Издаётся с 1924 года

РАДИО®

"Радиолюбитель"—"Радиофронт"—"Радио"

6•2020

МАССОВЫЙ ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

"Radio" is monthly publication on audio, video, computers, home electronics and telecommunication

12+

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ: ЗАО «ЖУРНАЛ «РАДИО»

Зарегистрирован Министерством печати и информации РФ 01 июля 1992 г.

Регистрационный ПИ № ФС77-50754

Адрес редакции: 107045, Москва, Селивёрстов пер., 10, стр. 1

Тел.: (495) 607-31-18. Факс: (495) 608-77-13

E-mail: **ref@radio.ru**

Группа работы с письмами — (495) 607-08-48

Отдел рекламы — (495) 607-31-18; e-mail: **advert@radio.ru**

Распространение — (495) 607-77-28; e-mail: **sale@radio.ru**

Подписка и продажа — (495) 607-77-28

Бухгалтерия — (495) 607-87-39

Наши платёжные реквизиты:
получатель — ЗАО "Журнал "Радио", ИНН 7708023424,
р/сч. 40702810438090103159
Банк получателя — ПАО Сбербанк г. Москва
корр. счёт 30101810400000000225 БИК 044525225

Подписано к печати 25.05.2020 г. Формат 60×84 1/8. Печать офсетная.

Объём 8 физ. печ. л., 4 бум. л., 10,5 уч.-изд. л.

В розницу — цена договорная.

Подписной индекс:

Официальный каталог ПОЧТА РОССИИ — П4014;

КАТАЛОГ РОССИЙСКОЙ ПРЕССЫ — 89032.

Отпечатано в ОАО «Подольская фабрика офсетной печати»
142100, Моск. обл., г. Подольск, Революционный проспект, д. 80/42.
Зак. 01753-20

Что дальше...

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"...иногда, даже если ты знаешь, чем это всё закончится, — это не значит, что ты не можешь насладиться всем этим".

(Тед Мосби)

Немного о том, что ждёт впереди. Помнится, нам обещали много интересного.

Сегодня каждый, кто не находится в бизнес-нокдауне, спешит воспользоваться вирусно-изозяционным моментом, чтобы развить решения по удалённой работе, развлекательному контенту, сетевым играм и далее — к полному цифровому аутизму. Вот в Китае уже появился полностью роботизированный ресторан.

Распространение 5G и уменьшение размеров VR-очков и шлемов расширят области применения виртуальной и дополненной реальности. Их объединяет термин extended reality (XR). В этом году XR-приложения будут использовать в школьном и профессиональном образовании. Например, для тренировок хирургов или строителей. По данным CB Insights, развитие AR и VR также приведёт к популярности виртуальных офисов — пространств для remote-сотрудников. Подобные решения уже есть на рынке. Датский стартап MeetinVR предлагает компаниям виртуальные митинг-румы, где могут проводить совещания и те, кто находятся в офисе, и те, кто работают удалённо. Другая компания, Spatial, позволяет проводить встречи с аватарами собеседников в дополненной реальности и использовать виртуальную переговорку как монитор.

Компании Google, Apple и Microsoft совершенствуют шлемы виртуальной реальности. Некоторые из них будут предназначены для использования в офисах, что способствует популяризации технологии.

Технологии всё быстрее входят в нашу жизнь. Вот Китай, к примеру, создаёт "цифровую диктатуру" (некоторые называют её цифровым концлагерем), чтобы установить контроль над 1,4 миллиардом своих граждан, понимая, как они исполняют законы, отдают ли вовремя кредиты и вообще как ведут себя в повседневной жизни. Для одних "кредит доверия" принесёт привилегии, для других — наказание.

Собственно то, что может казаться далёким будущим, уже происходит в Китае. И это уничтожает многие жизни. Коммунистическая партия Китая обещает, что эта система будет полностью функционировать уже в 2020 г. И утверждает, что она "позволит людям, заслуживающим доверие, свободно пользоваться всеми благами, в то время как дискредитированным людям будет трудно сделать и шаг". "Кредит доверия" подобен персональной системе показателей для каждого из 1,4 миллиарда граждан Китая.

В рамках пилотной программы, которая уже работает, каждому гражданину был присвоен свой персональный балл по 800-балльной шкале. Те граждане, которые имеют высокие баллы, получают VIP-обслуживание в отелях и аэропортах, дешёвые кредиты и быстрый доступ к лучшим университетам и рабочим местам. Те, кто находятся в самом низу шкалы, могут быть изолированы от общества и не допущены к путешествиям, а также лишены возможности получить кредит или работу в государственных организациях.

Эта система будет оснащена новейшими высокотехнологичными системами видеонаблюдения, поскольку Китай

стремится стать мировым лидером в области искусственного интеллекта. Камеры видеонаблюдения будут оснащены системой распознавания лиц, сканирования человека и геолокации, чтобы постоянно следить за каждым гражданином.

Приложения для смартфонов также будут использованы для сбора данных и мониторинга поведения человека в Интернете на ежедневной основе. Затем обработанные Большие Данные из разных других источников, таких как государственные архивы, включая образовательные и медицинские учреждения, оценки государственной безопасности и финансовые отчёты, будут включены в шкалу индивидуальных баллов.

Пилотные проекты системы "кредита доверия" в настоящее время находятся на различных стадиях внедрения, по меньшей мере в дюжине городов по всему Китаю. Несколько компаний работают с государством, чтобы национализировать систему, скоординировать и настроить технологию, а также доработать алгоритмы, которые будут определять национальный рейтинг граждан.

Это, вероятно, самый крупный проект социальной инженерии, созданный для слежения и контроля за более чем миллиардом людей. В случае успеха это и будет первая в мире цифровая диктатура. В целом она весьма привлекательна для любого правительства любого государства.

Разумеется, "кредит доверия" — неидеальная система, но пока это лучший способ управлять страной с самым большим населением в мире. "Я думаю, что люди в каждой стране хотят жить в стабильном и безопасном обществе, — говорит простой китаец. — Если каждый уголок общественного пространства будет оборудован камерами, я буду чувствовать себя в безопасности".

Финансовое поведение человека будет важнейшим показателем для оценки национального "кредита доверия". Согласно существующей финансовой системе под названием Sesame Credit, человек, имеющий высокий балл, например, 750 из 800 — является довольно надёжным гражданином Китая.

Приложение, установленное на каждом телефоне, даёт доступ к специальным привилегиям, таким как аренда автомобиля, гостиничного номера или дома без внесения депозита. Но "кредит доверия" будет зависеть не только от этого.

Кто является вашими друзьями, кто ваша семья — это тоже будет влиять на ваш рейтинг. Если ваш лучший друг или ваш отец скажут что-то плохое о своём правительстве, вы также можете потерять свои баллы. То, с кем вы встречаетесь и в конечном счёте сотрудничаете, также повлияет на рейтинг. Чем не иллюстрация к "1984" Джорджа Оруэлла? У тебя "нет ничего твоего, кроме нескольких кубических сантиментов в черепе", — это оттуда. "Свобода — это возможность сказать, что дважды два — четыре. Если дозволено это, всё остальное отсюда следует," — это тоже оттуда.

"Нам нужна такая система "кредита доверия", — говорит государственный служащий в Министерстве юстиции Китая. "Мы надеемся, что сможем помочь друг другу, любить друг друга и помочь каждому человеку стать успешным". Китай уже давно является государством, которое пристально наблюдает за своими гражданами, поэтому они привыкли к тому, что правительство берёт на себя определяющую роль в личных делах. Китайцы придают более высокое значение общественному благу по сравнению с личными правами, поэтому большинство китайцев считает, что если "кредит доверия" создаст более безопасное, надёжное и стабильное общество, то так тому и быть.

Однако большинство из них, похоже, не понимают, что всесторонний контроль уже имеет место быть, и на этот счёт не было никаких публичных обсуждений о внедрении системы внутри Китая.

Примерно около 10 миллионов человек уже были наказаны в рамках пилотной программы "кредита доверия". Уже много людей попали в чёрный список неправомерно, но они не могут выйти из него. Это разрушило их карьеру и изолировало от общества, и теперь они боятся за будущее своей семьи. Стоит заметить, что алгоритм наказаний может быть и другим (в зависимости от причёски, к примеру), не в нём суть. Главное — это создание технологии всестороннего сбора и обработки информации обо всех индивидах во имя их полного подчинения чьим-то желаниям. Мировая история говорит о том, что желания иногда становятся приговорами.

Сегодня, кстати, создаются системы, позволяющие читать мысли. Поэтому, похоже, всё вышесказанное — лишь начало. Начало чего-то большего и довольно тревожного. Допустим, наказания будут отданы на откуп системам искусственного интеллекта (а то за всеми не уследишь), дабы контролировать (а то и монетизировать) совесть каждого гражданина. Пусть нечестный платит, а потом пусть платит неправильно говорящий, а потом и неправильно думающий. На чём остановится подобная социальная инженерия? "Мыслепреступление не влечёт за собой смерть: мыслепреступление ЕСТЬ смерть", — это тоже из "1984".

Разумеется, для любой подобной глобальной системы нужна соответствующая инфраструктура. Например, Интернет вещей (IoT), на развитие которого направлены сети 5G, которые были доступны в некоторых городах США, Китая, Южной Кореи, Британии и Германии уже в 2019 г. Стоимость тарифов в США стартовала от 50 долл., в КНР — от 80 долл. В конце октября 2019 г. Китай, лидер рынка, объявил о планах запустить 5G во всей стране. К тому моменту среди тех, кто уже производил смартфоны с поддержкой технологии, были ZTE, Huawei, Xiaomi.

В 2020 г. эти сети увеличат охват, а стоимость услуг снизится. Распространение 5G ускорит внедрение других технологий. А главное — позволит IoT-устройствам собирать и обрабатывать больше информации, что расширит их возможности и области применения. Несомненно, основные риски новых сетей отнюдь не в распространении вируса, что нашло отклик у чуждого новым технологиям населения, громящего антенные мачты базовых станций, а в обеспечении тотального доступа ко всему сущему. Вот с помощью чего, к примеру, можно ограничить доступ к чему-либо в зависимости от кредита доверия? Хотя бы с помощью соответствующих датчиков IoT. Не заслужил доверия — дверь не откроешь или еду не закажешь. Это фантазии, конечно, но механизм для их воплощения уже создаётся.

Развитие промышленного Интернета вещей (IIoT) благодаря 5G повысит эффективность производств, а также точность и скорость принятия бизнес-решений. Увеличит и риски нарушения бизнес-процессов и безопасности вообще.

Кстати, при развитии квантовых вычислений безопасность информации окажется под угрозой. Шифры будет легко взломать, например, получить доступ к электронной почте любого пользователя или, к примеру, к его кредитной истории.

Но уже есть стартапы, которые занимаются постквантовым шифрованием. В числе перспективных — британский Crypto Quantique, работающий в сфере защиты IoT-устройств. Среди других направлений рынка безопасности — использование искусственного интеллекта для автоматической реакции на угрозы, а также противодействие применению технологий взлома систем распознавания лиц. Будьте уверены, вас распознают с высокой точностью.

Кстати, обычно все данные, собранные кем-либо, попадают в одно хранилище (data lake). Они часто содержат много "мусора", а натренированный на них искусственный интеллект ошибается или оказывается предвзятым. Поэтому автоматическим системам принятия решений (в части определения "кредита доверия", к примеру) до сих пор многие не доверяют. Чтобы решить проблему, нужны фильтры, отбрасывающие "грязные" данные до попадания в хранилище. Несомненно, подобные системы будут востребованы, в том числе и в Китае.

Но вернёмся к IoT. Всяческие фитнес-браслеты и smart-часы — это ни что иное, как нижняя ступень Интернета тел (IoB — Internet of Bodies) — сектора IoT, который объединяет все гаджеты, подключаемые к человеку. Вторая ступень — устройства, попадающие внутрь организма: кохлеарные импланты (нейропротезы для неслышащих и слабослышащих), кардиостимуляторы, цифровые таблетки. На самом верху пирамиды — устройства, которые становятся единым целым с человеком и остаются связанными с внешней системой в реальном времени.

Сегодня распространятся устройства, способные не только лечить пациента, но и транслировать данные о его состоянии. Например, инсулиновые помпы, измеряющие уровень глюкозы в крови и передающие информацию в

облако, и цифровые таблетки для лечения рака, общающиеся с врачами. Признавая перспективы рынка, Google и Microsoft инвестируют в digital health, а Apple запускает собственные исследовательские программы. Их результаты будут доступны пользователям в приложении Research app. Кроме того, Apple Watch последнего поколения уже включают функции для тех, кто страдает диабетом, а также устройства для ЭКГ.

Препятствия на пути IoB, с которыми следует считаться всем игрокам рынка, — угроза жизни и здоровью человека в случае хакерской атаки, а также вторжение в частную жизнь (запись имплантами окружающих звуков).

Разумеется, умные импланты и всезнающие трекеры облегчат жизнь пациентам со многими болезнями. Однако юридические нормы для IoB не разработаны, что чревато неприятными и опасными ситуациями.

Несомненно, новые медицинские устройства типа искусственной поджелудочной железы, дистанционно управляемых кардиостимуляторов и имплантов, помогающих победить паралич, значительно облегчат жизнь многих пациентов. Однако они также порождают новые риски.

Первая проблема заключается в том, что многие из умных медицинских приборов не регулируются достаточным образом. Например, в США фитнес-трекеры и датчики сна не подпадают под юрисдикцию FDA — регулятора, который одобряет все лекарственные средства и процедуры. Так что пока неясно, какое ведомство будет регулировать новые устройства IoB. Есть вероятность, что подобные вопросы лягут на плечи Федеральной торговой комиссии, которая занимается вопросами некачественных товаров, а также безопасности и конфиденциальности. Однако без дополнительных ресурсов это небольшое агентство не справится с взрывным ростом числа IoB-устройств.

Ещё одна проблема IoB связана с патентным правом. Проиграв процесс, компания может потерять право на производство или поддержку того или иного устройства. Тогда тысячам людей, в чьё тело оно установлено, придётся сделать выбор: оставить неработающий прибор или решиться на операцию по его удалению. Большинство высокотехнологических компаний полагается на лицензионные соглашения с конечными пользователями. Если клиент не согласен с изменившимися условиями, производитель оставляет за собой право деактивировать устройство. В случае смартфона подобная ситуация в худшем случае неприятна, но отказ от лицензионного соглашения на протез или кардиостимулятор может создать проблемы. Например, непонятно, за чей счёт будет проводиться удаление такого устройства. Банкротство производителя IoB-устройств также создаст сложности для клиентов. Договорные права и доступ к конфиденциальным данным часто рассматриваются как активы в процессах по банкротству, и суд может разрешить продать их другой компании — например, страховщикам. Чтобы обеспечить безопасность и конфиденциальность пользователей, необходимо пересмотреть закон о банкротстве.

Ещё одна проблема может возникнуть, если пользователь потеряет доверие. Вот как описана схожая ситуация столетней давности у Ярослава Гашека устами бравого солдата Швейка, когда один инвалид Первой Мировой войны, получивший от Австро-Венгрии серебряную медаль и искусственную ногу, разочаровался в идеалах империи и понёс закладывать медаль в ломбард. "Там его сцапали, и пошли неприятности. Существует какой-то там суд чести для инвалидов войны, и этот суд постановил отобрать у него эту серебряную медаль и, кроме того, присудил отобрать и ногу… В один прекрасный день пришла к нему комиссия, заявила, что он недостоин носить искусственную ногу, отстегнула у него её и унесла…".

Стоит ли говорить, что сегодня прогресс ушёл далеко вперёд, и с вышеизложенными ситуациями столкнётся каждое государство, которое захочет отрегулировать IoB.

Ещё один технологический тренд, способный преобразить жизнь людей, — распространение умных камер. Говорят, к 2022 г. подобные устройства появятся в каждой второй американской семье. Безусловно, отказ от приватности обеспечит множество новых возможностей и увеличит личное доверие, но…

Как снова стать свободным?

С одной стороны, цифровые шутники говорят, что самоизоляция не будет полной, если не ввести подъём, отбой, утренний развод на удалённые работы и вечернюю цифровую проверку.

С другой, — надо выбросить все смартфоны, гаджеты, кредитные карты и уехать куда-нибудь в глушь, чтобы перестать быть интересным для контролирующих органов. Или ещё один простой способ — тщательно соблюдать все новые правила и законы.

И наслаждаться цифровым будущим!

По материалам ***l-a-b-a.com, m.hightech.plus, nemnogoobovsem.com***