УДК 338:004.912:316.772.5

ІНСТИТУЦІЙНИЙ РЕІНЖИНІРІНГ РИЗИК-МЕНЕДЖМЕНТУ В ЦИФРОВІЙ ЕКОНОМІЦІ

©2018 КОЛОМІЄЦЬ Г. М., МЕЛЕНЦОВА О. В., ГУЗНЕНКОВ Ю. Г.

УДК 338:004.912:316.772.5

Коломієць Г. М., Меленцова О. В., Гузненков Ю. Г. Інституційний реінжинірінг ризик-менеджменту в цифровій економіці

Всеосяжна пенетрація цифрових технологій трансформує господарську систему. Запорукою ефективного господарювання є дослідження нових закономірностей її функціонування. Теоретичне усвідомлення суттєвих, прискорених змін обумовлює необхідність перебудови процесу управління в цілому і ризик-менеджменту зокрема. Оприлюднені осучаснені стандарти ISO 31000:2018 відображають новітні чинники, які має враховувати організація загалом. Разом з тим, парадигмальний перехід до домінування глобальних процесів над національними, зміни актуальної структури ризикопороджуючих чинників під впливом переходу до цифрової економіки потребує суттєвих трансформацій інститутів управління ризиками – інституційного реінжинірінгу ризик-менеджменту, пропонування певного алгоритму його здійснення.

Ключові слова: *інституційний реінжиніринг, ризик-менеджмент, глобальні інтернет-комунікації.*
Рис.: *11.* ***Бібл.:*** *15.*

Коломієць Ганна Миколаївна *– доктор економічних наук, професор, професор кафедри економічної теорії та економічних методів управління, Харківський національний університет ім. В. Н. Каразіна (пл. Свободи, 4, Харків, 61022, Україна)*
E-mail: *gkolomiets@karazin.ua*

Меленцова Ольга Володимирівна *– кандидат економічних наук, доцент кафедри економічної теорії та економічних методів управління, Харківський національний університет ім. В. Н. Каразіна (пл. Свободи, 4, Харків, 61022, Україна)*
E-mail: *omelentsova@karazin.ua*

Гузненков Юрій Георгійович *– старший викладач кафедри економічної кібернетики та прикладної економіки, Харківський національний університет ім. В. Н. Каразіна (пл. Свободи, 4, Харків, 61022, Україна)*
E-mail: *huznenkov@karazin.ua*

УДК 338:004.912:316.772.5

Коломиец А. Н., Меленцова О. В., Гузненков Ю. Г. Институциональный реинжиниринг риск-менеджмента в цифровой экономике

Всеобъемлющая пенетрация цифровых технологий трансформирует хозяйственную систему. Залогом эффективного хозяйствования является исследование новых закономерностей ее функционирования. Теоретическое осознание существенных, ускоренных изменений обусловливает необходимость перестройки процесса управления в целом и риск-менеджмента в частности. Обнародованные осовремененные стандарты ISO 31000:2018 отражают новейшие факторы, которые должна учитывать организация в целом. Вместе с тем, парадигмальный переход к доминированию глобальных процессов над национальными, изменения актуальной структуры рископорождающих факторов под влиянием перехода к цифровой экономике требуют существенных трансформаций институтов управления рисками – институционального реинжиниринга риск-менеджмента, предложения определенного алгоритма его осуществления.

Ключевые слова: *институциональный реинжиниринг, риск-менеджмент, глобальные интернет-коммуникации.*
Рис.: *11. Библ.: 15.*

Коломиец Анна Николаевна *– доктор экономических наук, профессор, профессор кафедры экономической теории и экономических методов управления, Харьковский национальный университет им. В. Н. Каразина (пл. Свободы, 4, Харьков, 61022, Украина)*
E-mail: *gkolomiets@karazin.ua*

Меленцова Ольга Владимировна *– кандидат экономических наук, доцент кафедры экономической теории и экономических методов управления, Харьковский национальный университет им. В. Н. Каразина (пл. Свободы, 4, Харьков, 61022, Украина)*
E-mail: *omelentsova@karazin.ua*

Гузненков Юрий Георгиевич *– старший преподаватель кафедры экономической кибернетики и прикладной экономики, Харьковский национальный университет им. В. Н. Каразина (пл. Свободы, 4, Харьков, 61022, Украина)*
E-mail: *huznenkov@karazin.ua*

UDC 338:004.912:316.772.5

Kolomiyets G. M., Melentsova O. V., Huznenkov Yu. G. The Institutional Reengineering of Risk Management in the Digital Economy

The comprehensive penetration of digital technologies transforms the economic system. The key to effective management is researching of new regularities of its functioning. The theoretical awareness of significant, accelerated changes necessitates the restructuring of management process in general and risk management in particular. The published updated standards ISO 31000:2018 reflect the latest factors that should be considered by an organization as a whole. At the same time, paradigmal transition to dominance of global processes over national, changes of current structure of risk-bearing factors under the influence of transition to digital economy require significant transformations of risk-management institutions – an institutional reengineering of risk management, proposal of a certain algorithm of its implementation.

Keywords: *institutional reengineering, risk management, global Internet communications.*
Fig.: *11.* ***Bibl.:*** *15.*

Kolomiyets Ganna M. *– D. Sc. (Economics), Professor, Professor of the Department of Economic Theory and Economic Methods of Management, V. N. Karazin Kharkiv National University (4 Svobody Square, Kharkiv, 61022, Ukraine)*
E-mail: *gkolomiets@karazin.ua*

Melentsova Olga V. *– PhD (Economics), Associate Professor of the Department of Economic Theory and Economic Methods of Management, V. N. Karazin Kharkiv National University (4 Svobody Square, Kharkiv, 61022, Ukraine)*
E-mail: *omelentsova@karazin.ua*

Huznenkov Yuri G. *– Senior Lecturer of the Department of Economic Cybernetics and Applied Economics, V. N. Karazin Kharkiv National University (4 Svobody Square, Kharkiv, 61022, Ukraine)*
E-mail: *huznenkov@karazin.ua*

Ризик-менеджмент став невід'ємною складовою сучасного процесу управління. Нагромаджений досвід управління узагальнено в міжнародних стандартах ISO 31000:2018 з ризик-менеджменту [1]. Утворені міжнародні інституції відстежують зміни відповідних практик і працюють над удосконаленням стандартів. Розвиваються теоретичні основи управління ризиками, які досить енергійно втілюються

в навчальних матеріалах. Аналіз фокусується на менеджменті мікрорівня окремих галузей господарської діяльності – ризиків фінансових технологій, ризиків банківської діяльності, валютних ризиків тощо [2–4]. Понад десять років виокремлюється система глобальних ризиків, здійснюється їх моніторинг і поглиблюється методологія дослідження глобальних ризиків [5].

Разом з тим, швидкозмінювана господарська реальність під впливом четвертої індустріальної революції [6] потребує переосмислення процесу управління ризиками загалом, його інституційного реінжинірингу. Ризики стають усе більш складними, що обумовлює їх переоцінку для досягнення стійкості, – підкреслює Роналд Купер – радник з питань складності, сталості перехідних процесів ВЕФ, співробітник Оксфордського університету [5, p. 54–55]. Міжнародні експерти звертають увагу на необхідність консолідації зусиль політичної, громадянської, професійної та бізнес-спільнот щодо зміни норм підвищення безпеки функціонування інтернету й проактивного регулювання пов'язаних з ним ризиків [7].

Мета статті – розглянути необхідність і зміст кардинальної перебудови системи норм управління ризиками в цифровій економіці.

Останніми роками відбулися еволюційні зміни як у формах і видах ризиків, так і в характері управління ними. Як наслідок, характеристики багатьох нових форм ризиків часто не дозволяють використовувати традиційні методи оцінки ризиків та управління ними або традиційну політику, яка застосовується на інституційному рівні. Оскільки інформаційні технології стали нормою життя в глобалізованому світі, але ще не мають адекватних норм регулювання, необхідні спільні зусилля по формуванню відповідних глобальних інститутів.

Експерти всесвітнього економічного форуму вже понад десять років тому запропонували аналізувати фундаментальну структуру ризикопороджуючих чинників і її зміни, виокремлюючи щорічно найбільш ймовірні та впливові (*рис. 1, рис. 2*), згрупувавши їх таким чином:

- економічні;
- оточуючого середовища;
- соціальні;
- геополітичні;
- технологічні.

З 2012 р. у складі найбільш ймовірних чинників були виокремлені технологічні, пов'язані з розвитком кіберпростору [5].

Ризикопороджуючі чинники взаємопов'язані, впливають один на одного, підсилюючи їх наслідки [5].

Експерти ВЕФ виокремили найбільш важливі тенденції, які будуть, за їх думкою, вливати в наступні 10 років на глобальний розвиток і ризики, що виникають у зв'язку з цим. Одна з провідних тенденцій – швидко прогресуюча на основі цифрових технологій, пов'язана з всеохоплюючою взаємозалежністю. Її дескриптором є підвищення цифрового взаємозв'язку людей, речей та організацій.

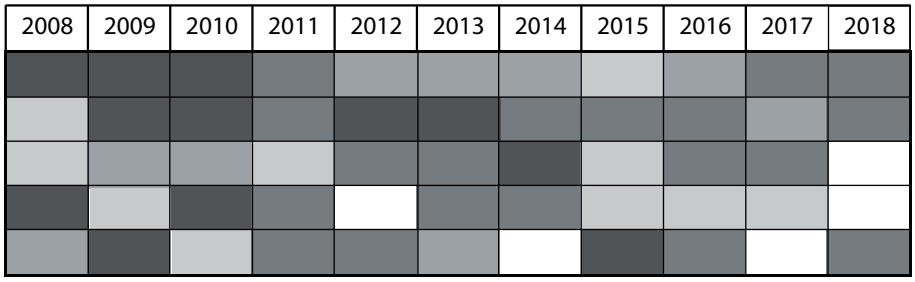

Рис. 1. Найбільш ймовірні ризикопороджуючі чинники [5]

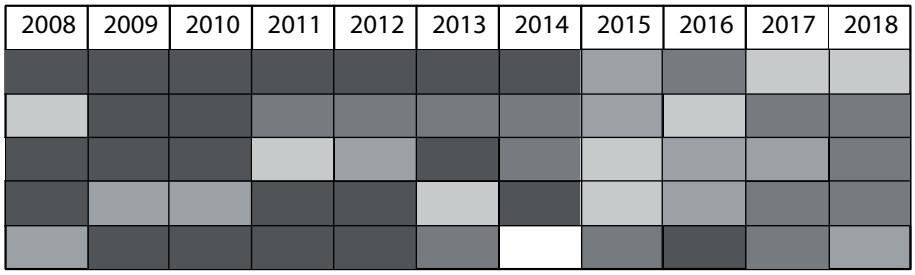

Рис. 2. Ризикопороджуючі чинники за силою впливу [5]

Умовні позначення:

- Економічні чинники
- Чинники оточуючого середовища
- Соціальні чинники
- Геополітичні чинники
- Технологічні чинники

Вона трансформує всі господарські відносини, зводить нанівець напрацьовані впродовж попереднього століття індустріальної епохи господарські інститути.

Посилення кіберзалежності спряжено з такими ризиками:

- несприятливі наслідки технологічного прогресу;
- шахрайство чи крадіжка даних;
- кібератаки;
- порушення критичної інформаційної інфраструктури (*рис. 3*).

Існує поняття «загроза інформаційній безпеці», під яким розуміється фактор або сукупність факторів, що створюють небезпеку функціонуванню та розвитку інформаційного е-середовища суспільства. Поняття загрози можна використовувати поряд з ризиком, оскільки існує цілий ряд деструктивних чинників, про які не цілком коректно говорити в імовірнісному ключі [8]. До них, наприклад, належать кібератаки на комп'ютерні системи або дії з розповсюдження негативного контенту в Інтернеті, з якими користувачі даних інформаційних систем стикаються постійно.

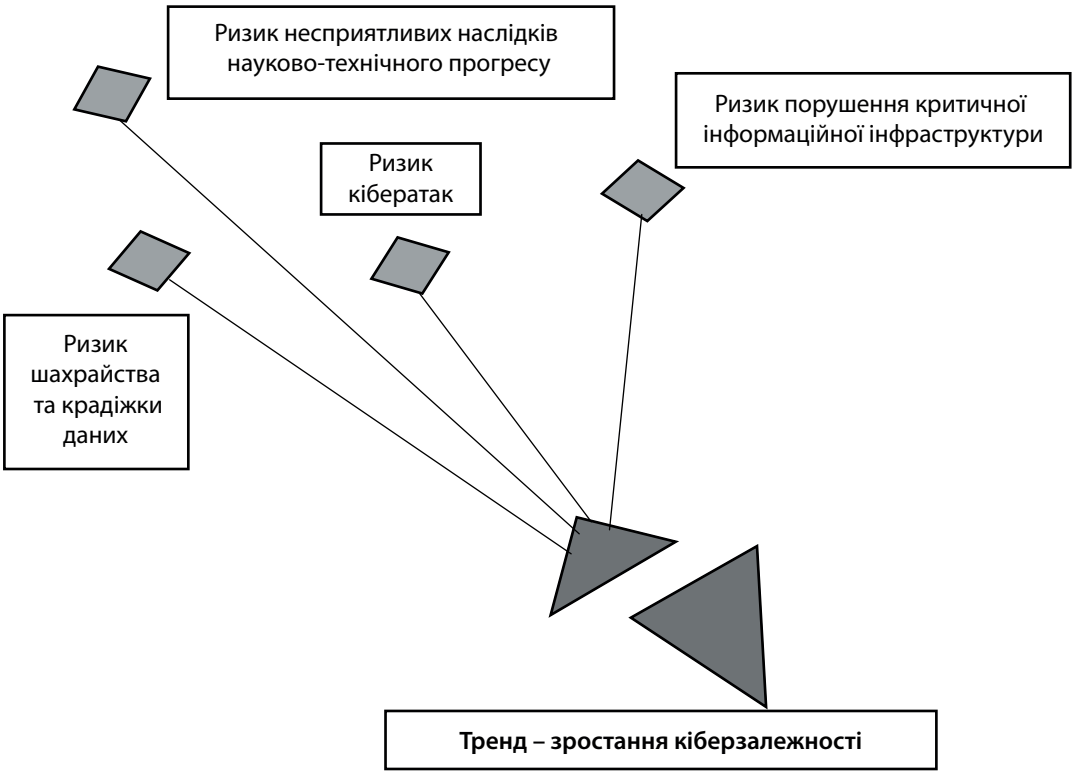

Рис. 3. Одна з ключових тенденцій – посилення кіберзалежності та ризики

Джерело: складено за [5].

Ризики, пов'язані з розвитком електронного середовища, – це складні ризики. Менеджмент вимагає їх редукції та ідентифікації. Ідентифікація ризиків потребує структурованої класифікації. Ризикологія напрацювала вже досить ємний теоретико-методичний базис такої класифікації, що дозволяє визначити місце кожного ризику в їх загальній системі.

В економічній літературі існує достатньо велика кількість різноманітних класифікацій ризику. Градація ризиків досить умовна, тому що окремі види ризиків можуть доповнювати, бути складовими одне одного.

Оскільки е-простор суттєво впливає і перетворює систему господарських практик, виникає ймовірність різноманітних наслідків, тобто ризиків впливу кіберсередовища на господарську систему.

Особливість ризиків і загроз полягає в їх новизні, оскільки вони не мають історичних аналогів. Дослідники характеризують такі ризики як один із наслідків «соціальних розривів» в умовах нелінійної соціокультурної динаміки, парадоксальність яких проявляється в розмиванні феномена історичної спадкоємності.

Оскільки кібер-ризики виникають на всіх рівнях господарської системи, то і управління ризиком має здійснюватися на різних рівнях (*рис. 4*):

- на наднаціональному (глобальному) рівні;
- на державному рівні;
- на рівні фірми;
- на індивідуальному рівні.

Глобалізація характеризує якісно новий стан світової економіки – перетворення її в цілісність –

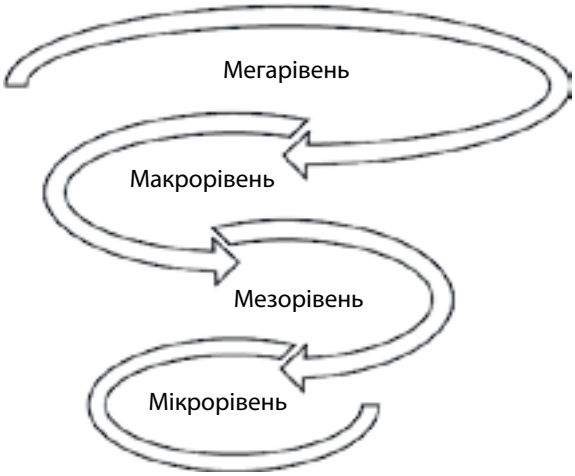

Рис. 4. Актуальна структура рівнів ризиків

і проявляється в інверсії рівнів домінантності розвитку. У системі всесвітнього господарства відбувається кардинальна зміна внутрішньо- і зовнішньоекономічних залежностей і закономірностей. Внутрішньоекономічні процеси втрачають властиву їм протягом багатьох століть первинність по відношенню до зовнішньоекономічних.

Відбувається парадигмальний перехід від пріоритетності національних акторів на світових ринках до світових гравців (мультинаціональних, транснаціональних, мультилокальних компаній, регіональних, трансрегіональних об'єднань і міжнародних економічних організацій) на національних полях.

Глобальні небезпеки – ризикопороджуючі чинники трансформують ризики мета-, макро-, мезо- та мікрорівнів, змінюючи фундаментальну структуру релевантних ризиків економічної діяльності в актуальну та коректуючи їх зміст.

Інверсія рівня домінант сучасного національного економічного розвитку обумовили суттєві зміни і в системі господарських ризиків. Так само, як глобальна господарська система стає визначальною для розвитку національних економік, так і в актуальній структурі ризикопороджуючих чинників і ризиків провідну роль починають відігравати саме глобальні ризики, котрі все більше привертають увагу вчених, експертів і практиків [9].

Саме глобальні ризикопороджуючі чинники, граючи основну роль в актуальній структурі ризиків, обумовлюють зміст і розміри країнових, галузевих і фірмових ризиків у системі. Разом з тим управління ризиком на різних рівнях має бути комплементарним. Залежно від масштабів дії ризикопороджуючих чинників і обсягів їх наслідків доцільно узагальнити відповідальність суб'єктів у формі моделі (*рис. 5*).

Усвідомлення нової актуальної структури ризиків і їх компліментарності визначає необхідність і алгоритм інституційного реінжинірингу ризик-менеджменту.

Очевидно, що необхідні скоординовані дії глобального регулювання та заходів національного рівня, в інтересах бізнес-середовища.

Послідовне реформування інститутів, за розробками експертів ВЕФ, потребує таких заходыв, що відображають алгоритм інституційного реінжинірингу ризик-менеджменту. Першочерговим є формування проактивного середовища трансформації ризик-менеджменту (*рис. 6*). Наступним має стати створення на основі новелізації світового досвіду міжнародних норм функціонування кіберпростору та узгодження з ними національних норм (*рис. 7*). У подальшому необхідне доопрацювання міжнародних норм з урахуванням міжнародних і національних практик (*рис. 8*).

Швидкий розвиток глобального діджітал-суспільства та запізнення з формуванням адекватного інституційного середовища [11] призводить до збільшення витрат суб'єктів мікро-, мезо- і макрорівнів, а іноді і до значних втрат.

За даними «Лабораторії Касперського», у 2017 р. частка фінансового фішингу досягла рекордного рівня – антифішингові технології виявили 246 231 645 спроб.

Більше половини (54%) всіх фішингових атак довелося на різні сайти, так чи інакше пов'язані з фінансовими послугами: банки, платіжні системи, інтернет- магазини і т. п. Роком раніше цей показник становив 48%, а ще раніше (у 2015 р.) – 34% (*рис. 9, рис. 10*).

Згідно зі звітом міжнародної компанії IDC і Національного університету Сінгапуру, майже дві третини витрат компаній, а саме – 315 млрд дол. США, будуть спрямовані на боротьбу з цільовими кібератаками. Частка витрат на інформаційну безпеку в IT-бюджетах досягла майже чверті (23%) [12].

Ризики	**За масштабами охоплення**	
За обсягом наслідків	*ідіосинкратичний*	*системний*
незначний	• фізичні особи та домогосподарства	• держава та міжнародне співтовариство
значний	• організації мікрорівня та підсистеми мезорівня	• держава та міжнародне співтовариство

Рис. 5. Матриця власників ризику

Джерело: складено за [10].

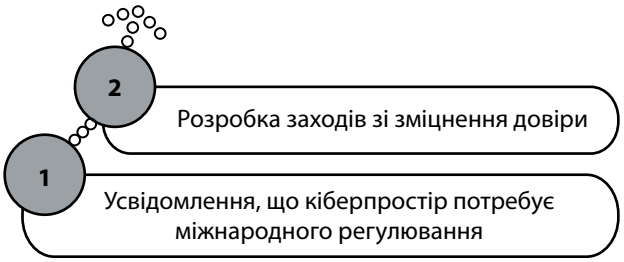

Рис. 6. Необхідні перетворення глобального інституційного середовища на сучасному етапі

Джерело: складено за [6].

Рис. 7. Необхідні перетворення глобального інституційного середовища в наступні 2–5 років

Джерело: складено за [6].

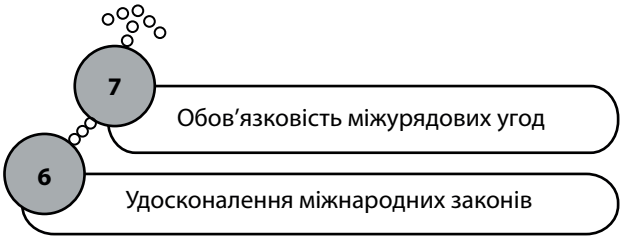

Рис. 8. Необхідні перетворення глобального інституційного середовища в подальшому

Джерело: складено за [11].

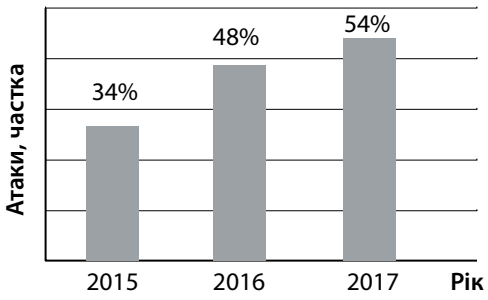

Рис. 9. Динаміка частки фінансових фішингових атак

Джерело: складено за [12].

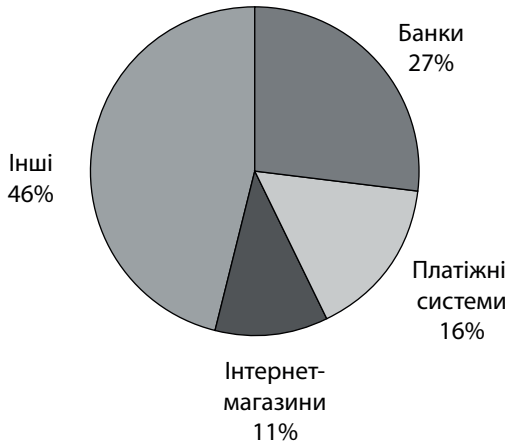

Рис. 10. Розподіл фішингових атак у 2017 р.

Джерело: складено за [12].

Втрати від кіберінцидентів також зростають. Так, за даними «Лабораторії Касперського», у 2017 р. ліквідація наслідків одного кіберінциденту обійшлася компаніям середнього та малого бізнесу у 87,8 тис. дол. Рік тому цей показник становив 86,5 тис. дол. У випадку з корпораціями цифра зросла ще сильніше – з 861 тис. дол. до 992 тис. дол. (*рис. 11*).

Однак зростання вкладень бізнесу в кібербезпеку не можна вважати достатнім на сучасному етапі розвитку. Загрозу несе як пасивне сприйняття державами кібер-ризиків, так і перекладання відповідальності на бізнес і громадянське суспільство.

У 2004 р. у межах ООН 15 держав на рівні урядових експертів розпочали розробку норм регулювання

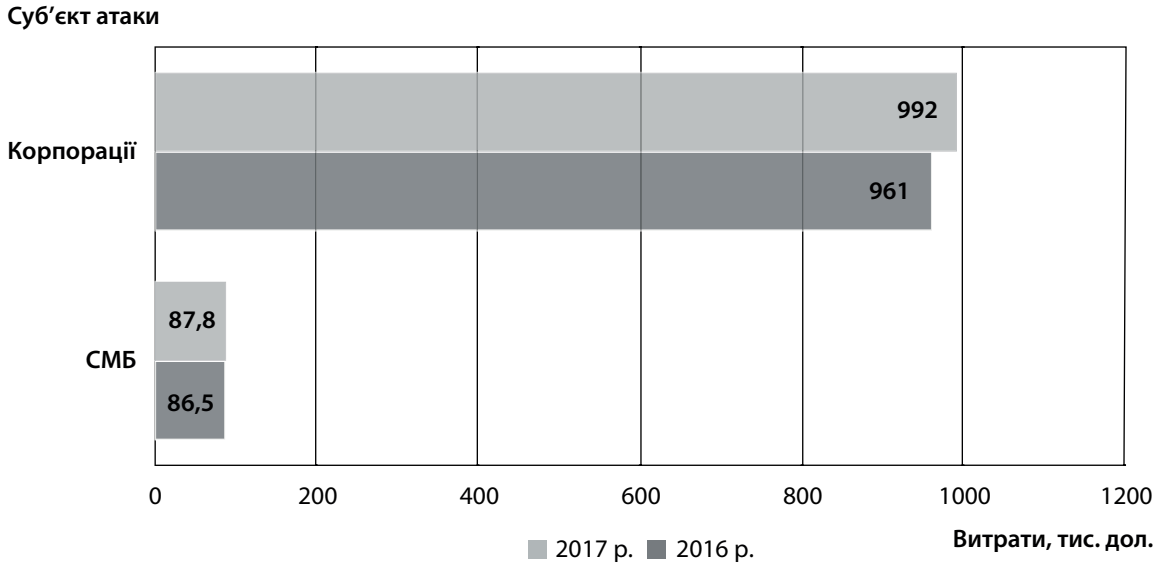

Рис. 11. Витрати на подолання наслідків одного кіберінциденту

Джерело: складено за [12].

функціонування глобального кіберпростору. У 2016 р. склад учасників збільшився до 25. Були підготовлені 5 звітів, але консенсусу не було досягнуто [13].

Розрізнені заходи суб'єктів мікро-, мезо- та макрорівнів суттєво не знижують ризики розвитку інтернет-технологій, а лише підштовхують окремих суб'єктів до самостійних контраверсійних дій [14].

ВИСНОВКИ

Прискорені зміни господарського середовища, детерміновані трансформацією технологічного устрою, обумовили зміни домінуючих рівнів розвитку господарської системи, фундаментальної структури ризикопороджуючих чинників. Пріоритетне значення набувають глобальні ризики інтернет-простору, які потребують спільних зусиль міжнародних організацій, узгодження позицій усіх держав з формування інститутів функціонування глобального інтернет-простору й адаптації до них національних регламентуючих систем. Без усвідомлення цих процесів і інституційного реінжинірингу ризик-менеджменту будуть зростати витрати на кібербезпеку і втрати суб'єктів усіх рівнів. ■

ЛІТЕРАТУРА

1. ISO 31000:2018 (en). Risk management – Guidelines. URL: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

2. Старостина А. О., Кравченко В. А. Ризик-менеджмент: теорія та практика. Київ : Кондор; Політехніка, 2009. 199 с.

3. Савчук В. Риск-менеджмент. Базовые принципы и современные технологии. Київ : Companion Group, 2014. 304 с.

4. Вяткин В. Н., Гамза В. А., Маевский Ф. В. Риск-менеджмент. М. : Юрайт, 2015. 353 с.

5. The Global Risks Report 2018. URL: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

6. Шваб К. Четвертая промышленная революция. М. : Эксмо, 2016. 138 с.

7. Коломієць Г. М. Ризик-менеджмент як фактор сталого розвитку світової економіки. *Актуальні проблеми економіки*. 2015. № 3. С.43–49.

8. Kaljurand M., Lewis J. Finding New Rules for the Stability of Cyberspace. URL: https://www.orfonline.org/wp-content/uploads/2017/11/Our-Common-Digital-Future.pdf

9. Коломієць Г. М., Гузненков Ю. Г. Категорія «ризиків» в дискурсі сучасної економічної теорії. *Вісник ХНУ імені В. Н. Каразіна. Економічна серія*. 2010. № 4. С. 29–34.

10. Меленцова О. В. Ризик-менеджмент у виборі вектору інституційних трансформацій зовнішньоекономічних відносин. *Інвестиції: практика та досвід*. 2016. № 24. С. 47–52.

11. Риски и возможности – управление рисками в интересах развития // Всемирный банк. 2013 год. Доклад о мировом развитии 2014. Вашингтон, округ Колумбия. URL: siteresources.worldbank.org

12. Ciglic K. Why we urgently need a Digital Geneva Convention. URL: https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention

13. Financial cyberthreats in 2017. February, 2018. URL: www.kaspersky.com

14. Schmitt M., Vihul L. International Cyber Law Politicized: The UN GGE's Failure to Advance cyber norms. URL: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/

15. Can state cyber attacks be justified under international law? URL: https://www.weforum.org/agenda/2018/04/can-offensive-cyber-attacks-be-justified-under-international-law

REFERENCES

"Can state cyber attacks be justified under international law?". https://www.weforum.org/agenda/2018/04/can-offensive-cyber-attacks-be-justified-under-international-law

Ciglic, K. "Why we urgently need a Digital Geneva Convention". https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention

"Financial cyberthreats in 2017. February, 2018". www.kaspersky.com

"ISO 31000:2018 (en). Risk management – Guidelines". https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Kaljurand, M., and Lewis, J. "Finding New Rules for the Stability of Cyberspace". https://www.orfonline.org/wp-content/uploads/2017/11/Our-Common-Digital-Future.pdf

Kolomiiets, H. M. "Ryzyk-menedzhment yak faktor staloho rozvytku svitovoi ekonomiky" [Risk management as a factor in the sustainable development of the world economy]. *Aktualni problemy ekonomiky*, no. 3 (2015): 43-49.

Kolomiiets, H. M., and Huznenkov, Yu. H. "Katehoriia «ryzykiv» v dyskursi suchasnoi ekonomichnoi teorii" [The category of "risks" in the discourse of modern economic theory]. *Visnyk KhNU imeni V. N. Karazina. Ekonomichna seriia*, no. 4 (2010): 29-34.

Melentsova, O. V. "Ryzyk-menedzhment u vybori vektoru instytutsiinykh transformatsii zovnishnyoekonomichnykh vidnosyn" [Risk management in the choice of the vector of institutional transformations of foreign economic relations]. *Investytsii: praktyka ta dosvid*, no. 24 (2016): 47-52.

"Riski i vozmozhnosti – upravleniye riskami v interesakh razvitiya" [Risks and opportunities - risk management for development]. *Vsemirnyy bank. Doklad o mirovom razvitii*. 2014. siteresources.worldbank.org

Savchuk, V. *Risk-menedzhment. Bazovyye printsipy i sovremennyye tekhnologii* [Risk management. Basic principles and modern technologies]. Kyiv: Companion Group, 2014.

Schmitt, M., and Vihul, L. "International Cyber Law Politicized: The UN GGE's Failure to Advance cyber norms". https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/

Shvab, K. *Chetvertaya promyshlennaya revolyutsiya* [The Fourth Industrial Revolution]. Moscow: Eksmo, 2016.

Starostyna, A. O., and Kravchenko, V. A. *Ryzyk-menedzhment: teoriia ta praktyka* [Risk Management: Theory and Practice]. Kyiv: Kondor; Politekhnika, 2009.

"The Global Risks Report 2018". http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Vyatkin, V. N., Gamza, V. A., and Mayevskiy, F. V. *Riskmenedzhment* [Risk management]. Moscow: Yurayt, 2015.