PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU
RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS nr 541 • 2018

ISSN 1899-3192
e-ISSN 2392-0041

Adam Śliwiński
Szkoła Główna Handlowa w Warszawie
e-mail: asliwin@sgh.waw.pl

RYZYKO CYFROWE WYZWANIEM SEKTORA UBEZPIECZEŃ

DIGITAL RISK AS AN INSURANCE SECTOR CHALLENGE

DOI: 10.15611/pn.2018.541.21
JEL Classification: D81, G22

Streszczenie: Celem artykułu jest przybliżenie pojęcia ryzyka cyfrowego, jego klasyfikacji i wzrostu jego znaczenia z punktu widzenia zagrożeń cywilizacyjnych. W artykule zawarto wyniki badań literaturowych związanych z ryzykiem cyfrowym. W tekście dokonano identyfikacji i klasyfikacji ryzyka cyfrowego i skoncentrowano się na przedstawieniu skali zagrożenia związanego z cyfryzacją. Opisano także nowe rodzaje ryzyka cyfrowego związanego z centralizacją baz danych oraz z tzw. flarami słonecznymi. Należy podkreślić, że dalszy rozwój cyfryzacji jest ściśle związany z działaniami sektora ubezpieczeń. Rozwój cyfryzacji stwarza szansę dla sektora na innowacyjność i na to, by realizując swoją misję wspomagania rozwoju cywilizacyjnego, w niedalekiej przyszłości stworzył adekwatną ofertę i aktywnie włączył się w działania majce na celu minimalizację opisanego ryzyka.

Słowa kluczowe: ryzyko cyfrowe, chmury danych, cyfryzacja, ubezpieczenia.

Summary: The aim of the paper is an approximation of the concept of digital risk, its classification and increasing importance from the point of view of the threats to civilization. In the text the identification and classification of digital risks has been described. The article focuses on the presentation of the scale of the threat associated with digitalization. The paper also describes new types of digital risk associated with centralizing databases and solar flares. Having regard to the nature and size of the losses, these risks are very difficult to insure. It should be pointed out that the further development of digitization is closely associated with the activities of the insurance sector. The development of digitalization creates the opportunity for the sector to be innovative and, in carrying out its mission to assist in the development of civilization, in the near future to create an adequate insurance offer. The sector should actively involve in activities to handle the described risk.

Keywords: digital risk, cloud computing, digitalization, insurance.

1. Wstęp

Powszechna cyfryzacja stanowi wyzwanie dla sektora ubezpieczeń. Podobnie jak nanotechnologia postęp cyfryzacji stwarza zarówno szanse, jak i zagrożenia. Nanotechnologia jest nowym podejściem badawczym do struktury i właściwości materii, która rozpatrywana jest w skali nano, czyli miliardowej części metra. Cyfryzacja natomiast dotyczy sposobów komunikowania się, wytwarzania, gromadzenia danych oraz innych sfer związanych z funkcjonowaniem jednostek.

Obok wielu korzyści, które wypływają z rozwoju cyfryzacji (szybkość komunikacji, możliwość gromadzenia olbrzymiej liczby danych, miniaturyzacja itd.), należy być świadomym zagrożeń, jakie z niej wynikają. Uświadomienie tych zagrożeń jest ważne zarówno ze strony biznesu ubezpieczeniowego, jak i klienta. Podejście do ryzyka i wybór metody obchodzenia się z nim ma bowiem dynamiczny charakter i zależy od zachowania otoczenia [Śliwiński, Klapkiv 2017, s. 21-36]. Celem artykułu jest przybliżenie pojęcia ryzyka cyfrowego, jego klasyfikacji i zwiększającego się znaczenia z punktu widzenia zagrożeń cywilizacyjnych.

W literaturze przedmiotu oraz wielu raportach o charakterze biznesowym ryzyko cyfrowe kojarzone jest z rozwojem cyfryzacji polegającej na realizacji wielu transakcji w sferze wirtualnej. Podstawowym wymienianym zagrożeniem jest zagrożenie związane z atakami polegającymi na przechwyceniu danych gromadzonych w funkcjonujących systemach. W artykule przedstawiono jeszcze jedną płaszczyznę generującą określone typy ryzyka związane z przestrzenią cybernetyczną. Jest to płaszczyzna powiązana z procesem gromadzenia danych w tzw. chmurach i wynikająca z tego centralizacja baz danych. Centralne bazy danych (biblioteki aleksandryjskie) w niedalekiej przyszłości mogą gromadzić większość danych światowych, generując ryzyko utraty tych danych przez ich właścicieli. Jednocześnie pojawia się problem dla administratorów baz danych, mający dwojaki charakter. Dotyczy zabezpieczenia danych w aspekcie technicznych oraz finansowym. I tu wkraczamy na grunt ubezpieczeń. Ryzyko związane z centralizacją baz danych powinno być traktowane jako ryzyko cyfrowe o charakterze katastroficznym, stanowiące wyzwanie dla sektora ubezpieczeń. Należy tu podkreślić, że płaszczyzną generującą ryzyko jest sam fakt centralizacji baz danych. W artykule poruszono także temat wybuchów na słońcu, które według fizyków mogą powodować zniszczenie systemów informatycznych[1].

[1] Patrz: Konferencja Cambridge Conference on Catastrophic Risk 2016 [Cambridge Conference…].

2. Ryzyko cyfrowe − identyfikacja

2.1. Pojęcie ryzyka cybernetycznego

W powszechnym ujęciu cyberryzyko[2] jest zwykle mylnie utożsamiane wyłącznie z zainfekowaniem komputera przez hakerów złośliwym oprogramowaniem (*malware*) [Strupczewski 2017, s. 66]. Termin „ryzyko cybernetyczne" odnosi się jednak do wielu różnych źródeł ryzyka. Przykłady zagrożeń cybernetycznych obejmują m.in. [Mational Association…]:

- kradzież tożsamości w wyniku naruszenia bezpieczeństwa,
- przerwanie działalności przez hakera zamykającego sieć,
- koszty związane z uszkodzeniem rekordów danych spowodowanych przez hakera,
- kradzież cennych zasobów cyfrowych, w tym list klientów, tajemnic handlowych i innych elektronicznych aktywów biznesowych,
- wprowadzenie złośliwego oprogramowania, robaków i innego złośliwego kodu komputerowego,
- błąd ludzki prowadzący do nieumyślnego ujawnienia poufnych informacji, takich jak wiadomość e-mail od pracownika do niezamierzonych odbiorców.

W literaturze przedmiotu podjęto wiele prób zdefiniowania terminu „cyberryzyko". Niektóre z nich zawierają dość wąskie ujęcie i określają ryzyko cybernetyczne jako ryzyko związane ze złośliwymi zdarzeniami elektronicznymi, które powodują zakłócenia w prowadzeniu biznesu i starty finansowe [Mukhopadhyay i in., s. 11-26]. Inne ujmują ryzyko cybernetyczne w szerszej perspektywie − jako ryzyko bezpieczeństwa informacji [Ögüt i in. 2011, s. 497-512]. Ryzyko cybernetyczne obejmuje więc wszelkie sytuacje narażenia na potencjalne straty w wyniku używania sprzętu elektronicznego, komputerów oraz przetwarzania informacji w wirtualnej rzeczywistości [Podolak 2015, s. 369-409]. Ryzyko cybernetyczne można zatem wiązać z aktywnością *online*, handlem internetowym, systemami elektronicznymi i sieciami technologicznymi, a także przechowywaniem danych, w tym danych osobowych [Olsen 2013].

Najczęściej spotykaną klasyfikacją ryzyka cybernetycznego jest jego podział ze względu na kryterium rodzaju szkodliwych działań prowadzących do materializacji strat, a więc przyczyn tzw. cyberszkód. Zdarzenia mogą być wynikiem umyślnie

[2] Termin „cyber" jest skrótem od słowa „cyberprzestrzeń". Po raz pierwszy pojęciem tym posłużył się w 1982 r. William Gibson, autor literatury science-fiction, który wprowadził je w noweli zatytułowanej *Burning Chrome* (opublikowanej w czasopiśmie „Omni"). Odwoływał się on najprawdopodobniej do pojęcia c y b e r n et y ki (*cybernetics*), przedstawionej przez Norberta Wienera jeszcze w 1948 r. i zdefiniowanej w tytule jego książki *Cybernetics: or Control and Communication in the Animal and the Machine* (New York 1948, John Wiley & Sons). Najczęściej używana definicja cyberprzestrzeni została skonstruowana przez Departament Obrony USA; określa ona cyberprzestrzeń jako: globalną domenę środowiska informacyjnego składającą się z współzależnych sieci tworzonych przez infrastrukturę, technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery.

złośliwych działań (np. działań hakera przeprowadzającego atak), ale mogą również być niezamierzone (np. błąd użytkownika, który powoduje, że system jest tymczasowo niedostępny). Zdarzenia mogą pochodzić z zewnątrz organizacji (cyberprzestępcy, partnerzy handlowi) lub z organizacji (pracownicy, podwykonawcy). Połączenie tych dwóch wymiarów prowadzi do kategoryzacji zagrożeń cybernetycznych na:

- wewnętrzne złośliwe − umyślne działania sabotażowe, kradzieże lub inne wykroczenia popełniane przez pracowników,
- wewnętrzne niezamierzone − akty prowadzące do uszkodzenia lub utraty wynikające z błędu ludzkiego popełnionego przez pracowników,
- zewnętrzne złośliwe − ataki ze strony osób trzecich, w tym cyberprzestępców, terrorystów, aktywistów (tzw. haktywistów) i organy wrogich państw czy firm (przykłady obejmują infiltrację sieciową i pobieranie własności intelektualnej oraz ataki DoS (*Denial-of-Service*)), które powodują problemy z dostępnością systemu, przerwy w działaniu firmy lub zakłócają prawidłowe działanie podłączonych urządzeń),
- zewnętrzne niezamierzone − podobnie jak w przypadku niezamierzonych wewnętrznych, powodują straty lub szkody, ale nie są celowe (np. klęski żywiołowe).

Cyberryzyko jest najczęściej rozumiane jako ryzyko operacyjne związane z zasobami informacyjnymi i technologicznymi.

2.2. Klasyfikacja ryzyka cyfrowego

Zgodnie z ramami ryzyka operacyjnego ustalonymi w Bazylei III i Wypłacalności II ryzyko cybernetyczne może być klasyfikowane w czterech grupach; są nimi: (1) działania ludzi, (2) awarie systemów i technologii, (3) nieudane procesy wewnętrzne i (4) zdarzenia zewnętrzne (patrz tab. 1). Cyberryzyko obejmuje także ryzyko reputacyjne, które w regulacjach rynku finansowego ujmowane jest odrębnie.

Podczas identyfikacji ryzyka cybernetycznego warto zwrócić uwagę także na pojęcie cyberterroryzmu. Federalne Biuro Śledcze definiuje cyberterroryzm jako celowy, motywowany politycznie atak przeciw informacji, systemom komputerowym, programom komputerowym i danym, który skierowany jest przeciw cywilnym i wojskowym celom przez państwowych i niepaństwowych aktorów. Należy go odróżnić od innych nielegalnych aktów, takich jak przestępczość komputerowa, szpiegostwo gospodarcze czy też wojna informacyjna [Janowska 2003, s. 448-449]. Aby konkretny atak w przestrzeni informatycznej uznać za terroryzm cybernetyczny, musi on skutkować pewnym stopniem przemocy w stosunku do ludzi lub ich własności, a przynajmniej wywoływać strach. Zatem o terroryzmie cybernetycznym możemy mówić jedynie wtedy, kiedy mamy do czynienia z politycznie motywowanym atakiem przy użyciu sieci teleinformatycznych. W pozostałych przypadkach takie ataki klasyfikuje się zazwyczaj jako przestępstwa cybernetyczne bez podtekstu politycznego [Biuro Bezpieczeństwa Narodowego 2009].

Tabela 1. Kategorie ryzyka cybernetycznego

Kategoria	Opis	Elementy
Podkategoria 1: działanie ludzkie		
1.1. Nieumyślne	niezamierzone działania bez złośliwego lub szkodliwego zamiaru	błędy, pominięcia
1.2. Rozmyślne	działania podjęte celowo z zamiarem wyrządzenia szkody	oszustwa, sabotaż, kradzież i wandalizm
1.3. Bezczynność	brak działania lub zaniechanie działania w danej sytuacji	brak odpowiednich umiejętności, wiedzy, wskazówek i dostępności personelu do działania
Podkategoria 2: awarie systemów i technologii		
2.1. Sprzęt komputerowy	ryzyko związane z awariami sprzętu	awarie z powodu zbyt niskiej wydajności, niewystarczającej konserwacji i przestarzałości, kompatybilność
2.2. Oprogramowanie	ryzyko wynikające z oprogramowania wszelkiego typu, w tym programów, aplikacji i systemów operacyjnych	zarządzanie konfiguracją, kontrola zmian, ustawienia bezpieczeństwa
2.3. Systemy	awarie zintegrowanych systemów działania niezgodne z oczekiwaniami	kodowanie i testowanie, specyfikacje, integracja i złożoność
Podkategoria 3: błędne/nieudane procesy wewnętrzne		
3.1. Projektowanie i/lub wykonanie procesów	awarie związane z wadliwym procesem lub nieosiągnięcie pożądanych efektów z powodu złego zaprojektowania i/lub wykonania procesów	dokumentacja procesu, role i obowiązki, powiadomienia i alerty, przepływ informacji, eskalacja problemów, umowy o poziomie usług i zlecanie zadań
3.2. Kontrola procesów	niewystarczająca kontrola	monitorowanie statusu, dane, okresowe przeglądy i własność procesu
3.3.Wspieranie procesów	niepowodzenie wsparcia	personel, księgowość, szkolenia i rozwój oraz zamówienia
Podkategoria 4: wydarzenia zewnętrzne		
4.1. Katastrofy	zdarzenia naturalne lub antropogeniczne, nad którymi nie ma kontroli i które mogą wystąpić niespodziewanie	wydarzenie pogodowe, pożar, powódź, trzęsienie ziemi, niepokoje
4.2. Problemy prawne	ryzyko regulacji prawnych	zgodność z przepisami, prawodawstwo i spory sądowe
4.3. Problemy biznesowe	ryzyko wynikające ze zmian w środowisku biznesowym organizacji	awaria dostawcy, warunki rynkowe i okoliczności gospodarcze
4.4. Zależności usługowe	ryzyko wynikające z podmiotów zewnętrznych wobec organizacji	media, służby ratunkowe, paliwo i transport
Ryzyko cyberterroryzmu		
Aspekty polityczne	celowy, motywowany politycznie atak przeciw informacji, systemom komputerowym, programom komputerowym i danym	cele cywilne i wojskowe

Źródło: opracowanie na podstawie [Cebula, Young 2010; Biener i in. 2015].

3. Zagrożenia cybernetyczne na świecie

Technologie informacyjne i komunikacyjne tworzące świat cyfrowy ewoluowały znacznie w ciągu ostatnich 50 lat (patrz tab. 2). Trzeba podkreślić, że sfera Internetu, mediów społecznościowych i technologii mobilnych zmienia się dynamicznie. Na

Tabela 2. Kroki milowe w technologii informacyjnej

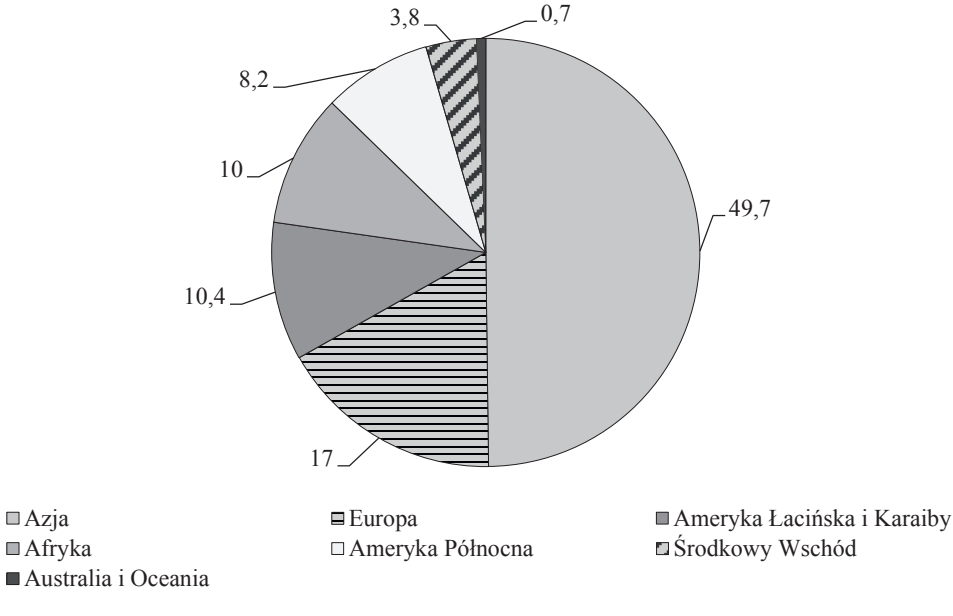
Lata	Wydarzenie
1940-1949	Zbudowano pierwsze komputery, używając lamp elektronowych
1962	Pierwszy modem komercyjny
1964	Pierwszy komputer *mainframe* (klasa komputerów używanych głównie przez duże organizacje dla krytycznych aplikacji (np. finansowych, statystycznych)
1971	Pierwszy wysłany e-mail
1972	Pierwszy mikroprocesor firmy Intel
1975	Bill Gates zakłada firmę Microsoft
1976	Steve Jobs i Steve Wozniak zakładają firmę Apple
1981	Pierwsze komputery personalne IBM PC
1983	Stworzona zostaje wojskowa sieć MILnet (uważana za początek Internetu)
1984	Pierwszy organizer osobisty (PSION), pierwsze CD-ROMy
1985	Pierwszy wirus, powstają pierwsze użytkowe sieci komputerowe (National Science Foundation tworzy NSFNET, sieć szybkich superkomputerów wykorzystywanych do celów naukowych)
1986	National Science Foundation zgadza się na utworzenie szkieletu Internetu, odkrycie standardu JPG
1990	Utworzono World Wide Web i pierwszą przeglądarkę internetową
1993	Apple wprowadza komputery PDA (palmtop) − pierwszy z ekranem dotykowym
1994	W USA dostępny jest już system nawigacji satelitarnej GPS
1996	Powstaje wyszukiwarka internetowa Google (w ramach projektu studenckiego na Uniwersytecie Stanforda); pierwsze DVD
1997	Uzgodniono standard Wi-Fi
1999	Stworzenie aplikacji Napster (aplikacja pozwalająca na wyszukiwanie, zakup oraz pobieranie plików mp3)
2000	Czasy klastrów komputerowych (*cluster* − grupa połączonych jednostek komputerowych, które współpracują ze sobą w celu udostępnienia zintegrowanego środowiska pracy)
2001	Powstaje iTunes
2002	Pierwszy smartfon BlackBerry
2003	Powstaje MySpace
2004	Powstaje Facebook
2006	Usługa przetwarzania w chmurze (*cloud computing*) Powstaje Twitter
2009	Publikacja przeglądu polityki dotyczącej cyberprzestrzeni w USA i Strategii bezpieczeństwa cybernetycznego w Wielkiej Brytanii
2010	Premiera iPada firmy Apple, wkrótce potentata na rynku Tablet PC.

Źródło: opracowanie własne na podstawie [Dudzik, Guzik 2011; Filipczak 1997].

przykład Polska jest krajem, gdzie dopiero w latach 50. ubiegłego wieku wdrażano powszechną elektryfikację [Ustawa o powszechnej elektryfikacji wsi i osiedli…], a 50 lat później zadziałało pierwsze połączenie internetowe [Internet 5].

O skali zagrożenia świadczyć może choćby liczba podmiotów korzystających na świecie z Internetu. Liczba internautów na świecie w końcu sierpnia 2017 roku wyniosła 3,819 miliarda osób (51% populacji korzysta z Internetu). Według danych Głównego Urzędu Statystycznego w Polsce w 2016 r. 80,1% gospodarstw domowych miało w domu przynajmniej jeden komputer. Dostęp do Internetu w 2016 r. posiadało 80,4% gospodarstw domowych, w tym 75,7% miało dostęp szerokopasmowy.

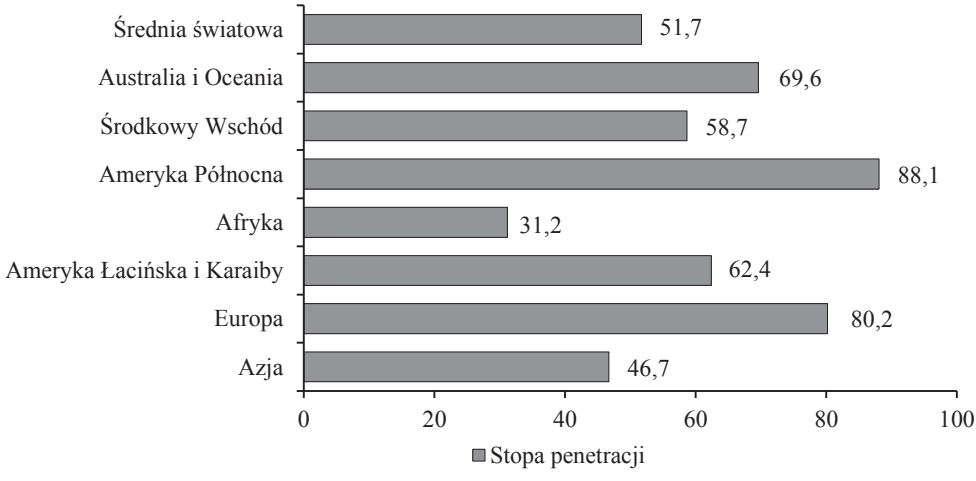
Wśród wszystkich światowych gospodarek najwyższy stan cyfryzacji odnotowuje się w Chinach, gdzie liczba aktywnych użytkowników Internetu wynosi około 640 milionów, co stanowi aż 49,6% wszystkich internautów na świecie. Dysproporcja rysująca się pomiędzy Chinami i resztą świata wynika z dwóch powodów: bardzo dużej populacji tego regionu oraz jego wysokiego zaawansowania technologicznego. Według danych Głównego Urzędu Statystycznego w Polsce w 2016 r. 80,1% gospodarstw domowych miało w domu przynajmniej jeden komputer. Dostęp do Internetu w 2016 r. posiadało 80,4% gospodarstw domowych, w tym 75,7% – szerokopasmowy [*Społeczeństwo informacyjne w Polsce*... 2016, s. 1].



Rys. 1. Struktura użytkowników Internetu w sierpniu 2017 r. [%]

Źródło: [Internet 1].

Najwyższy wskaźnik penetracji Internetu[3] odnotowuje się w Ameryce Północnej, gdzie z sieci korzysta ponad 88% społeczeństwa (rys. 2), najniższy − w Afryce (31,2%).



Rys. 2. Wskaźnik penetracji Internetu według regionów w sierpniu 2017 r.

Źródło: [Internet 1].

W krajach regionu Europy Środkowej i Wschodniej (CEE) najwyższy wskaźnik penetracji Internetu występuje w Czechach. Na kolejnym miejscu jest Polska, a dalej Rosja. W tabeli 3 zestawiono wskaźnik penetracji Internetu w wybranych krajach CEE w latach 2013-2019.

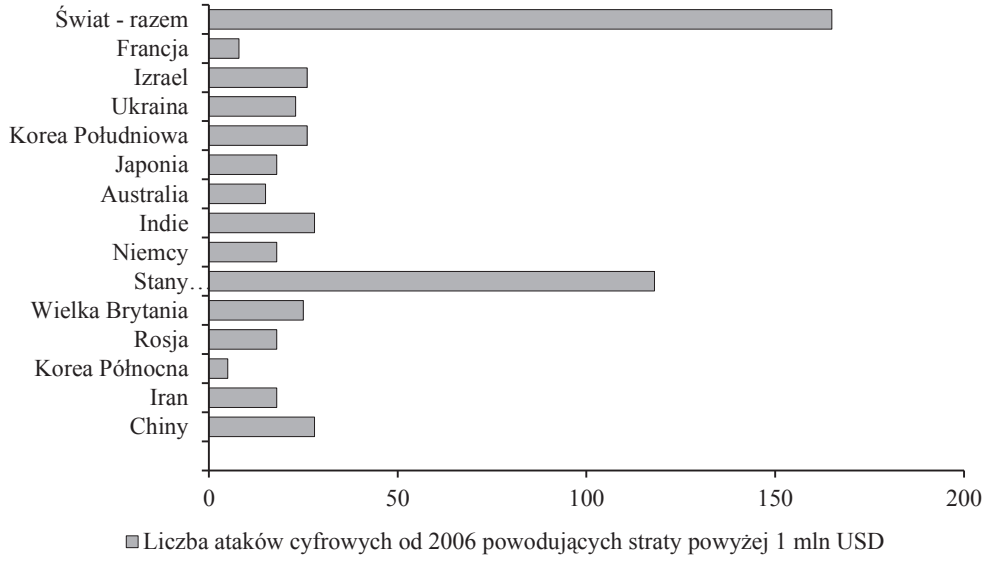
Tabela 3. Wskaźnik penetracji Internetu w krajach Europy Środkowo-Wschodniej w latach 2013-2019 [%]

Kraj	Rok						
	2013	2014	2015	2016	2017	2018	2019
Czechy	68,0	70,0	73,5	74,7	75,5	76,2	77,0
Rosja	54,4	58,2	61,3	64,2	66,3	68,0	69,6
Polska	58,8	59,8	60,8	61,8	62,8	63,8	64,8
Turcja	45,3	50,2	54,2	57,2	60,2	62,8	65,2
Pozostałe kraje	42,0	44,8	47,5	49,9	52,3	54,5	56,7
Europa Środkowa i Wschodnia	**48,9**	**52,2**	**55,2**	**57,7**	**60,0**	**61,9**	**63,8**

Źródło: [Internet 4].

[3] Wskaźnik penetracji Internetu (*Internet penetration rate*) wyraża procentowo udział liczby osób korzystających z Internetu w populacji całkowitej. Definicja wskaźnika − patrz na przykład [Internet 7].

Powszechność wykorzystania Internetu powoduje, że rośnie liczba ataków cybernetycznych. Na przykład w raporcie CSIS pokazano, że w latach 2006-2019 najwięcej ataków o znacznych stratach finansowych przeprowadzono w Stanach Zjednoczonych. Instytucjami najczęściej narażonymi na ataki cybernetyczne były instytucje finansowe[4].



Rys. 3. Liczba ataków cyfrowych powodujących szkody powyżej 1 mln USD; dane za okres 2006-2019 [szt.]

Źródło: [Internet 3].

W Europie w 2016 r. hakerzy najczęściej atakowali firmy finansowe, produkcyjne, telekomunikacyjne i rządy w Niemczech, Wielkiej Brytanii, Belgii, Hiszpanii, Danii, Szwecji, Norwegii i Finlandii[5].

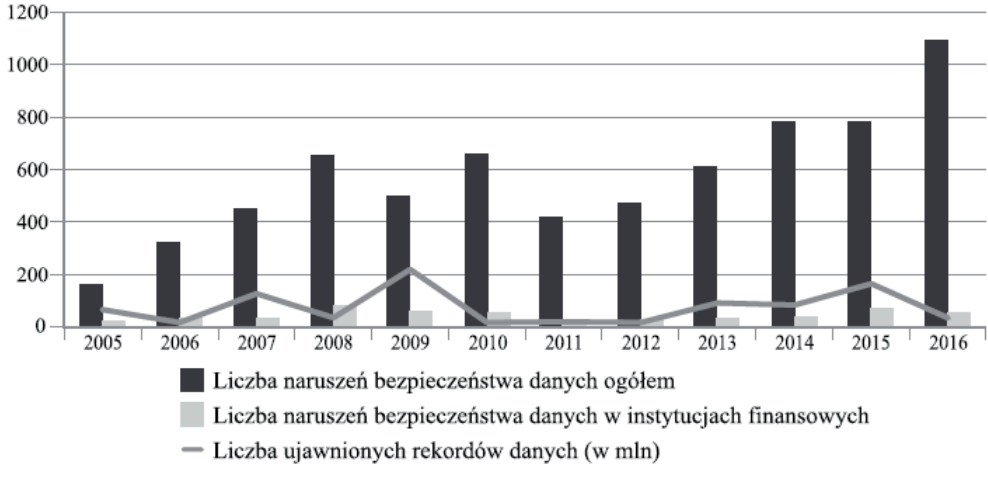
3.1. Skutki cyberataków

Na świecie roczne szacowane średnie straty finansowe przypisywane incydentom naruszania cyberbezpieczeństwa wyniosły w 2014 r. 2,7 mln USD, co stanowi znaczny, 34-procentowy wzrost w porównaniu z 2013 rokiem (podobnie jak łączna liczba incydentów). Światowy koszt cyberprzestępczości jest bardzo trudny do zweryfikowania. Dzieje się tak dlatego, że wiele ataków pozostaje niezgłoszonych, a wartość niektórych informacji, takich jak własność intelektualna, jest trudna do

[4] Patrz [Center For Strategic & International…].

[5] Więcej danych na temat ataków rządów poszczególnych krajów patrz: [Marsh and McLennan].

wyliczenia. Badania prowadzone przez Center for Strategic and International Studies wykazały, że roczny koszt cyberprzestępczości dla gospodarki światowej waha się w przedziale od 375 mld USD do 575 mld USD [Internet 3]. Kwota ta jest wysoka, jednak nawet w przybliżeniu jest niższa od strat, jakie mogą wystąpić w związku z kradzieżą tajemnic handlowych oraz własności intelektualnej. Wpływ tego rodzaju utraty informacji można mierzyć wskaźnikami finansowymi i niefinansowymi. Skutki finansowe mogą obejmować spadek przychodów, zakłócenia w działalności gospodarczej, kary od organów nadzoru i odpływ klientów. Skutki niefinansowe mogą zaś obejmować utratę reputacji, powstanie pirackich produktów, zmianę kierunku informacji dotyczących badań i rozwoju, negatywne skutki dla innowacji, kradzież projektów lub prototypów produktów, kradzież procesów gospodarczych lub produkcyjnych, a także utratę wrażliwych informacji, takich jak plany fuzji lub połączeń oraz strategii przedsiębiorstwa.



Rys. 4. Liczba wypadków naruszenia ochrony danych w USA

Źródło: [Strupczewski 2017].

Nie tylko firmy są zagrożone cyberprzestępczością. Odnotowuje się także wzrost ataków na urządzenia konsumenckie podłączone do globalnej sieci – takie jak urządzenia do monitorowania małych dzieci, termostaty czy telewizory – które składają się na Internet rzeczy (*Internet of things*). Jest on ekosystemem urządzeń, który wymienia między sobą informacje. Te urządzenia, podłączone do Internetu, są narażone na ataki, ponieważ nie mają podstawowych zabezpieczeń, co ostatnio potwierdziło badanie HP *Fortify on Demand*[6]. Badanie 46 światowych giełd, przeprowadzone przez Międzynarodową Organizację Komisji Papierów Wartościowych (IOSCO)

[6] Firma HP dokonała przeglądu 10 najczęściej używanych urządzeń i odkryła, że 70% z nich zawiera poważne luki w mechanizmach ochrony. Patrz: [Internet 8].

i Światową Federację Giełd, wykazało ponadto, że ponad połowa z nich (53%) padła ofiarą cyberataku [IOSCO and the World Federation of Exchanges Office 2013]. Eksperci wskazują, że w 2016 roku rosnącą liczbę ataków *ransomware* (szkodliwe oprogramowanie szyfrujące dane) najdotkliwiej odczuły branże: finansowa, produkcyjna, telekomunikacyjna, a także agencje rządowe i sektor zdrowotny. Najbardziej pożądane przez hakerów dane to tajemnice handlowe przedsiębiorstw (stanowiące 19% danych skradzionych w atakach cybernetycznych w Europie w minionym roku) oraz informacje dotyczące systemów kontroli i plany strategiczne (18%) [*Cyberprzestępczość może zmienić…*]. Ważnym problemem jest też możliwość uzyskania dostępu do danych osobowych. Ośrodek badawczy Identity Theft Resource Center (ITRC) gromadzi dane dotyczące wypadków naruszenia bezpieczeństwa prywatnych danych na rynku amerykańskim. Według informacji publikowanych przez wspomniany ośrodek rok 2016 był rekordowy pod względem liczby incydentów informatycznych, która ukształtowała się na poziomie 1093.

Jak wynika z analiz, współczesna gospodarka i społeczeństwo mimo świadomości zagrożeń płynących z cyberprzestrzeni oraz coraz większych nakładów na bezpieczeństwo IT, stają się coraz bardziej podatne na *cyberryzyko*. W literaturze przedmiotu wskazuje się dwie zasadnicze tego przyczyny [Strupczewski 2017, s. 72]:

- przesłanki techniczno-technologiczne – realizacja płatności – elektronicznych, praca w chmurze (*cloud computing*), dominacja oprogramowania Microsoft, wzrost złożoności programów komputerowych, stosowanie elektronicznych systemów sterowania infrastrukturą, maszynami i urządzeniami (tzw. systemy SCADA), rozwój bankowości elektronicznej oraz tzw. Internetu rzeczy;
- przesłanki społeczno-behawioralne – popularność mediów społecznościowych, posługiwanie się urządzeniami mobilnymi, korzystanie ze słabo zabezpieczonego przed „podsłuchiwaniem" dostępu do Internetu przez routery Wi-Fi (tzw. *sniffing*), nieklasyczne metody organizacji pracy (praca na odległość, wykorzystywanie w miejscu pracy prywatnego sprzętu komputerowego), powszechne wykorzystanie korespondencji e-mailowej w kontaktach biznesowych.

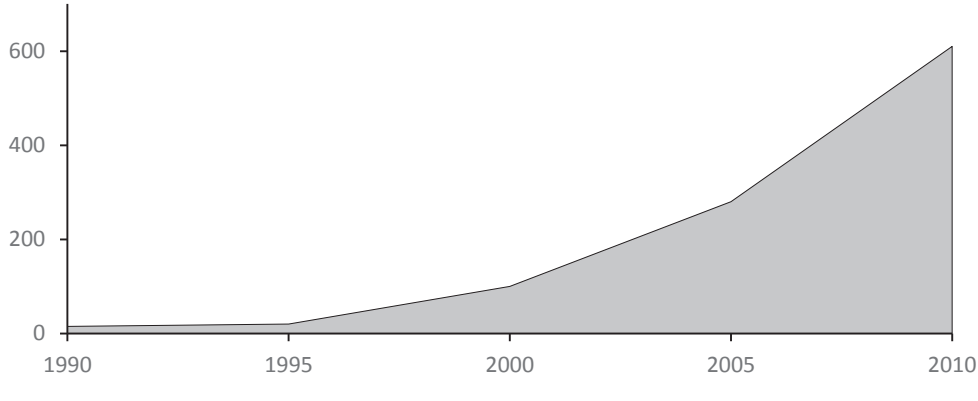
Analizując zagrożenia cybernetyczne, należy także wspomnieć o tym, że od kilkunastu lat, równolegle do konwencjonalnych działań wojennych, ma miejsce militarne zastosowanie Internetu. W lutym 2001 r. chińscy hakerzy dokonali ataków na największe japońskie firmy w odwecie za zaostrzenie polityki wobec Chin. Trzy miesiące później, w odpowiedzi na amerykańskie ataki wymierzone w chińskie portale internetowe, chińscy hakerzy włamali się na strony amerykańskiej administracji oraz biznesu [Janowska 2003, s. 446-450]. Powszechne jest także wykorzystywanie sieci przez terrorystów. Radykałowie używają sieci do rekrutacji nowych członków, szerzenia ideologii, zarządzania finansami, manipulacji opinią publiczną, a także koordynacji działań. Ekstremistom nowoczesne narzędzia komunikacji służą do prowadzenia wojny medialnej i kształtowania opinii publicznej. Na przykład w lutym 2000 r. unieruchomione zostały serwery Yahoo, Amazon, CNN, eBay. W ten sposób test skuteczności swoich działań przeprowadził Hezbollah [Biuro Bezpieczeństwa

Narodowego 2009]. Skuteczny atak na infrastrukturę krytyczną (w szczególności systemy: zaopatrzenia w energię i paliwa, teleinformatyczne, bankowe i finansowe, zaopatrzenia w żywność oraz wodę, a także opieki zdrowotnej, transportowe i komunikacyjne, ratownicze oraz zapewniające funkcjonowanie organów władzy administracji publicznej) jest w stanie znacznie wpłynąć na gospodarkę zaatakowanego państwa, a także spowodować olbrzymie straty wśród ludności cywilnej.

4. *Public cloud* i wybuchy słoneczne a cyberryzyko

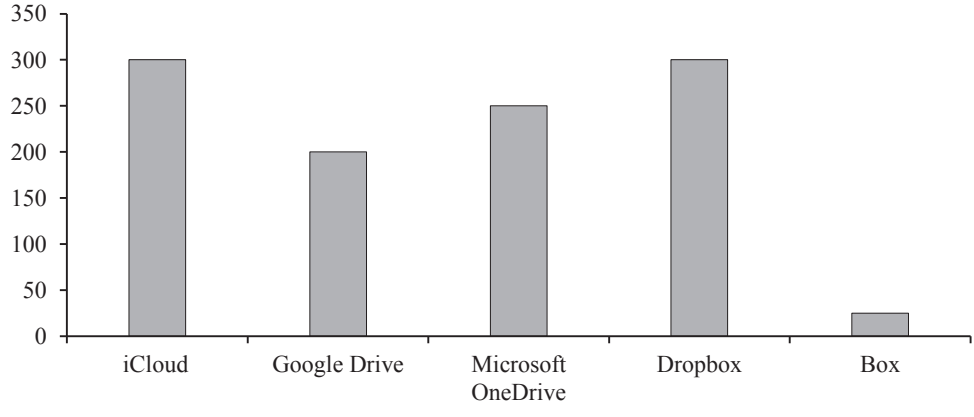
Chmura publiczna (*public cloud*) to pojęcie związane z tematyką chmury obliczeniowej, odnoszące się do tworzenia środowisk obliczeń rozproszonych oraz przenoszenia danych, systemów operacyjnych lub aplikacji wymagających dużej mocy obliczeniowej na serwer. Młode pokolenie coraz chętniej korzysta z możliwości, jakie stwarza chmura publiczna. Pozwala to, przy relatywnie niskim koszcie, dysponować wymaganą pojemnością dysków oraz korzystać z zaawansowanych programów obliczeniowych. Rosnąca liczba użytkowników Internetu (patrz rys. 5) zwiększa także popularność rozwiązań bazujących na chmurach. Już w 2014 r. w samych Stanach Zjednoczonych liczba użytkowników poszczególnych. chmur przekroczyła 1 bln (patrz rys. 6).

Korzystanie z zewnętrznych serwerów jest także coraz bardziej popularne wśród przedsiębiorstw. W założeniach firmy nie muszą utrzymywać własnej, często skomplikowanej i kosztownej infrastruktury oraz personelu do jej obsługi, a jednocześnie mogą podnieść elastyczność i dostępność systemów informatycznych. W efekcie są w stanie dynamicznie zwiększać moc środowiska informatycznego. Zasoby IT stają się w tym modelu dostępne dla użytkowników niezależnie od miejsca dostępu i od urządzenia, z którego w danym momencie korzystają. Duże przedsiębiorstwa mogą tworzyć chmury obliczeniowe w postaci tzw. chmury prywatnej. W takiej chmurze



Rys. 5. Liczba użytkowników poszczególnych serwisów

Źródło: [Internet System Consortium].



Rys. 6. Liczba użytkowników poszczególnych serwisów oferujących tzw. *cloud storage*

Źródło: raporty przedsiębiorstw.

dział informatyczny udostępnia infrastrukturę oraz aplikacje w formie usług wewnętrznych. Popularne oferty chmury publicznej, takie jak te od Amazon, Rackspace, Salesforce.com. Microsoft, IBM i Google, konkurują ze sobą w celu zapewnienia rozbudowanej oferty usług IT i aplikacji biznesowych.

Korzystanie z rozwiązań chmurowych z jednej strony niesie ze sobą określone wyzwania, ale i ograniczenia. Największym zagrożeniem jest bezpieczeństwo, kontrola i prywatność danych. W tradycyjnych rozwiązaniach przedsiębiorstwo miało nad nimi pełną kontrolę. W modelu chmurowym użytkownik nie ma wpływu na miejsce przechowywania danych. Chmura obliczeniowa może zapewnić wydajność niemożliwą do osiągnięcia dla wielu firm czy użytkowników indywidualnych, jednak możliwości te są często ograniczone przez szybkość transmisji między komputerem użytkownika a chmurą. Z ubezpieczeniowego punktu widzenia popularność tzw. chmury powoduje jeszcze jedno zagrożenie, mało rozpoznane i mogące stanowić niezwykłe wyzwanie dla branży ubezpieczeniowej. Chodzi tu o wspomnianą we wstępie centralizację baz danych. Utrzymywanie danych na zewnętrznych serwerach powoduje, że w razie szkody wynikającej na przykład z ataku cybernetycznego czy ze zwykłej awarii systemów użytkownicy tracą olbrzymią ilość danych. Centralizacja powoduje, że rozmiary szkód mogą być bardzo duże i mogą znacznie przekraczać możliwości ubezpieczycieli. Powoduje to, że ryzyko cyfrowe jest trudno ubezpieczalne.

Sektor ubezpieczeniowy w pełni nie uświadamia sobie tego zagrożenia. Istnieje jednak jeszcze inna jego płaszczyzna, związana z przenoszeniem i gromadzeniem danych cyfrowych i tzw. rozbłyskami słonecznymi (*solar flares*). Zagrożenie to jest niezwykle ważne z punktu widzenia ubezpieczeń. Rozbłysk słoneczny to zespół zjawisk i procesów fizycznych wywołany nagłym wydzieleniem w atmosferze słońca ogromnej ilości energii, spowodowany przez proces anihilacji pola magnetycznego.

Rozbłyski słoneczne mogą trwale uszkodzić twarde dyski łącznie ze znajdującymi się tam danymi. Ryzyko wybuchów solarnych zostało uznane za ryzyko zagrażające egzystencji człowieka[7]. Narzędzie, jakim jest ubezpieczenie, prawdopodobnie nie będzie miało tu zastosowania ze względu na rozmiar i charakter strat. Trzeba jednak pamiętać, że takie zagrożenie istnieje i powinno być ono uwzględniane w pracach naukowych.

5. Zakończenie

Postępująca globalizacja oraz rozpowszechnienie Internetu spowodowały wzrost znaczenia ryzyka cyfrowego. Ryzyko to dotyczy zarówno poszczególnych jednostek, gospodarstw domowych czy przedsiębiorstw, jak i bezpieczeństwa oraz obronności poszczególnych krajów. Ryzyko cyfrowe stanowi wyzwanie dla współczesnego człowieka. Rozwój Internetu i nowoczesnych form komunikacji oraz przechowywania danych zrewolucjonizował rozwój cywilizacyjny przez wpływ na wiele sfer życia człowieka. Cyfryzacja stwarza niewyobrażalne możliwości w wielu dziedzinach, takich jak na przykład komunikacja, finanse czy nawet przemysł. Obok wielu korzyści rozwój cyfryzacji naraża jednak naszą cywilizację na wzrost znaczenia wielu nowych typów ryzyka.

Na zakończenie można stwierdzić, że upowszechnienie i dalszy rozwój cyfryzacji są ściśle związane z działaniami sektora ubezpieczeń. Jak wspominano, rozwój ten stwarza szansę dla sektora na to, aby był innowacyjny, by realizując swoją misję wspomagania rozwoju cywilizacyjnego, w niedalekiej przyszłości stworzył adekwatną ofertę i aktywnie włączył się w działania majce na celu minimalizację ryzyka związanego z rozwojem cyfryzacji.

Literatura

Betterlay R., 2013, *Cyber/Privacy Insurance Market Survey 2013: Carriers Deepen Their Risk Management Services Benefits − Insureds Grow Increasingly Concerned with Coverage Limitation*, http://betterley.com/samples/cpims13_nt.pdf.

Betterlay R., *Understanding the Cyber Risk Insurance and Remediation Services Marketplace*. A report of on the Experience and Opinions of Middle Market CFOs, www.casact.org.

Biener C., Eling M., Wirfs J.H, 2015, *Insurability of Cyber Risk: an Empirical Analysis*, Working Papers on Risk Management and Insurance, no. 151, Insitute of Insurance Economics, University of St. Gallen.

Biuro Bezpieczeństwa Narodowego, 2009, *Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*, Warszawa, lipiec.

Cambridge Conference on Catastrophic Risk 2016, https://www.cser.ac.uk/events/CCCR-2016/.

Cebula J.J., Young L R., 2010, *A Taxonomy of Operational Cyber Security Risks,* Technical Note CMU/SEI-2010-TN-028, CERT Carnegie Mellon University.

Center For Strategic & International Studies, https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/financial-sector-cybersecurity (19.03.2019).

[7] Patrz: program konferencji [Cambridge Conference…].

Cyber Risk Survey, 2013, https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20Survey%2006-2013.pdf.

Cyberprzestępczość może zmienić rynek ubezpieczeń. Polisy od ataków hakerskich i innego cyberryzyka mogą się stać hitem, https://biznes.newseria.pl/news/cyberprzestepczosc,p1719534426 (15.10.2017).

Duch W., 1997, *Fascynujący świat komputerów,* Wydawnictwo Nakom, Poznań.

Dudzik P., Guzik A., 2011, *Historia informatyki i komputerów*, AGH, Kraków.

Filipczak M., Wykłady z przedmiotu „Historia informatyki", Wydział Matematyki, Uniwersytet Łódzki

IOSCO and the World Federation of Exchanges Office, 2013, Cyber-Crime, Securities Markets and Systemic Risk, lipiec.

Internet System Consortium, http://www.isc.org/solutions/survey/historyMarsh.

Janowska A., 2003, *Cyberterroryzm – rzeczywistość czy fikcja*?, [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość?,* Kraków.

Mukhopadhyay A., Chatterjee S., Saha D., Mahanti D., Sadhukan S., *Cyber-risk decision models: To insure IT or Not?,* Decision Support Systems, 56(1).

National Association of Insurance Commissioners, 2013, *Cyber Risk,* http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

Olsen T., 2013, *Insurance Cyber Ris*k, Willis, 18.06.2013.

Ögüt H., Raghunathan S., Menon N., 2011, *Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection*, Risk Analysis 31(3), s. 497-512.

Rejda G.E., 1998, *Prinncipel of Risk Management and Insurance*, Addison-Wesley.

Społeczeństwo informacyjne w Polsce w 2016, 2016, GUS, Warszawa.

Strupczewski G., 2017, *Zagrożenia cybernetyczne instytucji finansowych*, Rozprawy Ubezpieczeniowe. Konsument na Rynku Usług Finansowych, nr 24 (2/2017).

Śliwiński A., Klapkiv L., *Transformation of beliefs: an evaluation of economic risk under uncertainty,* „Olsztyn Economic Journal" 2017, Vol.12, No.1, s. 21–36

Ustawa o powszechnej elektryfikacji wsi i osiedli z dnia 28 czerwca 1950 r., http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19500280256.

Wasilewski J., 213, *Zarys definicyjny cyberprzestrzeni*, Przegląd Bezpieczeństwa Wewnętrznego, nr 9.

Wiener N., 1948, *Cybernetics: or Control and Communication in the Animal and the Machine*, John Wiley & Sons, New York.

Willis, *Willis Fortune 1000 Cyber Disclosure Report*, https://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf.

Internet

[1] http://www.internetworldstats.com/stats.htm (15.03.2019).
[2] https://biznes.newseria.pl/news/cyberprzestepczosc,p1719534426 (15.10.2017).
[3] https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.
[4] https://interaktywnie.com/biznes/artykuly/raporty-i-badania/polska-zanotuje-wskaznik-penetracji-internetu-powyzej-sredniej-ale-do-zachodu-nam-daleko-251748 (4.04.2019).
[5] https://pclab.pl/art33917-6.html.
[6 https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity (18.03.2019).
[7] https://www.igi-global.com/dictionary/internet-penetration-rate/15439 (3.04.2019).
[8] https://www.scmagazine.com/the-security-vulnerability-you-can-prevent/article/532843/ (15.10.2017).