Министерство образования Республики Беларусь
Учреждение образования
«Полоцкий государственный университет»

УСТОЙЧИВОЕ РАЗВИТИЕ ЭКОНОМИКИ: МЕЖДУНАРОДНЫЕ И НАЦИОНАЛЬНЫЕ АСПЕКТЫ

Электронный сборник статей
II Международной научно-практической конференции,
посвященной 50-летию Полоцкого государственного университета

(Новополоцк, 7–8 июня 2018 г.)

Новополоцк
Полоцкий государственный университет
2018

УДК 338.2(082)

Устойчивое развитие экономики: международные и национальные аспекты [Электронный ресурс] : электронный сборник статей II международной научно-практической конференции, посвященной 50-летию Полоцкого государственного университета, Новополоцк, 7–8 июня 2018 г. / Полоцкий государственный университет. – Новополоцк, 2018. – 1 электрон. опт. диск (CD-ROM).

Впервые материалы конференции «Устойчивое развитие экономики: международные и национальные аспекты» были изданы в 2012 году (печатное издание).

Рассмотрены демографические и миграционные процессы в контексте устойчивого развития экономики; обозначены теоретические основы, практические аспекты управления человеческими ресурсами; выявлены и систематизированы драйверы инклюзивного экономического роста в Беларуси и за рубежом; раскрыты актуальные финансовые и экономические аспекты развития отраслей; приведены актуальные проблемы и тенденции развития логистики на современном этапе; отражены современные тенденции совершенствования финансово-кредитного механизма; освещены актуальные проблемы учета, анализа, аудита в контексте устойчивого развития национальных и зарубежных экономических систем; представлены новейшие научные исследования различных аспектов функционирования современных коммуникативных технологий.

Для научных работников, докторантов, аспирантов, действующих практиков и студентов учреждений высшего образования, изучающих экономические дисциплины.

Сборник включен в Государственный регистр информационного ресурса. Регистрационное свидетельство № 3061815625 от 23.05.2018.

Компьютерный дизайн М. С. Мухоморовой
Технический редактор А. Э. Цибульская.
Компьютерная верстка Т. А. Дарьяновой.

211440, ул. Блохина, 29, г. Новополоцк, Беларусь
тел. 8 (0214) 53 05 72, e-mail: a.lavrinenko@psu.by

ISBN 978-985-531-601-6

ВИДЫ РИСКОВ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

***О.В. Терещенко**, канд. социол. наук, проф., Белорусский государственный университет*
г. Минск, Республика Беларусь

Интернет-пространство, как всякая, и особенно техногенная, среда обитания человека, несет в себе угрозы (социальные риски), вероятность осуществления которых не поддается точному определению. Рассмотрим виды рисков в среде интернета, представляющиеся наиболее распространенными, а именно, техногенные, ресурсные, личностные и коммуникативные.

Техногенные риски. К «чистым» техногенным рискам следует отнести, в первую очередь, *непрозрачность работы информационно-коммуникационных технологий* (ИКТ) – оборудования и программного обеспечения (приложений), – обеспечивающих доступ к ресурсам и сервисам интернета. Рядовой пользователь не получает от разработчиков объективной информации о том, какие данные используют и порождают приложения, выполняющие все более разнообразные функции. Поэтому он(а) имеет весьма поверхностное представление о том, кто и с какой целью использует его(её) данные, предоставленные однажды одному из интернет-ресурсов за предоставление некоторые преимущества, например, при регистрации в международной службе Uber или просто при получении дисконтной карты в магазине.

Огромными объемами информации, накапливающейся в компьютерных системах, ученые, а затем и коммерческие компании заинтересовались уже в 1960-х гг., когда появилась «наука о данных» (data sciences), которая в результате своего развития получила название «больших данных» (big data) к 2002 г., когда персональная информация пользователей, без информированного согласия и даже без ведома, стала доступна любым организациям, имеющим возможность нанять «специалистов по данным», а также частным лицам, располагающим соответствующей квалификацией. Даже Американская ассоциация исследователей общественного мнения, на протяжении десятилетий служившая образцом этичного поведения по отношению к респондентам, традиционно включающего конфиденциальность полученной информации, рассматривает «большие данные» (big data) как новую парадигму социальных исследований, хотя и признает в этом подходе наличие «этических и административных проблем» [10].

Помимо сбора данных об индивиде на разнообразных, в том числе организационных, интернет-ресурсах, возможен также доступ к информации в его личном компьютере, в частности, посредством нерекламируемых специальных функций «новых версий» программного обеспечения (ПО), постоянно навязываемых пользователям, вплоть до прекращения работы «устаревшего» ПО. Используется также возможность трекинга посещений пользователем интернет-ресурсов не только без его согласия, но даже и без извещения, посредством оборудования и ПО, используемого провайдерами.

Разнообразие технических возможностей получить несанкционированный или санкционированный, но не обеспеченный информированным согласием, доступ к персональной информации не позволяет установить полный круг лиц, способных «пробить по базам». Таким образом, непрозрачность ИКТ порождает *риски потери конфиденциальности*, неочевидные для собственников информации, или оцениваемые ими как неизбежные, и в чем-то даже удобные благодаря предоставляемым в обмен «бесплатным» услугам.

Информационные риски. Еще одна группа рисков связана с контентом интернет-ресурсов. В первую очередь, это *дилемма права на доступ к информации и авторских прав*. Право на свободный (бесплатный) доступ к информации, первоначально декларировалось как основополагающий принцип интернета, способствующий развитию демократии. Однако наряду с информацией (включая художественные произведения), размещаемой авторами и владельцами прав собственности, владельцы сайтов, не обладающие такими правами, стали размещать текстовые, аудио- и видеодокументы с целью привлечения посетителей, а затем и с коммерческими целями. В настоящее время право на свободный доступ распространяется, главным образом, на информацию о происходящих событиях (новости), официальную информацию, касающуюся функций государства и органов самоуправления, контент, распространяемый самими авторами; в том числе частично – на научную информацию, коды программного обеспечения, базы данных. Право на доступ к информации поддерживается идеологией сокращения цифрового разрыва (неравенства) между социальными группами и странами с разным уровнем жизни, в том числе Движением за свободный доступ, Движением открытого кода, рядом других влиятельных международных организаций. Основные риски при использовании открытой информации связаны с возможной недостоверностью, предвзятостью, тенденциозностью, неполнотой информации, предоставляемой как бесплатно и без ограничений, так и с определенными ограничениями.

Авторское право на информацию, в том числе находящуюся в открытом доступе, подтверждается знаком охраны авторского права ©, именем или наименованием правообладателя, годом первой публикации произведения. Риски, связанные с нарушениями авторских прав, могут заключаться в несанкционированном доступе к платной или закрытой информации, организации такого доступа (платно или бесплатно) для других пользователей интернета, не обладающих достаточной квалификацией, а также неправомерном использовании информации (например, плагиате).

Помимо рассмотренной выше дилеммы прав на информацию и авторскими правами, риски возникают также в связи с наличием и отсутствием *цензуры и рецензирования*, особенностями их реализации. Цензура применяется государственными органами в соответствии с принятым законодательством в ситуациях, когда контент является запрещенным или не соответствующим возрасту. Тем не менее, существуют риски, когда запрещенный или ограниченный по возрасту контент может не только оказаться доступным, но и навязываться пользователям интернета, включая несовершеннолетних. Рецензирование, в свою очередь, должно быть свойственно образовательным и научным ресурсам, и призвано быть гарантией достоверности, валидности, надежности, репрезентативности, объективности публикуемых результатов. Однако многие ресурсы, по крайней мере, русскоязычные, пренебрегают рецензированием или осуществляют его формально (например, предлагают автору представить вместе с текстом две рецензии докторов наук). Риски, связанные с отсутствием реального рецензирования, свойственны, главным образом, неопытным читателям научной и образовательной литературы (старшеклассникам, студентам).

Сама возможность мгновенного получения «знаний» посредством поисковых систем, у многих молодых людей порождает иллюзию, что знать терминологию становится необязательным, главное иметь – доступ к сети. Отсутствие знания терминологии не позволяет делать компетентные выводы, либо даже «быстрым» умом выводы будут делаться слишком медленно. Если интернет будет отключен или с прибором доступа к нему (компьютером, планшетом, телефоном) что-то случится, то «знания» у таких «специалистов» не останется.

Результаты применения «знаний», полученных в интернете и не подтвержденных другими источниками (фейков), может также привести к непредвиденным последствиям в разных сферах, что наиболее наглядно на примере медицины. Так, «медицинские» риски могут заключаться, в доверии к полученной в интернете консультации «врача», или информации, которой «искренне» делятся пользователи, – с целью продвижения непроверенных препаратов, или услуг «нетрадиционной» медицины. Также «схемы» для самостоятельной постановки диагноза и лечения может предлагаться самыми разнообразными источниками с неочевидными целями.

Личностные риски. *Интернет-зависимость*, которая рассматривается здесь в соответствии с определением О. В. Сергеевой [1, с. 125], представляет собой зависимость от функций, выполняемых компьютерами или другими коммуникационными устройствами – планшетом, мобильным телефоном и т. п. Основными функциями коммуникационных устройств являются доступ к информации, ее обработка и распространение, коммуникация (общение) и времяпрепровождение в виртуальном пространстве. Если у человека в компьютере «вся работа» или даже «вся жизнь» (включая связи с коллегами и родственниками, «френдами» в социальных сетях, постоянными членами форумов и команд в многопользовательских играх; а также галереи фотоснимков, коллекции кинофильмов, собрания шуток, etc.), любое нарушение работы устройства или системы связи может привести к негативным последствиям разной степени тяжести. Зависимость от интернета можно рассматривать в технологическом, социальном и личностном контекстах. Зависимость, связанную с неудобствами, испытываемыми каждым постоянным пользователем интернета при нарушении его работы или доступа к нему, является техногенной; риски здесь связаны, в первую очередь, с надежностью оборудования у самого пользователя и его провайдера, но также с изменениями, происходящими на макроуровне.

Социальные риски, связанные с интернет-зависимостью, обычно проистекают из чрезмерной вовлеченности в деятельность интернет-сообществ, которая может препятствовать успешной социализации в «реальной» среде. Особую опасность несет в себе деятельность ряда интернет-сообществ: деструктивных (например, клубы самоубийц, вич /спид-диссидентов [2, с. 137–146] и др.); пропагандирующих насилие и жестокость (дог-хантеры и др.); культивирующих ценность риска и рисковое поведение посредством продвижения рискованных видов «спорта» (паркур, зацепинг и др.); вербующих для участия в различных видах опасной или правонарушающей деятельности. Существуют также сообщества, нарушающие этические нормы (порнографические галереи, чайлд-фри сообщества и др.). Участник такого сообщества может подвергнуться настойчивым провокациям со стороны «друзей» и подстрекательствам к нанесению ущерба третьим лицам или организациям. Кроме того, в интернете ведут свою деятельность запрещенные, однако существующие в «реале» организации, например, деструктивные секты, террористические группы и др. Ложная анонимность, мнимая безнаказанность поведения в интернете способствуют вовлечению пользователей в рисковую деятельность интернет-сообществ.

Наибольшим разнообразием отличаются *поведенческие риски* в виртуальной среде, связанные с личностью интернет-пользователя. Влияние особенностей личности наиболее ярко проявляется в глубоких переживаниях и неадекватных реакциях (например, агрессии) при необходимости хотя бы на время оставить привычное занятие в виртуальной среде; неспособности сделать это без принуждения. В частности, это риски, связанные с развивающейся индустрией компьютерных игр (многопользовательские онлайн-игры, интернет-

казино, присутствие реальных казино в интернете, букмекерские конторы), которые отличаются значительно более низким барьером включения в игру, чем азартные игры в реальной среде. Они могут формировать стойкую игровую зависимость, приводить к значительным финансовым потерям, невыплаченным догам и реальной мести за них.

Виртуальная среда общения. Личностные риски также могут быть связаны с тем, что виртуальная среда в целом доступнее для общения и взаимодействия, чем среда реальная. Это может способствовать возникновению иллюзии контроля над интернет-ситуацией, особенно у тех, кто испытывает проблемы с общением в реальной среде. Может также приводить к нарушению самооценки как в сторону ее повышения, так и занижения (по сравнению с самооценкой в реале) даже на основе единственного критерия, например, числа полученных «лайков», – что в целом препятствует успешной социализации в реальной среде. В качестве причин этого явления студенты, в частности, говорят о недостаточных для офлайн социализации навыков коммуникации – умения обращаться лично, вступать в беседу, задавать вопросы и т.п. [3].

Приведем еще несколько частных примеров рисков на пересечении социальной среды и личностных качеств. Высокой сферой риска для детей являются знакомства с педофилами, ведущими в виртуальной среде активную деятельность. «Платонические» романтические отношения в социальных сетях могут способствовать не только ухудшению семейных отношений, но также увеличению числа жертв брачных аферистов. Коммуникативная культура многих дискуссионных интернет-сообществ (форумов, блогов) отличается грубостью лексики, оскорблениями, что является риском получения психологической травмы для «чужаков». В то же время любая страница в интернете или высказывание на форуме может подвергнуться атаке троллеров, совершаемой, например, ради изгнания «чужака» из не принимающего его сообщества, или просто ради развлечения. [4] Стирание граней между рабочим временем и досугом при дистанционной работе, которое на протяжении ряда лет воспринималось как исключительно позитивное, может приводить к интенсификации исполнения служебных обязанностей со стороны работника и, соответственно, повышению эксплуатации со стороны работодателя [1, с. 127-129].

Выводы. Как любая техногенная среда, интернет-пространство создает не только разнообразные возможности, которые ранее могли быть представлены только научными фантастами, но также новые социальные риски, порождаемые собственно используемыми технологиями, особенностями формирующейся в техногенном пространстве социальной среды, индивидуальными личностными чертами интернет-пользователей. В отличие от всех предыдущих технологий, интернет обладает следующими особенностями, порождающими новые риски 1. Непрозрачность ИКТ, использующих в своей работе персональные данные не только интернет-пользователей, но также клиентов организаций в «реальном» мире, например, владельцев дисконтных карт магазинов – нередко без получения от них информированного согласия. 2. Возможность несанкционированного доступа к персональным данным, хранящимся на разнообразных интернет-ресурсах, для значительного количество подготовленных компьютерных специалистов (data scientits). 3. Высокая скорость развития ИКТ по сравнению с любыми более ранние технологиями, предназначенными для широкого использования населением. Чем старше поколение, тем хуже оно адаптируется к новым возможностям – углубляется возрастной цифровой разрыв. 4. Существенные отличия социальной среды, формирующейся в виртуальном пространстве, от социальной среды в реальном мире. Например, виртуальной социальной среде свойственны иллюзии анонимности и без-

наказанности, а также более простые нормы поведения и общения, что препятствует адекватной оценке новых знакомых, самооценке и социализации молодых поколений. 5. Наконец, низкий, по сравнению с реальной жизнью, барьер включения в потенциально опасные виды деятельности (например, азартные игры) и сообщества (например, клуб СПИД-диссидентов).

В связи со всем вышесказанным, можно говорить о необходимости разработки и применения не только правовых инструментов предотвращения социальных рисков виртуальной среде, но также образовательных программ по информационной грамотности для учащихся, их родителей и учителей, осознанное выполнение которых позволит повысить безопасность всех видов деятельности в интернете.

Список использованных источников

1. Сергеева, О. В. Повседневность новых медиа / О.В Сергеева. – Волгоград: ВолГУ, 2012. – 200 с.

2. Мейлахс, П. А. Онлайновое сообщество СПИД-диссидентов в социальной сети «ВКонтакте»: структура и риторические стратегии / П.А. Мейлахс, Ю.Г. Рыков // XV апрельская международная научная конференция по проблемам развития экономики и общества. – Кн. 3. – М.: Издательский дом НИУ ВШЭ, 2015. – С. 137–146.

3. Елсукова, Н. А. Новые технологии: новые возможности и продуцируемые риски / Н.А. Елсукова // Коммуникация в социально-гуманитарном знании, экономике, образовании: материалы IV междунар. науч.–практ. конф. – Минск: БГУ, 2016. – С. 102–104.

4. Уитмор, Дж. Трололо: Нельзя просто так взять и выпустить книгу про троллинг / Дж. Уитмор. – М.: Альпина Паблишер, 1916. – 349 с.