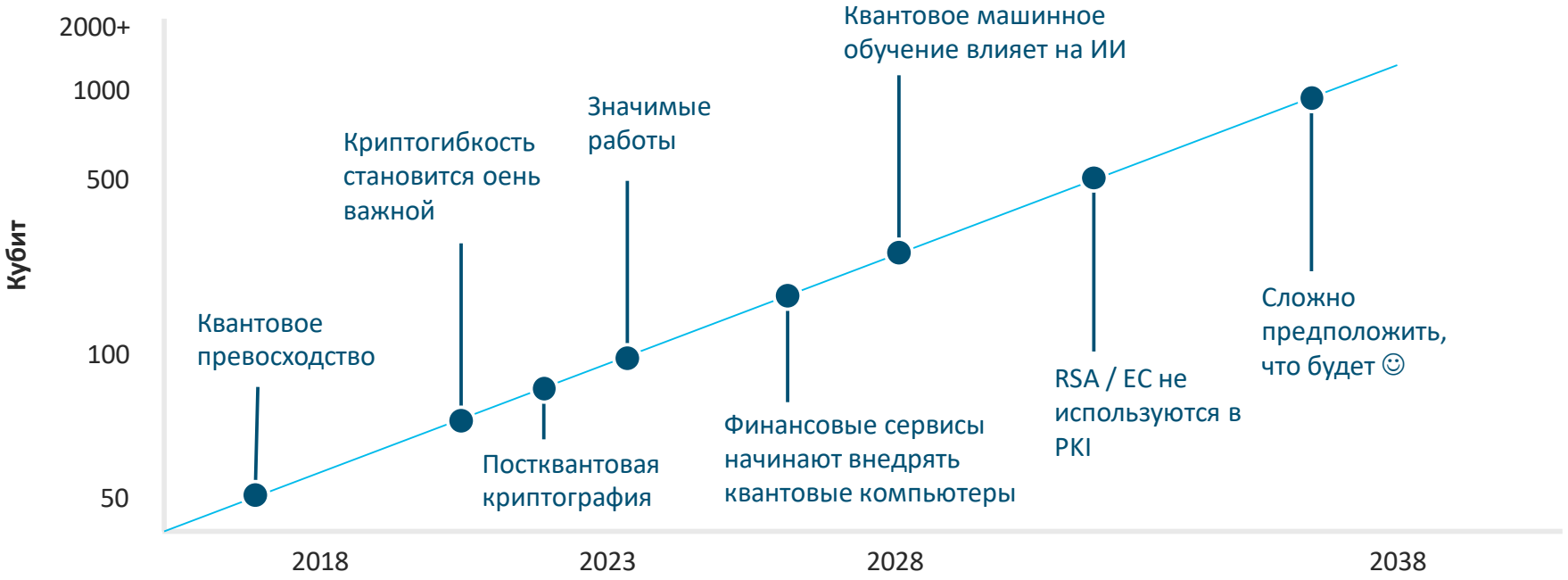
За «вещами» скрывается сложная инфраструктура



Пока лучше не становится...

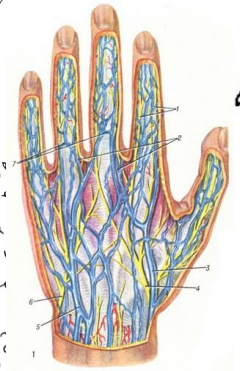
Квантовые компьютеры

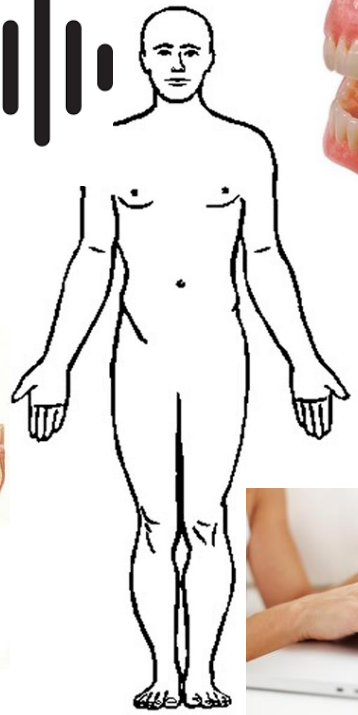
2027-й год – конец современной криптографии?

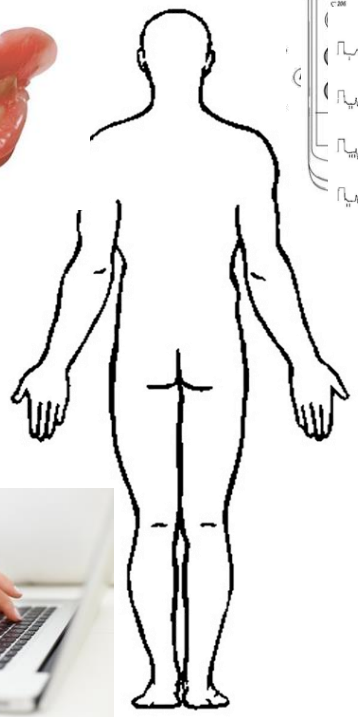


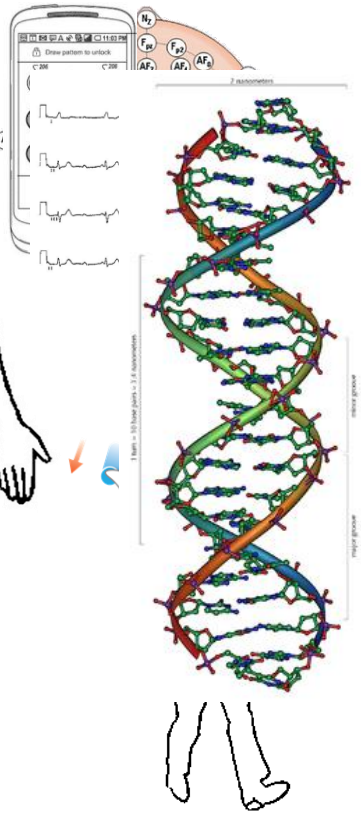
Биометрия

Что может стать идентификатором?









Взлом «расчленением»

Отрезанный палец

- Как поддерживать температуру тела?

Отрезанная рука

- Как поддерживать кровообращение?

Вырванный глаз

Взлом дублированием

Муляжи пальцев

- Для борьбы со сканерами - заполнение муляжа теплой водой и подача электричества для эмуляции «жизни»

Записанный голос

3D-изображения людей

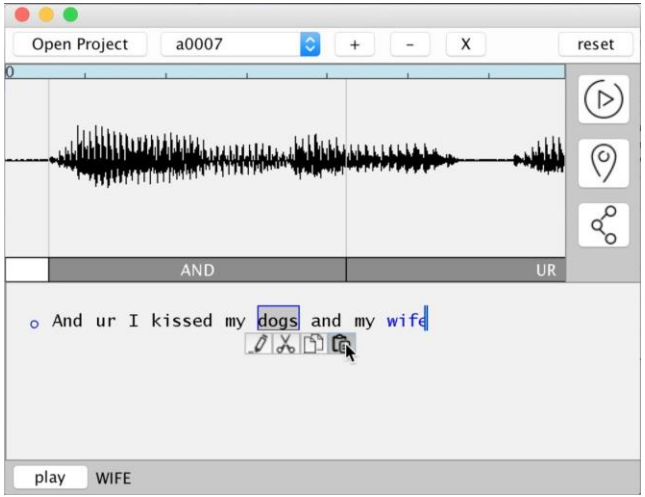
Люди-имитаторы

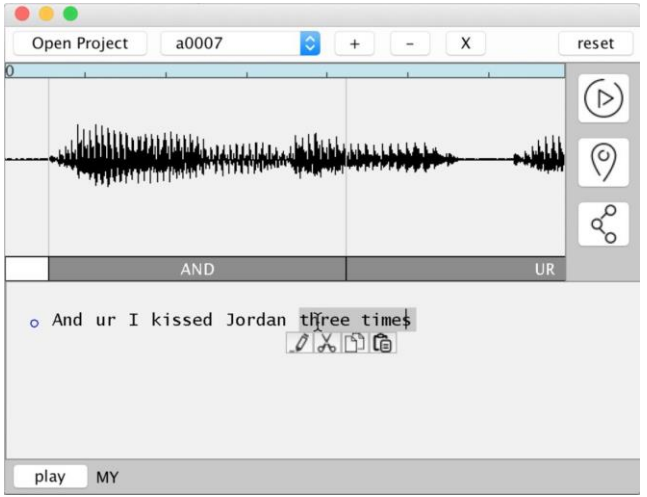
Клонирование

- Перспектива будущего

Аудиоредактор Adobe VoCo

Аудиоредактор Adobe VoCo (пока проект) позволяет «произнести» все, что угодно, голосом человека, которого предварительно «прослушивали» в течение 20 минут и более





Угрозы подмены

Селфи как угроза биометрии



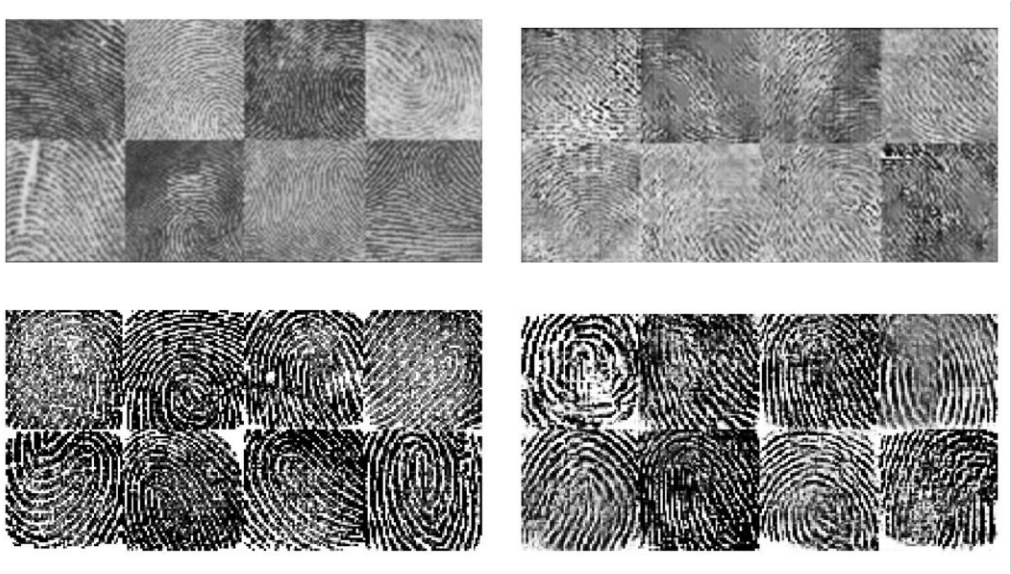



Проект Deep Master Prints

Нейросеть научилась генерить фальшивые отпечатки пальцев

Выборка на 5400 человек

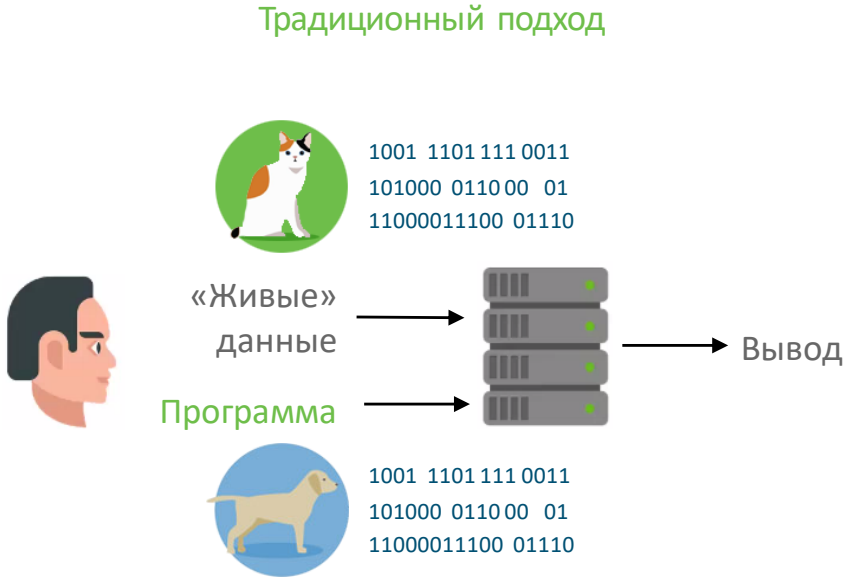
Эффективность системы для датчиков низшего уровня дактилоскопической идентификации (FAR = 0,01%) – 23%, для высшей (FAR – 1%) – 1,3%



Искусственный интеллект

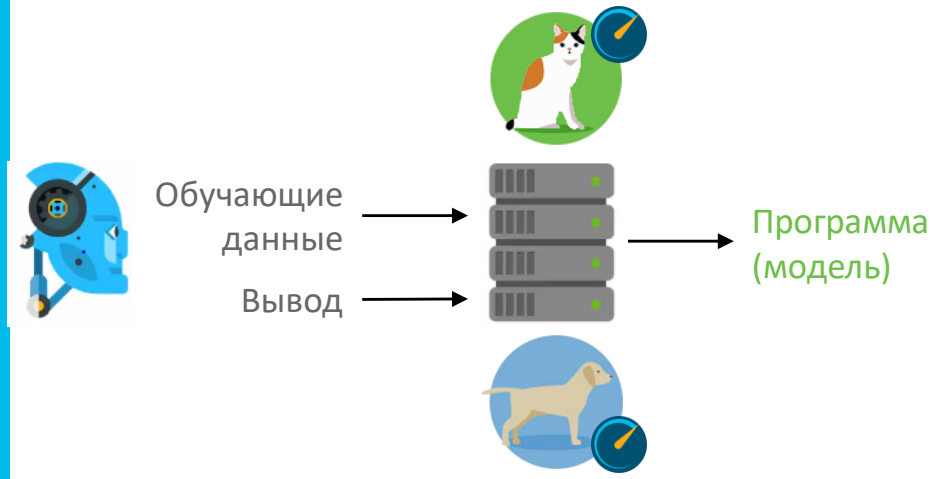
При традиционном подходе мы распознаем и заранее заносим в «черные списки» что-то плохое

Любая проблема, которая может быть «оцифрована» и имеет большие объемы собранных данных является кандидатом для машинного обучения



ML фундаментально отличается от обычной разработки – вы даете машине ответы и она пишет по ним код (модель)

Машинное обучение наиболее эффективно для новых и неизвестных данных

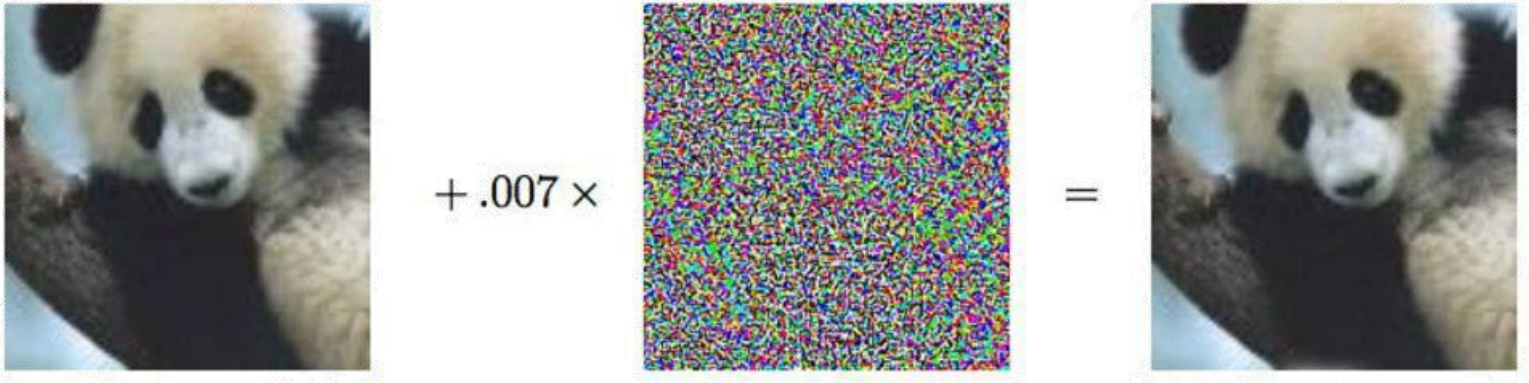


Когда злоумышленник знает как работает ИИ

Знак «СТОП» в 100%

Знаки распознаются автомобилями с автопилотом как «снижение скорости» в 100% случаев

Когда злоумышленник знает как работает ИИ



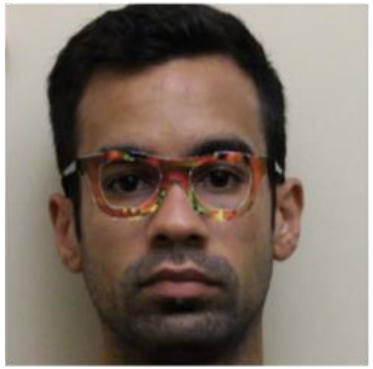
«Панда»
57,7% уверенности

«Гиббон»
99,3% уверенности

Именно поэтому контрольные точки проверки денежных купюр или биометрических данных держатся в секрете

Когда злоумышленник знает как работает ИИ





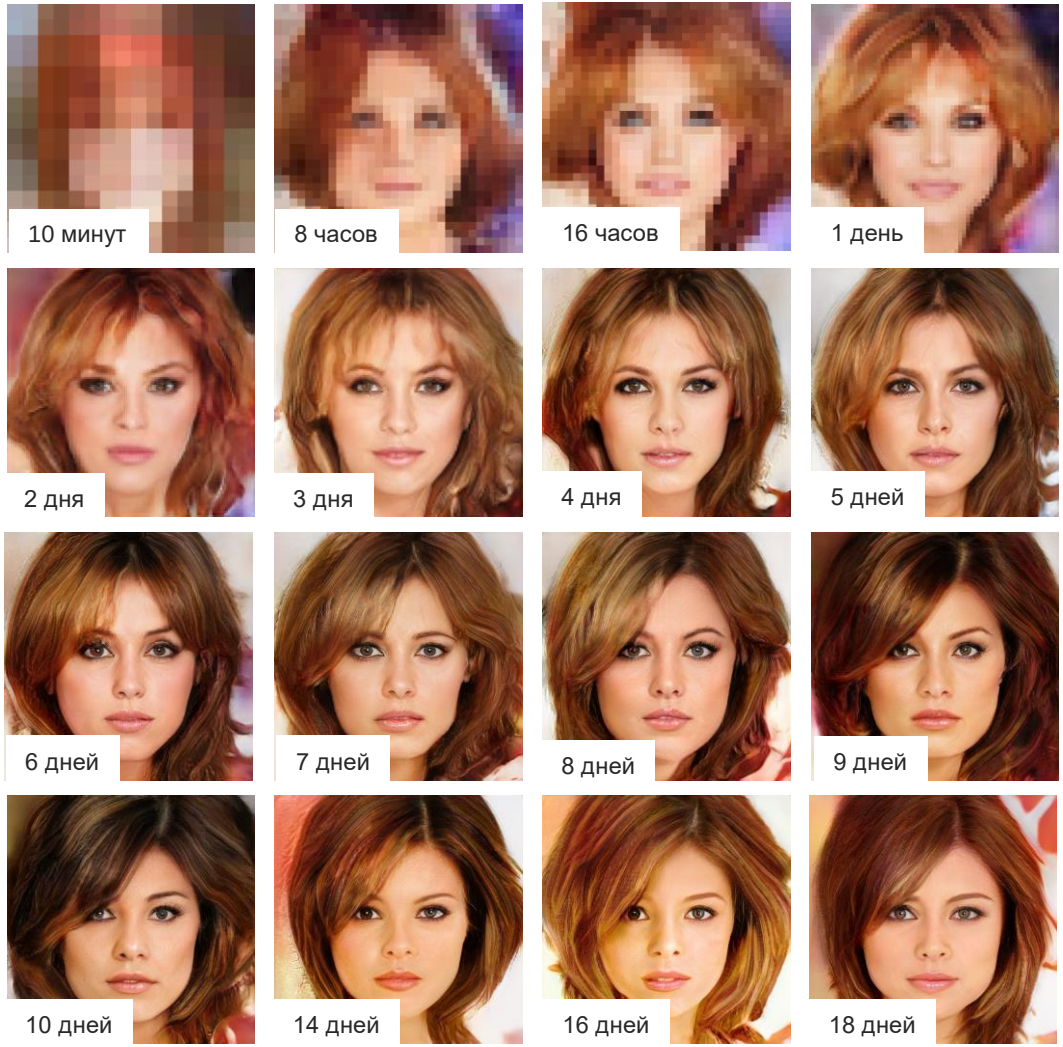

Когда злоумышленник знает как работает ИИ

Компания Microsoft запустила основанного на машинном обучении чат-бота Тай в 2016-м году

Группа злоумышленников, не имея доступа к исходным кодам, научила чат-бота ругаться и грубо общаться с пользователями

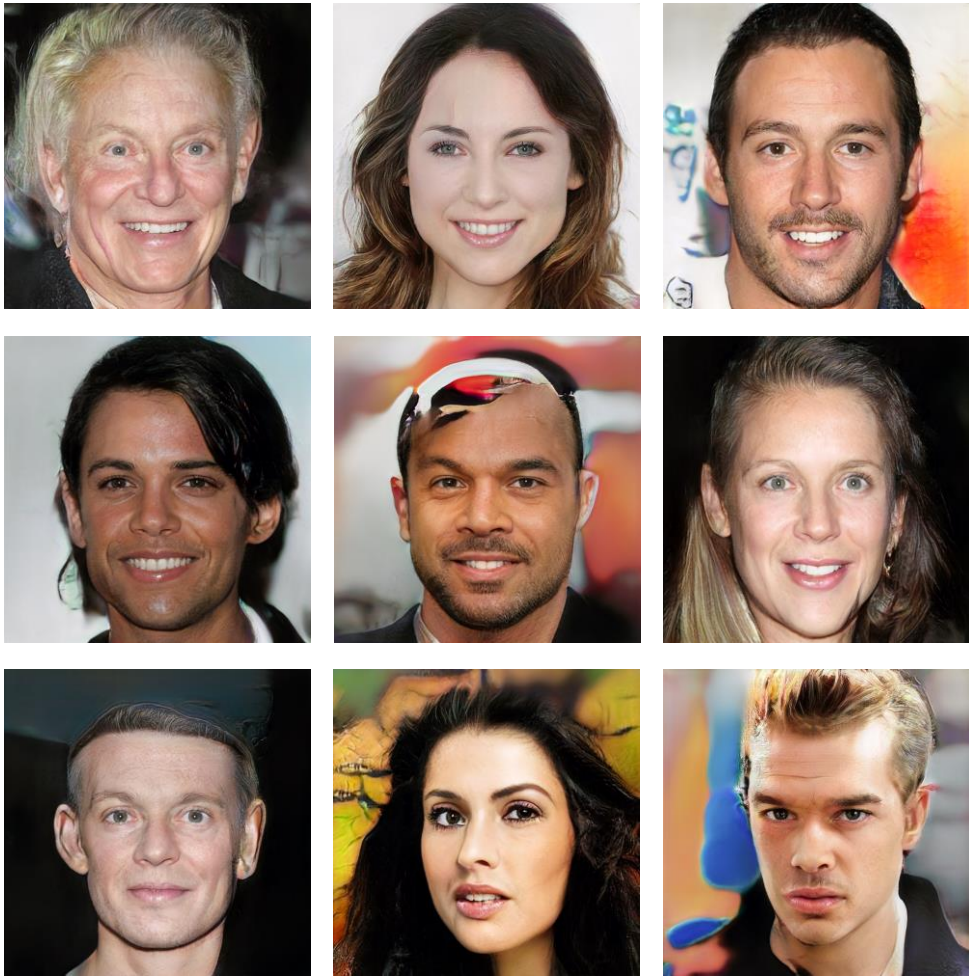
Давайте пройдем тест
Какое из двух фото синтезированное?

Компания Nvidia создала нейросеть, которая «научилась» за 18 дней создавать реалистичные фотографии людей



Вторая нейросеть Nvidia училась распознавать синтезированные фотографии

Нейросеть дала сбой и посчитала данные синтезированные фотографии реальными



А вы хотите стать «героем» порно?

Подмена лица порноактрисы в динамике на лицо актрисы Галь Гадот

Synthesizing Obama: Learning Lip Sync from Audio

Supasorn Suwajanakorn
Steven M. Seitz
Ira Kemelmacher-Shlizerman

University of Washington

SIGGRAPH 2017
http://grail.cs.washington.edu/projects/AudioToObama/

„Мои интересы находятся в будущем, потому что я собираюсь провести там оставшуюся часть моей жизни.“

Чарльз Франклин Кеттеринг

Спасибо!