УДК 330.131.7 **JEL Classification: E44, F01, O32**

Екатерина Даниловна Семенова,
канд. экон. наук, доцент, доцент кафедры статистики,
Одесский национальный экономический университет (г. Одесса, Украина);
Кристина Игоревна Тарасова,
канд. экон. наук, преподаватель, преподаватель кафедры статистики,
Одесский национальный экономический университет (г. Одесса, Украина)

СТАНОВЛЕНИЕ НОВОГО ЦИФРОВОГО МИРА И ПРОБЛЕМЫ МЕНЕДЖМЕНТА КИБЕР-РИСКОВ

В статье проведен анализ глобальных рисков, влияющих на все сферы жизни человечества. Охарактеризованы экономические риски, усложняющие ведение бизнеса в мире в целом и в Украине в частности. Проанализировано состояние и развитие цифрового мира современности: выделены положительные эффекты и проблемы информатизации общества. Изложены основные проблемные вопросы кибер-рисков и разработаны рекомендации по управлению ними на микро- и макроуровнях.

Ключевые слова: риск, глобальный риск, кибер-риск, IT-риск, кибер-атака, цифровая революция, цифровые дивиденды, риск-менеджмент.

DOI: 10.21272/mmi.2017.3-22

Постановка проблемы. Не смотря на то, что после глобального экономического кризиса 2008-2009 гг. прошло уже несколько лет, мировая экономика все еще пытается восстановить свои прежние позиции. В развитых странах наблюдаются существенные колебания экономического роста, а в развивающихся странах, хотя существуют определенные различия производительности, общий экономический рост находится значительно ниже собственного потенциала. Общие перспективы роста экономики на ближайшие несколько лет, по мнению ученых Группы Всемирного банка, остаются размытыми [1].

Сам экономический кризис и последующий период преодоления его последствий четко продемонстрировали, что существующие системы управления рисками во многом не соответствуют тем вызовам, которые бросают как предприятиям, так и целым государствам, современные условия хозяйствования. В этих экономических условиях основной задачей является обеспечение на новом качественном уровне создания системы выявления, идентификации, оценки и управления рисками. Важным вкладом в решение этой проблемы является анализ и обобщение наиболее опасных для человечества рисков, которые ежегодно представляет Всемирный экономический форум в Давосе [2, с. 19].

Участники форума в 2016 году распределили существующие глобальные риски по 5 следующим группам: геополитические, технологические, социальные, экономические и экологические. По степени влияния важнейшим риском участники форума назвали глобальное потепление и безуспешность мероприятий, направленных на предотвращение изменения климата. Этот риск был признан более опасным, чем будущий кризис водоснабжения, крупномасштабная миграция и изменение цен на энергоносители.

Наиболее серьезным риском для предпринимательской деятельности в развитых экономиках Японии, США, ФРГ, Швейцарии, Сингапура и др. стран являются риски кибер-атак.

В Украине существуют две группы рисков, которые вызывают наибольшие опасения для ведения бизнеса. К первой группе относятся риски, связанные с кризисом бюджетных средств, неуправляемой инфляцией гривны и национальным конфликтом. Ко второй группе относятся

риски, связанные со скачками цен на энергоносители, глубокой социальной нестабильностью и сбоями в системе финансовых институтов и механизмов.

Наиболее вероятными, с точки зрения возникновения, рисками в Украине, по мнению экспертов, являются следующие:

1. Несовершенство законодательной базы, нестабильность налогового законодательства, неправомерные или непредвиденные действия органов местной власти и местного самоуправления, нестабильность государственной власти и неэффективная экономическая политика (административно-законодательные риски).
2. Рост уровня ценовой и неценовой конкуренции (рыночные риски).
3. Неблагоприятные изменения курсов иностранных валют по отношению к отечественной валюте, финансовые потери предприятий от колебания цен на продукцию из-за инфляционных процессов (финансовые риски).
4. Невозможность партнера выполнить свои финансовые обязательства перед предприятием (риски ненадежности партнера).

Стоит отметить, что рассмотренные выше виды рисков за последние годы становятся все более взаимосвязанными, а влияние отдельных из них затрагивает в большинстве случаев не один конкретный рисковый фактор, а сразу несколько или все. Так, риски, относящиеся к категории экономических, вызывают наибольшую обеспокоенность с точки зрения высокой вероятности их возникновения и степени воздействия на макроэкономику в целом и экономику отдельных субъектов в частности, начиная с финансовых систем и инфраструктуры и заканчивая информационной безопасностью работы предприятий.

Анализ последних исследований и публикаций. Проведенный нами анализ научных исследований и публикаций показывает, что проблеме глобальных рисков посвящены работы многих современных ученых, в т.ч.: В. Г. Анисимова [3], Е. Н. Барикаева [4], У. Дайхманна и Д. Мишры [5] и так далее. Однако проблема исследования глобальных, и не только, рисков остается значимой и по сей день.

Выделение нерешенных ранее частей общей проблемы. Данный этап развития человечества характеризуется глобальной информационно-коммуникационной революцией, аналогов которой мир еще не знал. Так, более 40 % населения планеты имеет доступ к сети Интернет; мобильные телефоны имеются почти у 70 % тех, кто относится к нижнему квинтилю населения по уровню дохода. Более того, число беднейших домохозяйств, имеющих доступ к беспроводному интернету, является большим, чем число домохозяйств, имеющих доступ к чистой питьевой воде.

Обычный день в Интернет-сети состоит из 207 млрд. сообщений, отправленных по электронной почте, 2,3 млрд. гигабайт трафика, 152 млн. звонков по Skype, 36 млн. покупок в Amazon. В 2010-2015 гг. широкополосный доступ в интернет имели 9 из 10 компаний стран с высоким уровнем дохода, 7 из 10 – в странах со средним уровнем дохода, 4 из 10 – с низким уровнем [5, с. 6]. При этом показатели внедрения более сложных технологий, таких, как защищенные серверы и корпоративные сети в большинстве стран гораздо ниже. Это связано, прежде всего, с отсутствием понимания сложности рисков, возникающих в интернет-сетях, и отсутствием комплексного анализа таких рисков. В конечном итоге это приводит к тому, что предприятия порой не замечают возможной реализации рисков: так, в среднем компаниям необходимо около 90 дней, чтобы понять, что их систему взломали.

Все это доказывает, что риски информационных систем на современном этапе действительно носят глобальных характер, и подчеркивает особую актуальность их изучения с целью управления ними.

Цель статьи. Главной целью данной работы является анализ вызовов и ориентиров

деятельности субъектов хозяйствования в условиях нового цифрового мира с целью разработки рекомендаций по снижению уровня одних из самых опасных экономических рисков – IT-рисков.

Основной материал. Развитие и распространение информационно-коммуникационных технологий (ИКТ) является одним из первых глобальных вызовов современному человечеству, который кардинально изменил существующие условия хозяйствования. Распространение ИКТ обуславливает переход к инновационной модели развития экономики, новым формам организации предпринимательства, основанным на управлении информацией и знаниями. Рост нематериального производства становится ключевым элементом цифровой экономики, а ИКТ выступают сегодня движущей силой развития общества.

Примеры этому многочисленны. Так, поставщик платёжных услуг M-Pesa, используя экономию от масштаба оказания услуг за счет автоматизации, привносит значительные инновации в финансовый сектор Кении и соседних стран, а индийская система цифровой идентификации Aadhaar позволяет решать многочисленные информационные проблемы и помогает правительству обеспечить интеграцию социально-незащищенных слоев населения страны.

Наилучшей иллюстрацией быстрого распространения цифровых дивидендов служит так называемый «феномен Шацзи» или эффект «деревень Таобао». Если в прибрежных районах КНР в последние 30 лет экономический рост шел достаточно быстрыми темпами, то сельские западные районы в этом существенно отставали. Однако, широкомасштабные подключения деревень к сети Интернет (90% деревень в 2015 г.) уже принесли свои плоды. Торговля онлайн дала возможность сельским производителям выйти на национальный и даже на глобальный рынки по средствам Интернет-платформ. Торговый портал Taobao, созданный китайской корпорацией Alibaba, существенно снижает затраты на координацию деятельности компаний, тем самым повышая эффективность экономики КНР. Taobao и другие платформы данного типа – это инновации, вызванные экономией от масштаба, которая возникает при резком снижении транзакционных издержек. Сейчас в 200 «деревнях Таобао» торговлей занимаются более 70 тыс. человек, а так же множество жителей других сельских регионов. Примерно одну пятую новых владельцев бизнеса составляют бывшие безработные, одну треть – женщины и около 1 % – инвалиды [5, с. 10].

В таких странах, как Ботсвана и Уругвай, фермеры используют уникальные системы идентификации и отслеживания скота, которые удовлетворяют требованиям по экспорту мясных продуктов и значительно повышают эффективность национальных производственных процессов.

Во Вьетнаме темп роста производительности предприятий, участвующих в интернет-торговле, на 3,6 п.п. больше, чем у фирм, которые используют только традиционные формы продаж.

Американская компания UPS при помощи продвинутых алгоритмов маршрутизации избегает левосторонних поворотов, что позволяет экономить время и топливо в среднем на 4,5 млн. литров ежегодно.

Подключение к сети Интернет дает возможность, особенно новосозданным предприятиям, экспортировать большие объемы своей продукции на большее количество рынков. Учеными установлено, что расширение масштабов использования Интернета в стране-экспортере продукции на 10 % расширяет номенклатуру в торговом обороте между двумя странами на 0,4 %, а стоимостной объем торговли – на 0,6% [5, с. 12].

При этом вклад информационно-коммуникативных технологий в рост валового внутреннего продукта в последние годы существенно выше в развивающихся странах (табл. 1).

Данные таблицы свидетельствуют о том, что в развитых странах вклад ИКТ в рост ВВП в среднем каждые 5 лет снижался на 0,4 п.п. или на 15,7%, а в развивающихся странах он возрастал в среднем на 0,7 п.п. или на 17,4 %.

Таблица 1 – **Вклад ИКТ в рост ВВП развитых и развивающихся стран**
(составлено по данным [6])

Период	Вклад ИКТ в рост ВВП, %	
	развитые страны	развивающиеся страны
1996-2000	3,0	3,4
2001-2005	2,5	6,0
2006-2010	1,0	6,5
2011-2015	1,8	5,5

В то же время ежегодные темпы роста ВВП в развивающихся странах были существенно выше, чем в развитых странах, особенно в посткризисные годы (табл. 2). На протяжении 2010-2015 гг. относительная скорость роста ВВП в развивающихся странах опережала ее рост в развитых странах на 22,7%.

Таблица 2 – **Темпы роста ВВП в развитых и развивающихся странах**
(составлено по данным [6])

Год	Темпы роста ВВП, %	
	развитые страны	развивающиеся страны
2010	102,6	107,6
2011	101,5	106,0
2012	101,2	104,8
2013	101,0	104,6
2014	101,7	104,3
2015	101,9	103,8

Все вышеизложенное убедительно доказывает, что цифровые технологии качественно помогают предприятиям повышать эффективность работы, а населению – находить новые рабочие места и расширять свои возможности. ИКТ снижают стоимость социальных и экономических транзакций для предприятий и значительно способствуют внедрению инноваций. Они способствуют большей эффективности компаний, превращая существующие виды деятельности и услуг в более быстрые, удобные и дешевые. Также ИКТ способствует интеграции: предприятия и отдельные личности получают доступ к недоступным ранее видам услуг.

Однако у дивидендов нового цифрового мира существует и обратная сторона, которая указывает на всевозрастающее число возникающих рисков. Ускоряющаяся автоматизация может стать причиной опустошения рынков труда, безработицы и социального неравенства; низкая эффективность электронного правительства часто является свидетельством контроля над гражданами, а не расширением их прав и возможностей; отсутствие четкого регулирования и ограниченность конкурентной борьбы между онлайн-платформами может привести к опасной концентрации бизнеса; все более значимыми становятся IT-риски.

Одно из самых масштабных исследований предпринимательских рисков, представляющих опасность для ведения хозяйствования, было проведено компанией Global Corporate & Specialty, которая смогла выделить десять наиболее важных факторов риска как в мире в целом, так и в отдельных его регионах. Данные ранжирования факторов риска, в котором 1 означает наиболее опасный риск, а 10 – наименее опасный, представлены в табл. 3.

Согласно приведенной в табл. 3 информации, одними из наиболее опасных рисков для ведения бизнеса на данном этапе являются IT-риски или кибер-риски, которые наносят ущерб мировой экономике на сумму порядка 445 миллиардов долларов в год [7, с. 10].

IT-риски или кибер-риски представляют собой риски потерь и несанкционированного изменения информации, происходящие из-за сбоев в работе информационных систем, и наносящие ущерб предприятию. К этим рискам относятся и риски незаконного использования торговой или производственной марки, дезинформации, нарушения авторских прав на использование продукции интеллектуального труда и т. д. Иными словами, в категорию кибер-рисков также входят события, связанные с незаконным использованием информации или ее искажением и наносят ущерб предприятию путем прямого воздействия на окружающую среду.

Symantec Corporation утверждает, что использование продукции Apple и Cloud-технологий, а также дальнейшее развитие Интернета вещей, приведет к дальнейшему усугублению влияния IT-рисков и стремительному росту кибер-преступности [8].

С развитием ИКТ проблема кибер-рисков и обеспечения информационной безопасности приобретает особую актуальность. На киберпреступления приходится 38% экономических преступлений в секторе финансовых услуг, а жертвами мошенничества признали себя 45 % опрошенных экспертами PricewaterhouseCoopers участников мирового рынка [9]. Компьютерная сеть все чаще становится объектом покушения вредоносных программ: по данным Лаборатории Касперского за год веб-атакам подвергаются около 60 % пользователей ее продуктов. Количество официально зарегистрированных преступлений в Украине в области IT в 2014 г. составило 4800 ед., а в 2015 г. – 6025 ед. [5].

Таблица 3 – **Главные риски ведения бизнеса в 2016 году**
(построено согласно данным Allianz Global Corporate & Specialty [7])

Факторы риска	Ранг					
	мир в целом	Европа	Азия	Африка и Средний восток	Северная и Южная Америки	Австра-лия
Прерывание бизнеса (включая нарушения в цепи поставок товаров)	1	1	1	5	1	2
Развитие рынка (волатильность, конкуренция, стагнация рынка)	2	2	2	1	4	1
Кибер-инцинденты (кибер-преступность, утечка данных, ошибки IT-систем)	3	3	5	5	2	4
Природные катастрофы	4	6	3	3	3	5
Изменения в законодательстве и регулировании (экономические санкции, протекционизм)	5	4	7	3	5	7
Макроэкономические события (программы жесткой экономии, повышение цен на сырьевые товары, инфляция / дефляция)	6	5	4	1	8	3
Потеря репутации или стоимости бренда	7	7	6	-	6	5
Пожары, взрывы	8	8	8	8	6	8
Политические риски (в т.ч. война, терроризм)	9	10	10	7	-	-
Кража, мошенничество	10	-	-	9	9	-

Кибер-преступность не знает географических и государственных границ, а ее жертвами может стать кто угодно. За последние несколько лет кибер-атакам подвергались такие компании как Epsilon, Marks&Spencer, Betfair и Global Payments [7]. Украинские хакеры, участники группировки Carbanak, похитили порядка 1 млрд долларов из более чем 100 финансовых учреждений, а в 2015 г. на территории Украины были задержаны Европолом создатели вирусов Zeus и SpyEye, при помощи которых из мировых банков было украдено около 2 млн. долларов [6].

Исходя из изложенного выше, ситуацию с IT-рисками в ближайшем будущем мы представляем в виде следующих явных тенденций:

1. Рост общего количества неблагоприятных событий и их отягощение.
2. Увеличение количества целевых атак, увеличение случаев краж интеллектуальной собственности и кибер-вымагательства, рост числа ситуаций банковского фишинга и инцидентов с банкоматами.
3. Дальнейшее распространение рисков за пределы финансового рынка.
4. Рост уязвимости систем управления на предприятиях.
5. Ужесточение законодательства на глобальном уровне.
6. Рост осознания необходимости страхования IT-рисков и рост объемов страхования.

Мировая практика показывает, что защита информации, а, значит, и менеджмент кибер-рисков, должны стать приоритетными задачами для предприятий и других структур.

На наш взгляд, методика менеджмента кибер-рисков может быть рассмотрена на макро- и микро- уровнях. Так, риск-менеджмент на макроуровне должен включать разработку государственной политики информационной безопасности и мониторинг политики других государств относительно всех сетей и систем. Например, новые правила конфиденциальности, принятые на территории всего ЕС, призваны создать сильный закон о защите данных 500 миллионов граждан союза, упорядочить нормы законодательства между государствами-членами, создать единый цифровой рынок и улучшить сотрудничество в сфере безопасности. Эти меры обеспечат реальные возможности для подавления неправомерных действий, а предприятия, нарушающие правила защиты данных, могут быть оштрафованы на 4% от их годового оборота, что для крупных интернет-корпораций может составлять миллиарды евро [5].

Не смотря на то, что вопрос менеджмента кибер-рисков является общей проблемой, не все участники мирового рынка равны между собой. Страны с высоким уровнем дохода, как то США, члены ЕС, Япония, Южная Корея и Тайвань, больше других зависят от IT-технологий, и, следовательно, являются особенно уязвимыми перед лицом данных рисков. Таким образом, именно эти экономики должны значительно увеличить объем финансирования и сотрудничества в области управления кибер-рисками, а также продемонстрировать исключительную осторожность при использовании интернет-технологий в военных целях.

Политика развитых стран должна быть направлена на поощрение развития новых проектов в сфере интернет-безопасности, но не стоит ожидать, что только эти проекты решат все проблемы IT-системы. Не смотря на достаточно большие технические усилия, направленные на развитие более безопасного интернета, сделать его полностью безопасным в принципе невозможно, особенно теперь, когда множество компаний и простых пользователей являются обладателями всевозможных устройств.

В такой ситуации наилучшим способом управления рисками являются технологии, направленные на устранение кибер-атак определенного типа. Так, опрос, проведенный Атлантическим союзом среди экспертов по кибер-безопасности, показал, что даже масштабированный запуск центра обновления Windows от Microsoft с целью обновления софта, в определенной степени поможет защитить миллионы или миллиарды компьютеров.

Национальные политики государств также должны поощрять цифровую трансграничную торговлю и избегать рыночных ограничений в местах, где производятся информационно-коммуникационное оборудование. Даже если такие протекционистские ограничения на рынке имеют смысл в краткосрочной перспективе, в будущем они построят границы, которые будут тормозить национальный и глобальный рост ВВП. Ярким примером работы в данном направлении является Инициатива Международного центра по торговле и устойчивому развитию E15, направленная на улучшение глобальной торговой системы путем повышения экономической выгоды от цифровой экономики.

Также важно отметить, что национальные границы делают систему интернет еще более опасной, поскольку компании в области ИКТ, которые создают и поддерживают киберпространство, вынуждены отвечать на десятки национальных регуляторов и создавать внутреннюю инфраструктуру для соответствия местным законам.

В тоже время, к риск-менеджменту на микроуровне мы относим следующие обязательные элементы:

1. Обучение и подготовка пользователей с целью повышения их информированности.
2. Разработка процедур управления IT-инцидентами, в том числе процедур реагирования и ликвидации последствий их возникновения.
3. Разработка корпоративной политики безопасной сети.
4. Управление и контроль пользовательских привилегий.
5. Разработка руководства по кибер-безопасности.
6. Использование процедур защиты от вредоносных программ.
7. Контроль использования сменных носителей информации.
8. Страхование кибер-рисков.

Эти меры могут быть применимы на предприятиях всех форм собственности и вне зависимости от их отраслевой принадлежности и, по мнению многих экспертов, при правильном ведении политики риск-менеджмента в IT-сфере, помогут избежать около 80 % кибер-атак, что существенно снизит убытки компаний [10, с. 14].

Одной из относительно новых форм управления рисками IT-систем, которая набирает все большую популярность, выступает страхование. В мировой практике уже более 5 лет существует полис страхования кибер-рисков или Cyber Risk Insurance, который предлагает защиту предприятию в ходе кибер-угроз по следующим направлениям:

1. Финансовые убытки от потери данных.
2. Дополнительные расходы для минимизации последствий инцидентов.
3. Потери прибыли от сбоев в работе сети по причине нарушения системы безопасности.
4. Дополнительные покрытия (убытки от виртуального вымогательства, расходы на административные расследования в отношении хищения информации и т.п.).

Однако, мы считаем, что на данном этапе развития цифрового общества польза от страхования кибер-рисков пока еще слишком условна. Согласно исследованиям компании Ponemon «Cost of Data Breach Study: Global Analysis», если предположить, что стоимость утечки данных будет составлять 154 доллара, то применение ряда специальных мер поможет снизить стоимость потерь лишь на одну треть – на 55 долларов. При этом, только 4,4 доллара этого возмещения будут обусловлены страховкой. В тоже время инструктаж сотрудников и использование средств шифрования снизит потери предприятия на 32 доллара [11]. Низкая эффективность страхования связана, прежде всего, с тем, что в случае с кибер-рисками часто отсутствует четкое понимание предмета страхования, усугубленное нежеланием фирм сообщать о брешах в системах безопасности. Таким образом, схемы управления IT-рисками до сих пор являются несовершенными и требуют доработки.

Выводы и направления дальнейших исследований. Информационно-коммуникационные технологии трансформируют мир предпринимательства. Эти трансформации повышают производительность ведущих сил экономики и общества, однако многие отдельные предприятия, страны и слоя населения не ощущают даже минимальных преимуществ цифровой революции. Это говорит о том, что стремительно развивающиеся технологии необходимо дополнять улучшением ситуации в тех сферах, которые определяют способность предприятий, правительств и отдельных людей эффективно использовать новые цифровые инструменты. Для более быстрого распространения цифровых дивидендов необходимо решить и многие из старых

проблем развития общества – создать более благоприятную среду для ведения бизнеса, выстроить действенную в условиях информатизации систему подготовки кадров, сделать поставщиков услуг более восприимчивыми к запросам потребителей.

Развитие ИКТ помимо позитивного эффекта, несет и эффект негативный, который проявляется в стремительном росте кибер-рисков, наносящих значительный урон мировой экономике. Одним из способов ускорения распространения цифровых дивидендов сегодня является грамотный риск-менеджмент в IT-сфере, который требует дальнейших научных исследований, в частности, в сфере страхования и законодательства.

1. Global Economic Prospects. June 2016. Divergences and Risks [Electronic resource]. – 2016. – № 26. – Access mode: http://pubdocs.worldbank.org/en/842861463605615468/Global-Economic-Prospects-June-2016-Divergences-and-risks.pdf.
2. Иванов О.Б. Глобальные риски и экономические тенденции в современном мире / Иванов Олег Борисович // ЭТАП. – 2014. – №1. – С.18-33.
3. Введение в экономический риск-менеджмент : монография / В.Г. Анисимов [и др.] ; РТА. – М.: РИО РТА, 2008.
4. Барикаев Е.Н. Управление предпринимательскими рисками в системе экономической безопасности. Теоретический аспект: монография / Е.Н. Барикаев, Н.Д. Эриашвили, В.З. Черняк – 2-е изд. перераб. и доп. – М.: ЮНИТИ-ДАНА: Закон и право, 2015. – 159 с.
5. Digital Dividends. World development report 2016 [Electronic resource]. – Access mode: http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.
6. World Economic Situation and Prospects 2016 [Electronic resource]. – Access mode: http://www.un.org/en/development/desa/policy/wesp/index.shtml.
7. Allianz Risk Barometer Top Business Risks 2016 [Electronic resource]. – 2016. – № 5 – Access mode: http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf.
8. Symantec Predictions for 2016 – Looking Ahead [Electronic resource]. – Access mode: http://www.theborneopost.com/2015/12/08/symantec-predictions-for-2016-looking-ahead/.
9. The cyber-savvy CEO: Getting to grips with today's growing cyber threats [Electronic resource]. – Access mode: http://www.pwc.com/gx/en/services/audit-assurance/corporate-reporting/governance-reporting/combating-cyber-threats-on-the-internet.html.
10. A Guide to Cyber Risk. Managing the impact of increasing interconnectivity [Electronic resource]. – Access mode: https://www.allianz.com/v_1441789023000/media/press/document/other/Allianz_Global_Corporate_Specialty_Cyber_Guide_final.pdf.
11. Страхование кибер-рисков — это дорого и не всегда эффективно [Электронный источник]. – Режим доступа: http://forinsurer.com/news/16/06/02/33906.

1. The World Bank. (2016). Global Economic Prospects. June 2016. Divergences and Risks. *pubdocs.worldbank.org*. Retrieved from http://pubdocs.worldbank.org/en/842861463605615468/Global-Economic-Prospects-June-2016-Divergences-and-risks.pdf.
2. Ivanov, O.B. (2014). Globalnyie riski i ekonomicheskie tendentsii v sovremennom mire [Global risks and economic trends in the modern world]. *ETAP, 1*, 18-33 [in Russian].
3. Anisimov, V.G. (2008). *Vvedenie v ekonomicheskiy risk-menedzhment [Introduction to the economic risk-management]*. Moscow: RIO RTA [in Russian].
4. Barikaev, E.N., Eriashvili, E. N., & Chernyak, V. Z. (2015). *Upravlenie predprinimatelskimi riskami v sisteme ekonomicheskoy bezopasnosti. Teoreticheskiy aspect [Management of business risks in the economic security of the system. The theoretical aspect]*. Moscow: YUNITI-DANA [in Russian].
5. The World Bank Group. (2016). Digital Dividends. *documents.worldbank.org*. Retrieved from http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.
6. Hamid, R. (2016). World Economic Situation and Prospects 2016. *www.un.org*. Retrieved from http://www.un.org/en/development/desa/policy/wesp/index.shtml.
7. Allianz SE and Allianz Global Corporate & Specialty SE. (2016). Allianz Risk Barometer Top Business Risks 2016. *www.agcs.allianz.com*. Retrieved from http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf.
8. Borneo post online. (2015). Symantec Predictions for 2016 – Looking Ahead. *www.theborneopost.com.* Retrieved from http://www.theborneopost.com/2015/12/08/symantec-predictions-for-2016-looking-ahead/.
9. Beer, W. (2011). The cyber-savvy CEO: Getting to grips with today's growing cyber threats. *www.pwc.com*. Retrieved from http://www.pwc.com/gx/en/services/audit-assurance/corporate-reporting/governance-reporting/combating-cyber-threats-on-the-internet.html.
10. Allianz Global Corporate & Specialty. (2016). A Guide to Cyber Risk. Managing the impact of increasing interconnectivity. *www.allianz.com*. Retrieved from https://www.allianz.com/v_1441789023000/media/press/document/other/Allianz_Global_

Corporate_Specialty_Cyber_Guide_final.pdf.

11. Forinshurer insurance. (2016). Strahovanie kiber-riskov — eto dorogo i ne vsegda effektivno [Insurance of cyber risks - it is expensive and not always effective]. *forinsurer.com*. Retrieved from http://forinsurer.com/news/16/06/02/33906 [in Russian].

К.Д. Семенова, канд. екон. наук, доцент кафедри статистики**,** Одеський національний економічний університет (м. Одеса, Україна);

К.І. Тарасова, канд. екон. наук, викладач кафедри статистики, Одеський національний економічний університет (м. Одеса, Україна)

Становлення нового цифрового світу та проблеми менеджменту кібер-ризиків

У статті проведено аналіз глобальних ризиків, що впливають на всі сфери життя людства. Охарактеризовані економічні ризики, які ускладнюють ведення бізнесу в світі в цілому і в Україні зокрема. Проаналізовано стан і розвиток цифрового світу сучасності: виділені позитивні ефекти і проблеми інформатизації суспільства. Викладено основні проблемні питання кібер-ризиків і надані рекомендації по управлінню ними на мікро- і макрорівнях.

Ключові слова: ризик, глобальний ризик, кібер-ризик, IT-ризик, кібер-атака, цифрова революція, цифрові дивіденди, ризик-менеджмент.

K.D. Semenova, Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Statistics, Odessa National Economic University (Odessa, Ukraine);

K.I. Tarasova, Candidate of Economic Sciences, Lecturer, Lecturer of the Department of Statistics, Odessa National Economic University (Odessa, Ukraine)

Establishment of the new digital world and issues of cyber-risks management

The aim of the article. The purpose of the article is to analyze the challenges and targets of economic entities in the new digital world in order to develop recommendations for the management of one of the most dangerous economic risk - IT-risk.

The results of the analysis. This paper analyzes the state and development of the digital world of today. It is shown that this stage of human development is characterized by the global information and communication revolution, analogues of which the world has never known. The spread of information and communication technologies (ICT) causes a transition to an innovative model of economic development and new forms of business organization that are based on the management of information and knowledge. The growth of non-material production is becoming a key element of the digital economy and, ICTs are becoming the driving force behind the development of today's society.

The article dissects the dynamics of the ICT contribution to GDP growth in the developed and developing countries. The results of the analysis showed that in the developed countries the contribution of ICT to the GDP growth declined in recent years, while in developing countries it increased. At the same time, annual growth rate of GDP in the developing countries was significantly higher than in developed countries, especially in the post-crisis years. The analysis led to the conclusion that the digital technologies qualitatively help enterprises to improve operational efficiency, reduce the cost of social and economic transactions and significantly contribute to innovation. They increase the efficiency of companies, transforming the existing types of activities into fast, comfortable and cheap ones.

However, there is a downside to the dividends of the new digital world, which shows an increase in the number of emerging risks. The paper analyzes the most important risk factors in the world as a whole, and in its individual regions. It has been shown that the most dangerous risks of doing business at this stage are the IT-risks and cyber-risks, which cause considerable damage to the global economy. The following trends of IT-risks are substantiated:

- The growth in the total number of adverse events and their hardening;
- The increase in the number of targeted attacks, cases of intellectual property theft and cyber-extortion, the increase in the number of bank fishing situations;
- The further spread of risks beyond the financial market;
- The increase in the vulnerability of control systems of enterprises;
- The tightening of legislation at the global level;
- The increase in awareness of the need for insurance of IT-risks and the growth of insurance volumes.

Conducted analysis showed that the protection of information, and, hence, the cyber risk management, should be a priority for businesses and other entities. The article deals with the problems and challenges of cyber-risk management at both the macro and the micro levels. Risk management at the macro level should include the development of national information security policies and monitoring the policy of other countries regarding all networks and systems. Risk management at the micro level should include a system of measures, among which the insurance of cyber risks is gaining the greatest popularity.

Conclusions and directions of further research. The development of information and communication technologies in addition to the positive effect also bears a negative effect, which manifests itself into the rapid growth of cyber-risks causing significant damage as to separate business entities, and to the world economy as a whole. One way to speed up the spread of digital dividends today is a competent risk management in the IT-sphere, which requires further research, particularly in the insurance industry.

Keywords: risk, global risk, cyber risk, IT-risk, cyber-attack, digital revolution, digital dividends, risk-management.

Отримано 05.01.2017 р.