Научная статья
Original article

Анализ современных рисков развития цифровых технологий

Зяблина И.И.
Уральский федеральный университет, Екатеринбург, Россия
Автор-корреспондент: zyablinba-ii7@inbox.ru

Аннотация: В статье описаны опасности и риски, сопровождающие стремительное развитие цифровых технологий в экономической сфере. Определена роль процессов совершенствования средств и методов информационной защиты в становлении электронного бизнеса и коммерции.

Ключевые слова: цифровая трансформация, цифровая экономика, интернет вещей, блокчейн.

Для цитирования: Заблина И.И. Анализ современных рисков развития цифровых технологий. Умная цифровая экономика. 2022. Т.2, №3, с. 68-71

Analysis of modern risks of digital technologies development

Zyablina I.I.
Ural Federal University, Yekaterinburg, Russia
Corresponding author: zyablinba-ii7@inbox.ru

Abstract: The article describes the dangers and risks that accompany the rapid development of digital technologies in the economic sphere. The role of processes for improving the means and methods of information protection in the development of electronic business and commerce is determined.

Keywords: digital transformation, digital economy, internet of things, blockchain.

For citaion: Zyablina I.I. Analysis of modern risks of digital technologies development. Smart digital economy. 2022. Т.2, №3, pp. 68-71

Переход на цифровую экономику представляет собой перевод всех классических бизнес-процессов в электронную среду.

Возникновение, быстрое совершенствование инновационных информационных технологий несут в себе не только новые перспективы, но и неизвестные ранее угрозы и риски безопасности, которые следует просчитывать заранее в целях их предотвращения или минимизации [1, с. 150].

На сегодняшний день главными источниками угроз для экономической деятельности, основанной на цифровых технологиях, специалисты называют:

1. устройства, объединенные в компьютерную сеть для сбора, обработки, передачи информации иным объектам посредством программного обеспечения, приложений, технических устройств;

CC BY NC

2. интеллектуальные системы, обладающие творческими функциями;

3. Big Data;

4. последовательные цепочки содержащих данные блоков, выстроенные по определенным алгоритмам;

5. технологии, основанные на принципах квантовой механики.

Интернет вещей опасен прежде всего достаточно несложным подключением к IoT-устройствам, зачастую передающим приватные сведения, лиц с корыстными намерениями. Легкая доступность этих устройств объясняется их низкой производительностью, вынуждающей разработчиков устанавливать слабую защиту от взлома.

Искусственный интеллект пока еще не осознает себя в компьютерной среде, предназначен большей частью для решения ограниченного круга задач. Однако если нейросеть обучена правильно, она может выполнять весьма сложные работы. Главное не допустить неверного набора данных для ее обучения. Это позволить предотвратить ошибки ИИ. На сегодняшний день нет идеальных методик, исключающих неверное обучение сети. Единственным приемлемым способом является тщательная проверка осуществленных ею операций [2, с. 62].

Проблем, связанных с Big Data, две:

1. Гигантские размеры.

2. Сложности с одновременным анализом данных разных типов – информации, видео, программных кодов, сведений о пространственных объектах.

В настоящее время специалисты активно обучают нейросети анализировать и объединять массивы данных, на первый взгляд слабо связанных друг с другом, разъяснять человеку смысл, обнаруженный в результате установления связей между объектами в потоке информации.

Вследствие того, что в рамках технологии блокчейн данные содержатся не на одном сервере, а распределены по устройствам многих лиц, использующих действующую систему, им обеспечена высокая сохранность. Но и эта технология связана с многочисленными рисками. Для простоты восприятия на рисунке 1 показан принцип работы блокчейн-технологии

CC BY NC

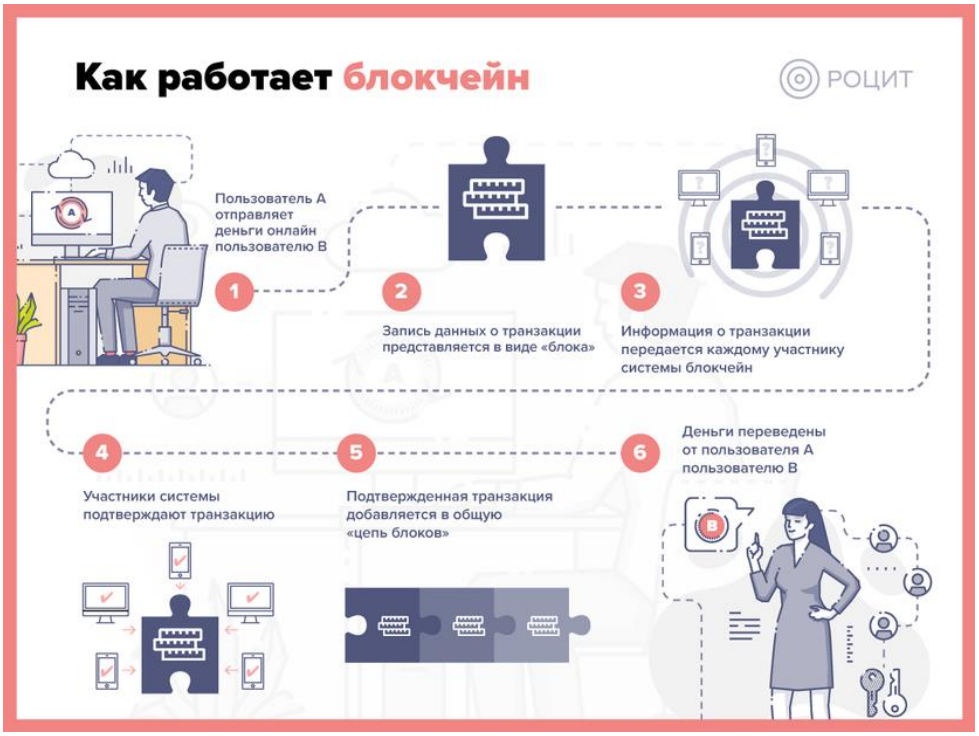

Рисунок 1 – Принцип работы блокчейн-технологии [1]

Во-первых, один участник, контролирующий большую долю вычислительной мощности распределенной сети (даже если совместно действуют несколько участников), может взять под единоличный контроль всю блокчейн-сеть.

Во-вторых, блокчейн практически не различает физические устройства. А это значит, что один ПК может выдать себя за несколько лиц, которые применяют систему. И это, в свою очередь, создаст предпосылки для 51%-ного захвата хершейта сети.

В-третьих, классический компьютер не может взломать мощную систему защиты блокчейна путем подбора пароля. Но с этой задачей легко справится квантовый компьютер, мгновенно осуществляющий перебор огромного количества значений.

Несмотря на то, что уже существуют устойчивые к квантовым вычислениям блокчейн-системы, до успеха в этой сфере еще далеко.

Компьютеры, основанные на квантовой запутанности, будут создавать не подлежащие взлому шифры. Но пока еще они находятся в стадии разработки.

Основными объектами, воздействие на которые вызывает разнообразные риски в электронных бизнесе и коммерции, являются люди, технологии, информация и экономика.

Для минимизации связанных с человеком опасностей необходимо четко определить его место и роль (потребитель, наблюдатель, создатель благ) в системе новых отношений.

В целях предупреждения выхода технологий из-под контроля людей следует осмыслить такое зарождающееся явление, как самопроизводство методов производственной деятельности, то есть массовое производство самим технологиями новых технологий.

В нынешнем обществе превалирующую роль исполняет информация, влияющая на политическую, экономическую, социальную сферы общественной жизни. Основой цифровой

CC BY NC

экономики становятся огромные массы и потоки сведений, что влечет за собой определенные угрозы.

Информация может быть противоречивой и недостоверной, так как из-за большой интенсивности ее трудно систематизировать и фильтровать.

Вследствие плюрализма мнений и множественности источников данных трудно выработать единообразное мнение, обнаружить истину [3, с. 11].

Повышение производительности труда, увеличение общего блага в результате внедрения цифровых технологий имеют и отрицательные последствия: замещение рабочих роботами ведет к технологической безработице, росту неравенства по возрасту, полу, образованию, исключению населения из экономики. Это может стать причиной мощных социальных взрывов.

Любой риск, связанный с цифровой трансформацией экономики, требует увеличения вложений в обеспечение информационной безопасности..

Список литературы

1. Голикова О.А. Цифровая экономика России: открывающиеся риски и возможности / Голикова О.А., Иода Е.В. // Социально-экономические явления и процессы, Липецк, 2018 г. – № 13 (4) – 147-157 с.
2. Коновалова В.Г. Оборотная сторона медали: социальные и этические проблемы внедрения цифровых технологий. // Управление персоналом и интеллектуальными ресурсами в России (№1 (40), 2019). – 61-67 с.
3. Эскиндаров М.А. Риски и шансы цифровой экономики в России / Эскиндаров М.А., Масленников В.В., Масленников О.В. // Финансы: теория и практика. Т. 23 – № 5. – 2019. – 6-17 с.
4. Пиле Я.Э. Цифровая экономика: точки роста интернет-торговли // Экономика: вчера, сегодня, завтра. 2019. Том 9. № 2А. С. 126-135.
5. Шеремет И.А. Цифровая экономика и кибербезопасность ее финансового сегмента // Научные труды Вольного экономического общества. 2018. Т. 210. № 2. С. 23–34.
6. Барабанов А.А. Социальная экология как фактор развития цифровой экономики в России // Научные труды Северо-Западного института управления РАНХиГС. 2019. Т. 10. № 2 (39). С. 28-33.

© Зяблина И.И., 2022. Умная цифровая экономика. 2022. Т.2, №3

CC BY NC