https://doi.org/10.5281/zenodo.4686878
УДК 330.88

Клоков Д.В.

Клоков Денис Викторович, кандидат экономических наук, доцент, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Россия, 119571, г. Москва, проспект Вернадского, 82, стр.1. E-mail: klokov-dv@ranepa.ru.

Цифровое общество: основные препятствия на пути цифровой трансформации

Аннотация. В статье раскрываются подходы к исследованию понятия «цифровое общество», рассматриваются пути перехода к нему. Автором систематизированы основные технологии, рассматриваемые исследователями в качестве основы цифровой трансформации. Доказано, что активное использование возможностей современных информационных технологий влечет за собой как позитивные, так и негативные последствия. Обозначены угрозы цифровой трансформации, даны рекомендации по их нейтрализации.
Ключевые слова: трансформация, цифровое общество, угрозы, большие данные, интернет вещей, умный дом, умный город.

Klokov D.V.

Klokov Denis Viktorovich, PhD in economics, associate professor, Russian Presidential Academy of National Economy and Public Administration, Russia, 119571, Moscow, prospekt Vernadskogo, 82, p.1. E-mail: klokov-dv@ranepa.ru.

Digital Society: Key Barriers to Digital Transformation

Abstract. The item shows approaches to the research of the concept of "digital society", discusses the ways of transition to it. The author systematizes the main technologies considered by researchers as the basis of digital transformation. It is proved that the active use of current information technologies entails both positive and negative consequences. The risks of digital transformation are identified, recommendations for their neutralization are given.
Key words: transformation, digital society, risks, big data, internet of things, smart home, smart city.

Цифровое общество рассматривают как пятый тип общества, которому последовательно предшествовали информационное общество, индустриальное, аграрное, общество охотников и собирателей. Рассуждая историческими категориями, информационное общество – это очередной этап развития, базирующийся на информационном обществе и отличающийся от него увеличением масштаба внедрения информационных технологий в различные сферы жизни.

Фундаментальной основой взаимодействия в цифровом обществе выступает всемирная сеть «Интернет», а в качестве важных технологий – Big Data, искусственного интеллекта (Artificial Intelligence), квантовые технологии, виртуальной реальности (Virtual Reality), дополненной реальности Augmented Reality и Blockchain. Процесс накопления ресурсов и знаний в цифровом обществе аккумулируется в сетевом пространстве с помощью технологий «Big Data», с помощью «искусственного интеллек-

та» принимается всё больше решений, в определённых сферах квантовые процессоры на порядок увеличили скорость вычислений, виртуальная и дополненная реальность кардинально изменяют восприятие окружающего мира, а технологии распределённого реестра создают доверенные и географически разнесённые вычислительные мощности.

Названные технологии становятся основными движущими силами в цифровой трансформации, посредством которой информационное общество преобразуется в цифровое общество. Современные информационные технологии принято считать «всепроникающими», в результате формируются новые модели взаимодействия в экономике, науке, культуре и других областях.

Таким образом, цифровую трансформацию следует рассматривать как «процесс интеграции, внедрения и проникновения цифровых технологий во все аспекты жизни общества, которые требуют коренных изменений технологий создания новых продуктов и услуг, изменения культуры социально-экономических отношений, проводимых изменений и принципов построения новых моделей государства и бизнеса» [1, С. 33].

Механизмы проникновения цифровых технологий в различные сферы жизни реализуются на основе концепции «Интернета вещей» (Internet of Things, IoT), далее на её фундаменте выстраиваются системы «умного дома» (smart home) и «умного города» (smart city). Internet of Things позволяет осуществить взаимодействие человека и объектов физического мира с помощью цифровых инструментов, которые проводят телеметрические измерения и на основе полученной информации принимают решения.

Технический прогресс более ста лет назад дал людям возможность использовать в промышленности, а позже в бытовом обиходе, автоматические датчики и инструменты управления, которые позже стали подключать к компьютерам и объединять в системы промышленного масштаба. Современные сенсоры сравнительно недороги в производстве и обслуживании, они доступны, их функции разнообразны и их количество постоянно расширяется.

Приобретаемый сегодня автомобиль считается несовременным, если у него отсутствует набор, включающий в себя датчики парковки, мёртвых зон, дождя и света. Умные элементы давно и прочно вошли в жизнь людей, которые привыкли к предлагаемым удобствам и вряд ли захотят с ними расстаться.

На базе интернета вещей создаются комплексные системы умного дома, формируется экосистема умных городов. Уже сейчас большинство Iot-устройств имеют подключение к интернету. Перечислять их преимущества можно долго, но существует один критически важный недостаток, способный нивелировать все приобретаемые плюсы. Это слабый уровень информационной безопасности Iot-устройств, вследствие чего возникают угрозы их неправомерного использования преступными элементами, компрометации и незаконной коммерциализации пользовательских данных. Решение проблемы защищённости умных устройств осложняется рядом факторов.

Это недостаточная осведомлённость пользователей Iot-устройств о потенциальных угрозах, непонимание возможных последствий невнимательного отношения к ним создают предпосылки к появлению инцидентов информационной безопасности. Единственное на что обращают внимание пользователи – это появление платных функций на таких устройствах. В остальном пользователи практически не изучают инструкции и предостережения, работают на заводских настройках по умолчанию, не следят за выходом обновлений.

С другой стороны, производители Iot-устройств не всегда стремятся вкладывать средства, силы и время в разработку инструментов защиты. Для организации работы по согласованию промышленных стандартов и необходимых требований по

безопасности относительно недавно сделаны первые шаги в сторону саморегулирования сферы Internet of Things. Ряд представителей профессионального сообщества предлагают определённую методику достижения оптимального уровня безопасности при использовании устройств Интернета вещей, объединяясь в саморегулируемые организации и следуя установленным в них правилам [2].

Отдельные Iot-устройства в рамках концепции «умный дом» объединяют в комплексно функционирующую систему, в её рамках происходит автоматизация рутинных действий, упрощение контроля и управления (приборы для сферы электро- и теплоснабжения, автоматические счётчики воды, управления автоматическим открытием/закрытием дверей и др.). Такие удобства имеют свои побочные эффекты, которые заключаются в практической сложности определения юридической ответственности в случае некорректного срабатывания устройств. В качестве примера: как определить виновника в ситуации дорожно-транспортного происшествия с беспилотным автомобилем, используемого в качестве такси, или ошибочного срабатывания системы умного дома, запирающего своего владельца и тем самым подвергающего его жизнь опасности.

Достаточный уровень безопасности должен выступать одним из приоритетных направлением развития Интернета вещей наряду с функциональными возможностями и удобством использования.

Технология «Умный город» включает более объёмный набор технологий, к которым помимо Интернета вещей относят составляющие транспортной инфраструктуры, необходимой для связи умных устройств, а также средства анализа, управления и унификации данных («Big Data»).

Следует отметить, что «проекты умный город требуют разработки концепции, принципов, архитектуры (модели), соответствующих региональной (городской) концепции развития и поддержанных основными заинтересованными сторонами – властью, бизнесом, горожанами» [3, С. 695]. Умный город – это комплекс взаимоувязанных систем из таких сфер, как энергетика, водоснабжение, транспорт, безопасность, образование и здравоохранение, государственного управления.

Каждая из обозначенных сфер требует пристального внимания к вопросам безопасности и обеспечения необходимого уровня защиты. Наибольшую обеспокоенность вызывает сфера энергетики, водоснабжения и транспорта, которые являются «артериями» любого крупного города. Ежегодно фиксируется кибератаки на промышленные объекты, часть из них достигает деструктивного результата. В 2010 году была выведена из строя система управления атомной электростанции в Иране, было остановлено более тысячи центрифуг по обогащению урана. В 2014 году была взломана корпоративная сеть южнокорейской управляющей компании, обслуживающей реакторы на атомных электростанциях «Кори» и «Вольсон» [4]. Не все результаты атак достигают производственных систем, но успех некоторых из них заставляет относится к вопросам безопасности с повышенным вниманием.

Постоянно расширяются масштабы распространения компонентов «носимого интернета» (Body net), которые условно можно разделить на следующие категории: 1) микрокомпоненты и миниатюрные устройства, имплантируемые в тело человека в следствии медицинских показателей (контроль уровня сахара, кардиостимулирующие устройства и др.); 2) элементы одежды, измеряющие телеметрические показатели или добавляющие комфорт (фитнесс-трэкеры, куртки с обогревающими элементами и пр.); 3) носимые устройства дополненной реальности, сбалансированные с точки зрения компактности, разрешения и размеров просмотровой области (самый популярный пример – Google Glass). Сохраняется тренд роста количества имплантируемых элементов. Эксперты считают, что в ближайшие десять лет такая практика перестанет быть

экзотической и будет рассматриваться в качестве повседневного явления.

Несмотря на очевидные плюсы и дальнейший потенциал использования, в технологии Body net следует так же учитывать аспект безопасности. Такие системы должны быть надёжно защищены, чтобы исключить ошибочные решения и потенциальную возможность несанкционированного подключения злоумышленника с целью навредить человеку. Периодически появляются сообщения о найденных уязвимостях в кардиостимуляторах, с помощью которых возможно их удалённое управление и принудительное включение неприемлемых для жизни и здоровья пациента режимов работы устройств [5].

Кроме того, процесс цифровой трансформации – это не только технологии, но и их грамотное применение, для которого требуются интеллектуальные лидеры и ответственные исполнители. Такое положение ставит амбициозные задачи для образовательной системы, как в сфере высшего, так и среднего образования. На российских площадках необходимо устраивать больше интеллектуальных баталий, формировать «фабрики идей», организовывать кооперацию сильнейших высших учебных заведений.

К понятию «цифровое общество» следует относиться как к многоаспектной категории, так как оно затрагивает сферу экономики, технологий, социокультурного взаимодействия. В таком обществе кардинальным образом меняется экономическая система, её правила, трансформируется характер труда. Одним из экономических приоритетов наравне с капиталом становится креативность появляющихся идей, открытые возможности для развития человека и общества, гарантией прав личности и его персональных данных, защитой членов общества от манипулирующих воздействий.

Успешная цифровая трансформация принципиально возможна в российских реалиях, в нашей стране есть необходимый потенциал. Важно правильно им воспользоваться, чтобы цифровая трансформация не осталось лишь модным трендом, а превратилась в полноценный инструмент достижения нашей страной высоких экономических показателей.

СПИСОК ЛИТЕРАТУРЫ

1. Удалов Д.В. Цифровая трансформация социально-экономического пространства // Вестник СГСЭУ. 2020. № 3 (82), С.33-36.
2. Internet of Things (IoT) Trust Framework v2.5. Режим доступа к журн. URL: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/ (дата обращения: 18.03.2021).
3. Кононова О.В. Павловская М.А. Технологии цифровой экономики в проектах умный город: участники и перспективы // Современные информационные технологии и ИТ-образование. Том 14. № 3 (2018), С. 692-706
4. Кибератаки на ядерные объекты. История вопроса. URL:https://www.kommersant.ru/doc/3196397 (дата обращения: 10.03.2021).
5. Американские кардиостимуляторы оказались уязвимы для хакеров. Режим доступа к журн. URL: https://www.vedomosti.ru/technology/articles/2017/08/31/731824-kardiostimulyatori (дата обращения: 18.03.2021).

REFERENCES (TRANSLITERATED)

1. Udalov D.V. Cifrovaja transformacija social'no-jekonomicheskogo prostranstva // Vestnik SGSJeU. 2020. № 3 (82), S.33-36.
2. Internet of Things (IoT) Trust Framework v2.5. Rezhim dostupa k zhurn. URL: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/ (data obrashhenija: 18.03.2021).

3. Kononova O.V. Pavlovskaja M.A. Tehnologii cifrovoj jekonomiki v proektah umnyj gorod: uchastniki i perspektivy // Sovremennye informacionnye tehnologii i IT-obrazovanie. Tom 14. № 3 (2018), S. 692-706
4. Kiberataki na jadernye ob#ekty. Istorija voprosa. URL:https://www.kommersant.ru /doc/3196397 (data obrashhenija: 10.03.2021).
5. Amerikanskie kardiostimuljatory okazalis' ujazvimy dlja hakerov. Rezhim dostupa k zhurn. URL: https://www.vedomosti.ru/technology/articles/2017/08/31/731824-kardiostimulyatori (data obrashhenija: 18.03.2021).

Поступила в редакцию 18.03.2021.
Принята к публикации 21.03.2021.

Для цитирования:
Клоков Д.В. Цифровое общество: основные препятствия на пути цифровой трансформации // Гуманитарный научный вестник. 2021. №3. С. 194-198. URL: http://naukavestnik.ru/doc /2021/03/Klokov.pdf