

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

"Стоит только попристальнее взглядеться в настоящее, будущее вдруг выступит само собою."

(Николай Васильевич Гоголь)

Самое время остановиться и оглянуться вокруг. Казалось бы, всё началось совсем неплохо, и мы хотели счастья для всех с "цифрой", с "оцифровкой", с "цифровизацией", с "цифровой трансформацией" или просто с жизнью в киберпространстве, где-таки, наконец, настанут те самые "свобода, равенство и братство". Компьютеры во всех воплощениях окружают нас со всех сторон, и уже нетрудно увидеть, как вскоре объединятся номера карт социального страхования, мобильных телефонов, кредитных карт и паспортов с аккаунтами в социальных сетях, создав единую базу пользователей (и процесс уже идёт), где биография и достижения (в том числе и довольно сомнительные) станут доступны не только тем, кому это положено по месту службы. Хорошо это? — Наверное, хорошо! А есть ли плохое? — Да есть, конечно.

Хорошо, что информацией, которую так трудно было добывать когда-то, теперь так легко управлять, получая её и отправляя, находить по любому запросу всё, что угодно, локализовать любые объекты с помощью данных геолокации, а также расплачиваться за любые продукты непосредственно с помощью смартфона. При этом большинство функций доступно любым пользователям скоростного Интернета, а не специально допущенным к информации людям, как это было ещё совсем недавно. Мошенники и войны также переместились в киберпространство. Как следствие, падают тиражи печатной продукции, серьёзно ограничилось хождение бумажных денег, и уже во многих случаях нет необходимости в посещениях чиновников, магазинов и отделений банков.

Хорошо известны прогнозы о том, что роботы вскоре заменят работников в разных сферах экономики. Собственно, на многих заводских конвейерах это уже свершилось. Следующими идут водители, на которых "наедет" беспилотный транспорт, а также различный обслуживающий персонал, — от кафе вплоть до банковской сферы. По прогнозам мировых экспертов, к середине 2030-х годов недвижимость и строительство станут четвёртой отраслью экономики по числу сотрудников, которых заменят роботы. К этому времени исчезнут или как

минимум сильно видоизменятся примерно 40 % профессий в этих сферах. Следом в колонне на выход идут журналисты, солдаты, врачи и, с учётом развития искусственного интеллекта, как говорится, далее везде.

Существует мнение, что цифровизация — отнюдь не всегда благо и бизнес-прорыв. Казалось бы, что-то цифровизировали, автоматизировали, изготовили цифровых двойников, и что? Где обещанная прибыль? Потратили больше, чем заработали? Но что вас гипнотизировал на такие траты? Ведь любая автоматизированная система — это, прежде всего, инновационная концепция обмена данными, и её надо вовремя разглядеть и воплотить в жизнь. А просто автоматизация — это никакая не цифровая трансформация, а повторение всех правильных и неправильных бизнес-процессов на немного другом уровне, что само по себе не даёт ни выигрыша, ни прибыли.

Опрос 4600 руководителей высшего звена более чем из 40 стран, проведённый год назад компанией Dell Technologies совместно с Intel в рамках исследования "Индекс цифровой трансформации" ([URL: http://www.delltechnologies.com/en-us/perspectives/digital-transformation-index.htm](http://www.delltechnologies.com/en-us/perspectives/digital-transformation-index.htm)), показал, что программы цифровой трансформации во многих компаниях по-прежнему находятся в зачаточном состоянии. Только 19 % участников опроса имеют готовый план и приступили к его реализации. Но даже наличие пошагового плана не гарантирует успеха, если он составлен без анализа конкретных бизнес-проблем, которые необходимо решить, и создания проекции будущего. В противном случае компании хаотично внедряют все новомодные технологии, а потом судорожно пытаются интегрировать их в масштабах своей организации. В итоге менеджмент разочаровывается в инновациях и сворачивает программы.

Цифровизацию недаром рассматривают как важный шаг на пути к новому, шестому технологическому укладу. Однако его невозможно сделать без активного использования достижений в области инфокоммуникаций. И если, к примеру, в США доля технологий пятого уклада ещё 10 лет назад сос-

тавляла 60 %, то в РФ она была на уровне 10 %. В итоге многие компании безуспешно затевают цифровизацию, не обладая необходимой технологической основой.

Исследование Университета Северных Каролины показало, что к 2019 г. главы компаний отошли от цифровой эйфории и уже воспринимают цифровую трансформацию в качестве главного фактора риска, хотя год назад она занимала лишь десятое место. Растущее беспокойство связано с тем, что универсальных рецептов трансформации не существует, и, как следствие, 70 % "цифровых" инициатив, которые пытаются реализовать компании, не достигают задуманных целей. Это значит, что из 1,3 трлн долл., потраченных на улучшение бизнес-процессов путём внедрения "цифры", примерно 900 млрд было выброшено на ветер. Собственно, большинство компаний даже не подозревают, насколько длительным и капиталоемким может оказаться процесс трансформации. В связи с тем, что цифровая трансформация относится к бизнес-проблемам, нужно быть готовыми к существенным инвестициям не только в информационную инфраструктуру, но и в преобразование операционных процессов, обучение клиентов и развитие абсолютно новых навыков у персонала.

Влияние цифровых технологий на повседневную жизнь человека хорошо видно на примере сферы образования. Во многих странах разрабатываются школьные и университетские реформы, направленные на внедрение умных устройств в процесс обучения. Как показывают исследования, интерактивные занятия более эффективны и вызывают большой интерес среди учащихся. Цифровизация образования направлена на обеспечение непрерывности процесса обучения в течение всей жизни (life-long-learning). Она заключается в самостоятельном поиске информации в Интернете и в использовании технологий виртуальной, дополненной и смешанной реальности, облачных вычислений и пр. Кроме того, нельзя отвергать одно из самых очевидных преимуществ цифровой эры — относительно простой доступ к учебным материалам и исследованиям. Другое дело, что этому кто-то должен научить, и не всегда оптимально, что этот "кто-то" является просто цифровым устройством.

Не так давно Билл Гейтс говорил: "Неужели через два или три года число деловых поездок сократится на 50 %? Вполне возможно. Ранее считалось: если вы продавец и звоните клиентам, чтобы предложить свою услугу, это несерьёзно. Но теперь цифровое подключение воспринимается обеими сторонами гораздо проще и эффективнее". В эти слова можно было верить или не верить, но вмешался очередной экономический кризис, усугубившийся пандемией вируса, и у части людей отпала необходимость в посещениях офисов, а сфера образования "подняла флаг" дистанционного образования. К примеру, по данным крупнейшей российской компании интер-



нет-рекрутмента HadHunter, число вакансий "на удалёнке" по всей России продолжает быть в плюсе. Так пандемия пассивно помогла всеобщей цифровизации, сменив концепцию развития различных отраслей и областей знаний.

Цифровизация человека из года в год будет только усиливаться — в этом уверены не только эксперты, стоящие за разработкой новых устройств и технологий, но и противники грядущих изменений. К примеру, цифровизация экономики намного шире, чем просто использование электронных сервисов. Понятие охватывает всю систему экономических отношений, которая основана на использовании информационно-коммуникационных технологий. Многие убеждены, что информационные технологии (ИТ) позволяют избавиться от существующих проблем, таких как коррупция, и развить экономику. В самом деле, стоимость услуг и товаров онлайн, как правило, ниже, что играет на руку и потребителю и производителю, снижающему затраты на содержание большого количества помещений. Международные транспортные компании позволяют без труда организовывать доставку практически в любой уголок Земли, а упрощённый контроль и анализ всех основных процессов позволяет всегда "держать руку на пульсе". В развитых странах практически все государственные сервисы и производства переведены в онлайн, что положительно сказалось и на состоянии экономики (в них даже появилась новая должность — министр по цифровой инфраструктуре). Другое дело, что присущая цифровым технологиям прозрачность обмена любой информацией объективно вызывает ожесточённое сопротивление тех, кому это не "на руку".

Оцифровка данных — бесспорно, удобно, но куда приведёт общество желание перенести львиную долю реальной жизни на просторы Интернета? Один из вариантов развития событий уже можно увидеть на примере КНР, где прикладываются большие усилия, чтобы занимать лидирующие позиции во всех сферах, включая ИТ. И речь идёт не только о выпуске смартфонов или домашних гаджетов, а о целом государственном плане: "Программа создания системы социального кредита (2014—2020)", о которой уже упоминалось на страницах журнала и которая становится популярной во многих странах.

Идея заключается в создании системы, с помощью которой будут отслеживать каждого жителя в режиме реального времени. На начальном этапе каждому участнику будут выставлены баллы, и в зависимости от числа нарушений или заслуг, эти баллы будут соответственно снижаться или добавляться. Будут оцениваться не только нынешние действия, но и вспомнятся прошлые поступки. Это становится возможным благодаря развитию технологии искусственного интеллекта и использованию современных систем обработки данных. Сложность использования технологии заключает-

ся ещё и в том, что контроль будет вестись не только за реальной жизнью, но и виртуальной, которая сегодня занимает порой большую часть повседневной жизни граждан. И если пользователь будет замечен в нарушении существующих доктрин (репосты, комментарии), то произойдёт не только автоматическая блокировка, но и соответствующий подсчёт баллов. Это касается не только профилей в социальных сетях, но и банковских карт. В качестве одного из наказаний — отказ в предоставлении государственных услуг. Основная цель — предоставление социальных благ и льгот для граждан, оправдавших доверие государства, и ограничения для обладателей низкого рейтинга. Последние могут испытывать сложности при устройстве на работу, получать запрет на выезд за границу, отказ в кредитах и пр. Говорят, крупные города Китая уже тестируют пилотную версию этой системы. Кстати, в распоряжении властей КНР есть система видеонаблюдения, насчитывающая свыше 170 млн видеорекамер. Но видеонаблюдение было бы менее эффективно без использования технологии распознавания лиц, а с недавних пор активно ведётся разработка алгоритма распознавания человека по походке или в медицинской маске. В частности, алгоритм распознавания человека по походке позволяет проводить идентификацию "объекта" на расстоянии 50 м. Обмануть систему (прихрамывая или по-другому искажая походку) практически невозможно — технология анализирует особенности всего тела. Как выяснилось, в процессе ходьбы человек совершает примерно 24 дополнительных движения, которые и позволят создать комплексную и точную оценку.

Кстати, недавно объявлено, что в РФ появится приложение для отслеживания социальных контактов россиян в рамках борьбы с коронавирусом, и Министерство цифрового развития сейчас завершает его тестирование. Смартфон будет сканировать окружение человека в радиусе до 10 м. Власти уверяют, что полученная таким образом информация будет анонимной. Конечно, не очень понятно, как всё это соотносится с действующими правами граждан, но, похоже, если к любому действию добавить фразу "в рамках борьбы с коронавирусом", то уже, вроде бы как, и ничего.

С одной стороны, повсеместное использование подобных систем поможет решить многие социальные проблемы, вроде борьбы с уличной преступностью, с эпидемиями и с терроризмом, а также с коррупционными схемами и махинациями, всех фигурантов, которых можно "вычислить" с помощью технологии BigData.

Вроде бы подобные программы "социального кредита" имеют только плюсы для добропорядочных граждан, ибо в первом приближении они направлены на шунтирование таких известных социальных явлений, как ложь и воровство. Однако следует понимать, что система будет направлена на

фиксацию любых отклонений от нестандартного поведения до излишне близкого контакта. И если, например, появится желание бросить работу, отправиться в бесконечное путешествие или отказаться от благ цивилизации и вернуться к истокам, программа сделает соответствующие выводы. Не исключены и ошибки. Ну, а самое главное — в чьих руках окажется система управления "социальным кредитом" и какие цели он будет преследовать. Выведет ли он наверх новую элиту или же элита текущая приложит все силы, чтобы собою и остаться. Поэтому вышеприведённые радужные перспективы могут иметь и весьма пугающую сторону, идентифицируемую от Большого Брата до Цифрового Концлагеря, называть можно, как кому нравится.

С другой стороны, несмотря на все достижения цифровых технологий, куда сразу не денутся мошенничество, вывод денег, воровство, оргпреступность или даже простое разгильдяйство, не говоря уже о политических мотивах. Конечно, хорошо верить, что порядок наведёт какой-нибудь искусственный интеллект, но ведь алгоритмы его работы тоже составляются людьми по желанию других людей, в том числе и желающих управлять и извлекать прибыль.

У каждой страны свой путь к отслеживанию граждан. К примеру, в 2001 г. 43-й президент США Джордж Буш-младший спустя месяц после серии терактов 11 сентября 2001 г. подписал закон о борьбе с терроризмом, который расширял область применения электронных средств слежения и позволял осуществлять обмен разведанными с другими государствами. Так называемый "Патриотический акт" фундаментально менял и подавлял свободу коммуникаций, передвижения, частной жизни и собственности, наделив все силовые структуры возможностями, которых не было у спецслужб за всю историю США. Благодаря "Патриотическому акту" администрация Джорджа Буша смогла внедрить ряд мер, которые до тех пор считались нарушениями демократии в стране. Тотальную контрольную подвергались телефонные переговоры, все сообщения и абсолютно каждое письмо в электронной почте. Спецслужбы имели право отслеживать, что читают американцы, какие книги берут в библиотеке, какие сайты посещают на компьютерах, установленных в общественных местах. Если у ФБР закрадывались подозрения в отношении определённого лица, любую дополнительную информацию о нём можно было запрашивать в других государственных и коммерческих учреждениях.

Считается, что "Патриотический акт" действовал в США на протяжении 14 лет, до 1 июня 2015 г., а вместо него власти страны приняли "Акт о свободе США", который якобы запрещает Агентству национальной безопасности вести электронную слежку и прослушку разговоров, а также собирать информацию о гражданах США. Но это в корне не так, потому что законы, кото-

рые были приняты изначально, действуют и не обновляются до сих пор. Спецслужбы Штатов продолжают следить за гражданами не только своей страны, но и других государств. Они всё также получают записи звонков как назначенных целей, так и тех, с кем они общаются, — это выглядит не менее агрессивно.

За несколько лет до окончания действия "Патриотического акта" экс-сотрудник американских спецслужб Эдвард Сноуден обнародовал данные о секретной операции, в ходе которой полный контроль осуществлялся за информацией о пользователях мобильной связи и Интернета. Из данных следовало, что интерес американских спецслужб не ограничивался только простыми американцами, а заходил куда дальше — в страны Европы и Латинской Америки. Барак Обама оправдывал это тем, что США обещивают безопасность всего мира, подчёркивая, что безопасность и личная информация не могут быть отделены друг от друга на 100 %, и это должен понимать абсолютно каждый человек.

В качестве дополнительного "усилителя" цифровой идентификации граждан предлагается вживлять в них соответствующие чипы, и уже сравнительно давно нашлись желающие произвести над собой подобную операцию. Вероятно, более полного контроля над гражданами трудно себе представить.

Технологии развиваются настолько стремительно, что правовое регулирование (разумеется, в том числе и в России) не успевает вовремя среагировать на то или иное изменение. Многие направления экономики, такие как беспилотники, телемедицина, финансовые технологии, автоматизированный бухчёт, где могут успешно применяться цифровые технологии, находятся если не вне закона, то в так называемой серой зоне, не говоря уже о программе "социального кредита". А ведь только недавно были разработаны нормативные акты, регулирующие электронный документооборот, вопросы электронной подписи и удалённой идентификации в цифровом пространстве. Отдельной головной болью является хранение и защита данных в рамках исполнения законодательства в области персональных данных. Год назад Роскомнадзор выявил нарушения в 80 % проворок, что лишь подтверждает сказанное.

В ногу с цифровизацией идёт параллельное усиление коммуникации граждан и их же одиночества, что логично. С одной стороны, связаться (в том числе и наблюдать за кем-либо) теперь действительно можно множеством способов, а с другой — наличие множества средств доставки колоссальных объёмов контента ставит эту коммуникацию на второй план после развлечений. Собственно, в этом нет ничего нового, если вспомнить известную формулу "хлеба и зрелищ", тем более, что с хлебом дела обстоят пока в целом неплохо.

Возможность относительно простого получения любой информации в Интернете не проходит даром для целого ряда граждан. Тотальное оглушение — одна из тёмных сторон внедрения ИТ, о которой не принято много говорить. Неоконсерваторы, которые врвутся к власти в США, как раз на нём и паразитируют. Мол, наберём профессионалов — так с ними считаться придётся. Ну а кесарю — кесарево. Остальным же придётся довольствоваться той информацией, которую им предоставят. К примеру, так называемые суперразвитые ИТ — это когда человек находится просто под воздействием информационного цунами. Паразитируют они на том, что, как это ни прискорбно, большинство людей не очень умны. Они не могут быстро проводить синтез и анализ, не могут восстанавливать цепочку причинно-следственных связей и понимать то, что произошло, вызвано такими-то причинами. "Вешать лапшу на уши" — это как раз то, что происходит повсеместно. А с использованием фабрик фейков (о чём уже шла речь на страницах журнала), в чём человечество за последнее время весьма преуспело, — тем более. Подчас делается это с размахом и с тратой огромных денег.

В частности, именно с подобной "лапшой" вербовка молодёжи террористическими движениями стала более продвинутой и оттого ещё более коварной. Экстремисты завлекают неокрепшие умы своими профессионально срежиссированными видеороликами во всех соцсетях. Или вот — после последней армяно-азербайджанской войны в Интернете нашлось почти 6,5 тыс. фейковых аккаунтов, с которых в армянских соцсетях проводили кампанию по дезинформации о конфликте в Карабахе. С разных IP-адресов из Азербайджана, Турции и Великобритании начали массово регистрировать новые аккаунты от имени, якобы, армянских пользователей и сеять панику, срамливая пользователей. В целом же благодаря информационным технологиям перманентная кибервойна (как составная часть так называемой гибридной войны) всех против всех идёт повсеместно на бытовом, деловом, политическом и международном уровнях. Ну, а если говорить об оружии массового поражения в кибервойне, то его роль с успехом сыграла та же цифровизация, а преимущество будет иметь тот, кто контролирует Интернет и его приложения. Потенциальным управляемым объектом для подобного оружия может стать любой индивидуум с цифровым паспортом, не говоря уже об обладателях вживлённых чипов. Следует понимать, кем произведены и контролируются практически все компьютеры, смартфоны, а также соцсети.

Параллельно идёт борьба за индивидуума и его персональные данные. Не секрет, что сегодня процветает торговля данными (пусть даже, как это обещается, обезличенными) как чужой собственностью. Возможность получения дополнительной прибыли

за счёт получения информации о местонахождении, предпочтениях, предыдущих приобретениях, здоровье, поездках и пр. успешно преодолевает барьеры приличия (как, впрочем, и неприличия тоже). Сегодня появилась масса желающих обогатиться, заполнив просторы Интернета опросами, исследованиями и рекламой, причём занимаются этим даже вполне благопристойные организации, вроде операторов мобильной связи или банковских организаций. Вот уже замечено, как упоминание в телефонном разговоре, к примеру, сорта кофе приводит к поступлению на смартфон говорившего рекламы именно того же кофе. Получается, граждан уже подслушивают отнюдь не те, кому это положено по закону. Ну а предупреждения владельцев телевизоров с выходом в Интернет о том, что вся медиаинформация, генерируемая в месте установки подобного устройства, может быть доступна в любом другом месте, свидетельствуют о том же самом. А как вообще вернуть владельцам их права обладания персональными данными? К примеру, можно заставить платить за доступ к персональным данным. Вы мне платите — я смотрю вашу рекламу. Какие для этого могут быть инструменты? Они уже создаются.

Шестидесятипятилетний изобретатель WWW Тимоти Джон Бернерс-Ли объявил о выходе на рынок корпоративной версии конфиденциальной платформы Solid, представляющей собой проект децентрализованной всемирной паутины с возможностью для рядовых пользователей контролировать свои личные данные. По мнению "отца Интернета", доступ к Сети должен быть открытым и бесплатным. Однако в последние 20 лет крупные высокотехнологические компании получили возможность зарабатывать на конфиденциальных данных пользователей. Целью Бернерс-Ли является возвращение пользователям Интернета возможности полного контроля своих данных, для чего и выводится на рынок проект с открытым кодом Solid.

Разработка Solid осуществлялась в Массачусетском технологическом институте, а продвигать платформу на рынке будет стартап Inrupt, основанный Бернерсом-Ли три года назад. Принцип работы основан на создании крупными компаниями, правительственными органами и учреждениями приложений, позволяющих гражданам полностью управлять доступом к личным данным, размещённым в индивидуальных онлайн-хранилищах. Личные данные могут быть использованы различными приложениями, позволяющими, например, провести расчёт и оплату налогов или контролирующими состояние здоровья пользователя. Для работы с личными данными приложение запрашивает разрешение у пользователя каждый раз, когда необходимо получить к ним доступ. В любой момент пользователь сможет закрыть доступ к конфиденциальным данным. В настоящее время платформа Solid используется BBC и

Национальной службой здравоохранения Великобритании. Платформа использует стандартные технологии и методики, применяемые при создании web-сайтов, что обеспечивает возможность применения Solid в любых браузерах.

Говорят, что мир стоит на пороге новой революции, лозунгами которой будут "несвобода, неравенство и небратство", которые будут вводиться энтузиастами и оптимизаторами, а развиваться сущностями с достаточно простым цифровым мышлением, для которых цифры — это, прежде всего, номиналы денежных купюр. Довольно сложно будет говорить о свободе под вездесущими видеокамерами, микрофонами и утекающими персональными данными. Как говорил Альбер Камю, "свободен лишь тот, кто может позволить себе не врать", однако

большинство институтов человеческой цивилизации (в том числе и цифровизированных) призвано определять, врут люди или нет. Закрепляется социальное неравенство в зависимости от доступности цифровых сервисов (а кто-то ожидал что-то другое при капитализме?). Да и какое уж тут братство, если идёт разрыв привычных связей, которые делают нас нациями, единым человечеством, просто каким-либо сообществом. Связи будут заменены цифровым кодом, QR-пропусками и пр. Как говорится, за что боролись?

Вероятно, всему этому можно противопоставить лишь только моральные ценности. Ведь мы — не товар и не цифровой код. В связи с этим существует мнение, что создаваемое ныне на планете — не что иное, как духовно-интеллектуальная чёрная

дыра, общечеловеческое безумие, построенное на ложной мировоззренческой основе, извращённом целеполагании, криминально-грабительской методологии. Очевидно, всем нам ещё придётся разбираться в том, по чьей именно вине человечество увели в сторону от оптимального пути гармоничного развития. А заодно и понять, что это за путь и является ли он цифровым навсегда или лишь на определённом этапе развития.

По материалам riaan.ru, habr.com, aif.ru, ria.ru, mentamo-re.com, www.it-world.ru, rossaprimavera.ru, 19rus.info, zen.yandex.ru, nakanune.ru, russian.rt.com, svpressa.ru