Институт статистических исследований и экономики знаний

unesco Chair

приоритет2030^ лидерами становятся

Центр междисциплинарных исследований человеческого потенциала

Политика и регулирование

Расширение цифрового контроля

Институт статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ представляет результаты исследования трендов развития человеческого потенциала. Методология исследования включает методы интеллектуального анализа больших данных на базе системы iFORA, созданной в ИСИЭЗ НИУ ВШЭ, а также экспертные сессии и опрос Дельфи с участием более 400 ведущих иностранных и российских ученых в области человеческого потенциала.

Проект реализуется в рамках деятельности Научного центра мирового уровня «Центр междисциплинарных исследований человеческого потенциала» и Кафедры ЮНЕСКО по исследованиям будущего (сеть UNESCO Futures Literacy Chairs).
Полный перечень трендов представлен в уникальной общедоступной базе данных (https://ncmu.hse.ru/chelpoten_trends).

Трендлеттер подготовлен по данным alliedmarketresearch.com, gov.cn, washingtonpost.com, ec.europa.eu, mordorintelligence.com, globenewswire.com, tass.ru и др.

Структура тренда

- **Распространение инструментов цифрового контроля**
- **Контроль за контентом и уровнем влияния социальных сетей**
- **Создание цифровых профилей людей**

Цифровые инструменты контроля распространяются повсеместно: для охраны объектов инфраструктуры и производства, поиска преступников, поддержания правопорядка и трудовой дисциплины, измерения показателей здоровья человека и др. Пандемия COVID-19 во многом легитимировала использование технологий слежения в целях обеспечения общественной безопасности: они применялись для дистанционного сбора биометрических данных и мониторинга соблюдения режима изоляции, отслеживания контактов заболевших и обнаружения скоплений людей.

Заметной тенденцией стало усиление контроля за данными, размещаемыми в социальных сетях, чему способствуют ряд факторов. Интернет упростил коммуникацию террористов и возможности вербовки, через него может распространяться информация, нарушающая законодательство и побуждающая к социально неприемлемому поведению. При этом «репортером» в цифровой среде становится любой человек, имеющий устройство с выходом в сеть и не связанный ни официальными обязательствами, ни этическими принципами профессиональной журналистики.

В масштабах страны контроль на уровне гаджетов впервые применил Китай. Технологии сбора и анализа информации обеспечивают работу китайской системы социального кредита, которая предполагает не только санкции за нарушения, но и поощрения за поведение, соответствующее принятым стандартам. Крупнейшей в мире системой цифровой идентификации, содержащей биометрические данные и привязанной к SIM-картам, банковским счетам, каналам социального и пенсионного обеспечения, является индийская Aadhaar, которая хранит информацию о 1.3 млрд человек. Сеть позволит более точно определять категории нуждающихся и эффективнее распределять средства государственной поддержки, а также составить всеиндийский реестр граждан.

Несмотря на глобальный характер тренда, он имеет локальные особенности. Так, в западных странах подобные системы чаще критикуются за несовершенство функционирования, возможные нарушения прав граждан и злоупотребления со стороны правоохранительных органов. В апреле 2021 г. Европейская комиссия представила комплексный законопроект, посвященный детальному регулированию искусственного интеллекта, в том числе применительно к распознаванию лиц.

Быстрорастущим сегментом мирового рынка систем контроля стало видеонаблюдение, чему способствуют развитие технологии облачных вычислений, совершенствование программного обеспечения, стремление к повышению безопасности, особенно в производственном, банковском, финансовом, транспортном и торговом секторах. Одним из драйверов VSaaS (video-surveillance-as-a-service – «видеонаблюдение как услуга»), является распространение IP-камер.

Власти продолжат развивать экосистемы цифровой идентификации для подтверждения личности граждан, обеспечения доступа к государственным услугам и бесшовного (многоканального) взаимодействия. К 2024 г. правительства более трети стран будут использовать показатели вовлеченности для отслеживания масштабов и качества участия населения в принятии политических и бюджетных решений. Однако чрезмерный надзор посредством использования современных технологий может привести к цифровой дискриминации – нарушению прав граждан на приватность и защиту своей сетевой идентичности.

Ключевые оценки

90.3 млрд долл.

может достичь мировой рынок систем видеонаблюдения в 2026 г. (в 2020 г. – 52.4 млрд долл.)

8.5 млрд долл.

составит мировой рынок технологий распознавания лиц в 2025 г. (в 2020 г. – 3.8 млрд долл.)

Параметры тренда

Влияние на человеческий потенциал[1]

1	2	3

Слабый сигнал[2]

Системы социальных рейтингов и биометрической идентификации

Период максимального проявления

2026–2030 гг.

Джокер[3]

Тотальный контроль над населением

Влияние пандемии COVID-19

Усилила тренд

Последствия реализации джокера

Цифровая дискриминация / цифровая асимметрия

Уровень проявления в России

Сопоставим с мировым

[1] 1 – слабое влияние, 2 – среднее, 3 – сильное.

[2] Слабый сигнал (weak signal) – событие, обладающее низкой степенью значимости (упоминаемости, популярности), но указывающее на радикальные трансформации тренда в будущем.

[3] Джокер – слабопредсказуемое событие, которое в случае его реализации может оказать значительное влияние на развитие тренда.

Драйверы и барьеры

Драйверы

- Развитие новых форматов предоставления госуслуг и взаимодействия с гражданами
- Потребность в обеспечении общественного правопорядка, поиске правонарушителей
- Поддержание санитарно-эпидемиологических мер при распространении инфекций
- Совершенствование технологий

Барьеры

- Недостатки работы систем наблюдения
- Правозащитная деятельность
- Негативная общественная реакция

Эффекты

Возможности

- Улучшение каналов взаимодействия граждан и государственных структур
- Повышение уровня общественного правопорядка
- Рост раскрываемости преступлений
- Расширение участия граждан в принятии политических и бюджетных решений

Угрозы

- Нарушение прав и свобод граждан
- Злоупотребления со стороны правоохранительных органов
- Утечки данных
- Возникновение цифровой асимметрии между гражданами и властью