

Недостатки аддитивных технологий [1]:

1. Благодаря специфике наращивания деталей в ее структуре могут образовываться маленькие поры, которые не могут использоваться для хранения некоторых жидкостей (как пример – гелия).

2. Если сравнивать с цельным куском металла, обработанного точением и сверлением, наращенный металлический порошок из-за своей структуры имеет сравнительно меньшую прочность.

3. Дорогие расходные материалы, что связано с использованием при наращивании большого количества металлического порошка и инертных газов.

4. Из-за скорости печати возможны отклонения в производстве, которые в последствии необходимо устранять традиционной обработкой.

5. Деталь содержит много ненужных структур, которые используются в качестве поддержки. Данный недостаток устраняется при помощи фрезерного станка, токарного станка или ручной обработкой. Некоторые станкостроительные предприятия предлагают гибридные станки, сочетающие в себе аддитивные и фрезерные технологии, которые помогают устранить данный недостаток.

Аддитивное производство развивается стремительными темпами, дополняя традиционное создание деталей, а местами даже заменяя его. Уже в ближайшем будущем найдутся решения, которые обратят недостатки наращивания деталей в преимущество, и тогда уже можно будет говорить о полноценной замене традиционного производства аддитивным.

Нами предлагается рассматривать данные разработки, а именно аддитивное производство и 3D-печать, в качестве базового проекта цифровой трансформации предприятий сельскохозяйственного машиностроения Республики Беларусь.

Нами рекомендуется для ускорения успеха цифровой трансформации предприятий сельскохозяйственного машиностроения Республики Беларусь следующее: 1. Ввести аудит состояния цифровой трансформации на промышленном предприятии и в отрасли в целом. 2. Организовать непрерывное обучение работников предприятия овладению новыми технологиями. 3. Определять объемы инвестиций с требованиями цифровой трансформации. 4. Разработать дорожную карту по поэтапному внедрению новых технологий в соответствии с цифровой трансформацией промышленного предприятия по схеме «От простого к сложному». 5. Сделать приоритетной цифровую трансформацию и инновации.

Библиографические ссылки

1. Аддитивные технологии : [Электронный ресурс]. URL: <https://tjournal.ru/flood/168194-additivnye-tehnologii-cto-eto/> (дата доступа: 15.09.2021).

2. «Консом групп»: цифровизация руками системного интегратора : [Электронный ресурс]. URL: <https://controleng.ru/wp-content/uploads/9312.pdf/> (дата доступа: 15.09.2021).

3. Коробач А. А. Необходимость и предпосылки инновационного развития сельскохозяйственного машиностроения Республики Беларусь в современных условиях // Известия Гомельского государственного университета имени Ф. Скорины. Социально-экономические и общественные науки. № 5. С. 140–146.

УДК 338.23

РИСКИ И ОПАСНОСТИ ЦИФРОВОЙ ЭКОНОМИКИ

В. В. Кравцова¹⁾, Д. В. Ковалевич²⁾, Л. О. Кулакова³⁾ (научный руководитель)

¹⁾ студент, Брестский государственный технический университет, Брест,
Республика Беларусь, bella_belkaa@mail.ru

²⁾ студент, Брестский государственный технический университет, Брест, Республика Беларусь, bella_belkaa@mail.ru

³⁾ старший преподаватель, Брестский государственный технический университет, Брест, Республика Беларусь, lejla67@mail.ru

В статье рассматриваются проблемные вопросы, связанные с рисками и опасностями цифровой экономики. Проанализирована проблематика сущности и положения о цифровой экономике, соотнесены материальные и нематериальные аспекты рассматриваемого вопроса. В работе большое внимание уделяется понятиям цифровой экономики и проводится сравнительная характеристика. Автор формулирует предложения по совершенствованию формирования информационной деятельности. Большое внимание в статье уделяется рискам цифровой экономики, исходящим от сквозных технологий, которые требуют ответных действий.

Ключевые слова: сквозные технологии; цифровая экономика; квантовые технологии; интернет вещей; нейронная сеть.

RISKS AND DANGERS OF THE DIGITAL ECONOMY

V. V. Kravtsova¹⁾, D. V. Kovalevich²⁾, L. O. Kulakova³⁾ (supervisor)

¹⁾ Student, Brest State Technical University, Brest, Republic of Belarus, bella_belkaa@mail.ru

²⁾ Student, Brest State Technical University, Brest, Republic of Belarus, bella_belkaa@mail.ru

³⁾ Senior Lecturer, Brest State Technical University, Brest, Republic of Belarus, lejla67@mail.ru

The article examines problematic issues related to the risks and dangers of the digital economy. The problematics of the essence and provisions of the digital economy are analyzed, the material and non-material aspects of the issue under consideration are correlated. The work pays great attention to the concepts of the digital economy and provides a comparative characteristic. The author formulates proposals for improving the formation of information activities. The article focuses on the risks of the digital economy posed by end-to-end technologies that require a response.

Keywords: end-to-end technologies; digital economy; quantum technologies; internet of things; neural network.

Прежде всего, для понимания важности цифровой экономики, следует понимать, чем на самом деле она является. Под цифровой экономикой понимают деятельность по созданию, распространению и использованию цифровых технологий сбора, хранения, обработки, поиска, передачи и представления данных в электронном виде и связанных с ними продуктов и услуг. При переходе к цифровой экономике изначально предполагался перенос обычных коммерческих сделок в цифровую среду, однако в последнее десятилетие термин цифровой экономики быстро расширяется: до цифрового образования, здравоохранения, а в самых высокоразвитых странах до «электронных» правительств и государств [1].

Возникновение и быстрое развитие новых информационных технологий нередко несет в себе не только лишь новые возможности, которые содействуют оптимизации процессов взаимодействия, но и сопровождается возникновением новых угроз безопасности, которые, в случае их игнорирования, могут сильно навредить и сократить полезность от внедрения технологий в больших размерах. Информационные технологии нуждаются в усиленной безопасности, что вынуждает просчитывать предварительно все опасности и риски.

На данный период сквозными технологиями, оказывающими большое воздействие на развитие экономики, а значит и основными ключами угроз в цифровой экономике являются: интернет вещей (IoT – Internet of Things), искусственный интеллект, Big Data, блокчейн и квантовые технологии.

В последние годы производителям стали доступны беспрецедентно недорогие высокотехнологические устройства, способные сочетать в себе функции, которые еще несколько десятилетий назад требовали по отдельному устройству для каждой задачи. На базе интернета вещей разрабатываются технологии мониторинга здоровья, окружающей среды. С развитием цифровой экономики все интернет вещей все глубже вводится во все аспекты человеческой жизни, на сегодняшний день даже государственные структуры сильно зависимы от интернета.

Основная угроза, несомая интернет вещей – вероятность подключения злоумышленников к IoT-устройствам. IoT-устройства не обладают высокой производительностью и, как правило, предназначены для выполнения элементарных функций, но при этом могут обладать датчиками, способными предоставлять приватную информацию: диктофоны, камеры. Невысокая производительность вынуждает разработчиков снабжать свои устройства слабой, не требовательной к производительности защитой от взлома, что делает их легкодоступной целью. Ярким примером может стать ботнет Mirai: сеть из полумиллиона взломанных веб-камер, входящих в интернет вещей, при поддержке которой была совершена самая сильная DDoS атака на 2016 год.

Следующая технология – искусственный интеллект (ИИ). Первым делом, следует отметить, что нынешний «искусственный интеллект» таким не является – это не осознающая себя программа в компьютерной среде, а в лучшем случае, нейронная сеть, заточенная под исполнение какой-либо поставленной задачи. Этот тип ИИ называется «слабым ИИ». Нейронные сети всего за несколько лет плотно интегрировались в цифровую экономику: их используют для создания подробных, точных прогнозов, анализа больших объемов информации и для узнавания образов.

Нейронная сеть не программируется в прямом смысле данного слова, а обучается сама на основе данных, предоставленных людьми. Учитывая очень высокую точность работы правильно обученных нейросетей, люди могут перекладывать на них все более серьезные задачи, не учитывая один фактор: набор данных, датасет, на котором проводилось обучение, может оказаться неверным, из-за случайности или по вине злоумышленников. Если нейросеть обучить на неправильном наборе данных, она будет непрерывно ошибаться. Данное явление, приводящее к ошибочному обучению сети, называют DataPoisoning. К настоящему моменту не изобретено действенного способа противодействия, помимо прямой проверки работы, выполненной нейросетью.

Третья сквозная технология – Big Data, или большие данные. Изначально термин обозначал быстрый рост объема цифровой информации после начала 21 века. В современном контексте большие данные – по-настоящему большой набор слабосвязанных между собой данных, которые, до недавнего времени, не могли быть обработаны как единое целое. Проблема анализа Big Data содержится не только в размере: в большие данные могут входить не только стандартизированные базы данных, но и всевозможные другие виды информации, текст, видеозаписи и изображения, программный код, геоданные; достаточно проблематично анализировать все эти типы данных разом. С развитием перечисленных ранее технологий искусственного интеллекта появилась вероятность полного анализа: специально обученная нейросеть может проанализировать внешне слабосвязанный массив данных и объединить их, установить связи между объектами в наборе информации и извлечь из всего массива смысл, очевидный человеку.

Четвертая сквозная технология – блокчейн. Технология блокчейна практически гарантирует безопасность данных пользователей. По сути, это база данных, однако находящаяся не на одном сервере, а распределенная по устройствам пользователей. Впервые эта технология была использована в первой криптовалюте, биткойне [2]. Основная

задача блокчейна в системе биткоина – сдерживание повторной траты средств. В материальном мире после приобретения товара потребитель отдает деньги продавцу, и не может израсходовать те же деньги второй раз. В цифровом пространстве при условии недоступности контроля со стороны регулирующих органов правонарушитель может создать копию цифровой валюты. Система блокчейна не позволяет потратить одну сумму несколько раз.

Особенно удобен блокчейн для записи факта перевода средств и подтверждения подлинности личности (путем предоставления индивидуального ключа) так что неудивительно, что первыми заинтересованными в ней лицами были банки.

С начала существования технологии было открыто множество ее уязвимостей:

1. Атака 51 %. Если большая доля вычислительной мощности всей распределенной сети контролируется одним участником, или несколькими, функционирующими сообща, этот участник может контролировать всю блокчейн-сеть.

2. Атака Сибиллы. Технология блокчейна не позволяет наверняка отличать физические устройства; проще говоря, один компьютер может выдавать себя за несколько пользователей, что позволяет устроить атаку 51 %.

3. Квантовые вычисления. Вся система блокчейна держится на мощной защите от взлома, так, чтобы подобрать пароль для взлома одного аккаунта через перебор паролей, одному компьютеру может понадобиться миллион лет. Эта задача непосильна для обычных компьютеров, но как будто специально создана для квантовых: самой сильной стороной квантовых вычислений принято считать задачи на перебор значений. Так, первые прототипы квантовых компьютеров, например D-Wave от Google, производительнее классических в несколько тысяч раз. Уже сегодня проводятся разработки блокчейн-систем, устойчивых к квантовым вычислениям, но пока абсолютный успех достигнут не был.

Заключительной ключевой технологией, упоминаемой в статье, будут квантовые технологии.

На основе квантовых технологий разрабатываются компьютеры, использующие квантовые эффекты, прежде всего, эффект квантовой запутанности, когда два атома сопряжены между собой и моментально реагируют на изменения друг друга. Как было сказано выше, квантовые компьютеры способны на вычисления, которые выглядят невыполнимыми для обычных компьютеров, на базе квантовой запутанности можно создать шифр, который не взломать в принципе – это прописано законами физики, создать моментальную связь методом квантовой телепортации и т. п. Создание первого полноценного квантового компьютера предполагается к 2025–2030 годам.

Таким образом, нынешние сквозные технологии, находящиеся еще в зачаточном состоянии, стремятся к полноценному выходу на рынок цифровой экономики, невзирая на неполную оценку угроз, исходящих от них. Своевременная оценка всех опасностей, угрожающих цифровой экономике и выработка соответственных ответных мер, обязана стать одной из основ формирования информационной отрасли [3].

Библиографические ссылки

1. Юдина Т. Н. Осмысление цифровой экономики // Теоретическая экономика. 2016. 16 с.
2. Афонасова М. А. Системная трансформация и блокчейн технологии в сфере государственного управления // Системный анализ в проектировании и управлении» (SAEC-2018) : труды XXII Междунар. науч.-практ. конф. СПб. : Изд-во политехн. ун-та, 2018. 319 с.
3. Алексеев И. В. Цифровая экономика: особенности и тенденции развития электронного взаимодействия // Актуальные направления научных исследований : материалы X Междунар. науч.-практ. конф., Чебоксары, 18 дек. 2016 г. / редкол. Широков О. Н [и др.]. Чебоксары : Интерактив плюс, 2016. № 4(10). С. 42–45.