

Раздел 2. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

2.1 Современное состояние и перспективы развития информационного общества в России

Ключевым для этой сферы цифровой экономики является понятие прав человека. Риски и угрозы, которые создает в этой сфере распространение информационных технологий, следует взвешивать и оценивать именно в том контексте, как эти технологии воздействуют на **обеспечение основных прав людей**: на безопасность жизни и деятельности, право на безопасные коммуникации (общение), права на собственность, работу, отдых, семью, убежище, на саму жизнь.

При этом мы видим, что само по себе только распространение информационных технологий никак не обеспечивает этих прав не гарантирует. Напротив, недооценка новых рисков и угроз, которые несут с собой новые информационные системы, создает такие опасности, с которыми общество ранее не сталкивалось и с которыми не знает, как справиться.

В частности, это – **опасности открытых социальных сетей**, в которые есть допуск для анонимных пользователей. Любая криминальная деятельность заметно ослабляется, когда правонарушителей лишают права на анонимность. К примеру, в свое время была целая волна телефонного терроризма, но как только телефонные компании научились четко идентифицировать отправителей телефонных звонков, эта волна сразу сошла на нет.

ИТ-средства коммуникаций открыли новое пространство для злоупотреблений **вторжениями в личное пространство людей**: личные странички в социальных сетях, расчетные операции, личные кабинеты при разного рода сервисах.

С этой новой проблемой государственные власти многих стран и регулирующие органы пока не знают как справиться.

Новые современные информационные технологии и повседневная жизнь людей. Как она может измениться? Приведем отрывок из недавней статьи эксперта по современному Китаю Ковачича⁶:

«Всевидящее око XXI века пришло в Китай. И имя ему – система социального кредита. <...> Госсовет КНР в 2014 году опубликовал новый документ – «Программу создания системы социального кредита (2014-2020)» <...> Из программы следует, что к 2020 году не только каждая компания, но и каждый житель материкового Китая будет отслеживаться и оцениваться этой системой в режиме реального времени.

Рейтинг доверия физических лиц будет привязан к внутреннему паспорту. Рейтинги будут публиковаться в централизованной базе данных в интернете в свободном доступе. Обладатели высокого рейтинга будут пользоваться различными социальными и экономическими льготами. А тем, у кого рейтинг будет низкий, придется страдать – на них обрушится вся мощь административных санкций и ограничений.

Главная задача, и это прямым текстом указывается в «Программе Госсовета», чтобы «оправдавшие доверие пользовались всеми благами, а утратившие доверие не могли сделать ни шагу <...>

И эта система уже работает – пока в пилотном режиме – примерно в тридцати городах Китая. Передовиком в этом деле стал город Жунчэн в провинции Шаньдун. Всем жителям города (670 тысяч человек) дается стартовый рейтинг 1000 баллов. Далее в зависимости от их поведения рейтинг либо растет, либо падает.

Самая разнообразная информация о жизни и деятельности гражданина поступает из муниципальных, коммерческих, правоохранительных, судебных органов в единый информационный центр, где обрабатывается с помощью технологии big data, и рейтинг гражданина, соответственно, либо повышается, либо снижается. Сейчас в Жунчэне единый информационный центр анализирует жизнь людей по 160 тысячам различных параметров из баз данных 142 учреждений.

⁶ См. «Большой брат 2.0. Как Китай строит цифровую диктатуру» // carnegie.ru/commentary/71546.

Что же касается количественных параметров системы, то если в наборе рейтинга больше 1050 баллов, ты – образцовый гражданин и маркируешься тремя буквами А. С тысячей баллов можно рассчитывать на АА. С девятьюстами – на В. Если рейтинг упал ниже 849 – ты уже подозрительный носитель рейтинга С, тебя выгонят со службы в государственных и муниципальных структурах.

А тем, у кого 599 баллов и ниже, и вовсе несдобровать. Их записывают в черный список с припиской D, они становятся изгоями общества, их не берут почти ни на какую работу (даже в такси с черной меткой D работать нельзя), не дают кредиты, не продают билеты на скоростные поезда и самолеты, не дают в аренду автомобиль и велосипед без залога. Соседи от тебя шарахаются как от огня, ведь не дай бог, кто-то увидит, как ты общаешься с человеком D, на тебя сразу донесут, и твой рейтинг тоже стремительно пойдет вниз». И это не какие-то фантазии, это уже реальность.

И на самом деле, *Big data* открывают широчайшие возможности для анализа и оценки всех ваших действий, делает вашу жизнь полностью прозрачной перед государством. А переход на безналичные расчеты и прочая «оцифровка» экономики делает возможным отключение от экономической системы, от потребления экономических благ.

В РФ вопросам развития и распространения современных информационных технологий тоже уделяется большое внимание. Объявлено о запуске масштабной программы развития экономики нового технологического поколения.⁷ Появилась уверенность, что эпоха нефти и газа, как основных двигателей экономики страны заканчивается и, что теперь именно ИТ-технологии могут лечь в основу богатства страны.

Действительно, сейчас в России быстрыми темпами развивается мобильная связь, что ведет к не менее активному развитию интернет-услуг, использованию населением общения и коммуникаций в социальных сетях. Необходимо отметить, что цифровая модель экономики может повысить конкурентоспособность как государства в целом, так и российского бизнеса на глобальных мировых рынках, может обеспечить условия для поэтапного перехода на уровень инновационной экономики и экономики знаний, а также, в

⁷ <https://ria.ru/20161201/1482599952.html>.

перспективе, способна повысить качество и уровень жизни населения страны. В качестве средств обеспечения такого перехода многие ученые и эксперты на первое место выдвигают такие технологии и направления, как блокчейн, новые компании-платформы, распределенные базы данных, криптовалюты, Big data и т. д.

При этом **цифровизацию российской экономики** начали с таких отраслей, как здравоохранение, образование, наука, промышленность, сельское хозяйство, ретейл, транспорт, электроэнергетика, ЖКХ и рынок финансовых услуг. Благодаря внедрению цифровых технологий станет возможным, в том числе, развитие телемедицины, онлайн-обучения, беспилотного транспорта, систем «умный дом» и «интернета вещей»; оно обеспечит прозрачность управления бизнесом и государством на всех уровнях.

Первые шаги в этом направлении в стране уже сделаны. Активно функционирует и получила популярность **электронная система государственных услуг** на сайте www.gosuslugi.ru. Ресурс позволяет удаленно решить многие вопросы. Например, осуществить платежи, подать заявку в детский сад, записаться на прием и пр. Ожидается, что к 2022 году доля граждан, использующих его возможности, достигнет 70%, а 95% населения страны будут подключены к всемирной сети. Специалисты отмечают, что зарождается система Электронного правительства и развивается концепция открытых данных.

Но помимо очевидных выгод, цифровая экономика несет с собой и очевидные **вызовы и угрозы**, которые напрямую связаны с ее особенностями и характеристиками.

Так, расширение спектра и индивидуализация цифровых услуг ведет к тому, что контроль в области цифровых сервисов снижается, а возможности для **мошенничества** увеличиваются. Значительно повышаются риски утечек информации, что требует повышения уровня защиты, выделения дополнительных инвестиций в информационную безопасность.

Однако цифровизация в то же время предоставляет и новые возможности организации управления – с использованием технологий больших данных, аналитики и прогнозирования. А расширение спектра услуг предоставляет возможности российским компаниям выйти на международный рынок.

Рост роли информационных услуг ведет также к существенному росту перераспределения доли добавленной стоимости в сторону информационноёмких отраслей, таких как финансы, СМИ, телекоммуникации. Но при этом повышается **риск утечки информации**, что ведет за собой требование повышения уровня защиты.

Киберпреступность становится все более организованной, как показало растущее число инцидентов, растет количество взломанных программ и устройств.

Серьезной угрозы информационной безопасности со стороны киберпреступников опасаются и представители финансовой сферы. Так, они считают, что основными вызовами являются **атаки на мобильные устройства** и финансовые мобильные приложения как части инфраструктуры дистанционного банковского обслуживания.

Также все большее внимание должно быть обращено на развитие *антифрод-систем* из-за возрастающего с каждым годом объема безналичных переводов и огромного количества провайдеров и пользователей платежных систем и сервисов.

Антифрод-система (от англ. anti-fraud «борьба с мошенничеством»), или фрод-мониторинг – система, предназначенная для оценки финансовых транзакций в интернете на предмет подозрительности с точки зрения мошенничества и предлагающая рекомендации по их дальнейшей обработке. Как правило, сервис антифрода состоит из стандартных и уникальных правил, фильтров и списков, по которым и проверяется каждая транзакция.

Чтобы как-то **минимизировать риски** поставлена задача, чтобы в ближайшие 3-5 лет цифровые технологии в России стали предметом национального и наднационального регулирования, и одновременно решать задачи продвижения отечественных услуг на международный рынок.

Необходимо отметить, что при глобальных процессах цифровой экономики на первом плане должна быть защита данных: при электронном взаимодействии пользователей интернета на территории России обработка данных планируется на местных серверах, данные российских пользователей начнут передаваться внутри страны, по

сетям российских операторов. В сетях операторов для безопасности планируется увеличить долю оборудования связи и софта отечественного происхождения.

Кроме того, продукция и услуги, поставляемые из-за рубежа при помощи интернета, должны проходить сертификацию и лицензирование. Предлагается также блокировать программное обеспечение, товары и услуги, продающиеся через интернет иностранными компаниями, не соблюдающими российское законодательство. В развитие этих направлений уже разработана дорожная карта Ассоциации компаний интернет-торговли (АКИТ). Это и защита граждан от контрафакта, и выравнивание налоговых условий при ведении бизнеса российскими и зарубежными компаниями, и меры таможенного контроля и сертификации для товаров, заказанных через интернет, а также блокировка ресурсов иностранных компаний, реализующих через интернет товары или услуги и не соблюдающих российское законодательство.

Предложения АКИТ нацелены также на выравнивание конкурентных условий отечественных и зарубежных онлайн-ритейлеров, а также защиту российских потребителей от недобросовестных игроков рынка.

Правильной стратегией является как импортозамещение, так и экспортозамещение – **создание уникальных разработок в области технологий, которым нет аналогов в мире.**

Как очевидно, эффективное и безопасное развитие цифровой экономики возможно только при адекватном развитии человеческого капитала. Успехи любой страны в области развития электронной экономики будут заметны в мире, если государство целенаправленно станет поддерживать научные исследования в области компьютерных технологий, с привлечением университетов, которые, помимо научной базы, обладают также ресурсом, необходимым для инновации в области ИКТ. Новые электронные технологии требуют не только обновления человеческих ресурсов, но и повышения компетенций людей. Необходимо активно реформировать общественные коммуникации, больше внимания уделять новым электронным СМИ и качественной работе с ними. Еще в одном документе изложены основные принципы и цели инновационного развития в нашей стране – **«Стратегия научно-технологического развития России»**. В нем особое внимание уделено образованию.

Одна из главных целей, которая поставлена в нем – провести **интернет во все образовательные организации страны**, включая периферийные. Это откроет две возможности. Во-первых, возможность дистанционного обучения. Например, на Западе уже успешно проявила себя система онлайн-курсов и лекций от преподавателей ведущих университетов мира. В России университеты предоставляют услуги дистанционного образования, но данный формат не должного уровня и недостаточно защищен с правовой точки зрения.

Во-вторых, **широкополосный доступ** стимулирует научно-техническую деятельность в образовательных учреждениях. Стартапы в университетах и научных центрах смогут совместно генерировать идеи и объединяться для реализации проектов с участниками из других городов и даже стран. Институты развития и научные центры должны выступить площадкой для воплощения новаторских идей, создавая условия для разработок. Для этого требуется их модернизация, разработка новой методологии, формирование культуры взаимодействия институтов и рабочих групп, привлечение инвесторов, а также популяризация научно-исследовательских и опытно-конструкторских работ.

Как очевидно, сейчас на первый план выходит потребность в объединении мирового сообщества не только для создания нового многополярного мира, но и для **снижения киберпротивостояния** между странами как в части неправомерного доступа к информационным ресурсам, так и в части информационных войн. А электронная экономика оцифровывает не только бизнес, но и повседневную жизнь общества.

2.2 Big data: большие возможности и большие риски

В настоящее время главная задача государственной политики, всех программ цифровизации в нашей стране заключается в том, чтобы конкретно увязать произведенные затраты с полученными результатами. В принципе любая программа по ее завершении должна проверяться на полученный эффект.

Цифровизация – это преобразование информации в цифровую форму. По сути, это внедрение современных технологий в любые сферы жизни общества. Речь идет не только о применении нового оборудования, а о коренных изменениях в различных областях жизни. В результате цифровизации многие процессы в нашей повседневной жизни становятся гораздо проще.

При этом следует отметить, что процессы цифровизации выявляют две разные части в деятельности государства. Первая часть – это традиционные сферы его деятельности: правопорядок, оборона, социальные услуги. В этих сферах процессы цифровизации обычно оцениваются по модели затраты – некий набор показателей.

При этой модели проблема возникает с правильным выбором показателя; а если их несколько, то выбора из них главного или распределения в избранном наборе показателей их относительного веса.

Это весьма сложная задача, и единого, универсального метода ее решения, по-видимому, не существует. В качестве частного примера можно привести меры по ограничению потребления алкоголя и табака (ограничения доступности этих товаров, запрет на он-лайн продажи и отпуск их несовершеннолетним и т.д.).

Вторая часть относится к собственно цифровой экономике. В ней, как и в любом виде хозяйственной деятельности, правильная модель может быть следующей: затраты – их окупаемость – прибыль.

В сфере цифровой экономики необходимо либо научить чиновников думать и работать как предпринимателей (для успешного развития), либо отдать всю эту сферу частному бизнесу, предусмотрев при этом условия его косвенной поддержки (например, налоговыми льготами) и стимулирования его деятельности именно в желательном для государства направлении (примерно так, как США содействуют развитию международных систем торговли).

В связи с этим можно предложить следующее: для финансирования каждой программы (направления) цифровизации необходимо разработать механизм (модель) возврата государству средств, вложенных в ее реализацию – с определением сроков окупаемости и ответственных за эту окупаемость лиц.

Необходимо отметить, что распространение безналичных расчетов – не самое главное. Главный узел цифровой экономики – как ее на самом деле реализуют во многих странах – это вовсе не безналичные расчеты сами по себе, не повсеместный доступ к интернету, не интернет вещей, не дополненная (виртуальная) реальность и т.п.

Главное, это – **Big data** (большие данные), огромные объемы данных о реальных людях и их действиях, которые создает цифровая экономика, и технологии их обработки. Строители цифрового будущего представляют big data неизбежностью, неотъемлемой частью цифровой экономики. Хотя, на самом деле, использование интернета, безналичных расчетов и всего того, что действительно сокращает издержки, упрощает нашу жизнь, вовсе не связано с big data. Телефонный разговор сокращает расходы, ускоряет рабочий процесс, но вот его хранение и анализ экономическому росту, в целом, никак не помогает. Использование интернета и обработка данных о всех ваших действиях в интернете – это две большие разницы. Безналичные расчеты и анализ ваших личных безналичных платежей – это не одно и то же.

Big data — подход/метод обработки большого числа структурированных и неструктурированных данных для получения новой информации, которые тяжело обработать обычными способами.

Неструктурированные данные – данные, которые находятся в хранилище организации без какого-либо намерения их «оркестровки», структурирования или категоризации. Как правило, анализ неструктурированных данных включает анализ каждого объекта. К ним относятся документы, медиа-файлы и изображения. Анализ неструктурированных данных обычно проводится для поиска информации, скрытых тенденций и взаимосвязей внутри элементов информационного потока.

Действительно, между IT-технологиями и тотальной обработкой информации о ваших действиях нельзя ставить знак равенства. При этом важно понять, что Big data может стать крайне опасной вещью, которая в потенциале может создавать небывалые риски и угрозы как государству (его политическому строю), так и населению страны.

Конечно, о неизбежности использования новых технологий можно и нужно говорить, они дают реальные и ощутимые экономические выгоды, а значит этот процесс всегда будет естественно развиваться.

Но любые выгоды в этой сфере всегда следует соотносить с рисками и новыми угрозами, которые они несут.

Итак, дает ли экономические выгоды стране развитие цифровой экономики? Да, например, снижение транзакционных издержек.

Но полностью полагаться на цифровую экономику как на главный локомотив роста в XXI веке нельзя, цифровая экономика – лишь часть реальной экономики, отдельные бизнес-процессы, ушедшие в IT-сферу. Хлеб, как и раньше, нужно выращивать, даже если есть возможность его заказа в интернете. Человек существует в материальном мире и его материальные потребности от всеобщего перехода на «цифру» никуда не денутся.

Цифровая экономика может улучшить отдельные сферы и отрасли экономики, а некоторые даже преобразовать. Но никакого фундаментального решения экономических вопросов она, в принципе, дать не может.

Цифровая экономика создает колоссальные массивы информации о всем населении, о его действиях – именно те самые Big data. И ключевой вопрос здесь – **кто будет контролировать эти данные? Поскольку тот, кто будет контролировать эти базы данных, будет иметь подавляющее влияние на все население страны.**

Будет ли эти данные контролировать **только и исключительно** государство, в лице государственных банков, профильных министерств и специальных служб. Ведь к этой информации обязательно сразу захотят получить несанкционированный доступ. А, имея неограниченные финансовые и технологические возможности, некоторые организации вполне могут получить определенный доступ.

Уже сегодня они обладают большей частью подобных данных – смартфоны и планшеты работают на iOS или Android, на персональных компьютерах установлена Windows, а карты банка – это во многом Visa или Master Card. И это не говоря уже про «железо»: платежная и сетевая инфраструктура, сами хранилища данных и многое другое.

Поэтому главный вопрос сейчас: стоит ли спешить перевести всю страну на «цифру» с обязательной обработкой информации на big

data, ведь предварительно необходимо обеспечить **национальные интересы** в этой сфере – защитить информацию людей и государства.

Можно утверждать, что любые выгоды государства от использования big data должны быть соизмеримы с угрозами в виде потенциальной утечки собираемой информации к другим государствам.

Многие эксперты полагают, что на начальном этапе необходимо добиться, как минимум, трех **концептуальных ограничений** на законодательном уровне, которые жизненно необходимы для сохранения свободы и безопасности.

Первое – необходимо сохранить все нецифровые альтернативы в нашей жизни – от наличных денег до почтовых отправлений. **Второе** – необходимо создать такие условия, при которых данные, при наличии технической возможности, передавались бы человеком сознательно и исключительно на добровольной основе.

И третье – использование собираемых личных данных должно быть строго ограничено. К примеру, можно анализировать административные правонарушения населения, но нельзя на основании этого анализа осуществлять какие-либо санкции, меры наказания или поощрения в отношении конкретного лица.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Риски и угрозы в сфере распространения информационных технологий.
2. Взаимосвязь основных прав человека и угроз внедрения цифровых технологий.
3. Киберпреступность как основная угроза информационной безопасности.
4. Основные положения «Стратегии научно-технологического развития России».
5. Проблема контроля сверхобъемных баз данных (Big data).