УДК 004.7+338.2
JEL Classification Code: C40, C89, F20, K33

Скоробогатова Н. Є.
к.е.н., доцент, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Проценко К. Р.
студентка факультету менеджменту та маркетингу Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

АНАЛІЗ ПОШИРЕННЯ КІБЕРЗАГРОЗ У ГЛОБАЛЬНІЙ ЕКОНОМІЦІ ТА МІНІМІЗАЦІЇ ЗБИТКІВ ВІД НИХ

У статті досліджено масштаби поширення кібератак та світовий досвід формування системи кібербезпеки. Проаналізовано основні етапи ідентифікації ризиків кіберзагроз. Для більш глибинного дослідження обрано дванадцять країн. На основі рівня економічного розвитку та інноваційної активності обрані країни поділено на три групи: країни-лідери (Сінгапур, Сполучені Штати Америки, Канада та Республіка Корея); стабільні країни (Європейські країни, такі як Франція, Німеччина, Великобританія та Норвегія), постсоціалістичні країни (Україна, Польща, Естонія, Російська Федерація). Здійснено кореляційний аналіз взаємозв'язку між основними показниками, що впливають на рівень кіберзагроз: кількість користувачів інтернету, глобальний інноваційний індекс, індекс розвитку людського потенціалу, кількість захищених інтернет-серверів, ВВП загалом та на душу населення, експорт ІКТ, індекс розвитку ІКТ, індекс людського розвитку. Результати кореляційного аналізу показали, що у групі країн-лідерів та стабільних країн наявна схожа залежність між показниками, у той час як у постсоціалістичних країнах відсутня пряма взаємозалежність між аналізованими показниками. З метою попередження кіберзагроз та забезпечення мінімізації збитків від них запропоновано розробку та впровадження комплексної політики інформаційної безпеки господарюючих суб'єктів.

Ключові слова: глобальна економіка; кіберзагрози; кібербезпека; кореляційний аналіз; імпорт-експорт; валовий внутрішній продукт.

Постановка проблеми. Новітні інформаційно-комунікаційні технології (ІКТ) стали важливою складовою суспільного розвитку і розвитку глобальної економіки у цілому. Вони увійшли до числа найбільш суттєвих факторів, які впливають на формування інформаційного середовища та дають можливість на якісно новому рівні вести свою повсякденну оперативну роботу, здійснювати аналіз стану та перспектив діяльності, а також здобувати дані, які необхідні для прийняття управлінських рішень [6].

Темпи інформатизація виробництва та власного життя обумовлюють актуальність проблеми аналізу кіберзагроз у глобальній економіці з метою розвитку системи забезпечення кібербезпеки держави, створення та удосконалення методів, засобів та заходів кіберзахисту. Кількість кібератак у світі з кожним роком зростає, а разом з тим і рівень збитків, які несе держава та інші суб'єкти господарювання.

Аналіз останніх досліджень і публікацій. Результати досліджень сутності кіберзагроз, їх різновидів, класифікація збитків від кібератак та загроз, представлені у працях таких вчених, як І. Діордіца, О. Запорожець, О. Косогов,

М. Грайворонський, М. Ожеван, Д. Дубов, О. Кондрат'єв, В. Панченко, С. Гватюк, В. Бурячок, В. Куцаєв, В. Фурашев та інші. Проте, незважаючи на значну кількість наукових напрацювань залишаються недостатньо дослідженими прояви та наслідки кіберзагроз у глобальній економіці, а також розробка інструментів їх попередження й мінімізації негативних наслідків.

Мета. Метою дослідження є аналіз масштабів поширення кіберзагроз у світовій економіці та узагальнення світового досвіду мінімізації негативних наслідків від них.

Виклад основного матеріалу. Динамічне поширення атак на кіберпростір спричинило низку проблем в процесі дотримання світового правопорядку. Розвиток загроз кібербезпеці демонструє взаємовплив цифрових доменів на загальний стан національної безпеки, адже при сталому розвитку технологій виникають як внутрідержавні, так і міжнародні суперечки.

Задля того, щоб країна і окремі підприємства змогли вчасно застосувати заходи задля перешкоді кібератакам, потрібно вчасно вміти їх ідентифікувати. Науковці виділяють декілька основних етапів ідентифікації [1]:

1.Пошук ризиків і їх розташування – цей крок покаже, що може становити інтерес для кіберзлодія. Дані про клієнтів часто є найбільш важливими для захисту, тому що, хоча прямі витрати на його втрату можуть бути невеликими в порівнянні з даними досліджень або інтелектуальною власністю, але, ймовірно, будуть великі втрати за рахунок штрафів і судових процесів. Крім того, витрати на імідж і втрату довіри клієнтів можуть зайняти роки для відновлення. Також важливо проаналізувати інформацію, де вона зберігається, хто має до неї доступ і які процедури безпеки вони повинні пройти, щоб досягти цього.

2. Моніторинг внутрішньої і зовнішньої небезпеки – після того як все визначено і задокументовано, де компанія може бути в небезпеці, наступним кроком буде зосередити увагу на тих, хто може мати бажання поставити під загрозу безпеку. На даному етапі відбувається аналіз: які види кіберзлочинів можуть загрожувати компанії і як вони зазвичай реалізуються, щоб краще захистити себе.

3. Визначення уразливої системи – має бути чітке уявлення про те, хто може націлитися на ваш бізнес і де вони знаходяться. Пошук недоліків у безпеці даних, перш ніж кіберзлочинці це зроблять. Використовування різних методів для аналізу безпеки систем і мереж. Такі інструменти дозволяють оновлювати програмне забезпечення і визначати відомі уразливості.

4. Визначення впливу загроз та ймовірності їх виникнення – аналіз бізнес-ефекту може допомогти визначити ймовірні результати різних видів порушень кібербезпеки. Таке порушення може мати наслідки, які можуть виходити за рамки фінансових втрат, наприклад, на операції можуть вплинути, оскільки ви вживаєте кроки для відновлення після впливу і застосовуєте нові заходи для захисту від майбутніх атак і будь-якого збитку для громадського іміджу і рейтинг довіри матиме серйозні наслідки для відносин з існуючими та потенційними новими клієнтами, а також з пресою.

5. Пріоритет ризиків та їх дозвіл – після аналізу того, які наслідки можливо понести, необхідно визначити найбільш актуальні проблеми безпеки. Починають зі складання списку пріоритетів і опрацьовують їх один за одним,

впровадивши необхідні заходи.

З метою деталізації аналізу ризиків, нами було проаналізовано рівень кібербезпеки країн. Глобальний індекс кібербезпеки (Global Cybersecurity Index – GCI) – характеризує здатність протистояти кібератакам та забезпечити функціонування критичної цифрової інфраструктури в інтересах продуктивної та безпечної економіки. Він обчислюється на основі інтегральної оцінки зваженої суми за категоріями: нормативно-правове регулювання кіберпростору; економічний і соціальний контекст; технологічна інфраструктура; промислове застосування інформаційно-комунікаційної інфраструктури у різних галузях [2].

З метою ґрунтовного аналізу кіберзагроз у глобальній економіці нами було обрано для дослідження три групи краї за критеріями рівня економічного розвитку та інноваційної активності (табл. 1):

I група – «країни-лідери»: Сінгапур, Сполучені Штати Америки, Канада та Республіка Корея;

II група – «стабільні країни»: Європейські країни, такі як Франція, Німеччина, Великобританія та Норвегія.

III група – «постсоціалістичні країни»: Польща, Естонія, Російська Федерація та Україна.

Таблиця 1 – Глобальний індекс кібербезпеки [2]

№	Країна	Індекс		Динаміка зміни,%
		2015	2017	
I група				
1	Сінгапур	0,676	0,925	36,83
2	Сполучені Штати Америки	0,824	0,919	11,53
3	Республіка Корея	0,706	0,782	10,76
4	Канада	0,794	0,818	3,02
II група				
5	Франція	0,588	0,819	39,29
6	Німеччина	0,706	0,679	-3,82
7	Великобританія	0,706	0,783	10,91
8	Норвегія	0,735	0,786	6,94
III група				
9	Польща	0,529	0,622	17,58
10	Естонія	0,706	0,846	19,83
11	Російська Федерація	0,500	0,788	57,60
12	Україна	0,353	0,501	41,93

Стосовно нарощування потенціалу кібербезпеки, такі країни як Україна, Франція та Сінгапур в динаміці підвищили глобальний індекс кібербезпеки більше ніж на 35%. Хоча, одна з провідних країн світу Німеччина показала зменшення глобального індексу кібербезпеки на 3%.

Для здійснення моніторингу та порівняння розвитку інформаційно-комунікаційних технологій експертами Міжнародного союзу електрозв'язку (МСЕ) було розроблено методику розрахунку Індекс розвитку ІКТ (*IDI*: ICT Development Index). Індекс розвитку ІКТ складається з трьох субіндексів, які сумарно мають значення від 0 до 10:

1. Субіндекс доступу – наявність відповідної інфраструктури: фізична можливість користувача бути підключеним до Інтернет мережі, до мобільного або фіксованого зв'язку;

2. Субіндекс використання – інтенсивність застосування послуг Інтернет

мережі, мобільного та фіксованого зв'язку;

3. Субіндекс практичних навиків – маються на увазі ефективне використання як програмного забезпечення різних ІТ-пристроїв, так і глобальної мережі Інтернет [3]. Значення Індексу розвитку ІКТ за обраними для дослідження країнами наведені в табл. 2.

Дані табл. 2 свідчать про тенденцію до зростання рівня розвитку ІКТ з періодичними коливаннями.

Таблиця 2 – Індекс розвитку ІКТ [3]

№	Країна	Індекс розвитку ІКТ								
		2007	2008	2010	2011	2012	2013	2015	2016	2017
I група										
1	Сінгапур	6,47	6,65	7,47	7,66	7,85	7,90	8,08	7,85	8,05
2	США	6,33	6,54	7,11	7,75	7,90	8,03	8,19	8,13	8,18
3	Республіка Корея	7,23	7,68	8,45	8,56	8,81	8,85	8,93	8,78	8,85
4	Канада	6,30	6,49	6,87	7,04	7,37	7,62	7,76	7,64	7,77
II група										
5	Франція	6,09	6,55	7,08	7,30	7,73	7,87	8,12	8,05	8,24
6	Німеччина	6,60	6,95	7,18	7,39	7,75	7,90	8,22	8,20	8,39
7	Великобританія	6,70	7,07	7,35	7,75	8,28	8,50	8,75	8,53	8,65
8	Норвегія	6,78	7,11	7,39	7,52	8,35	8,39	8,49	8,45	8,47
III група										
9	Польща	4,95	5,29	6,09	6,19	6,63	6,60	7,76	7,64	7,77
10	Естонія	5,86	6,41	6,36	6,81	7,53	7,68	8,05	8,16	8,14
11	Російська Федерація	4,13	4,54	5,61	6,00	7,48	7,70	6,91	6,91	7,07
12	Україна	3,56	3,87	4,20	4,40	4,97	5,15	5,23	5,31	5,62

З метою виявлення залежності індексом розвитку ІКТ, індексом людського розвитку, глобальним індексом інновацій [4] та іншими інтегральними показниками, було здійснено кореляційний аналіз (рис. 1). Після проведення кореляційного аналізу по Сінгапуру можна зазначити, що залежність між всіма обраними показниками пряма і має значення більше 0,5.

Найменша залежність спостерігається між кількістю захищених інтернет-серверів країни та глобальним індексом інновацій – 0,504, найбільша залежність між ВВП на душу населення та кількістю користувачів інтернетом – 0,994. Аналогічна картина спостерігається і в США, що пояснюється збалансованим розвитком країни.

Найслабша залежність, так само як в Сінгапурі, спостерігається між кількістю захищених інтернет-серверів країни та глобальним інноваційним індексом – 0,358, між глобальним інноваційним індексом та кількістю інтернет-користувачів, кількістю захищених інтернет-серверів та індексом розвитку ІКТ, 0,453 та 0,446 відповідно. У Республіці Корея також спостерігається пряма залежність між аналізованими показниками.Кореляційний аналіз інтегральних показників Канади показав відсутність єдиної картини їх зміни, зокрема, між показникам існує як пряма, так и обернена залежність. На відміну від всіх країн даної групи в Канаді обернена залежність між індексом розвитку ІКТ та ВВП – -0,506. У Франції між глобальним інноваційним індексом та ВВП майже відсутній взаємозв'язок – коефіцієнт кореляції 0,016, проте між індексом розвитку ІКТ, індексом людського розвитку та ВВП обернена залежність – -0,578 та -0,570 відповідно. Таким чином, в цих двох країнах інформаційні технології зворотнім чином впливають на ВВП.

Сінгапур									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,534	1							
К3	0,954	0,761	1						
К4	0,915	0,504	0,836	1					
К5	0,962	0,892	0,981	0,841	1				
К6	0,994	0,653	0,966	0,957	0,972	1			
К7	0,957	0,648	0,916	0,965	0,950	0,975	1		
К8	0,778	0,764	0,922	0,757	0,896	0,846	0,887	1	
К9	0,911	0,780	0,878	0,891	0,914	0,979	0,978	0,919	1

США									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,453	1							
К3	0,966	0,672	1						
К4	0,855	0,358	0,763	1					
К5	0,932	0,651	0,971	0,847	1				
К6	0,929	0,654	0,968	0,830	0,9997	1			
К7	0,894	0,768	0,953	0,922	0,979	0,975	1		
К8	0,660	0,942	0,802	0,446	0,837	0,840	0,914	1	
К9	0,846	0,762	0,834	0,643	0,981	0,982	0,993	0,920	1

Республіка Корея									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,499	1							
К3	0,983	0,816	1						
К4	0,766	0,885	0,859	1					
К5	0,973	0,750	0,991	0,805	1				
К6	0,966	0,600	0,978	0,811	0,988	1			
К7	0,836	0,702	0,872	0,707	0,927	0,937	1		
К8	0,575	0,758	0,890	0,587	0,821	0,698	0,842	1	
К9	0,882	0,740	0,959	0,434	0,986	0,946	0,977	0,852	1

Канада									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,605	1							
К3	0,985	0,743	1						
К4	0,795	0,111	0,786	1					
К5	0,858	0,341	0,892	0,678	1				
К6	0,990	0,699	0,986	0,745	0,884	1			
К7	0,874	0,417	0,909	0,670	0,998	0,901	1		
К8	0,972	0,497	0,812	0,053	-0,506	0,951	-0,378	1	
К9	0,978	0,589	0,956	0,246	-0,388	0,930	-0,252	0,968	1

Франція									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,671	1							
К3	0,962	0,799	1						
К4	0,795	0,567	0,895	1					
К5	0,887	0,016	0,861	0,123	1				
К6	0,971	0,723	0,963	0,919	0,794	1			
К7	0,930	0,730	0,934	0,897	0,800	0,969	1		
К8	0,964	0,774	0,868	0,873	-0,578	0,928	0,966	1	
К9	0,799	0,203	0,312	0,711	-0,570	0,661	0,620	0,737	1

Німеччина									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,292	1							
К3	0,958	0,791	1						
К4	0,949	0,543	0,934	1					
К5	0,913	0,380	0,930	0,507	1				
К6	0,874	0,774	0,953	0,953	0,852	1			
К7	0,921	0,737	0,965	0,910	0,919	0,987	1		
К8	0,803	0,718	0,893	0,885	-0,239	0,972	0,960	1	
К9	0,828	0,732	0,863	0,935	-0,006	0,988	0,936	0,986	1

Великобританія									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,611	1							
К3	0,972	0,374	1						
К4	0,801	0,054	0,661	1					
К5	0,924	0,689	0,958	0,256	1				
К6	0,943	0,626	0,968	0,631	0,876	1			
К7	0,955	0,683	0,976	0,655	0,943	0,972	1		
К8	0,848	0,827	0,613	-0,225	0,892	0,870	0,919	1	
К9	0,883	0,273	0,880	-0,393	0,589	0,898	0,815	0,657	1

Норвегія									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,576	1							
К3	0,939	0,457	1						
К4	0,979	0,604	0,825	1					
К5	0,818	0,272	0,821	0,518	1				
К6	0,922	0,647	0,925	0,798	0,956	1			
К7	0,848	-0,033	0,881	0,712	0,881	0,934	1		
К8	0,851	0,709	0,713	0,732	-0,177	0,429	0,288	1	
К9	0,983	0,596	0,913	0,890	-0,419	0,143	-0,029	0,829	1

Польща									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,337	1							
К3	0,935	0,577	1						
К4	0,860	0,465	0,952	1					
К5	0,940	0,355	0,909	0,441	1				
К6	0,944	0,732	0,988	0,873	0,903	1			
К7	0,944	0,579	0,963	0,834	0,920	0,990	1		
К8	0,878	0,528	0,921	0,916	-0,594	0,944	0,894	1	
К9	0,794	0,664	0,969	0,831	-0,058	0,970	0,904	0,906	1

Естонія									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,578	1							
К3	0,983	0,822	1						
К4	0,986	0,594	0,952	1					
К5	0,947	0,764	0,964	0,756	1				
К6	0,958	0,792	0,986	0,956	0,961	1			
К7	0,932	0,729	0,959	0,878	0,975	0,988	1		
К8	0,901	0,765	0,988	0,927	0,638	0,984	0,919	1	
К9	0,899	0,834	0,959	0,917	0,704	0,996	0,915	0,985	1

Російська Федерація									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,760	1							
К3	0,961	0,601	1						
К4	0,729	0,428	0,653	1					
К5	0,737	0,270	0,904	-0,167	1				
К6	0,955	0,933	0,979	0,447	0,891	1			
К7	0,885	0,502	0,963	0,160	0,961	0,967	1		
К8	0,766	0,715	0,937	0,254	0,406	0,886	0,738	1	
К9	0,962	0,849	0,869	0,602	0,854	0,854	0,497	0,852	1

Україна									
	К1	К2	К3	К4	К5	К6	К7	К8	К9
К1	1								
К2	0,679	1							
К3	0,835	0,763	1						
К4	0,851	0,431	0,610	1					
К5	0,455	0,026	0,825	-0,413	1				
К6	0,838	0,529	0,966	0,391	0,767	1			
К7	0,903	0,700	0,886	0,445	0,779	0,923	1		
К8	0,951	0,731	0,726	0,750	-0,324	0,497	0,639	1	
К9	0,812	0,822	0,923	0,495	-0,017	0,769	0,855	0,927	1

К1 – кількість користувачів інтернету
К2 – глобальний інноваційний індекс
К3 – індекс розвитку людського потенціалу
К4 – кількість захищених інтернет-серверів
К5 – ВВП, млрд дол.
К6 – ВВП на душу населення, дол.
К7 – експорт ІКТ, млн дол.
К8 – індекс розвитку ІКТ, од.,
К9 – індекс людського розвитку, од.

Рисунок 1 – Кореляційний аналіз макроекономічних показників
(розроблено авторами)

У Німеччини обсяг ВВП більшою мірою визначається саме розвитком людського потенціалу, коефіцієнт кореляції між ними становить 0,988. Інформаційні технології тут, як і в Канаді, не мають визначального характеру.

У Великобританії спостерігається низька залежність між кількістю захищених інтернет-серверів та індексом глобальної інновації – 0,054, між індексом розвитку ІКТ і кількістю захищених інтернет-серверів та кількістю захищених інтернет-серверів і індексом людського розвитку – -0,225 та -0,393 відповідно.

Норвегія також немає сталого зв'язку між аналізованими показниками – присутня як пряма, так і зворотна залежність. Зокрема, слабка обернена залежність спостерігається між експортом ІКТ та глобальним інноваційним індексом, експортом ІКТ та індексом людського розвитку – -0,033 та -0,029 відповідно.

Розглядаючи результати кореляційного аналізу постсоціалістичних країн, слід відзначити відсутність єдиної тенденції. Зокрема, у Польщі між індексом людського розвитку та ВВП майже відсутній взаємозв'язок, коефіцієнт кореляції -0,058. Обернена залежність спостерігається між ВВП та індексом розвитку ІКТ (-0,594). В Естонії спостерігається пряма залежність між всіма аналізованими показники. В цій країні навпаки, найбільший ступінь впливу людського розвитку на ВВП (0,996). Між обсягом ВВП та глобальним інноваційним індексом України, а також індексом людського розвитку майже не спостерігається залежності – 0,026 та -0,017 відповідно, що свідчить про відсутність впливу інновацій та людського капіталу на обсяги вироблюваного ВВП.

Сьогоднішні темпи інформатизації провідних країн та загальносвітовий розвиток ІТ-технологій обумовлюють актуальність проблеми побудови та розвитку глобальної системи забезпечення кібернетичної безпеки держави, створення та удосконалення методів, засобів та заходів кібернетичного захисту. Опрацювання аналітичних даних дають змогу дійти висновку, що масштабні кібератаки відбуваються на великі корпорації, банки та страхові компанії. Втрати від кібератак у більшості країн у 2017 році збільшились порівняно з 2016 роком. Найбільший обсяг збитків від кібератак зазнали США, що майже на 10 млн дол. більше, ніж в Німеччині [5].

З метою захисту від об'єктів від кібератак та мінімізації збитків від них вважаємо необхідним розроблення комплексної політики інформаційної безпеки господарюючих суб'єктів, що базуватиметься на концептуальних засадах державної політики інформаційної безпеки. Зокрема, дана політика має відображати специфіку діяльності конкретного підприємства, для якої вона розробляється. Законом України «Про захист персональних даних» власник персональних даних зобов'язаний здійснювати їх захист від випадкових втрати або знищення, а також від незаконної обробки. Окрім того, з метою ефективної реалізації розробленої політики має здійснюватися постійний моніторинг дотримання її вимог.

Висновки. В результаті проведеного аналізу системи кіберзахисту на міжнародному рівні та міжнародних стратегій забезпечення кібербезпеки встановлено, що національні потреби й проблеми істотно різняться залежно від регіону, рівня розвитку держави та інших специфічних чинників.

Новизною роботи є виявлення взаємозв'язку між основними макроекономічними показниками та рівнем інформаційної безпеки країн в залежності від рівня їх економічного розвитку та інноваційної активності. Обрані для дослідження країни було поділено у три групи: країни-лідери, стабільні та постсоціалістичні. На основі кореляційного аналізу виявлено основні чинники, що впливають на рівень кібербезпеки: індекс розвитку ІКТ, індекс людського розвитку тощо. При чому обрані для дослідження групи країн мають різну тенденцію, що визначається особливостями їх економічного укладу.

З метою попередження кібератак та мінімізації збитків від них запропоновано розроблення комплексної політики інформаційної безпеки підприємств, що базуватиметься на концептуальних засадах державної політики інформаційної безпеки.

Список використаних джерел

1. Cornell, B., 2017. Identifying and overcoming cybersecurity risks: 5 steps. *Data Center Journal*. [online]. Available through: http://www.datacenterjournal.com/identifying-overcoming-cybersecurity-risks-5-steps/.

2. Global Cybersecurity Index, 2017. *International Telecommunication Union*. [online]. Available through: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [Accessed 10 September 2018].

3. ICT Development Index, 2017. *International Telecommunication Union*. [online]. Available through: https://www.itu.int/net4/ITU-D/idi/2017/ [Accessed 10 September 2018].

4. Global Innovation Index, 2017. *Cornell University, INSEAD, and the World Intellectual Property Organization*. [online]. Available through: https://www.globalinnovationindex.org [Accessed 5 August 2018].

5. Cost of cyber crime study, 2017. *Ponemon Institute LLC and Accenture*. [online]. Available through: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf [Accessed 15 August 2018].

6. Новікова А. П. та Скоробогатова, Н. Є., 2018. Аналіз розвитку світового та українського ринку ІТ-послуг. *Інвестиції: практика та досвід.* 3, С. 52-56.

Скоробогатова Н. Е.
к.э.н., доцент, Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского»
Проценко К. Р.
студентка факультету менеджмента и маркетинга Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского»

АНАЛИЗ РАСПРОСТРАНЕНИЯ КИБЕРУГРОЗ В ГЛОБАЛЬНОЙ ЭКОНОМИКЕ И МИНИМИЗАЦИЯ УБЫТКОВ ОТ НИХ

В статье исследованы масштабы распространения кибератак и мировой опыт формирования системы кибербезопасности. Проанализированы основные этапы идентификации рисков киберугроз. Для более глубокого исследования отобраны двенадцать стран. На основе уровня экономического развития и инновационной активности данные страны разделены на три группы: страны-лидеры (Сингапур, США, Канада и Республика Корея), стабильные страны (Европейские страны, такие как Франция, Германия, Великобритания и Норвегия), постсоциалистические страны (Украина, Польша, Эстония, Россия). Проведен корреляционный анализ взаимосвязи

между основными показателями, влияющими на уровень киберугроз: количество пользователей интернета, международный инновационный индекс, индекс развития человеческого потенциала, количество защищенных интернет-серверов, ВВП в целом и на душу населения, экспорт ИКТ, индекс развития ИКТ, индекс человеческого развития. Результаты корреляционного анализа показали, что в группе стран-лидеров и стабильных стран имеется похожая зависимость между показателями, в то время как в постсоциалистических странах отсутствует прямая взаимозависимость между рассматриваемыми показателями. С целью предупреждения киберугроз и обеспечение минимизации ущерба от них предложена разработка и внедрение комплексной политики информационной безопасности хозяйствующих субъектов.

Ключевые слова: глобальная экономика; киберугрозы; кибербезопасность; корреляционный анализ; импорт-экспорт; валовой внутренний продукт.

Skorobogatova N. Ye.
PhD of Economic sciences, Associate Professor
Igor Sikorsky Kyiv Polytechnic Institute
Procenko K. R.
Student of the Faculty of Management and Marketing,
Igor Sikorsky Kyiv Polytechnic Institute

ANALYSIS OF THE SPREAD OF CYBER THREATS IN THE GLOBAL ECONOMY AND MINIMIZATION OF LOSSES FROM THEM

The article presents the results of a study of the spread of cyber-attacks and world experience in the formation of a cybersecurity system. The main stages of identifying risks of cyber threats were analyzed. For a more in-depth study, twelve countries were selected. Based on the level of economic development and innovation activity, these countries were divided into three groups: the leading countries (Singapore, USA, Canada and the Republic of Korea), stable countries (European countries such as France, Germany, Great Britain and Norway) and post-socialist countries (Ukraine, Poland, Estonia and Russia). A correlation analysis of the relationship between the main indicators affecting the level of cyber threats: the number of Internet users, international innovation index, human development index, number of protected Internet servers, GDP in general and per capita, ICT export, ICT development index, human development index . The results of the correlation analysis showed that in the group of leading countries and stable countries there is a similar relationship between indicators, while in the post-socialist countries there is no direct interdependence between the indicators under consideration. In order to prevent cyber threats and ensure minimization of damage from them, it was proposed to develop and implement a comprehensive information security policy for business entities.

Key words: global economy; cyber threats; cyber security; correlation analysis; import-export; gross domestic product.

Скоробогатова Н. Є.
natasha1978@ukr.net