REDAKCJA
NAUKOWA

MACIEJ CYCOŃ

TOMASZ JEDYNAK

GRZEGORZ STRUPCZEWSKI

NOWE TRENDY I INNOWACJE W ZARZĄDZANIU RYZYKIEM I UBEZPIECZENIACH

PRZEGLĄD UBEZPIECZEŃ 2018

FUNDACJA UNIWERSYTETU EKONOMICZNEGO W KRAKOWIE

Nowe trendy i innowacje w zarządzaniu ryzykiem i ubezpieczeniach

Przegląd Ubezpieczeń 2018

redakcja naukowa

Maciej Cycoń

Tomasz Jedynak

Grzegorz Strupczewski

Fundacja Uniwersytetu Ekonomicznego w Krakowie

Kraków 2018

Recenzenci
dr hab. Robert Kurek, Prof. UE we Wrocławiu
dr Anna Ostrowska-Dankiewicz
dr Robert Dankiewicz

ISBN 978-83-65907-23-3
pdf online

Publikacja została wydana w ramach projektu „Nowe trendy i innowacje w zarządzaniu ryzykiem i ubezpieczeniach" realizowanego przez Koło Naukowe Ubezpieczeń „Risk Management" oraz Katedrę Zarządzania Ryzykiem i Ubezpieczeń w latach 2017-2018 r.

Wydawnictwo:
Fundacja Uniwersytetu Ekonomicznego w Krakowie
ul. Rakowicka 27, 31-510 Kraków

Spis treści

Wstęp

Początek dwudziestego pierwszego stulecia został naznaczony głębokimi przemianami w sferze społecznej, gospodarczej i politycznej. Jednym z głównych katalizatorów tych zmian był postęp technologiczny, którego intensywność i dynamika osiągnęły bezprecedensową skalę w ostatnich latach. Konsekwencje zachodzących zmian widoczne są nie tylko w sferze realnej, ale i finansowej. Do nowej rzeczywistości dostosować muszą się rynki finansowe, w tym rynek ubezpieczeniowy, usytuowany na styku obu tych sfer.

W obliczu zachodzących przemian w makrootoczeniu pojawiają się nowe i intrygujące poznawczo tematy badawcze, do których należą m.in.: 1) nowe warunki prowadzenia gospodarki finansowej zakładów ubezpieczeń; 2) nowa rola ubezpieczeń ryzyk finansowych wobec niestabilności otoczenia gospodarczego; 3) redefinicja funkcji ubezpieczenia turystycznego wobec rosnącej mobilności o charakterze zarobkowym i niezarobkowym; 4) kreacja nowych ryzyk wynikających z cyfryzacji i automatyzacji gospodarki, których potrzeba ubezpieczenia stawia towarzystwa ubezpieczeń wobec konieczności rozszerzania oferty produktowej.

Potrzeba zgłębienia wskazanych obszarów stała się inspiracją do zainicjowania projektu naukowego zrealizowanego przez Katedrę Zarządzania Ryzykiem i Ubezpieczeń Uniwersytetu Ekonomicznego w Krakowie wraz z Kołem Naukowym Ubezpieczeń Risk Management pt. „Nowe trendy i innowacje w zarządzaniu ryzykiem i ubezpieczeniach”. Jednym z efektów tego projektu jest przedkładana publikacja, której struktura odzwierciedla zrealizowane przez poszczególnych autorów tematy badawcze.

Monografia składa się siedmiu rozdziałów tworzących spójną całość. Rozdział pierwszy traktuje o polityce rezerw techniczno-ubezpieczeniowych zakładów ubezpieczeń majątkowych w kontekście stabilności ich funkcjonowania. W rozdziale drugim podjęto problematykę ubezpieczenia kredytu kupieckiego jako metody zarządzania niewypłacalności partnera biznesowego. W kolejnym rozdziale dokonano analizy przyczyn przerw w prowadzeniu działalności gospodarczej, skutkujących utratą lub zmniejszeniem zysku przedsiębiorstwa, co jest przedmiotem ochrony w ubezpieczeniu *business interruption*.

Tematyka rozdziału 4 obejmuje zagadnienie ubezpieczeń turystycznych, których rola w ostatnich latach znacząco wzrosła.

Kolejne trzy rozdziały tworzą blok tematyczny koncentrujący się na konsekwencjach cyfryzacji i automatyzacji gospodarki. Wyzwania dla sektora ubezpieczeń wynikające z wdrażania konceptu pojazdów autonomicznych są przedmiotem szczegółowych analiz w rozdziale 5. Działania ponadnarodowych grup przestępczych w cyberprzestrzeni stały się źródłem nowej formy terroryzmu – cyberterroryzmu. Ta nowa forma zagrożenia globalnego stała się inspiracją do przeprowadzonych w rozdziale 6 rozważań na temat ubezpieczalności tego rodzaju ryzyka. Kontynuacją wątku zarządzania ryzykiem cybernetycznym jest charakterystyka i analiza światowego rynku ubezpieczeń cybernetycznych zawarta w rozdziale 7.

Wierzymy, że przekazywana w ręce czytelników monografia może stanowić cenne źródło wiedzy dla studentów, ludzi nauki, praktyków z dziedziny ubezpieczeń oraz samorządowców i pracowników różnego rodzaju organów i instytucji publicznych. Mamy również nadzieję, że zawartość publikacji będzie stanowiła źródło inspiracji dla kolejnych badań mających na celu zgłębienie złożonej problematyki ubezpieczeń gospodarczych.

Niniejsza publikacja nie powstałaby bez wsparcia licznego grona osób. Poza autorami poszczególnych rozdziałów i redaktorami naukowymi w badaniach, których efektem jest ta książka brali również udział pozostali pracownicy Katedry Zarządzania Ryzykiem i Ubezpieczeń, a także studenci z Koła Naukowego Ubezpieczeń „Risk Management", których nie sposób wymienić tutaj wszystkich z imienia i nazwiska. Za okazane wsparcie w procesie wydawniczym dziękujemy pracownikom Fundacji Uniwersytetu Ekonomicznego w Krakowie oraz Sekcji Promocji Uniwersytetu Ekonomicznego w Krakowie. Ponadto szczególne podziękowania należą się recenzentom – prof. UE dr hab. Robertowi Kurkowi z Uniwersytetu Ekonomicznego we Wrocławiu oraz dr. Annie Ostrowskiej-Dankiewicz i dr. Robertowi Dankiewiczowi z Politechniki Rzeszowskiej.

Maciej Cycoń

Tomasz Jedynak

Grzegorz Strupczewski

Rozdział 1.
Rezerwy techniczno-ubezpieczeniowe jako warunek stabilności funkcjonowania zakładów ubezpieczeń

Klaudia Ciach*

1.1. Wprowadzenie

Prowadzenie działalności ubezpieczeniowej wiąże się z wysokim stopniem ryzyka. W rachunkowości i w zarządzaniu zakładem ubezpieczeń bardzo ważną rolę odgrywają rezerwy techniczno-ubezpieczeniowe. Są tworzone obligatoryjnie i przeznaczone na pokrycie bieżących i przyszłych zobowiązań, wynikających z zawartych umów ubezpieczeniowych, których wysokość i dokładny czas występowania nie jest znany. Zajmują ważne miejsce w pasywach zakładu ubezpieczeń. Metody i zasady naliczania rezerw techniczno-ubezpieczeniowych ze względu na ich znaczenie i tworzenie istotnej pozycji pasywów w bilansach zakładów ubezpieczeń, powinny być w sposób dokładny, staranny i jednoznaczny zdefiniowane w zakładowych planach kont ubezpieczycieli.

Celem artykułu jest udowodnienie tezy, że rezerwy te są warunkiem stabilnego funkcjonowania zakładów ubezpieczeń. Na potrzeby pracy sformułowano następujące problemy badawcze:

- Czym są rezerwy techniczno-ubezpieczeniowe?
- Jakie są rodzaje rezerw techniczno-ubezpieczeniowych?
- Jakie są metody tworzenia rezerw techniczno-ubezpieczeniowych?
- Jakie miejsce w pasywach zajmują rezerwy techniczno-ubezpieczeniowe oraz jak ważną pozycję stanowią w pasywach ogółem?

Treść tekstu została podzielona w sposób umożliwiający udzielenie odpowiedzi na powyższe pytania. Najpierw została przedstawiona charakterystyka rezerw techniczno-

* Koło Naukowe Ubezpieczeń „Risk Management”, Katedra Zarządzania Ryzykiem i Ubezpieczeń, Uniwersytet Ekonomiczny w Krakowie.

ubezpieczeniowych, a następnie rodzaje i metody ich tworzenia. W ostatniej części przedstawiono ich miejsce i udział w pasywach ogółem.

1.2. Pojęcie rezerw techniczno-ubezpieczeniowych

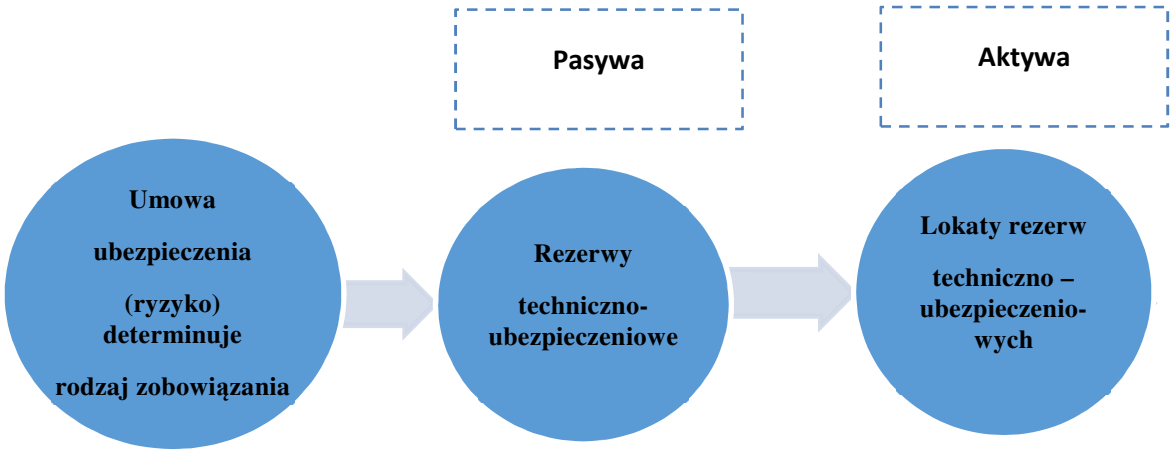
Na podstawie Dyrektywy Rady Europejskiej z dnia 17 maja 2006 r. w sprawie rocznych i skonsolidowanych sprawozdań finansowych zakładów ubezpieczeń oraz Rozporządzenia Ministra Finansów z dnia 12 kwietnia 2016 r. w sprawie szczególnych zasad rachunkowości zakładów ubezpieczeń i zakładów reasekuracji, rezerwy techniczno-ubezpieczeniowe powinny zapewnić pełne pokrycie wszelkich bieżących i przyszłych zobowiązań, jakie mogą wyniknąć z zawartych umów ubezpieczenia.

Zakłady ubezpieczeń majątkowych i na życie dla zapewnienia swojej płynności finansowej oraz wypłacalności muszą tworzyć odpowiednie rezerwy techniczno-ubezpieczeniowe. Są one wyrazem zabezpieczania się ubezpieczyciela przed ujemnymi skutkami wysokiego ryzyka gospodarczego, a w szczególności poniesienia nieprzewidywalnych strat w przyszłości, a także przejawem szczególnej ,,ostrożności" w prowadzonej przez zakład ubezpieczeniowy polityce finansowej[1].

Konieczność tworzenia rezerw wypływa z podstawowej zasady gospodarki finansowej zakładu ubezpieczeń, czyli współmierności przychodów i kosztów z danego okresu ubezpieczeniowego do okresu sprawozdawczego. Motywem tworzenia rezerw techniczno-ubezpieczeniowych jest fakt powstania zobowiązania zakładu ubezpieczeniowego wobec ubezpieczonego. Charakter oraz rodzaj tworzonych rezerw są determinowane przez ryzyko wynikające z umowy ubezpieczenia. Znajduje to odzwierciedlenie w aktywach i pasywach zakładu ubezpieczeń. Rezerwy, które są składnikiem kapitałów obcych, mają charakter ewidencyjny, a ich fizycznym obrazem są lokaty (rys. 1.1)[2].

[1] E. Spigarska, *Rezerwy techniczno-ubezpieczeniowe jako podstawa wypłacalności i stabilności finansowej zakładów ubezpieczeń*, „Prace i Materiały Wydziału Zarządzania Uniwersytetu Gdańskiego" 2009 nr 3/1, Gdańsk 2009, s. 362.

[2] K.. Rybicka, *Rezerwy w rachunkowości zakładu ubezpieczeń,* „Zeszyty Naukowe Uniwersytetu Szczecińskiego" nr 765, „Finanse, Rynki Finansowe, Ubezpieczenia" nr 61 (2013), Szczecin 2013, s. 195.



Rysunek 1.1. Tworzenie rezerw techniczno-ubezpieczeniowych
Źródło: opracowanie własne

1.3. Rodzaje rezerw techniczno-ubezpieczeniowych

Rezerwy techniczno-ubezpieczeniowe stanowią środki przeznaczone na pokrycie bieżących i przyszłych zobowiązań wynikających z zawartych umów ubezpieczenia, umów gwarancji ubezpieczeniowych lub umów reasekuracji[3]. Do celów rachunkowości wyróżnia się następujące rodzaje rezerw:

1. rezerwę składek,
2. rezerwę na ryzyka niewygasłe,
3. rezerwę na niewypłacone odszkodowania i świadczenia, w tym rezerwę na skapitalizowaną wartość rent,
4. rezerwę na wyrównanie szkodowości,
5. rezerwę ubezpieczeń na życie,
6. rezerwę ubezpieczeń na życie, gdy ryzyko lokaty ponosi ubezpieczający,
7. rezerwę na premie i rabaty dla ubezpieczonych,
8. rezerwę na zwrot składek dla członków tuw,

[3] Art. 227 pkt 1 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej.

9. inne rezerwy techniczno-ubezpieczeniowe określone w statucie.

Rezerwę składek tworzy się jako składkę przypisaną przypadającą na przyszłe okresy sprawozdawcze, proporcjonalnie do okresu, na jaki składka jest przypisana lub w relacji do stopnia ryzyka przewidzianego w następnych okresach sprawozdawczych.

Rezerwa na ryzyka niewygasłe jest uzupełnieniem rezerwy składek. Tworzona jest, gdy zakład ubezpieczeń przewiduje, że rezerwa składek nie pokryje zobowiązań w okresie przyszłym.

Rezerwa na niewypłacone odszkodowania i świadczenia jest tworzona w wysokości ustalonej lub przewidywanej wielkości wypłat odszkodowań i świadczeń związanych ze szkodami, zaistniałymi do dnia ustalenia rezerwy, powiększonej o koszty likwidacji szkód. W przypadku ubezpieczeń na życie jest to kwota należna ubezpieczonym, uprawnionym lub uposażonym, powiększona o koszty związane z wypłatą świadczeń.

Rezerwa na wyrównanie szkodowości jest tworzona w wysokości mającej zapewnić wyrównanie wahań współczynnika szkodowości w przyszłości. Współczynnik szkodowości to stosunek odszkodowań i świadczeń, z uwzględnieniem zmiany stanu rezerw na niewypłacone odszkodowania i świadczenia, do składki zarobionej. Przy kalkulacji wskaźnika uwzględnia się koszty likwidacji szkód i windykacji regresów oraz regresy i odzyski otrzymane. Rezerwa ta tworzona jest dla każdej grupy ubezpieczeń osobno.

Rezerwa ubezpieczeń na życie jest kalkulowana przy uwzględnieniu wszystkich zobowiązań wynikających z zawartych umów ubezpieczenia oraz kosztów obsługi umów i kosztów związanych z wypłatą odszkodowań i świadczeń. Przy jej tworzeniu uwzględnia się przyszłe wpływy z tytułu składek należnych zgodnie z zawartymi umowami ubezpieczenia.

Rezerwa ubezpieczeń na życie, jeżeli ryzyko lokaty ponosi ubezpieczający tworzona jest w wysokości wartości lokaty. Nie stanowi własności zakładu ubezpieczeń, lecz ubezpieczonych, gdyż są to ich oszczędności.

Rezerwa na premie i rabaty dla ubezpieczonych jest tworzona w wysokości kwot, o które powiększane są przyszłe świadczenia lub pomniejszane przyszłe składki.

Rezerwę na zwrot składek dla członków towarzystwa ubezpieczeń wzajemnych tworzy się do wysokości osiągniętego dodatniego wyniku technicznego, o ile obowiązek zwrotu składek

wynika z umowy ubezpieczenia. Tworzy się ją w podziale na grupy ubezpieczeń dla każdego roku zawarcia umów ubezpieczenia odrębnie[4].

Strukturę rezerw wszystkich zakładów ubezpieczeń w Polsce na dzień 31.12.17 r. przedstawia tabela 1.1.

Tabela 1.1. Struktura rezerw techniczno-ubezpieczeniowych brutto działu I i II w IV kwartale 2017 roku

Rezerwy techniczno-ubezpieczeniowe	Udział procentowy
Rezerwa składek i rezerwa na pokrycie ryzyka niewygasłego	17,40%
Rezerwa ubezpieczeń na życie	17,52%
Rezerwy na nie wypłacone odszkodowania i świadczenia	24,45%
Rezerwy na premie i rabaty dla ubezpieczonych	0,12%
Rezerwy na wyrównanie szkodowości (ryzyka)	0,80%
Rezerwy na zwrot składek dla członków	0,00%
Pozostałe rezerwy techniczno - ubezpieczeniowe określone w statucie	0,23%
Rezerwa ubezpieczeń na życie, gdy ryzyko lokaty (inwestycyjne) ponosi ubezpieczający	39,48%

Źródło: Opracowanie własne na podstawie skonsolidowanych raportów KNF z IV kwartału 2017 roku

Z powyższej tabeli wynika, iż dominującą pozycję zajmowały rezerwy ubezpieczeń na życie, gdy ryzyko lokaty ponosi ubezpieczający oraz rezerwy ubezpieczeń na życie wynoszące odpowiednio 39,48% i 17,52%. Wynika to stąd, iż w odróżnieniu do pozostałych rezerw, ryzyko na które tworzone są rezerwy ubezpieczeń na życie jest największe (śmierć jest pewna).

1.4. Metody tworzenia rezerw techniczno-ubezpieczeniowych

Rezerwy techniczno-ubezpieczeniowe są ustalane w drodze oszacowań, a na ich wysokość mają w szczególności wpływ: kwoty szkód lub odszkodowań, koszty sporów z klientami, koszty do zwrotu ubezpieczającemu oraz inne koszty związane z roszczeniami ubezpieczonych[5].

[4] B. Putelbergier, *Rezerwy techniczno-ubezpieczeniowe*, „Gazeta Ubezpieczeniowa", 24 stycznia 2006, (http://www.gu.com.pl/index.php?option=com_content&view=article&id=12184&catid=122&Itemid=153), dostęp: 8.03.2018 r.

[5] W. Gos, S. Hońko, *Branżowe problemy rachunkowości i podatków*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" nr 373, Wrocław 2014, s. 46.

Rezerwy techniczno-ubezpieczeniowe powinny być ustalane w wielkości zapewniającej pełne pokrycie wszelkich bieżących i przyszłych zobowiązań zakładu ubezpieczeń, jakie mogą wyniknąć z zawartych umów ubezpieczenia. Zatem ogromnego znaczenia nabiera poprawność oszacowania przez zakład ubezpieczeń ich wysokości.

Metody i zasady naliczania rezerw techniczno-ubezpieczeniowych, ze względu na ich znaczenie i tworzenie znaczącej pozycji pasywów w bilansach zakładów ubezpieczeń oraz długoterminowość zawieranych umów ubezpieczeniowych, powinny być w sposób dokładny, szczegółowy, jasny i jednoznaczny zdefiniowane w zakładowych planach kont ubezpieczycieli. Zgodnie z zasadą ciągłości bilansowej, metody i zasady tworzenia rezerw nie mogą być zmieniane w ciągu roku obrotowego. Ewentualne zmiany mogą być dokonane dopiero począwszy od pierwszego dnia następnego roku obrotowego i opisane w informacji dodatkowej z podaniem wpływu zmian na wynik finansowy ubezpieczyciela. Metody tworzenia rezerw techniczno-ubezpieczeniowych wynikają z Rozporządzenia w sprawie szczególnych zasad rachunkowości zakładów ubezpieczeń[6] i są to:

- metoda indywidualna,
- metoda ryczałtowa,
- metoda aktuarialna.

Metoda indywidualna polega na ocenie lub oszacowaniu pojedynczej szkody lub wypadku zgłoszonych zakładowi ubezpieczeń i przez niego zarejestrowanych oraz ustalaniu odrębnie dla każdej umowy ubezpieczenia lub każdej szkody dokładnej wielkości rezerwy, a w przypadku niemożności ustalenia dokładnej wielkości rezerwy – zastosowanie jej wiarygodnego oszacowania.

Metoda ryczałtowa polega na ustaleniu rezerwy zbiorczo dla całego portfela ubezpieczeń lub jego części, jako procentu składki lub wartości wypłaconych odszkodowań i świadczeń. Metoda ta może być stosowana tylko wtedy, jeżeli uzyskane przy jej użyciu wyniki będą zbliżone do wyników uzyskanych przy użyciu metody indywidualnej. Wskaźnik ryczałtowy

[6] Rozporządzenie Ministra Finansów z dnia 12 kwietnia 2016 r. w sprawie szczególnych zasad rachunkowości zakładów ubezpieczeń i zakładów reasekuracji (Dz.U. 2016 poz.562).

powinien być ustalany przy zachowaniu zasady ciągłości, a nieuzasadnione zmiany wielkości wskaźnika są niedopuszczalne.

Metoda aktuarialna polega na ustaleniu rezerwy z zastosowaniem metod matematyki ubezpieczeniowej, finansowej i statystyki.

Odrębne zasady stosuje się przy obliczaniu wielkości rezerwy na wyrównanie szkodowości. W przypadku ubezpieczeń bezpośrednich dla grup ubezpieczeń działu II, z wyjątkiem grupy 14 (ubezpieczenie kredytu), rezerwę tworzy się w takiej wysokości, aby przy zmianie stanu rezerwy współczynnik szkodowości dla danego roku obrotowego był równy średniej ważonej ze współczynników szkodowości w danej grupie ubezpieczeń z ostatnich 5 lat obrotowych, obliczonych bez uwzględnienia zmian rezerwy na wyrównanie szkodowości (ryzyka). W przypadku, gdy zakład ubezpieczeń prowadzi działalność krócej niż 6 lat, dla danej grupy ubezpieczeń nie tworzy się rezerwy na wyrównanie szkodowości (ryzyka). Dla grupy 14 działu II stosuje się ''metodę nr 1'', ''metodę nr 2'' oraz metodę aktuarialną, o których mowa w załączniku nr 7 do rozporządzenia.[7]

Konieczność szczegółowego określenia metod tworzenia rezerw techniczno-ubezpieczeniowych, a tym samym określenia ich wysokości, spowodowana jest tym, że poziom tych rezerw i rzetelność w przestrzeganiu procedur związanych z ich tworzeniem odgrywają kluczową rolę w mechanizmie ekonomicznym, mającym zagwarantować pełną wiarygodność finansową zakładów ubezpieczeń, bowiem zastosowanie określonej metody naliczenia rezerw uzależnione jest od rodzaju rezerw techniczno-ubezpieczeniowych jakie tworzą zakłady ubezpieczeń[8].

1.5. Miejsce rezerw techniczno-ubezpieczeniowych w pasywach bilansu zakładów ubezpieczeń

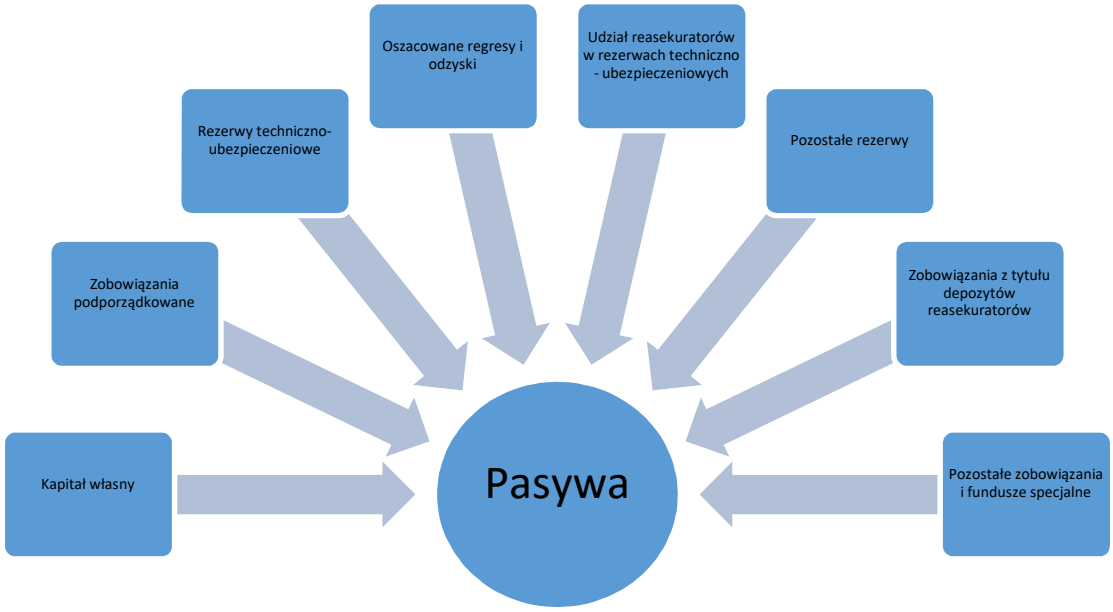
Pasywa zakładów ubezpieczeń i zakładów reasekuracji odzwierciedlają pochodzenie środków finansowych, które jako aktywa lokowane są w różne instrumenty finansowe. Są źródłami finansowania majątku przedsiębiorstw ubezpieczeniowych i dzielą się na kapitały

[7]Rozporządzenie Ministra Finansów z dnia 12 kwietnia 2016 r. w sprawie szczególnych zasad rachunkowości zakładów ubezpieczeń i zakładów reasekuracji (Dz.U. 2016 poz.562).
[8]E. Radawiecka, *Rezerwy techniczno-ubezpieczeniowe warunkiem stabilności funkcjonowania zakładów ubezpieczeń*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" nr 765, Szczecin 2013, s.172.

własne, które przysługują akcjonariuszom lub członkom towarzystw ubezpieczeń oraz kapitały obce, które przysługują wierzycielom.

Kapitały własne odgrywają bardzo ważną rolę w zarządzaniu finansami przedsiębiorstwa ubezpieczeniowego. Stanowią główne źródło w budowie pewności jego działania, a w konsekwencji możliwości rozwojowych.

Najważniejszą pozycją kapitałów obcych zakładów ubezpieczeń i zakładów reasekuracji są rezerwy techniczno-ubezpieczeniowe. Są specyficzne i znajdują odzwierciedlenie tylko w sprawozdaniu finansowym zakładów ubezpieczeń i zakładu reasekuracji[9]. Ich miejsce w bilansie prezentuje rysunek 1.2.



Rysunek 1.2. Miejsce rezerw techniczno-ubezpieczeniowych w pasywach bilansu zakładu ubezpieczeń
Źródło: opracowanie własne

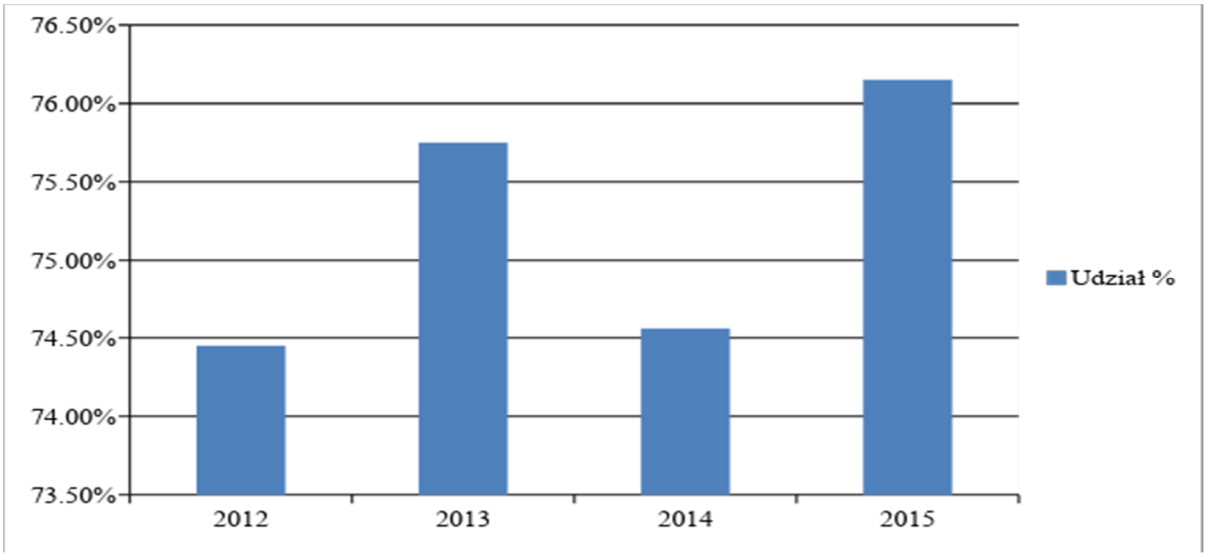
Powyższy rysunek prezentuje wszystkie pozycje pasywów bilansu zakładów ubezpieczeń. Jedną z nich są charakterystyczne rezerwy techniczno-ubezpieczeniowe. Dokładną strukturę pasywów przedstawia poniższa tabela oraz wykres, na którym wyraźnie przedstawiono udział poszczególnych pozycji w pasywach ogółem.

[9] E. Radawiecka, *Porównanie bilansu zakładów ubezpieczeń i zakładów reasekuracji do bilansu innych jednostek*, „Zeszyty Naukowe Wydziału Nauk Ekonomicznych" nr 17, Koszalin 2013, s. 217.

Tabela 1.2. Struktura pasywów zakładów ubezpieczeń działu I i II w 2015 r.

Wyszczególnienie	Stan w dniu (w tys. zł)		Udział % w pasywach	
	01.01.2015	31.12.2015	1.01.2015	31.12.2015
A.Kapitał własny	34 537 669	34 076 423	19,38%	18,90%
B. Zobowiązania podporządkowane	176 864	431 124	0,10%	0,24%
C. Rezerwy techniczno- ubezpieczeniowe	133 016 744	137 173 337	74,66%	76,09%
D. Udział reasekuratorów w rezerwach techniczo-ubezpieczeniowych (wielkość ujemna)	7 200 449	9 753 829	4,04%	5,41%
E. Oszacowane regresy i odzyski (wielkość ujemna)	371 131	347 111	0,21%	0,19%
F. Pozostałe rezerwy	2 547 537	2 324 964	1,43%	1,29%
G. Zobowiązania z tytułu depozytów reasekuratorów	1 539 952	1 407 143	0,86%	0,78%
H. Pozostałe zobowiązania i fundusze specjalne	11 739 306	11 939 875	6,59%	6,62%
I.Rozliczenia międzyokresowe	2 187 305	3 025 821	1,23%	1,68%
Pasywa razem	**178 173 796**	**180 277 747**	**100,00%**	**100,00%**

Źródło: Opracowanie własne na podstawie raportów finansowych KNF z 2015 roku



Rysunek 1.3. Udział rezerw techniczno-ubezpieczeniowych w pasywach zakładów ubezpieczeń działu I i II w latach

Źródło: Opracowanie własne na podstawie raportów KNF

Z przedstawionych danych wynika, że rezerwy techniczno-ubezpieczeniowe stanowią główną pozycję pasywów zakładów ubezpieczeń. Udział rezerw techniczno-ubezpieczeniowych w ogólnej sumie bilansowej oscyluje w granicach 75% na przełomie lat 2012–2015. Oznacza to, że znacząca część majątku (aktywów) zakładów ubezpieczeń ma pokrycie w kapitałach obcych. Świadczy to również o dużym znaczeniu rezerw techniczno-ubezpieczeniowych.

1.6. Zakończenie

Zakład ubezpieczeń, tak jak każde inne przedsiębiorstwo, w związku z prowadzoną przez siebie działalnością, narażony jest na różne rodzaje ryzyka mogące zagrozić jego egzystencji i doprowadzić do bankructwa. Jednak obok tych rodzajów ryzyka, które są typowe dla wszystkich instytucji (m.in. ryzyka inwestycyjnego, dopasowania aktywów i pasywów czy ryzyka ogólnego, takiego jak np. złe zarządzanie), w działalności zakładów ubezpieczeń występują rodzaje ryzyka właściwe tylko dla ubezpieczycieli. Szczególnie istotne spośród nich jest ryzyko związane z szacowaniem bieżących i przyszłych zobowiązań, jakie mogą wyniknąć z zawartych umów ubezpieczenia, czyli rezerw techniczno-ubezpieczeniowych, a głównie rezerw na niewypłacone odszkodowania i świadczenia.

Ryzyko dla zakładu ubezpieczeń generowane jest przede wszystkim przez niedoszacowanie rezerw. Niedostateczne oszacowanie wartości rezerw technicznych może spowodować, że zakład ubezpieczeń nie będzie w stanie realizować wszystkich swoich zobowiązań wynikających z umów ubezpieczenia lub będzie musiał realizować je z dodatkowych środków. Zawyżenie rezerw może wydawać się pozytywne z punktu widzenia wypłacalności, lecz może wywołać interwencję ze strony urzędów skarbowych w celu ujawnienia i opodatkowania rzeczywistych dochodów zakładu ubezpieczeń (zawyżone rezerwy powodują bowiem zmniejszenie wyniku technicznego zakładu ubezpieczeń).

Podsumowując, rezerwy techniczno-ubezpieczeniowe są warunkiem stabilnego funkcjonowania zakładów ubezpieczeń. Świadomość ich roli ma potwierdzenie choćby w udziale rezerw w pasywach ogółem, gdzie rezerwy stanowią ok. 75%.

Rozdział 2.
Ubezpieczenie kredytu kupieckiego a ryzyko niewypłacalności kontrahentów w Polsce

Aleksandra Bazan*

2.1. Wprowadzenie

Funkcjonujące w obecnych czasach przedsiębiorstwa napotykają na coraz silniejszą konkurencję. Jednym ze sposobów radzenia sobie z konkurencją jest liberalizacja warunków dostaw, której konsekwencją jest wydłużenie terminów płatności oraz okresu ściągania należności. Wynika to ze sposobu i warunków płatności w transakcjach handlowych[10]. Stosowanie odroczonego terminu płatności, w momencie gdy pojawia się problem niewypłacalności, stanowi zagrożenie płynności finansowej, zwłaszcza dla małych i średnich przedsiębiorstw, które mają niski poziom kapitału własnego, małe rezerwy finansowe oraz ograniczony dostęp do zewnętrznych źródeł finansowania.

Kredyt kupiecki jest wykorzystywany w relacjach handlowych zarówno między przedsiębiorstwami krajowymi, jak i w transakcjach zagranicznych. Jego idea polega na odroczeniu zapłaty za towar bądź usługę. Jest alternatywą wobec kredytu bankowego i stanowi pozabankową formę finansowania działalności gospodarczej. Dla dostawcy jest elementem strategii sprzedaży, a dla odbiorcy źródłem zewnętrznego finansowania[11].

Powszechność wykorzystywania kredytu kupieckiego w obrocie gospodarczym stwarza niebezpieczeństwo powstawania należności przeterminowanych lub nieściągalnych. Realizacja ryzyka związanego z udzielaniem kredytu kupieckiego wpływa na wyniki finansowe

* Koło Naukowe Ubezpieczeń „Risk Management", Katedra Zarządzania Ryzykiem i Ubezpieczeń, Uniwersytet Ekonomiczny w Krakowie.

[10] R. Dankiewicz, *Ubezpieczenia kredytu kupieckiego w procesie zarządzania ryzykiem utraty należności w okresach wahań koniunktury w gospodarce,* „Zarządzanie i finanse", 2012, Nr 4, s. 7.

[11] E. Wierzbicka, *Ubezpieczenie jako ekonomiczny instrument zarządzania należnościami małych i średnich przedsiębiorstw,* „Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne", 2015, Nr 5, s. 11.

danego przedsiębiorstwa. Niezapłacone lub nieterminowo zapłacone wierzytelności mogą zachwiać płynnością, a nawet doprowadzić do bankructwa. Dlatego ryzyko związane z należnościami handlowymi można ubezpieczyć i przenieść na ubezpieczyciela. W związku z tym problem badawczy niniejszej pracy można przedstawić w postaci następujących pytań: *Jakie są cechy charakterystyczne ubezpieczenia kredytu kupieckiego? Czy w obecnej sytuacji na rynku warto nabyć ten produkt? Jak kształtuje się terminowość płatności w Polsce? Czym spowodowana jest rosnąca niewypłacalność firm w Polsce?* W kontekście tak sformułowanego problemu badawczego, za główne cele badawcze przyjęto charakterystykę elementów składowych ubezpieczeń kredytu kupieckiego oraz analizę rynku w Polsce pod kątem zapotrzebowania na ten produkt. Do realizacji tych celów wykorzystano dostępną literaturę przedmiotu, aktualne oferty ubezpieczeń kredytu kupieckiego w Polsce oraz raporty przygotowane przez międzynarodowe zakłady ubezpieczeń dotyczące terminowości płatności oraz niewypłacalności przedsiębiorstw na polskim rynku.

2.2. Istota ubezpieczenia kredytu kupieckiego

Ubezpieczenie kredytu kupieckiego[12] jest formą zabezpieczenia przedsiębiorstwa przed ryzykiem braku zapłaty ze strony kontrahenta. Jego podstawową funkcją jest łagodzenie negatywnych skutków zdarzeń losowych i przywrócenie, bądź utrzymanie, dotychczasowej pozycji ekonomicznej w przedsiębiorstwie[13]. Nieopłacone należności mogą skutkować utratą płynności finansowej i prowadzić do pogorszenia rentowności przedsiębiorstwa. Aby tego uniknąć wymagane jest posiadanie aktualnej i pełnej wiedzy o podmiotach działających na danym rynku, o danej branży, oraz o tym jak zmienia się gospodarka. Ubezpieczenie to nie tylko umożliwia wyrównanie ewentualnych strat wynikłych z utraty należności, ale przede wszystkim minimalizuje ryzyko ich powstania. Ubezpieczyciel pomaga ocenić i monitorować wiarygodność finansową partnerów biznesowych ubezpieczającego[14]. Zakład ubezpieczeń gromadzi informacje na temat kontrahentów oraz podmiotów gospodarczych z różnych

[12] Ubezpieczenie kredytu kupieckiego funkcjonuje również pod nazwami: ubezpieczenie kredytu handlowego oraz ubezpieczenie należności.
[13] J. Lisowski, *Specyfika gospodarki finansowej ubezpieczycieli kredytu kupieckiego w Polsce,* Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010, s. 129.
[14] E. Wierzbicka, *op. cit*., s. 16.

źródeł, między innymi: korzystając z dostępnych archiwów, historii płatniczej kontrahenta, raportów finansowych czy informacji uzyskanych od wszystkich ubezpieczających, którzy sprzedają swoje towary i usługi tym samym klientom, a także odwiedzając tych klientów. Dane te są cały czas aktualizowane oraz weryfikowane w dostępnych źródłach. Jeżeli okazuje się, że jeden z partnerów ma trudności finansowe, ubezpieczyciel powiadamia ubezpieczającego o podwyższonym ryzyku oraz pomaga ustalić plan działania, który zmniejszy lub wykluczy straty.

Dzięki zawarciu polisy ubezpieczenia należności, przedsiębiorca może zaoferować swoim kontrahentom lepsze warunki współpracy, np. poprzez wydłużenie kredytu kupieckiego. Dodatkowo ma on możliwość bieżącej kontroli i monitorowania ryzyka dzięki ocenie wiarygodności odbiorców oraz ulepszeniu wewnętrznych procedur zarządzania ryzykiem. Utrzymanie płynności finansowej jest możliwe nie tylko dzięki odszkodowaniu, lecz również poprzez bieżące dochodzenie przeterminowanych należności przez zakład ubezpieczeń. Przedsiębiorca dzięki ubezpieczeniu należności może zrezygnować z tworzenia rezerw na należności przeterminowane. W sytuacji wystąpienia szkody ubezpieczenie umożliwia skorzystanie z pomocy windykacyjnej oraz wypłatę odszkodowania również w walucie kontraktu eksportowego[15].

Do głównych zalet ubezpieczenia kredytu kupieckiego można zatem zaliczyć:

- bezpieczniejsze zarządzanie finansami firmy, co umożliwia ich stabilny rozwój[16],
- transfer ryzyka na ubezpieczyciela,
- minimalizacja ryzyka nieotrzymania zapłaty za wysłany towar lub wykonanie usługi,
- minimalizacja ryzyka wystąpienia złych długów,
- więcej kapitału obrotowego dzięki rezygnacji z innych zabezpieczeń, takich jak gwarancja bankowa czy akredytywa,
- ochrona przed stratami, które mogą zagrozić płynności przedsiębiorstw i doprowadzić do upadłości,
- dodatkowe korzyści dostarczane przez ubezpieczyciela o charakterze komplementarnym, takie jak: weryfikacja wiarygodności kontrahentów, pomoc

[15] *Ibidem*, s.17.

[16] A. Szewczuk*, Ubezpieczenie należności jako efektywny instrument zarządzania ryzykiem handlowym w warunkach kryzysu finansowego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2010, Nr 43, s.336.

prawna oraz doradcza w zakresie formułowania kontraktów i przyjmowanych zabezpieczeń, monitoring płatności, a także, gdy zajdzie taka potrzeba, uzyskanie pomocy w windykacji,

- większa wiarygodność przedsiębiorstwa jako partnera gospodarczego, a także klienta banku[17],
- większa konkurencyjność poprzez oferowanie kontrahentom lepszych warunków płatności,
- dostęp do informacji o sytuacji finansowej kredytobiorcy[18].

2.3. Cechy specyficzne ubezpieczenia kredytu kupieckiego

Ubezpieczenie kredytu kupieckiego jest produktem ubezpieczeniowym należącym do grupy 14 działu II, obejmującej swym zakresem ubezpieczenia kredytu. Przedmiotem ubezpieczenia w ubezpieczeniach kredytu są przysługujące kredytodawcy bezsporne należności z tytułu zawartych umów, które nie zostały zapłacone w określonym terminie lub w określonej kwocie[19]. Interes ubezpieczeniowy wierzyciela wiąże się z ochroną majątku przed ryzykiem niesolidności płatniczej kredytobiorcy, przejawiającej się opóźnieniem lub też brakiem zapłaty należności[20]. Można wyróżnić dwie strony umowy ubezpieczenia, to znaczy ubezpieczyciela oraz ubezpieczającego, którym jest zawsze dostawca[21]. Ubezpieczyciel zobowiązany jest do pokrywania strat ubezpieczającego wynikających z nieotrzymania przez niego zapłaty za sprzedaż towarów i usług, natomiast ubezpieczający zobowiązuje się do przestrzegania warunków umowy ubezpieczyciela, w tym przede wszystkim do terminowego regulowania składki ubezpieczeniowej. Produkt ten przeznaczony jest dla przedsiębiorstw, które realizują sprzedaż krajową i/lub eksportową w kredycie kupieckim. Przedmiotem ubezpieczenia są wierzytelności wynikające z faktur należne ubezpieczającemu od kontrahentów za sprzedaż towarów i usług z odroczonym terminem płatności, dla których

[17] *E. Wierzbicka, op. cit., s.* 19.
[18] R. Jagoda, *Koszty i korzyści a ryzyko ubezpieczenia należności*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 2015, Nr 398, s.173.
[19] *Współczesne ubezpieczenia gospodarcze*, pod red. W. Sułkowskiej, Wyd. Uniwersytetu Ekonomicznego w Krakowie, Kraków 2013, s. 165.
[20] *Ubezpieczenia*, pod red. M. Iwanicz-Drozdowskiej, Polskie Wydawnictwo Ekonomiczne, Warszawa 2013, s. 370.
[21] J. Kufel, *Ubezpieczenia gospodarcze w orzecznictwie sądowym,* Wydawnictwo Branta, Bydgoszcz 2002, s. 242.

ubezpieczyciel ustalił limity kredytowe. Ochroną ubezpieczeniową, do wysokości uzgodnionej w umowie ubezpieczenia, objęte są te wierzytelności, które są bezsporne oraz nie podlegają wyłączeniom lub ograniczeniom[22].

Ubezpieczyciel przydziela specjalny limit kredytowy kontrahentom, z którymi wymiana handlowa objęta jest ubezpieczeniem. Limit ten stanowi górną granicę, do której ubezpieczyciel wypłaci ubezpieczonemu odszkodowanie, w przypadku zajścia szkody. Limit określany jest w wyniku procesu weryfikacji kontrahenta, podczas którego zakład ubezpieczeń analizuje jego zdolność kredytową oraz stabilność finansową. Na proces ten składają się elementy związane z oceną kredytodawcy, kredytobiorcy, branży, w której podmioty prowadzą działalność oraz w przypadku transakcji zagranicznych – oceną kraju odbiorcy. Od uzyskanej oceny zależy wysokość przyznanego limitu. Ubezpieczający może wnioskować o przyznanie limitu kredytowego klientowi, z którym dopiero zamierza rozpocząć współpracę, jak i o podwyższenie limitu dla klienta, z którym łączą go już stosunki handlowe. Ponieważ w zakresie odpowiedzialności zakładu ubezpieczeń leży ciągłe i aktywne monitorowanie każdego z ubezpieczonych klientów, w razie potrzeby oceni on ryzyko związane z podniesieniem limitu kredytowego. Czas limitu może być określony, poprzez wskazanie konkretnego okresu jego obowiązywania, jak również nieokreślony.

Warunki umowy ubezpieczenia umożliwiają ubezpieczycielowi obniżenie lub anulowanie wcześniej przyznanego limitu. Przyczynami takiego postępowania mogą być:

- całkowite lub częściowe zaprzestanie działalności dłużnika lub zmiana jej profilu,
- istotne zmiany prawne, własnościowe bądź związane z pełnionym zarządem,
- pogorszenie się sytuacji finansowej dłużnika lub podmiotów z nim powiązanych, co stanowi odzwierciedlenie w jego sprawozdaniach finansowych,
- trudności w ocenie sytuacji finansowej dłużnika w związku z nieprzekazywaniem przez niego na czas sprawozdań finansowych,
- zgłoszenie przez dłużnika lub podmioty z nim powiązane wniosku o przeprowadzenie postępowania upadłościowego, układowego lub naprawczego,

[22] A. Becella, *Kierunki rozwoju ubezpieczenia kredytu kupieckiego w Polsce*, „Studia Oeconomica Posnaniensia" 2015, vol. 3, nr 2, s. 96.

- pogorszenie moralności płatniczej dłużnika skutkujące powstałymi opóźnieniami płatniczymi względem kontrahentów,
- pozyskanie przez ubezpieczyciela innych informacji wpływających na decyzję o redukcji limitu,
- decyzje ubezpieczyciela względem kraju, w którym podmiot rezyduje, będące konsekwencją pogarszającej się sytuacji ekonomicznej lub politycznej,
- niedopełnienie przez ubezpieczającego warunków formalnych dotyczących sprawozdawczości jego współpracy z dłużnikiem[23].

Na podstawie zaprezentowanych czynników, można zauważyć, że zakład ubezpieczeń posiada szeroki wachlarz możliwości zmniejszenia ekspozycji ryzyka. Polityka regulowania poziomu limitów przez zakład ubezpieczeń musi być prowadzona starannie, opierając się na zgromadzonych danych oraz przeprowadzonych analizach, ponieważ redukcja lub anulowanie limitu może wywołać negatywne skutki w gospodarce finansowej kredytodawcy[24].

Wypłata odszkodowania następuje po zajściu wypadku ubezpieczeniowego oraz zgłoszeniu szkody. Wysokość szkody oblicza się poprzez pomniejszenie należnej od dłużnika kwoty płatności na dzień zajścia szkody o płatności, korekty, potrącenia, roszczenia wzajemne, dochody z realizacji zabezpieczeń, dochody uzyskane z odzyskanych towarów itp[25]. Schemat obliczania wysokości szkody i należnego odszkodowania zazwyczaj przebiega etapowo i może wyglądać w ten sposób:

- wstępne ustalenie wysokości należności objętych ubezpieczeniem z uwzględnieniem przyznanych limitów ubezpieczeniowych,
- ustalenie, jaka część należności jest rzeczywiście niespłacona (uwzględnia się wszelkie kwoty odzyskane, jak i ewentualne kompensaty),
- ustalenie wartości szkody, na którą składać się mogą niespłacone należności oraz poniesione przez kredytodawcę koszty akceptowalne przez ubezpieczyciela,
- ustalenie wysokości szkody po uwzględnieniu korekt wynikających z udziału własnego oraz zastosowanych klauzul podziału ryzyka (np. franszyzy redukcyjnej),

[23] *Ibidem*, s.99.
[24] J. Kukiełka, *Ubezpieczenie kredytu*, Centrum Edukacji i Rozwoju Biznesu Olympus, Warszawa 1994, s. 71.
[25] *Ubezpieczenia*, pod red. W. Ronki-Chmielowiec, Wyd. C.H.Beck, Warszawa 2016, s. 389.

- wypłata odszkodowania, którego wysokość w przypadku należności eksportowych może być różna, w zależności od przyjętego sposobu wyznaczania kursu waluty, według którego ma nastąpić wypłata odszkodowania[26].

Po wypłacie odszkodowania zakład ubezpieczeń wymaga scedowania na siebie wszystkich posiadanych od danego kontrahenta zabezpieczeń, nawet jeżeli nie były one wcześniej wymagane. Na ubezpieczyciela przechodzi prawo dochodzenia zwrotu niezapłaconej należności do wysokości wypłaconego odszkodowania[27]. Tak zwane prawo regresu powstaje dla zakładu ubezpieczeń *ex lege*. Musi mieć ono charakter odszkodowania za szkodę i stanowić zwrot tego, co ubezpieczyciel faktycznie pokrył. Na postępowanie regresowe składają się takie elementy jak: przejście prawa, odzyskiwanie długów oraz podział kwot odzyskanych i kosztów odzyskania[28]. Ubezpieczający bez zgody zakładu nie może zrzec się swego roszczenia w stosunku do sprawcy szkody[29].

Treść umowy ubezpieczenia kredytu kupieckiego określa również warunki powstania odpowiedzialności odszkodowawczej. Wypadkiem ubezpieczeniowym może być prawnie stwierdzona trwała niewypłacalność kredytobiorcy lub jego domniemana niewypłacalność.

Domniemana niewypłacalność rozumiana jest jako zachwianie płynności kredytobiorcy, skutkujące przewlekłą zwłoką w spłacie należności. W zależności od zakładu ubezpieczeń oraz kraju, w obrębie którego prowadzi działalność, pojęcie przewlekła zwłoka może być różnie definiowane[30].

Trwała niewypłacalność występuje, gdy jest ona potwierdzona zgodnie z przepisami prawa. Według polskiego prawa potwierdzeniem niewypłacalności przedsiębiorstwa najczęściej jest:

- sądowe ogłoszenie upadłości podmiotu gospodarczego,
- otwarcie postępowania układowego albo też zawarcie układu,
- bezskuteczność egzekucji z majątku przedsiębiorstwa,

[26] R. Dankiewicz, *Odpowiedzialność ubezpieczyciela w ubezpieczeniu kredytu kupieckiego. Wybrane aspekty*, „Wiadomości ubezpieczeniowe", „Nauka dla praktyki", PIU Nr 01/2009, s. 68.
[27] R. Dankiewicz, *Determinanty rozwoju rynku ubezpieczeń kredytu kupieckiego w Polsce,* „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", 2011, Nr 228, s. 117.
[28] J. Lisowski, *op.cit.,* s. 154.
[29] R. Dankiewicz, *op.cit*., s.69.
[30] M. Iwanicz-Drozdowska, *op.cit*., s. 375.

– zgłoszenie wniosku o przeprowadzenie likwidacji przedsiębiorstwa[31].

Istnieją okoliczności, które mogą ograniczyć lub wyłączyć odpowiedzialność ubezpieczyciela z tytułu ubezpieczenia należności. Aby dana okoliczność wyłączyła odpowiedzialność zakładu ubezpieczeń musi być główną i bezpośrednią przyczyną powstania szkody oraz musi pozostawać z nią w związku przyczynowo-skutkowym. Ciężar udowodnienia zaistnienia danych okoliczności oraz tego, że są one główną i bezpośrednią przyczyną szkody ubezpieczonego spoczywa na zakładzie ubezpieczeń. Zaistnienie danych okoliczności może niekiedy skutkować wypowiedzeniem umowy jeszcze w trakcie jej trwania, zwłaszcza w sytuacji, gdy dochodzi do znaczącego wzrostu ryzyka[32].

Do wyłączeń odpowiedzialności zakładu ubezpieczeń można zaliczyć:

– nacjonalizację, konfiskatę, wywłaszczenie majątku dłużnika[33],
– wierzytelności od podmiotów, w których ubezpieczający pośrednio bądź bezpośrednio posiada większość udziałów lub może w inny sposób zdecydowanie wpływać na ich zarządzanie,
– należności przysługujące od instytucji rządowych i innych podmiotów, których upadłość nie może być ogłoszona zgodnie z przepisami prawa obowiązującymi w Rzeczypospolitej Polskiej,
– należności uboczne ubezpieczającego (odsetki za zwłokę, kary umowne, odszkodowania za poniesione szkody i straty, koszty sądowe, opłaty bankowe lub opłaty z tytułu najmu),
– straty powstałe w wyniku niewypełnienia lub nienależytego wypełnienia przez ubezpieczającego warunków umowy sprzedaży w stosunkach z klientem,
– fizyczne uszkodzenie towarów, będących przedmiotem ubezpieczonej wierzytelności,
– straty wynikłe ze sporów pomiędzy ubezpieczającym a klientem, w tym koszty postępowania sądowego,
– straty spowodowane okolicznościami o charakterze politycznym i społecznym, tj. wojna, rewolucja, strajki, zamieszki, akty terroru, klęski żywiołowe lub katastrofy spowodowane pośrednio lub bezpośrednio przez energię jądrową,

[31] R. Dankiewicz, *op.cit*., s.70.
[32] *Ibidem*, s.72.
[33] W. Ronka-Chmielowiec, *op.cit.,* s.387.

- straty będące konsekwencją decyzji władz, które uniemożliwiają bądź ograniczają możliwość realizacji transakcji,
- straty wynikające z niewypłacalności podmiotu pośredniczącego w zapłacie należności,
- straty, które mogłyby być pokryte z innego ubezpieczenia posiadanego przez ubezpieczającego,
- należności, co do których ubezpieczający uzgodnił ze swoim klientem terminy płatności dłuższe niż standardowo zapisane w warunkach ubezpieczenia, chyba że ubezpieczyciel potwierdził w decyzji kredytowej objęcie ich ochroną[34].

Istotne znaczenie mają sankcje za niewłaściwe wykonanie umowy ubezpieczenia przez ubezpieczającego, mogące skutkować wyłączeniem lub ograniczeniem odpowiedzialności, a w przypadku zrealizowania się ryzyka objętego umową ubezpieczenia nawet odmową wypłaty odszkodowania.

2.4. Analiza produktów ubezpieczeniowych z zakresu ubezpieczenia kredytu kupieckiego dostępnych na polskim rynku

Na polskim rynku istnieje stosunkowo niewiele zakładów ubezpieczeń mających w swojej ofercie ubezpieczenie kredytu kupieckiego. Wśród nich zdecydowanie dominują zagraniczne podmioty o globalnym zasięgu tj. Euler Hermes, Atradius czy Coface. Przyczyną takiego stanu rzeczy może być bariera wejścia wymuszająca na ubezpieczycielach znajomość zasad przebiegu cyklu koniunkturalnego w określonych branżach oraz umiejętne wykorzystanie informacji gospodarczych. Jednocześnie pokonanie tych barier daje duże możliwości osiągnięcia przewagi konkurencyjnej na rynku m.in. poprzez konkurowanie ceną, zakresem bądź warunkami ochrony ubezpieczeniowej[35].

W tabeli 2.2 porównano niektóre elementy umów ubezpieczenia zakładów ubezpieczeń oferujących ubezpieczenie kredytu kupieckiego.

[34] *Ibidem*, s.73.
[35] J. Lisowski, *op. cit*., s. 166-167.

Tabela 2.1. Oferty ubezpieczenia kredytu kupieckiego dostępne na polskim rynku

Zakład ubezpieczeń	Maksymalny okres kredytu	Przewlekła zwłoka	Składka	Maksymalna wysokość odszkodowania	Ubezpieczenie ryzyka politycznego
Atradius Credit Insurance N.V. S.A. Oddział w Polsce	w zależności od umowy	- w zależności od umowy - liczona od pierwotnego terminu płatności najwcześniej wymagalnej ubezpieczonej wierzytelności	stała kwota składki	w zależności od umowy	-
Coface S.A. Oddział w Polsce	w zależności od umowy	- w zależności od umowy - liczona od dnia zgłoszenia przeterminowanych należności, jednocześnie ze zleceniem dochodzenia należności	w oparciu o wartość obrotu	25-krotność składki zapłaconej za dany okres ubezpieczeniowy	-
Ergo Hestia S.A.	do 120 dni	180 dni od upływu określonego w fakturze terminu zapłaty	w oparciu o wartość obrotu	Ściśle określona suma pieniężna i/lub wielokrotność zapłaconej składki	-
Euler Hermes S.A.	do 180 dni	- liczona od dnia zlecenia windykacji spółce - 60 dni dla klientów z siedzibą w krajach UE, Andorze, Australii, Islandii, Japonii, Kanadzie, Lichtensteinie, Monako, Nowej Zelandii, Norwegii, Szwajcarii i USA - 210 dni dla klientów z siedzibą w pozostałych krajach	w oparciu o wartość obrotu oraz współczynnik szkodowości	25-krotność składki zapłaconej za dany okres ubezpieczeniowy	-

KUKE S.A.	- poniżej roku w przypadku sprzedaży krajowej - poniżej dwóch lat w przypadku sprzedaży eksportowej	120 dni od daty otrzymania przez zakład ubezpieczeń wniosku ubezpieczającego o interwencję	w oparciu o wartość obrotu	wielokrotność zapłaconych składek, określana w warunkach szczegółowych ubezpieczenia	+*

* Dotyczy ryzyka politycznego związanego z krajem kontrahenta lub państwa trzeciego.
Źródło: opracowanie własne na podstawie OWU poszczególnych zakładów ubezpieczeń.

Można zauważyć, że przedstawione oferty różnią się głównie pod względem sposobu naliczania okresu przewlekłej zwłoki. Przewlekła zwłoka jest wypadkiem ubezpieczeniowym wywołującym odpowiedzialność odszkodowawczą ubezpieczyciela. Okres przewlekłej zwłoki nie jest jednak jednoznacznie zdefiniowany. Dlatego w praktyce długość oraz sposób naliczania tej zwłoki różni się w zależności od zakładu ubezpieczeń, np. Atradius i Ergo Hestia rozpoczynają naliczanie przewlekłej zwłoki od upływu terminu określonego w fakturze, a Coface, Euler Hermes oraz KUKE naliczają ten okres od daty otrzymania zlecenia dochodzenia należności. Ponadto Euler Hermes wyróżnia dwa warianty przewlekłej zwłoki w zależności od kraju, w którym klient prowadzi działalność. Również maksymalny okres udzielanego kredytu różni się w zależności od ubezpieczyciela i waha się od 120 dni w zakładzie ubezpieczeń Ergo Hestia do 2 lat w przypadku sprzedaży eksportowej w KUKE. W większości ubezpieczeń kredytu kupieckiego składka obliczana jest na podstawie zgłoszonego obrotu kredytowego, czyli od sumy każdorazowo udzielonych kredytów. Składka zazwyczaj płacona jest z dołu na podstawie miesięcznych deklaracji wypełnianych przez kredytodawcę na specjalnych formularzach[36]. Maksymalne odszkodowanie w większości przypadków stanowi wielokrotność składek zapłaconych za dany okres ubezpieczeniowy, nie może być jednak większe niż wysokość przyznanego limitu pomniejszonego o udział własny kredytodawcy. Warto zaznaczyć, że KUKE jako jedyne towarzystwo ubezpieczeń w Polsce posiada gwarancje

[36] *Ibidem,* s. 219.

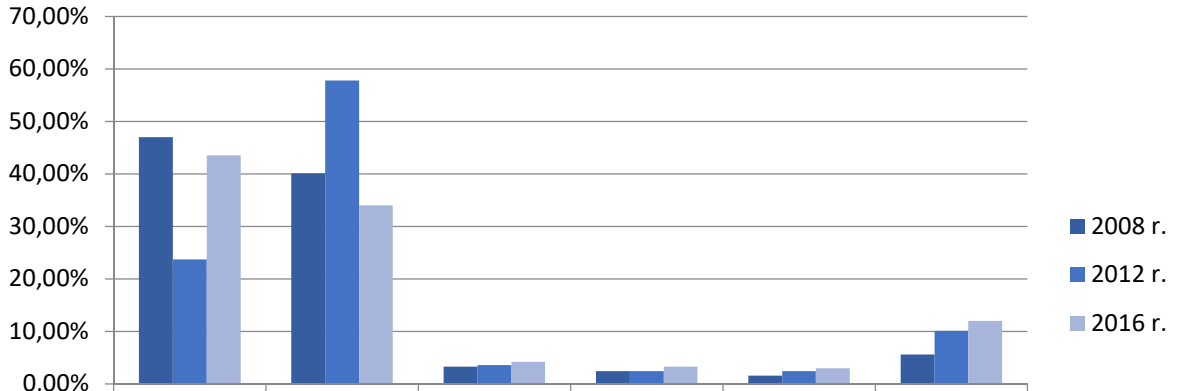
Skarbu Państwa przyznane na mocy ustawy[37], w wyniku których w przypadku sprzedaży eksportowej może ubezpieczać także ryzyko niehandlowe, w tym ryzyko polityczne[38].

2.5. Moralność płatnicza w Polsce

Wskaźnik moralności płatniczej (ang. *Payment Morality Index*, PMI) to dynamiczny wskaźnik pokazujący, jakie są skłonności kontrahentów do terminowego regulowania zobowiązań. Jest to ocena wystawiana na podstawie analizy przeszłych oraz bieżących zachowań płatniczych kontrahentów, która umożliwia przedsiębiorcom podejmowanie odpowiednich decyzji biznesowych wobec klientów. Przedsiębiorcom udzielającym kredyt kupiecki wskaźnik ten pozwala poznać zachowania i zwyczaje płatnicze kontrahentów, a dzięki temu ograniczyć ryzyko utraty płynności finansowej.

Moralność płatnicza w Polsce, w porównaniu z innymi krajami europejskimi, jest na bardzo niskim poziomie. Na rysunku 1 przedstawiono jak kształtowała się terminowość płatności polskich przedsiębiorstw w latach 2008, 2012 i 2016. Według statystyki CRIBIS D&B *Payment Study* w Polsce w 2016 r. zaledwie 43,5% faktur było płaconych w terminie[39]. Dla porównania w Danii, będącej w czołówce pod względem terminowej płatności, faktury płacone na czas stanowiły aż 86,5% wszystkich faktur. Polska jest drugim krajem w Europie, zaraz po Rumunii, z największym odsetkiem płatności z przekroczonym terminem o ponad 90 dni.

[37] Ustawa z dnia 7 lipca 1994 r. o gwarantowanych przez Skarb Państwa ubezpieczeniach kontraktów eksportowych, Dz.U. 1994 nr 86 poz. 398 z późn. zm.
[38] W. Sułkowska, *op. cit*., s. 166.
[39] *Payment Study* 2017, CRIBIS D&B 2017, (https://www.dnb.ru/media/entry/54/Payment_Study_2017_Light.pdf) dostęp:31.03.2018 r.

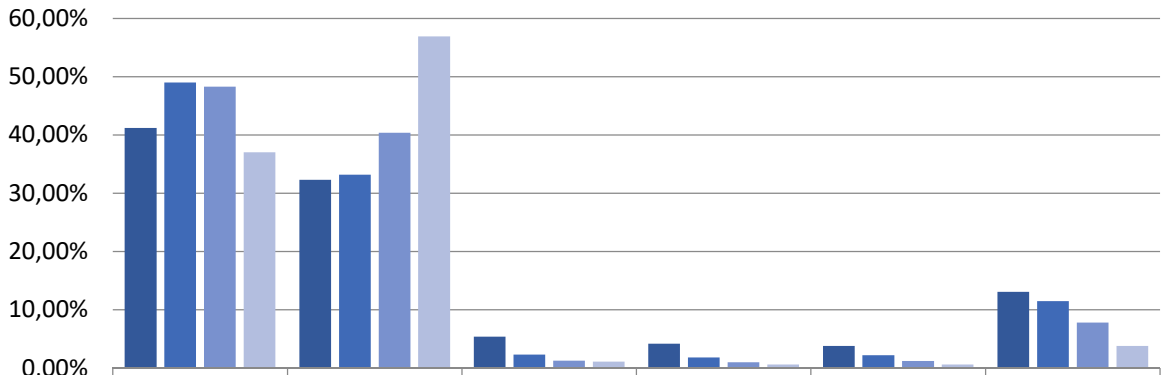


	w terminie	<30	30-60	60-90	90-120	>120
2008 r.	47,00%	40,10%	3,30%	2,40%	1,60%	5,60%
2012 r.	23,70%	57,80%	3,60%	2,40%	2,40%	10,10%
2016 r.	43,50%	34,00%	4,20%	3,30%	3,00%	12,00%

Rysunek 2.1. Terminowość płatności polskich przedsiębiorstw w latach 2008, 2012 i 2016 (w %)

Źródło: Opracowanie własne na podstawie raportu CRIBIS D&B, *Payment Study* 2017

W 2016 r. płatności z przekroczonym terminem o ponad 90 dni składały się na 15% ogółu, z czego aż 12% stanowiły faktury przeterminowane o ponad 120 dni. Jest to wzrost o ponad 6 punktów procentowych względem roku 2008, gdzie tylko 5,6% faktur było płaconych z przekroczonym terminem o ponad 120 dni. Znacznej poprawie uległy, w porównaniu z rokiem 2012, płatności realizowane w terminie – wzrosły z 23,7% do 43,5%. Do tak relatywnie złych wyników, w porównaniu do innych krajów UE, w dużym stopniu przyczyniają się firmy mikro i małe. Najdłużej zwlekają one z zapłatą, co zaprezentowano na rysunku 2. Odsetek płatności powyżej 90 dni w przedsiębiorstwach z tego sektora jest znacznie wyższy niż w większych firmach: w mikro i małych firmach są to łącznie odpowiednio 16,9% i 13,7%, podczas gdy w średnich i dużych firmach płatności te plasują się na poziomach 9% oraz 4,4%. Warto zauważyć, że najniższy udział płatności realizowanych terminowo posiadają przedsiębiorstwa duże, u których przeważają płatności regulowane do 30 dni.



	w terminie	<30	30-60	60-90	90-120	>120
mikro	41,20%	32,30%	5,40%	4,20%	3,80%	13,10%
małe	49,00%	33,20%	2,30%	1,80%	2,20%	11,50%
średnie	48,30%	40,40%	1,30%	1,00%	1,20%	7,80%
duże	37%	56,90%	1,10%	0,60%	0,60%	3,80%

Rysunek 2.2. Terminowość płatności polskich przedsiębiorstw w 2016 r. w zależności od wielkości prowadzonej działalności (w %)
Źródło: Opracowanie własne na podstawie raportu CRIBIS D&B, *Payment Study* 2017

Według analizy *Payment Practices Barometer Poland 2017* firmy Atradius, Polska jest jednym z najmniej skłonnych do sprzedaży na warunkach kredytowych krajów Europy Wschodniej. W 2017 r. wartość sprzedaży na kredyt spadła z wysokości 33,9% w 2016 r. do poziomu 28,9%. Średnio 32% sprzedaży na rzecz krajowych klientów B2B[40] pochodziło z kredytu, natomiast w przypadku klientów zagranicznych wartość sprzedaży udzielonej na kredyt stanowiła 25,7%. W obu przypadkach w 2017 r. nastąpił spadek o około 5 punktów procentowych w porównaniu z rokiem ubiegłym. Wyższy udział sprzedaży na kredyt dla klientów krajowych może wynikać z większej znajomości krajowych praktyk biznesowych i wyższego poziomu zaufania w stosunku do rodaków. Odsetek przeterminowanych faktur B2B w Polsce od kilku lat ciągle wzrasta. Pomimo, że udział zaległych faktur B2B w Polsce wzrósł o pięć punktów procentowych w porównaniu z rokiem 2016 (do 38,8%), to wciąż pozostaje niższy niż średnia regionalna (41,5%). Opóźnienia w płatnościach na rzecz polskich przedsiębiorców występują równie często od krajowych klientów B2B, jak i tych zagranicznych i plasują się na poziomie 89,2%. Częstotliwość ta jest najwyższa w tej części Europy, gdzie

[40] Ang. business-to-business, pojęcie to odnosi się do relacji zachodzących pomiędzy przedsiębiorstwami.

średnia to 83,7%. Zapytana o przyszłość 57,6% polskich respondentów stwierdziło, że nie spodziewają się zmian pod tym względem[41].

W 2017 r. ogłoszono niewypłacalność 900 firm w Polsce, co stanowi wzrost o 12% w porównaniu do roku 2016. W samym trzecim kwartale w Monitorach Sądowych opublikowano informacje o niewypłacalności aż 255 polskich firm - najwięcej w ciągu kwartału od 5 lat, kiedy to w czwartym kwartale 2012 r. liczba opublikowanych niewypłacalności wynosiła 260. Sektorami, które przyczyniły się do tak wysokiego wzrostu są transport, usługi oraz produkcja[42]. Niewypłacalności w transporcie wzrosły o 43%. Znaczny wpływ na to miały międzynarodowe regulacje prawne, stałe problemy z transportem na wschód, a także walka o klienta objawiająca się koniecznością inwestycji w jakość obsługi, skonfrontowana z niską marżą. Jedną z głównych przyczyn zwiększonej niewypłacalności w sektorze produkcji były rozrastające się sieci handlowe, które wspierają mniejszych handlowców i wywierają presję cenową na producentach. Mimo, że sektor budownictwa nie odnotował wzrostu upadłości w 2017 r., przyczynił się do powstania kłopotów u wielu dostawców i firm usługowych, w efekcie czego podmioty związane z budownictwem stanowiły 40% niewypłacalności[43].

Głównym problemem przedsiębiorców są wydłużające się terminy płatności, przyczyniające się do powstawania zatorów płatniczych. Najczęściej upadają młode firmy: po pierwszym roku działalności upada 30%, a po 5 latach aż 70% małych i średnich firm. Do najistotniejszych trudności, na jakie narażone są młode firmy należą duża konkurencja oraz bardzo niska rentowność (na poziomie 1–1,5% od obrotu). Przy tak niskiej rentowności nawet bieżące obroty i płynność finansowa nie dają gwarancji ochrony przed nieprzewidywalnymi zdarzeniami. Niskie marże i duża konkurencja nie stwarzają dobrych warunków do przeprowadzania inwestycji, czy też do budowania zaplecza finansowego na nieprzewidziane zdarzenia. To wszystko wpływa na krótki okres finansowania – najczęściej warunki kredytowe z bankami odnawiane są co roku. Finansowanie firm uzależnione jest od ich bieżącej sytuacji. Nawet chwilowe zawirowania mogą spowodować wycofanie się instytucji finansowych z

[41] *Payment Practices Barometer Poland 2017*, Atradius 2017, (https://atradius.pl/reports/payment-practices-barometer-poland-2017.html) dostęp:21.04.2018 r.
[42] W *III kwartale 2017 roku najwyższa liczba niewypłacalności od 5 lat,*(https://www.windykacja.pl/raporty,w-iii-kwartale-2017-roku-najwyzsza-liczba-niewyplacalnosci-od-5-lat.html), dostęp: 04.04. 2018 r.
[43] *W 2017 roku ogłoszono niewypłacalność 900 firm w Polsce,* (https://www.windykacja.pl/raporty,w-2017-roku-ogloszono-niewyplacalnosc-900-firm-w-polsce.html) dostęp:02.04.2018 r.

finansowania danego przedsiębiorstwa. Przedsiębiorcy muszą sobie radzić także z zatorami płatniczymi, które powodują zmniejszony przepływ środków pieniężnych. Z Programu Analiz Należności Euler Hermes wynika, że średnie opóźnienie w spłacie należności w Polsce wynosi 3 tygodnie. Biorąc pod uwagę przeciętny odroczony termin płatności udzielony nabywcy, który wynosi 56 dni, data faktycznego otrzymania zapłaty wydłuża się aż o 38%. Gdyby przedsiębiorcy otrzymywali na czas wszystkie należności, to regularny zastrzyk gotówki pozwalałby im na rozwój firmy i inwestycje, a nie tylko na bieżące funkcjonowanie

Istotne znaczenie z perspektywy zaistnienia ryzyka nieotrzymania zapłaty od kontrahenta mają także zmiany w prawie upadłościowym z 2016 r., które ułatwiły wchodzenie w postępowania restrukturyzacyjne i przyspieszyły całą procedurę. Obecnie prawo wymusza na właścicielach i zarządach firm szybsze podejmowanie decyzji o upadłości bądź restrukturyzacji długów, czym zwykle zaskakują rynek i partnerów handlowych. Wszystkie te czynniki powodują, że dostawcy dóbr i usług, mimo wzrostu gospodarczego muszą liczyć się z coraz większym ryzykiem niewypłacalności zarówno swojej, jak i swoich kontrahentów[44].

2.6. Zakończenie

Ubezpieczenie kredytu kupieckiego stosowane jest w celu zmniejszenia, bądź też wyeliminowania strat powstałych w związku z wystąpieniem nieterminowych płatności lub ogłoszenia niewypłacalności przez dłużnika. Możliwe jest to dzięki zastosowaniu limitów kredytowych oraz bieżącemu monitorowaniu kontrahentów przez zakład ubezpieczeń. Ubezpieczenie należności chroni przed skutkami kredytowania się dłużników kosztem przedsiębiorcy oraz zapewnia płynność i pokrycie ewentualnych strat wynikających z braku płatności. Pośrednio ułatwia również osiąganie założonych celów takich jak: maksymalizacja wartości firmy, planowany poziom zysku czy harmonijny rozwój.

Pomimo tych wszystkich zalet produkt ten nie cieszy się zbyt dużym zainteresowaniem wśród polskich przedsiębiorców. Przyczyną takiego stanu rzeczy może być brak lub niedostatek wiedzy o sposobie funkcjonowania ubezpieczenia kredytu kupieckiego. Inną barierą, na którą natrafiają przedsiębiorcy są liczne obowiązki po stronie ubezpieczającego,

[44] *Problemy sektora MSP i Budownictwa*, Euler Hermes (http://www.eulerhermes.pl/euler-hermes-w-polsce/centrum-prasowe/wiadomosci/Pages/170823_Problemy-sektora-MSP-i-budownictwa.aspx) dostęp: 04.04.2018 r.

których przestrzeganie warunkuje odpowiedzialność ubezpieczyciela. Obowiązki te można podzielić na trzy grupy: obowiązki związane ze zgłoszeniem kontrahentów do ubezpieczenia, obowiązki związane ze składką oraz obowiązki informacyjne. W ubezpieczeniu kredytu kupieckiego wymagana jest ciągła współpraca zakładu ubezpieczeń z ubezpieczającym na każdym etapie umowy[45]. Przedsiębiorców może odstraszać również wysoki koszt takiego ubezpieczenia. Do kosztów ubezpieczenia kredytu kupieckiego, obok składki, należy również zaliczyć opłaty za ocenę i monitorowanie kontrahentów oraz opłaty za udział ubezpieczyciela w windykacji należności[46]. Na dzień dzisiejszy głównym celem zakładów ubezpieczeń oferujących ten wyspecjalizowany produkt powinna być analiza barier, które stoją na przeszkodzie pozyskaniu nowych klientów oraz wypracowanie sposobu na ich wyeliminowanie bądź złagodzenie.

[45] J. Lisowski, op.cit., s. 150-151.
[46] R. Dankiewicz, *Składka a faktyczny koszt ubezpieczenia kredytu kupieckiego*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", 2010, Nr 105, s. 68.

Rozdział 3.
Zróżnicowanie przyczyn szkód w ubezpieczeniach *business interruption*

Anna Kozubal, Dominika Wolniak*

3.1. Wprowadzenie

Prowadzenie działalności gospodarczej związane jest z różnymi rodzajami ryzyka. Za działalność gospodarczą w rozumieniu ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej uważa się zarobkową działalność wytwórczą, budowlaną, handlową, usługową oraz poszukiwanie rozpoznawanie i wydobywanie kopalin ze złóż, a także działalność zawodową wykonywaną w sposób zorganizowany i ciągły[47]. Natomiast ryzyko, według nurtu klasycznego, jest zobiektywizowaną niepewnością wystąpienia niepożądanego zdarzenia[48]. We współczesnych warunkach gospodarowania podejmowanie działań w kierunku redukcji ryzyka należy traktować jako jedną z podstawowych funkcji systemu zarządzania działalnością gospodarczą[49]. Przedsiębiorstwa narażone są na straty, spowodowane ich działalnością operacyjną, inwestycyjną czy finansową. Istnieją jednakże mniej oczywiste, w powszechnej świadomości, przyczyny utraty zysku, jak chociażby przerwa w działalności gospodarczej (ang. *BI- business interruption*), która stanowi poważne zagrożenie dla płynności firmy. Jest to zjawisko o tyle niebezpieczne, że pomimo zastoju w przychodach, przedsiębiorstwo nadal musi ponosić koszty stałe, związane z jego funkcjonowaniem, takie jak np. opłaty czynszowe czy niezależne od obrotu podatki i opłaty. Skutkiem tego może być

* Koło Naukowe Ubezpieczeń „Risk Management", Katedra Zarządzania Ryzykiem i Ubezpieczeń, Uniwersytet Ekonomiczny w Krakowie.

[47] *Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej* (tekst jedn. Dz. U. z 2004 r., poz. 1807), art. 2.

[48] W. Sułkowska (red.), *Współczesne ubezpieczenia gospodarcze*, Wyd. Uniwersytetu Ekonomicznego w Krakowie, Kraków 2013 r., s. 13.

[49] S. Nahotko, *Ryzyko ekonomiczne w działalności gospodarczej*, TNOiK: Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego, Bydgoszcz 1997, s. 110.

znaczące zachwianie zdolności kredytowej firmy. Przez zmniejszenie, a nawet niedobór środków finansowych pozwalających pokryć zobowiązania pojawia się niebezpieczeństwo utraty wiarygodności w oczach partnerów biznesowych i kontrahentów[50]. Rynek ubezpieczeniowy oferuje zabezpieczenie przed tego typu ryzykiem w postaci ubezpieczenia od utraty zysku. Analizując ten typ ryzyka ubezpieczeniowego ze względu na najczęściej spotykane klasyfikacje możemy przyjąć, że ma ono charakter: finansowy - spowodowana szkoda ma charakter finansowy, partykularny - skutki tego ryzyka dotyczą jednostki, dynamiczny - przyczyny przerwy w działalności mogą zmieniać się wraz z postępem technologicznym i cywilizacyjnym, majątkowy - zagrożone są dobra majątkowe, czysty - jego zrealizowanie się powoduje stratę, a nie zrealizowanie nie niesie za sobą żadnych konsekwencji.

Istotą ubezpieczeń BI jest zapewnienie ochrony ubezpieczeniowej, która w razie szkody losowej umożliwi przedsiębiorstwu przetrwanie i odzyskanie pozycji sprzed szkody[51]. Dzięki niemu przedsiębiorstwo nie jest narażone na utratę płynności, a w konsekwencji pozycji na rynku. Ma to również znaczenie dla pracowników, którzy nie muszą obawiać się zwolnienia, pomimo zastoju w działaniu przedsiębiorstwa.

Celem niniejszej pracy jest przedstawienie: głównych przyczyn przerw w działalności gospodarczej na świecie, przyczyn szkodowości w zależności od położenia geograficznego, podziału przyczyn ryzyka przerwy w działalności gospodarczej ze względu na branżę oraz rozbieżności wartości roszczeń ze względu na przyczynę szkody. Do rozważenia powyższych problemów, przeanalizowano literaturę krajową oraz badania przeprowadzone przez instytucje rynku ubezpieczeniowego, takie jak: Allianz SE i Marsh LLC.

3.2. Charakterystyka ubezpieczeń Business Interruption

Podstawowym celem funkcjonowania ubezpieczeń od utraty zysku jest zapewnienie ciągłości działania przedsiębiorstwa. Jest ona rozumiana jako zdolność organizacji do reagowania na zakłócenia warunków normalnej działalności, aby tam gdzie to możliwe

[50] E. Wierzbicka (red.), *Ubezpieczenia dla przedsiębiorstw*, Oficyna Wydawnicza Szkoła Główna Handlowa w Warszawie, Warszawa 2014 r., s. 183.
[51] E. Wierzbicka (red.), *Ubezpieczenia non- life*, CeDeWu, Warszawa 2010, s. 221.

szybko przywrócić te normalne warunki, a tam, gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczego wykonywania zadań[52].

Ubezpieczenie BI jako produkt cechuje się pewnymi szczególnymi parametrami, które wyróżniają je na rynku ubezpieczeń. Po pierwsze, najczęściej jest ono bezpośrednio związane z polisą ubezpieczenia mienia. W związku z tym okres ubezpieczenia nie może być dłuższy niż okres ubezpieczenia mienia, jak również zakres ubezpieczenia nie może wykraczać poza ryzyka objęte ubezpieczeniem mienia. Bardzo ważną zasadą jest powstawanie odpowiedzialności odszkodowawczej ubezpieczyciela z tytułu utraty zysku, o ile szkoda w zysku brutto jest następstwem szkody materialnej w ubezpieczonym mieniu, powstałej w miejscu ubezpieczenia, na skutek zmaterializowania się ryzyka objętego zakresem ubezpieczenia BI[53]. W praktyce reguła ta okazuje się być problematyczna, gdy np. szkoda powodująca przerwę w działalności gospodarczej wystąpiła w mieniu wynajmowanym, które nie jest ubezpieczone w ramach polisy ubezpieczenia mienia.

Bardzo ważne w ubezpieczeniach BI jest określenie maksymalnego okresu odszkodowawczego. Stanowi on maksymalny okres rozpoczynający się w dniu powstania szkody, w którym ubezpieczyciel może ponosić odpowiedzialność za niekorzystne dla przedsiębiorstwa skutki, jakie szkoda ta będzie wywierać na prowadzoną przez nie działalność gospodarczą[54]. Okres odszkodowawczy zaś jest to faktyczny okres, liczony od momentu powstania szkody do chwili, gdy przestanie ona wywierać negatywny wpływ na działalność firmy. Nie może być on dłuższy niż maksymalny okres odszkodowawczy.

Nietypową cechą w tego typu ubezpieczeniach jest możliwość zastosowania, w ramach określania wysokości franszyzy redukcyjnej, tzw. okresu wyczekiwania. Jest to uzgodniony w polisie okres wyrażony liczbą dni roboczych, rozpoczynający się od dnia, w którym ubezpieczający został zmuszony do ograniczenia lub wstrzymania działalności, w następstwie szkody rzeczowej, po upływie którego rozpoczyna się faktyczna odpowiedzialność ubezpieczyciela za stratę w zysku brutto poniesioną przez ubezpieczającego w okresie odszkodowawczym. Jest to jednak dosyć kłopotliwe rozwiązanie, gdyż wymaga określenia

[52] I. Staniec, J. Zawiła- Niedźwiecki (red.), *Ryzyko operacyjne w naukach o zarządzaniu*, Wyd. C. H. Beck, Warszawa 2015, s. 281.
[53] E. Wierzbicka (red.), *Ubezpieczenia non- life…*, op. cit., s. 223.
[54] J. Monkiewicz, *Podstawy ubezpieczeń. Tom II – produkty,* Poltext, Warszawa 2001, s. 237.

oddzielnie strat, jakie nastąpiły w okresie obowiązywania franszyzy czasowej. Powszechnie okres wyczekiwania jest stosowany w przypadku klauzuli przerwy w dostawie energii, wody i gazu[55].

Dla ubezpieczeń BI charakterystyczny jest przedmiot ubezpieczenia, który stanowi zysk brutto. Aby go wyliczyć należy znać wartości: zysku operacyjnego, operacyjnych kosztów stałych oraz kosztów częściowo zmiennych. Istnieją dwie metody ustalenia sumy ubezpieczenia- metoda sumy i metoda różnicy. Chcąc wyliczyć sumę ubezpieczenia pierwszą z metod, należy dodać koszty stałe do zysku ze sprzedaży. Uzyskany wynik jest odpowiednio korygowany o spodziewany wzrost (lub spadek) obrotów w roku ubezpieczeniowym lub następnym. Na zysk netto w rozumieniu ubezpieczeniowym składają się: bilansowy zysk brutto oraz odpisy na otwarte fundusze rezerwowe poniesionych w ostatnim roku obrachunkowym[56]. Natomiast w przypadku obliczania sumy ubezpieczania przy pomocy metody różnicy od przychodu ze sprzedaży należy odjąć koszty zmienne. Metoda sumy jest bardziej narażona na ryzyko niedoubezpieczenia, dlatego częściej spotykaną jest druga z nich[57]. Jej zaletą jest brak konieczności ujawnienia szczegółowych danych finansowych. Ponadto prawdopodobieństwo pominięcia jakiejś pozycji kosztów jest mniejsze niż w przypadku metody sumy. Należy jednak pamiętać, że w praktyce ubezpieczeniowej po zakończeniu okresu ubezpieczenia osiągnięty zysk brutto podlega weryfikacji i jest możliwe ewentualne rozliczenie składki. Na wypadek niedoszacowania sumy ubezpieczenia przedsiębiorstwo może wykupić dodatkową sumę ubezpieczenia, zwaną prewencyjną. Dozwolone jest także ograniczenie zastosowania zasady proporcji, która stanowi pewnego rodzaju sankcję za niedoubezpieczenie mienia. Reguła ta polega na stosownym zmniejszeniu odszkodowania o stopień niedoubezpieczenia[58].

Konsekwencją wystąpienia przerwy w działalności gospodarczej jest nie tylko strata w zysku brutto, ale także konieczność poniesienia kosztów towarzyszących, które nie pojawiłyby się, gdyby funkcjonowanie przedsiębiorstwa nie zostało zakłócone wystąpieniem

[55] Z. Jęksa, *Ubezpieczenia majątku i zysku firmy,* Poltext, Warszawa 1999, s. 129.
[56] M. Cycoń, T. Jedynak, *Ubezpieczenie utraty zysku jako metoda zarządzania ryzykiem w działalności gospodarczej*, Ekonomiczne Problemy Usług nr 63, Zeszyty Naukowe Uniwersytetu Szczecińskiego, 2011 r., s. 311.
[57] W. Ronka-Chmielowiec (red.), *Ubezpieczenia wobec wyzwań XXI wieku*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2011, s. 398.
[58] W. Ronka-Chmielowiec (red.), *Ubezpieczenia,* Wyd. C. H. Beck, Warszawa 2016, s. 348.

szkody. Tego rodzaju koszty dodatkowe również mogą zostać objęte polisą od utraty zysku. Przykładami tego typu wydatków mogą być: koszty wynajęcia lub zbudowania pomieszczeń zastępczych, koszty tymczasowego wynajmu maszyn, koszty pracy w godzinach nadliczbowych, koszty wynikające z konieczności zrealizowania umownych zobowiązań (jak odsetki od zaciągniętego kredytu na prowadzoną działalność) czy dodatkowe koszty podróży służbowych. W przypadku niektórych przedsiębiorstw samo ubezpieczenie kosztów dodatkowych może okazać się wystarczające. Są to chociażby wszelkiego rodzaju instytucje finansowe, obiekty biurowe, administracyjne i usługowe, gdzie rzadko dochodzi do długiej przerwy w działalności[59].

Oprócz zastosowania typowych wyłączeń i ograniczeń spotykanych w innych ubezpieczeniach jak np. wina umyślna, akty terrorystyczne czy ryzyko polityczne, istnieją ograniczenia specyficzne dla ubezpieczeń od utraty zysku. Są to: opóźnienie we wznowieniu działalności z powodu braku wystarczającego kapitału, nieuzasadniona zwłoka we wznowieniu działalności, opóźnienie we wznowieniu działalności wynikające z decyzji administracyjnych wydanych przez organy władzy publicznej, innowacje i ulepszenia wprowadzone w trakcie odbudowy, odtworzenia lub naprawy zniszczonego mienia, niemożność odzyskania należności w wyniku zniszczenia lub utraty dokumentów księgowych oraz spadek wartości nieuszkodzonych towarów[60] [61] [62].

Co dzieje się w sytuacji, gdy przedsiębiorstwo mimo, że posiada ubezpieczenie mienia, nie może kontynuować działalności? Na polskim rynku przyjęło się, że wypłacana jest jedynie kwota poniesionych kosztów stałych i zysku operacyjnego, jaki zostałby osiągnięty w najkrótszym przewidywanym okresie odszkodowawczym[63].

Istnieją również sytuacje, gdy szkoda w zysku brutto ubezpieczonego przedsiębiorstwa powstała w rezultacie wystąpienia szkody fizycznej w mieniu innego podmiotu. Mówimy wówczas o szkodach skutkowych bądź interakcyjnych. Wśród szkód interakcyjnych wyróżniamy np. utratę zysku na skutek szkody u dostawców lub odbiorców, czy na skutek

[59] Z. Jęksa, *Ubezpieczenia majątku i zysku firmy...*, op. cit., s. 156.
[60] E. Wierzbicka (red.), *Ubezpieczenia non- life…*, op. cit., s. 237.
[61] Z. Jęksa, *Ubezpieczenia majątku i zysku firmy...*, op. cit. s. 134.
[62] E. Wierzbicka (red.), *Ubezpieczenia dla przedsiębiorstw…*, op. cit., s. 189.
[63] E. Wierzbicka (red.), *Ubezpieczenia non- life…,* op. cit., s. 240.

przerwy w dostawie mediów[64]. Warto jednak podkreślić, iż pokrywane są tylko te szkody, których przyczyną jest przerwa lub zakłócenie w dostawie spowodowane szkodą w mieniu dostawcy (odbiorcy) przez zdarzenia losowe. Nie jest więc wypadkiem ubezpieczeniowym niewywiązywanie się kontrahentów ze zobowiązania na skutek innych przyczyn[65]. Z kolei przykładami szkód skutkowych są brak dostępu do miejsca ubezpieczenia i spadek atrakcyjności lokalizacji, w wyniku szkody materialnej w mieniu innego podmiotu. Wraz z rozwojem technologii na rynku pojawiają się innowacyjne formy ubezpieczeń od tych szkód, jak np. utrata zysku wskutek zakłócenia działania systemów informatycznych, czy ubezpieczenie w oparciu o derywaty pogodowe. Wzrastające potrzeby zabezpieczenia systemów informatycznych zmotywowały ubezpieczycieli do opracowania polisy, gwarantującej rekompensatę z tytułu utraty przychodów spowodowanej naruszeniem bezpieczeństwa sieci, wirusa komputerowego, nieuprawnionego użycia komputera lub usługi sieciowej[66]. Jak wcześniej wspomniano, korporacje ubezpieczeniowe pracują także nad skonstruowaniem i ulepszaniem ubezpieczenia dla wszystkich segmentów rynku w oparciu o derywaty pogodowe. Mają one za zadanie chronić zyski firmy przed zmianami (normalnymi i nadzwyczajnymi) warunków meteorologicznych: szczególnie temperatury, opadów atmosferycznych lub wiatru[67]. Ta innowacyjna forma zyskuje na popularności szczególnie w branży turystyczno- hotelarskiej, gdzie niekorzystne warunki atmosferyczne znacząco wpływają na liczbę turystów[68]. To ubezpieczenie skierowane jest także dla przedsiębiorstw z branży spożywczej, ciepłowniczej i energetycznej.

Klasyczne ubezpieczenia od utraty zysku nie są w stanie ochronić przed wszystkimi rodzajami ryzyka. W związku z tym wykształtowały się produkty pochodne. Należą do nich ubezpieczenia związane z utratą zysku: w następstwie awarii maszyn, na skutek szkody w sprzęcie elektronicznym czy w rezultacie szkód objętych ubezpieczeniem ryzyk budowlanych lub montażowych.

---

[64] *Ibidem*, s. 241.

[65] T. Sangowski (red.), *Ubezpieczenia gospodarcze,* Poltext, Warszawa, 1998, s. 207.

[66] A. Szewczuk, *Business Interruption - Ewolucja kompleksowego programu ubezpieczeniowego dla sektora małych i średnich przedsiębiorstw*, Ekonomiczne Problemy Usług nr 50, Zeszyty Naukowe Uniwersytetu Szczecińskiego, 2010, s. 527.

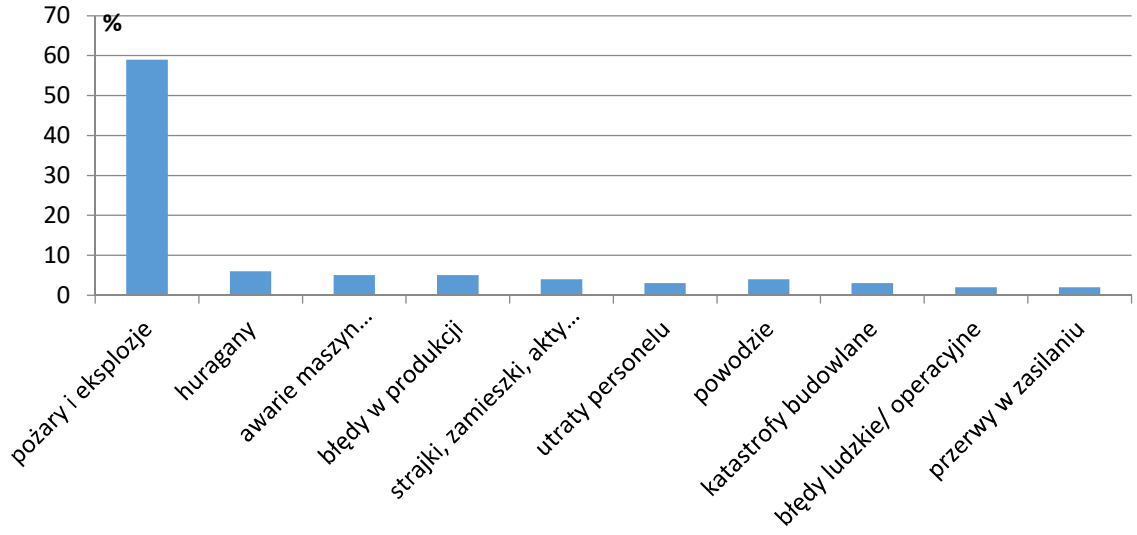
[67] J. Miazek- Popłacz*, Dla kogo ubezpieczenie utraty zysku?*, Miesięcznik Ubezpieczeniowy 2014, styczeń, s. 32.

[68] A. Szewczuk, *Business Interruption - Ewolucja kompleksowego programu ubezpieczeniowego dla sektora małych i średnich przedsiębiorstw*…, op. cit., s. 528

3.3. Przerwanie ciągłości działalności gospodarczej jako wypadek ubezpieczeniowy

3.3.1. Główne przyczyny przerw w funkcjonowaniu przedsiębiorstw na świecie

Rozmaite zjawiska mogą powodować zakłócenia w prowadzeniu działalności gospodarczej. Możemy wyróżnić wśród nich takie grupy jak: katastrofy naturalne, czynniki społeczne, a także problemy technologiczne. Rysunek 3.1 ilustruje najczęściej występujące przyczyny przerw w działalności gospodarczej na świecie.



Rysunek 3.1. Przyczyny przerw w działalności gospodarczej na świecie w latach 2010-2014 r.

Źródło: opracowanie własne na podstawie: *Global Claims Review 2015: Business Interruption in Focus. Global trends and development in business interruption claims*, Allianz Global Corporate & Speciality, 2015, s. 12.

Jak możemy zauważyć, najpowszechniej spotykane szkody związane są z pożarami i eksplozjami - 59%. Wypadki te są związane z podstawowym rodzajem ubezpieczenia od ognia i innych zdarzeń losowych. Pożary i eksplozje mogą przynieść olbrzymie straty, a proces odbudowywania środków trwałych, niezbędnych do prowadzenia działalności, może zająć dużo czasu. Najbardziej zagrożone są firmy o złożonym procesie produkcyjnym, w których zniszczenie jednego urządzenia może zablokować cały cykl wytwórczy. Drugim w kolejności czynnikiem powodującym przerwę w działalności gospodarczej są huragany - 6%. Należy tutaj pamiętać, że decydujący wpływ na tę przyczynę ma klimat. Podobna liczba - 5% głównych przyczyn przerw w funkcjonowaniu przedsiębiorstw na świecie stanowią: awarie maszyn produkcyjnych czy błędy w produkcji. Pozostałe czynniki, takie jak strajki, akty wandalizmu, utrata personelu powodzie, katastrofy budowlane, itd. pojawiają się znacznie

rzadziej, co nie znaczy, że są bez znaczenia, ponieważ ich występowanie jest zależne od rodzaju prowadzonej działalności gospodarczej czy strefy geograficznej.

Zła sytuacja przedsiębiorstwa spowodowana katastrofą naturalną jest często nasilana przez niepewność związaną z ochroną zapewnianą przez program ubezpieczenia[69]. Po pierwsze, problem dotyczy limitów stawianych przez ubezpieczycieli, które mogą ograniczać wypłatę środków ubezpieczającym. Drugą podstawową kwestią są wątpliwości co do efektywności pokrycia strat wywołanych przerwaniem ciągłości działalności firmy. Tabela 3.1 przedstawia ubezpieczone straty, jako procent całkowitych strat, w związku z katastrofami naturalnymi.

Tabela 3.1. Zależność pomiędzy wielkością straty, a jej ubezpieczoną częścią

Katastrofy naturalne	Ubezpieczona strata (US $ mld)	Całkowita strata (US $ mld)	Ubezpieczony odsetek
Huragan Katrina w 2005 r.	62,2	125	49,8%
Trzęsienie ziemi w Japonii w 2011 r.	40	210	19%
Powódź w Tajlandii w 2011 r.	16	43	37,2%
Huragan Sandy w 2012 r.	30	65	46,2%
Tajfun Haiyan w 2013 r.	0,7	10,5	6,7%
Powodzie w Europie w 2013 r.	3	15,2	19,7%

Źródło: opracowanie własne na podstawie: *Business interruption Insurance Efficacy: Five Key Issues*, Marsh & McLennan Companies, Marsh Risk Management Research, February 2015, s. 6.

Obserwując powyższą tabelę możemy zauważyć, że w przypadku katastrof naturalnych, powodujących znaczne straty finansowe często występuje sytuacja, w której wypłacone odszkodowanie nie jest w stanie zrekompensować znacznej części szkód. Najwyższy odsetek ubezpieczonej wartości straty wystąpił w związku z huraganem Katrina (49,8%), jednakże był to procent zbyt niski, aby pokryć choćby większość szkody.

Z przeprowadzonych przez *Marsh & McLennan Companies* badań wynika, że średnio 64% całkowitych strat w USA jest ubezpieczonych, co stanowi duży odsetek w porównaniu z innymi częściami świata (na przykład w Europie odsetek ten wynosi zaledwie 16%, a w Azji mniej niż

[69] *Business interruption Insurance Efficacy: Five Key Issues, Marsh & McLennan Companies*, Marsh Risk Management Research, February 2015, s. 6.

1%). Istnieje wiele przyczyn takiego niedoubezpieczenia, mogą to być świadome decyzje lub wyłączenia branżowe (takie jak katastrofy nuklearne). Niebezpieczne mogą być także dopiero powstające, nieznane ryzyka, dla których nie poszukiwano jeszcze ubezpieczenia[70].

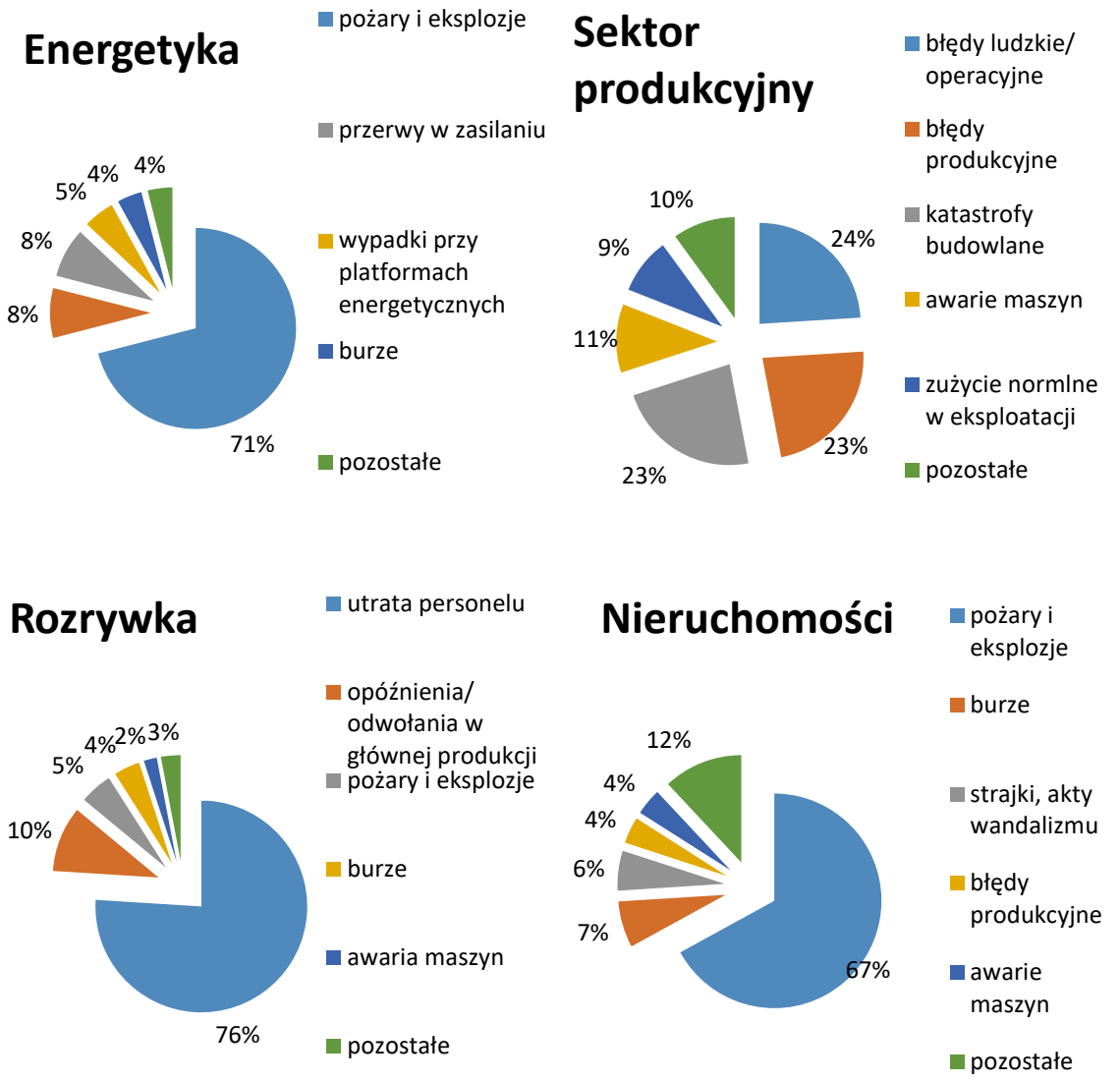
3.3.2. Przyczyny roszczeń z tytułu przerwy w działalności z podziałem na sektory

Warte uwagi jest rozpatrywanie przyczyn przerw w działalności gospodarczej w różnych sektorach rynku. W naszym opracowaniu wyróżniono cztery podstawowe branże – energetyczną, produkcyjną, rozrywkową oraz sektor nieruchomości. Podział przyczyn ze względu na sektory gospodarki ilustruje Rysunek 3.2. Pierwszym z nich jest sektor energetyczny, który ma kluczowe znaczenie dla gospodarek wielu państw na świecie. Skutki szkód w tej gałęzi dotykają nie tylko bezpośrednio danego przedsiębiorstwa, ale mogą wpłynąć też na funkcjonowanie zwykłych ludzi oraz innych podmiotów rynkowych. Ze względu na specyfikę tej dziedziny, związanej z wydobywaniem surowców paliwowych i wytwarzaniem energii, nie dziwią dane wskazujące na to, że główną przyczyną są pożary i eksplozje, które stanowią, aż 71% (Rys. 3.2). Ponadto istotny wpływ mają także awarie maszyn, najczęściej spowodowane przestarzałym sprzętem. Podobne znaczenie mają przerwy w zasilaniu, bez którego nie ma możliwości funkcjonowania tego rodzaju koncernów.

Następnym analizowanym działem gospodarki narodowej jest sektor produkcyjny. Występują w nim trzy decydujące powody zastoju cyklu wytwórczego. Są to błędy ludzkie (operacyjne), błędy produkcyjne i katastrofy budowlane. Łącznie stanowią około ¾ wszystkich przyczyn strat w tej branży. Są to charakterystyczne dla tego sektora problemy, których nie sposób uniknąć.

W branży nieruchomości podstawową przyczyną szkodowości są pożary i eksplozje. Stanowią one wyraźnie ponad połowę przypadków.

[70] *Ibidem*, s. 6.



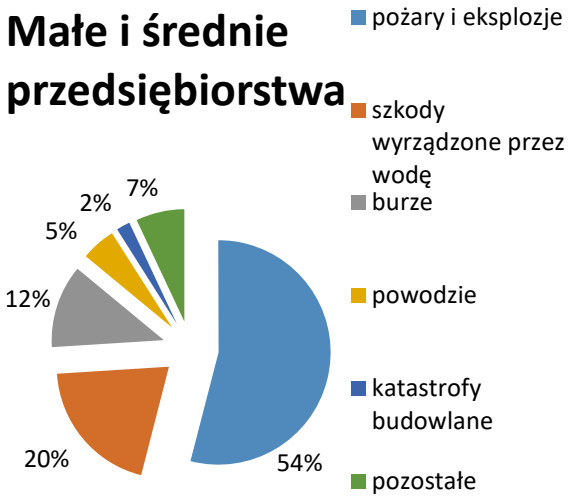
Rysunek 3.2. Procentowe zróżnicowanie przyczyn utraty zysku ze względu na typy roszczeń w wybranych branżach gospodarki.

Źródło: opracowanie własne na podstawie: *Global Claims Review 2015: Business Interruption in Focus. Global trends and development in business interruption claims*, Allianz Global Corporate& Speciality, 2015, s.15.

Zupełnie odmiennie kształtują się przyczyny przerw w działalności gospodarczej w firmach związanych z przemysłem rozrywkowym, gdzie główną rolę pełnią pracujący dla niej ludzie. Dlatego też utrata personelu np. na skutek choroby może powodować duże straty, prowadząc do opóźnień czy konieczności odwoływania wydarzeń rozrywkowych, narażając firmę na zwiększone koszty.

Godnym uwagi byłby także podział przyczyn szkód wynikających z ubezpieczenia BI ze względu na wielkość przedsiębiorstw. Dane dotyczące sektora małych i średnich

przedsiębiorstw przedstawia Rysunek 3.3. Jak można zauważyć, głównymi powodami są tutaj pożary i eksplozje, a także szkody spowodowane przez wodę (np. butwienie drewna). Niestety do pełnego porównania brakuje w literaturze danych, przedstawiających przyczyny utraty zysku w dużych firmach.



Rysunek 3.3. Procentowe zróżnicowanie przyczyn utraty zysku w małych i średnich przedsiębiorstwach.

Źródło: opracowanie własne na podstawie: *Global Claims Review 2015: Business Interruption in Focus. Global trends and development in business interruption claims*, Allianz Global Corporate& Speciality, 2015, s. 15.

3.3.3. Podział geograficzny przyczyn szkód

Jak już wspominano klimat jest jednym z czynników, które w znaczny sposób mogą wpływać na zdarzenia uniemożliwiające płynne działanie przedsiębiorstwa. Coraz większa liczba i skala burz, pożarów i eksplozji i innych katastrof jest źródłem dodatkowych kosztów dla przedsiębiorstw, a w efekcie całych branż. Nasilające się efekty przeobrażeń klimatu mogą być źródłem zysków i skłaniają ubezpieczycieli do dostosowania produktów do potrzeb rynkowych, np. poprzez oferowanie polis ze zniżkami, dla podmiotów podejmujących czynności przystosowawcze do zmian klimatycznych[71].

Godnym uwagi jest zatem rozważenie zróżnicowania przyczyn szkód w oparciu o podział geograficzny. Dane konieczne do takiej analizy zawiera Tabela 2.

[71] K. Lewandowska, *Zmiany klimatu a ryzyko dla przedsiębiorstwa, Wybrane problemy gospodarki światowej pierwszej dekady nowego wieku*, W. Michalczyka (red.), Uniwersytet Ekonomiczny we Wrocławiu. Katedra Międzynarodowych Stosunków Gospodarczych, Wrocław: 2009, s. 166.

Tabela 3.2. Zróżnicowanie geograficzne przyczyn szkód

Region / Przyczyna	Afryka	Ameryka Płd.	Ameryka Płn.	Azja	Bliski Wschód	Europa	Karaiby i Ameryka Środkowa
Awaria maszyn	4%	5%	0%	0%	0%	3%	16%
Burze	0%	0%	14%	9%	0%	0%	33%
Błędy ludzkie/ operacyjne	0%	18%	0%	0%	14%	2%	0%
Błędy produkcyjne	5%	0%	0%	0%	0%	8%	0%
Kolizje	0%	0%	0%	0%	0%	0%	1%
Inne	1%	1%	17%	11%	13%	7%	1%
Powodzie	0%	5%	4%	13%	0%	0%	0%
Pożary i eksplozje	21%	61%	52%	10%	23%	78%	31%
Przerwy w zasilaniu	10%	0%	0%	0%	19%	0%	0%
Utraty personelu	0%	0%	8%	0%	0%	0%	0%
Strajki, zamieszki, akty wandalizmu	0%	0%	0%	51%	23%	0%	0%
Szkody wyrządzone przez wodę np. butwienie drewna, czy zalania	0%	0%	5%	0%	0%	0%	0%
Śnieżyce	0%	0%	0%	0%	0%	2%	0%
Trzęsienia ziemi	0%	10%	0%	0%	0%	0%	0%
Katastrofy budowlane	59%	0%	0%	0%	0%	0%	18%
Zużycie normalne w eksploatacji	0%	0%	0%	6%	8%	0%	0%
Suma	100%	100%	100%	100%	100%	100%	100%

Źródło: opracowanie własne na podstawie: *Global Claims Review 2015: Business Interruption in Focus. Global trends and development in business interruption claims*, Allianz Global Corporate& Speciality, 2015, s. 16.

Pierwszy z analizowanych obszarów stanowi kontynent afrykański, który charakteryzuje się niskim poziomem rozwoju rynku ubezpieczeń. Najważniejszą przyczyną przerw w działalności gospodarczej są tutaj katastrofy budowlane, co wskazuje na częste błędy w sztuce budowlanej. Istotne znaczenie mają również pożary i eksplozje, których powstawaniu sprzyja suchy i gorący klimat.

Ameryka Południowa charakteryzuje się jeszcze wyższą częstotliwością występowania pożarów i eksplozji. Ważnym czynnikiem są także błędy ludzkie, operacyjne, co wskazuje na niską efektywność pracy. Warte podkreślenia są straty wywołane przez trzęsienia ziemi. Dobrym przykładem ilustrującym to zjawisko było trzęsienie ziemi w Chile w 2010 roku, które doprowadziło do przerwy w działalności kopalni miedzi i rafinerii ropy naftowej.

Następnym regionem jest Ameryka Północna, gdzie ponad połowę przyczyn przerw w działalności gospodarczej stanowią pożary. Równocześnie występują liczne nieklasyfikowane problemy (kategoria inne - 17%). W Ameryce Północnej szczególnie ważny jest sektor związany z rozrywką, w którym utrata personelu jest jednym z istotnych powodów utraty zysku. Duża część strat wywoływana jest również przez zjawiska hydrologiczne i atmosferyczne, jak np. powodzie czy huragany.

Przenosząc się w nieco inny region świata - do Azji, łatwo zaobserwować zupełnie inne przyczyny szkodowości. Ważną rolę odgrywają zjawiska społeczne, takie jak strajki, zamieszki czy akty wandalizmu, którym może sprzyjać wysoki stopień przyrostu naturalnego, bieda, czy problemy polityczne. W przeciwieństwie do poprzednio omawianych kontynentów widzimy, że zaledwie 10% strat powodowane jest przez pożary i eksplozje. Z drugiej strony, w Azji częściej w porównaniu do pozostałych obszarów pojawiają się powodzie.

Charakteryzując trudności na Bliskim Wschodzie można zauważyć podobny wpływ zjawisk ogniowych, jak i strajków, zamieszek czy aktów wandalizmu. Cechą wyróżniającą Bliski Wschód na tle innych regionów jest wysoka szkodowość spowodowana przerwami w dostawie mediów i wysokim stopniu zużycia urządzeń i obiektów produkcyjnych.

Kontynent europejski charakteryzuje dominujący odsetek (około 80%) pożarów i eksplozji jako przyczyn przerwy w działalności gospodarczej. Przez klimat panujący w Europie przedsiębiorstwa narażone są na takie zjawiska atmosferyczne, jak śnieżyce, które tylko na tym kontynencie występowały jako źródło utraty zysku.

Istotną rolę środowiska geograficznego dostrzegamy patrząc na przykład regionu Karaibów i Ameryki Środkowej, gdzie głównym motywem strat są burze i pożary, stanowiące ponad 2/3 wszystkich przyczyn strat. Podobnie jak w Afryce, jednak w dużo mniejszym stopniu, zauważalny jest problem katastrof budowlanych.

3.4. Średnie wartości roszczeń wynikających z ubezpieczeń BI ze względu na wybrane przyczyny strat.

Ważne jest nie tylko ujęcie procentowe informujące o częstotliwości występowania przyczyn strat, wynikających z wstrzymania działalności gospodarczej, ale również zobrazowanie skali tych szkód w wyrażeniu wartościowym. Umożliwia to analiza średnich wartości roszczeń, które dane przedsiębiorstwa zgłaszają w wyniku wypadków objętych ubezpieczeniem BI. Dane na ten temat zawiera Tabela 3.3.

Tabela 3.3. Średnie wartości roszczeń wynikających z ubezpieczeń Business Interruption ze względu na wybrane przyczyny strat w latach 2010- 2014

Przyczyny strat	Wartości roszczeń (w euro)
Wypadki związane z platformą wiertniczą	4 160 000
Strajki, zamieszki, akty wandalizmu	3 810 000
Śnieżyce	2 220 000
Błędy ludzkie/operacyjne	1 770 000
Pożary i eksplozje	1 670 000
Błędy produkcyjne	1 570 000
Trzęsienia ziemi	1 360 000
Przerwy w zasilaniu	1 230 000
Powódź	1 190 000
Katastrofy budowlane	909 150
Zużycie normalne w eksploatacji	838 773
Huragany	776 449
Awarie maszyn produkcyjnych	580 504

Erupcje wulkanu	100 526
Kradzieże, włamania	66 903

Źródło: opracowanie własne na podstawie: *Global Claims Review 2015: Business Interruption in Focus. Global trends and development in business interruption claims*, Allianz Global Corporate& Speciality, 2015, s. 14.

Przyglądając się powyższemu zestawieniu można zaobserwować, że najbardziej kosztowne są szkody w sektorze energetycznym, wynika to ze specyfiki tej gałęzi przemysłu, w której sam majątek przedsiębiorstw jest znacznej wartości. Przeciętna wysokość szacowanej straty zysku wynosi tutaj 4,16 mln euro (Tabela 3.3). Niebagatelną wartość mają także roszczenia spowodowane czynnikami społecznymi, takimi jak: strajki, zamieszki, akty wandalizmu. Protesty pracownicze potrafią sparaliżować funkcjonowanie całych przedsiębiorstw. Trzecią pozycję pod względem wielkości roszczeń - 2,22 mln euro, zajmują szkody spowodowane przez śnieżyce, pomimo tego, że nie są częstą przyczyną występowania zniszczeń w większości regionów świata. Równie istotne są błędy powodowane przez pracę ludzi, czy też związane z działalnością operacyjną. Następnie warto zwrócić uwagę, że choć pożary i eksplozje są najbardziej rozpowszechnionym powodem strat, jednak pod względem wartości są dopiero na piątym miejscu. Z kolei trzęsienia ziemi, choć jak wcześniej wykazano, są zagrożeniem głównie w Ameryce Południowej powodują bardzo kosztowne straty. W pierwszej piętnastce najpoważniejszych roszczeń znajdują się także inne katastrofy naturalne, jak powodzie, huragany, czy erupcje wulkanów.

3.5. Zakończenie

Ryzyko przerwy w działalności gospodarczej może okazać się dużym zagrożeniem dla funkcjonowania przedsiębiorstw na całym świecie. W każdej szkodzie majątkowej straty materialne to zaledwie 40% jej wartości, pozostałe 60% stanowi wartość utraconego zysku[72]. Jak zostało jednak ukazane w tej pracy, przyczyny powodujące to zjawisko są zróżnicowane ze względu na branżę, w jakiej działa dana firma oraz region geograficzny, w którym się znajduje. Choć widać wyraźną dominację pożarów i eksplozji, jako najczęstszych przyczyn utraty zysku, nie dla każdego sektora gospodarki stanowią one największe niebezpieczeństwo. Można też zauważyć, zestawiając Rysunek 3.1. z Tabelą 3.3, że średnie wartości roszczeń nie

[72] T. Rydzicki, *Polisa na utracone zyski,* „Gazeta Małych i Średnich Przedsiębiorstw", 2007 r., nr 61.

są bezpośrednio powiązane ze skalą częstości występowania zjawisk, które powodują przerwę w działalności gospodarczej.

Równie ważna jest odpowiedź na pytanie, w jakiej części świata firma zamierza prowadzić działalność, gdyż niektóre ryzyka związane są typowo z danym klimatem, jak np. śnieżyce czy trzęsienia ziemi. Pod uwagę należy wziąć także fakt, że istotna jest nie tylko liczba zdarzeń na tle innych przyczyn, ale także ich ciężar finansowy - niektóre ze szkód ze względu na specyfikę działalności danego przedsiębiorstwa charakteryzują się wyższą w porównaniu do pozostałych wartością roszczeń, wynikających z ubezpieczenia BI. Nie ulega jednak wątpliwości, że ubezpieczenia te mogą mieć kluczowe znaczenie dla przetrwania firmy w trudnym okresie, następującym po szkodzie materialnej. Do odzyskania pozycji na rynku konieczna jest przecież nie tylko finansowa refundacja szkody bezpośredniej, ale również rekompensata utraconego zysku, który w normalnych warunkach trafiłyby do przedsiębiorstwa.

Rozwój ubezpieczenia od utraty zysku na świecie uwarunkowany jest sytuacją finansową przedsiębiorców, poziomem rozwoju gospodarczego, świadomością ubezpieczeniową i znaczącą rolą banków, które wymagały ubezpieczenia BI w kredytowanych przez siebie inwestycjach[73]. Na polskim rynku ubezpieczeniowym jest to wciąż mało popularny produkt, chociaż świadomość korzyści jakie może on przynieść przedsiębiorstwu, powinna wpływać na wzrost liczby zawieranych umów ubezpieczenia BI.

[73] M.Z. Broda, *Nowe wyzwania BI, cz. 2,* Dziennik Ubezpieczeniowy 2008, nr 2103.

Rozdział 4.
Ubezpieczenia turystyczne w Polsce

Kinga Stokłosa*

4.1. Wprowadzenie

Turystyka jest zjawiskiem powszechnym i masowym. Większości podróżującym zależy, aby ich wyjazd odbył się bezpiecznie, a przy tym był jak najmniej kosztowny. Nie należy jednak zapominać, że turystyce towarzyszą liczne zagrożenia. Pomocnym narzędziem w minimalizacji skutków tych zagrożeń stają się ubezpieczenia turystyczne, które zaspakajają potrzeby bezpieczeństwa klientów. Coraz więcej turystów zwraca uwagę na ubezpieczenia turystyczne, ich koszty oraz zakres ochrony. W związku z tym problem badawczy niniejszej pracy może być przedstawiony w postaci pytań: *Jakie są determinanty popytu na ubezpieczenia turystyczne? Czym są kluczowe czynniki różnicujące zakres ubezpieczenia i ich wpływ na koszty ubezpieczenia?* Za główne cele pracy przyjęto:

1. Przedstawienie ustawy o usługach turystycznych jako podstawowego aktu prawnego regulującego warunki świadczenia usług turystycznych oraz dokonanie charakterystyki systemu bezpieczeństwa finansowego biur podróży.
2. Dokonanie analizy ryzyka w turystyce oraz przedstawienie możliwości ograniczenia niektórych rodzajów ryzyka w turystyce wynikających z ustanowienia Unii Europejskiej.
3. Dokonanie charakterystyki ubezpieczeń turystycznych oraz identyfikacja kluczowych czynników różnicujących zakres ubezpieczenia i ich wpływ na koszty ubezpieczenia na przykładzie PZU Wojażer.

* Koło Naukowe Ubezpieczeń „Risk Management", Katedra Zarządzania Ryzykiem i Ubezpieczeń, Uniwersytet Ekonomiczny w Krakowie.

Do pełnego zobrazowania i realizacji wyżej wymienionych celów wykorzystano dostępną na rynku literaturę oraz aktualnie proponowane oferty ubezpieczeń turystycznych.

4.2. Ustawa o usługach turystycznych

Ustawa o usługach turystycznych stanowi podstawowy akt prawny regulujący warunki świadczenia przez przedsiębiorców usług turystycznych na terenie Rzeczypospolitej Polskiej oraz za granicą, jeśli umowy z klientami są zawieranie na terytorium Rzeczypospolitej Polskiej, a także zasady funkcjonowania Turystycznego Funduszu Gwarancyjnego.

Przez użyte w ustawie terminy należy rozumieć[74]:

- usługi turystyczne – usługi przewodnickie, hotelarskie, a także wszystkie inne usługi świadczone turystom i odwiedzającym,
- impreza turystyczna – co najmniej dwie usługi turystyczne, które tworzą jednolity program i są objęte wspólną ceną. Usługi te muszą obejmować nocleg, zmianę miejsca pobytu lub trwać ponad 24 godziny,
- wycieczka – rodzaj imprezy turystycznej, której plan obejmuje zmianę miejsca pobytu uczestników,
- organizowanie imprez turystycznych – oferowanie lub przygotowanie, a także proces realizacji imprez turystycznych,
- organizator turystyki – przedsiębiorcę, który organizuje imprezę turystyczną,
- pośrednik turystyczny – przedsiębiorcę, który na zlecenie klienta wykonuje czynności faktyczne i prawne związane z zawieraniem umów dotyczących świadczenia usług turystycznych,
- agent turystyczny – przedsiębiorcę, który stale pośredniczy w zawieraniu umów o świadczenie usług turystycznych. Swoją działalność wykonuje na rzecz organizatorów turystyki, którzy posiadają zezwolenia w kraju lub siedzibę na terytorium Rzeczypospolitej Polskiej,
- przewodnik turystyczny – osobę, która zawodowo oprowadza odwiedzających lub turystów po wybranych terenach, miejscowościach i obiektach oraz udziela o nich

[74] Ustawa z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz.U. 1997 Nr 133 poz. 884, z późn. zm.).

fachowej informacji, a także sprawuje nad odwiedzającymi i turystami opiekę w zakresie wynikającym z wykonywanej umowy,

- pilot wycieczek – osobę towarzyszącą, która w imieniu organizatora turystyki sprawuje opiekę nad uczestnikami imprezy turystycznej oraz czuwa nad sposobem wykonywania usług na ich rzecz. Ponadto pilot wycieczek przekazuje podstawowe informacje dotyczące odwiedzanego miejsca lub kraju,
- usługi hotelarskie – krótkotrwałe, a zarazem ogólnodostępne wynajmowanie miejsc noclegowych, domów, mieszkań, pokoi oraz miejsc na ustawienie namiotów lub przyczep samochodowych oraz obowiązek świadczenia, w obrębie obiektu, usług z tym związanych,
- turysta – osobę, która podróżuje do innego miasta poza swoim stałym miejscem pobytu na czas nieprzekraczający 12 miesięcy, a celem jej podróży nie jest podjęcie pracy w odwiedzanym miejscu i która przynajmniej przez jedną dobę korzysta z noclegu,
- odwiedzający – osobę, która podróżuje do innego miasta poza swoim stałym miejscem pobytu, a celem jej podróży nie jest podjęcie pracy w odwiedzanym miejscu oraz niekorzystającą z noclegu,
- klient – osobę, która zawarła lub zamierza zawrzeć umowę o świadczenie usług turystycznych na swoją rzecz lub na rzecz innej osoby oraz zawarcie tej umowy nie stanowi przedmiotu prowadzonej przez nią działalności gospodarczej, jak i osobę, na rzecz której umowa ta została zawarta, jak również osobę na rzecz której przekazano prawo do korzystania z usług turystycznych objętych umową,
- przedsiębiorca – przedsiębiorcę i przedsiębiorcę zagranicznego w rozumieniu ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej[75].

[75] Zgodnie z definicją zawartą art. 4. ustawy o swobodzie działalności gospodarczej (Dz.U. 2004 Nr 173 poz. 1807, z późn. zm.) przedsiębiorcą jest osoba fizyczna, osoba prawna oraz jednostka organizacyjna niebędąca osobą prawną, której odrębna ustawa przyznała zdolność prawną – wykonująca działalność gospodarczą we własnym imieniu. Przedsiębiorcami są także wspólnicy spółki cywilnej w zakresie wykonywanej przez nich działalności. Zgodnie z definicją zawartą art. 5. ustawy o swobodzie działalności gospodarczej (Dz.U. 2004 Nr 173 poz. 1807, z późn. zm.) przedsiębiorcą zagranicznym jest osoba zagraniczna, która wykonuje działalność gospodarczą za granicą oraz obywatel Rzeczypospolitej Polskiej wykonujący działalność gospodarczą za granicą.

Warto również nadmienić, że z dniem 1 lipca 2018 r. zacznie obowiązywać nowa ustawa o imprezach turystycznych i powiązanych usługach turystycznych. Zastąpi ona ustawę z dnia 29 sierpnia 1997r. o usługach turystycznych i stanie się najważniejszym aktem prawnym regulującym działalność turystyczną[76].

Ustawa modyfikuje niektóre pojęcia oraz wprowadza nowe. Do zmienionych terminów należą[77]:

- usługa turystyczna – przewóz pasażerów, zakwaterowanie, które ma inny cel niż pobyt oraz nie jest nieodłącznym elementem przewozu osób, wynajem samochodu lub innego pojazdu silnikowego, a także inna usługa świadczona podróżnym, która nie stanowi integralnej części usług wskazanych wcześniej,
- impreza turystyczna – połączenie co najmniej dwóch różnych kategorii usług turystycznych na potrzeby wakacji lub tej samej podróży,
- organizator turystyki – przedsiębiorca turystyczny, który tworzy i sprzedaje, a także oferuje do sprzedaży imprezy turystyczne. Sprzedaż ta odbywa się bezpośrednio lub za pośrednictwem innego przedsiębiorcy turystycznego lub razem z nim. Przedsiębiorcom turystycznym jest także osoba, która przekazuje dane podróżnego innemu przedsiębiorcy turystycznemu,
- agent turystyczny – przedsiębiorca turystyczny inny niż organizator turystyki, który na podstawie umowy agencyjnej może sprzedawać lub oferować do sprzedaży imprezy turystyczne stworzone przez organizatora turystyki.

Ustawa o imprezach turystycznych i powiązanych usługach turystycznych wprowadza również nowe pojęcia, takie jak:

- umowa o udział w imprezie turystycznej – umowa dotycząca imprezy turystycznej jako całości, lub jeśli taka impreza realizowana jest na podstawie odrębnych umów to wszystkie umowy obejmujące oddzielne usługi turystyczne w ramach tej samej imprezy turystycznej,

[76] *Ustawa o imprezach turystycznych i powiązanych usługach turystycznych*, (https://www.msit.gov.pl/pl/aktualnosci/7570,Ustawa-o-imprezach-turystycznych-i-powiazanych-uslugach-turystycznych.html), dostęp: 02.05.2018 r.

[77] Ustawa z dnia 24 listopada 2017 r. o imprezach turystycznych i powiązanych usługach turystycznych (Dz.U. 2017 poz. 2361).

- rozpoczęcie imprezy turystycznej – rozpoczęcie wykonywania usług turystycznych w ramach tej samej imprezy turystycznej,
- powiązane usługi turystyczne – niestanowiące imprezy turystycznej połączenie co najmniej dwóch odrębnych usług turystycznych nabytych na potrzeby wakacji lub tej samej podróży, które są objęte różnymi umowami z dostawcami poszczególnych usług turystycznych,
- podróżny – każdy, kto chce zawrzeć umowę turystyczną lub jest uprawniony do podróżowania na podstawie umowy zawartej w obrębie stosowania umowy,
- przedsiębiorca turystyczny – przedsiębiorca, który ułatwia nabywanie usług turystycznych, organizator turystyki, agent turystyczny lub dostawca usług turystycznych, będący przedsiębiorcą w rozumieniu art. 43^5 ustawy z dnia 23 kwietnia 1964r. – Kodeks cywilny albo prowadzącego odpłatną działalność[78],
- trwały nośnik – materiał lub narzędzie, które umożliwia przedsiębiorcy turystycznemu lub podróżnemu na przechowywanie informacji kierowanych osobiście do niego, w sposób, który umożliwia dostęp do informacji w przyszłości przez czas odpowiedni do celów, jakim te wiadomości służą, i które pozwalają na odtworzenie przechowywanych w nim informacji w niezmienionej postaci,
- punkt sprzedaży – stałe lub ruchome miejsce prowadzenia sprzedaży imprez turystycznych lub powiązanych usług turystycznych, a także strony internetowe sprzedaży lub punkty sprzedaży online, z uwzględnieniem przypadków, gdy strony i punkty są przedstawiane podróżnym jako jeden punkt obsługi, w tym także usługa dostępna telefonicznie,
- powrót do kraju – powrót podróżnego do miejsca rozpoczęcie przez niego podróży lub do innego miejsca uzgodnionego przez obie strony umowy,
- turystyczny rachunek powierniczy – rachunek powierniczy w rozumieniu ustawy z dnia 29 sierpnia 1997r. – Prawo bankowe (dz. U. z 2017 r. poz. 1876) należący do przedsiębiorcy ułatwiającego nabywanie powiązanych usług turystycznych lub

[78] Zgodnie z definicją zawartą art. 43^1. ustawy z dnia 23 kwietnia 1964r. – Kodeks cywilny (Dz.U. 1964 nr 16 poz. 93) przedsiębiorcą jest osoba fizyczna, osoba prawna i jednostka organizacyjna prowadząca we własnym imieniu działalność gospodarczą lub zawodową.

organizatora turystyki, służący zbieraniu środków pieniężnych wpłacanych przez podróżnych,

- zabezpieczenie finansowe – gwarancja ubezpieczeniowa, gwarancja bankowa, umowa o turystyczny rachunek powierniczy lub umowa ubezpieczenia na rzecz podróżnych,
- nieuniknione i nadzwyczajne okoliczności – sytuacja pozostająca poza kontrolą strony powołującej się na takie zdarzenie, której skutków nie można było uniknąć, nawet w przypadku gdyby podjęto wszelkie rozsądne działania,
- niezgodności – nienależyte wykonanie lub niewykonanie usług turystycznych objętych impreza turystyczną.

4.3. System bezpieczeństwa finansowego biur podróży

Zgodnie z ustawą o usługach turystycznych organizator turystyki oraz pośrednik turystyczny mają obowiązek zapewnienia klientom, na wypadek swojej niewypłacalności, pokrycie kosztów ich powrotu do kraju oraz wzrostu całości lub części wpłat wniesionych tytułem zapłaty za imprezę turystyczną[79].

System bezpieczeństwa finansowego na wypadek niewypłacalności organizatorów turystyki lub pośredników turystycznych składa się z dwóch filarów[80]:

- I filar – tworzy zabezpieczenie finansowe w postaci gwarancji bankowej lub ubezpieczeniowej, umowy ubezpieczenia na rzecz klientów biur lub przyjmowania wpłat na rachunek powierniczy,
- II filar – stanowią środki zgromadzone w Turystycznym Funduszu Gwarancyjnym (TFG).

I filar zabezpieczenia finansowego tworzy m.in. gwarancja bankowa, której udzielenie znajduje podstawę prawną w Ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe, zgodnie z którą banki mogą udzielać gwarancji bankowych na zlecenie. Gwarancja bankowa stanowi jednostronne zobowiązanie banku (gwaranta), że po spełnieniu przez uprawniony do tego

[79] A. Jędrzychowska, *Ubezpieczenia turystyczne*, [w:] *Ubezpieczenia*, pod red. W. Ronka-Chmielowiec, Wydawnictwo C.H. Beck, Warszawa 2016, s. 449.

[80] *Turystyczny Fundusz Gwarancyjny,* (https://www.ufg.pl/infoportal/faces/pages_home-page/Page_3dc12681_156b6b90c42__7ff6/Page_3dc12681_156b6b90c42__7ff5/Page_3dc12681_156b6b90c42__7ff2?_afrLoop=9143258310815940&_afrWindowMode=0&_adf.ctrl-state=k968gqp1s_38), dostęp: 28.04.2018 r.

podmiot (beneficjent gwarancji) określonych warunków zapłaty, bank zrealizuje świadczenie pieniężne na rzecz beneficjenta tej gwarancji.

W praktyce wykorzystanie gwarancji bankowej dla zabezpieczenia wpłat klientów biur podróży związane jest ze wskazaniem beneficjenta gwarancji. Określenie beneficjenta jest konieczne dla sformułowania gwarancji, natomiast w chwili, w której jest wystawiana klienci biura podróżnego nie są jeszcze znani, dlatego nie mogą zostać wskazani w tej gwarancji. Problem ten może być rozwiązany w dwojaki sposób: poprzez określenie podmiotu występującego jako beneficjent udzielanych gwarancji bankowych w interesie przyszłych klientów lub poprzez wymienienie jako beneficjentów wszystkich klientów zlecającego. W praktyce dominuje pierwsze rozwiązanie, a jako beneficjenta wskazuje się wojewodę. To oznacza, że klienci którzy chcą skorzystać z takiej formy zabezpieczenia przedkładanej przez biuro podróży, powinni zgłosić swoje roszczenia do wojewody lub zawiadomić go o konieczności sprowadzenia ich z powrotem do kraju.

W przypadku gwarancji ubezpieczeniowej stosuje się podobne zasady, jednak podstawą jej udzielania dla towarzystw ubezpieczeniowych jest Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, wskazującą gwarancję ubezpieczeniową jako wyodrębnioną grupę ryzyka ubezpieczeniowego – Dział II grupa 15.

Następnym elementem I filaru jest umowa ubezpieczeniowa na rzecz klientów. Umowa ta jest zawierana pomiędzy ubezpieczycielem (zakładem ubezpieczeń) a ubezpieczającym, który z tego tytułu opłaca składkę ubezpieczeniową. Ubezpieczonym może być ubezpieczający albo osoba trzecia wymieniona w umowie ubezpieczenia. Ubezpieczyciel zobowiązany jest do wypłaty określonego świadczenia (zwykle wypłaty odszkodowania) w przypadku, gdy nastąpi określone w umowie przyszłe i niepewne zdarzenie tzw. ryzyko ubezpieczeniowe. Ryzykiem ubezpieczeniowym, przed którym jest chroniony klient będzie sytuacja nie sprowadzenia turysty do kraju wbrew obowiązkowi organizatora, a także utrata wpłaconej opłaty za niewykonane usługi turystyczne. W roli ubezpieczającego występuje organizator turystyki lub pośrednik turystyczny, natomiast klient jest ubezpieczonym.

Inną formę zabezpieczenia finansowego może stanowić rachunek powierniczy. Jest to rachunek bankowy, który tworzą przedsiębiorcy turystyczni, w celu gromadzenia środków finansowych powierzonych im przez osoby trzecie na podstawie odrębnych umów. Umowa

o rachunek powierniczy wyznacza warunki, na jakich pieniądze mogą być wypłacane posiadaczowi rachunku, a w szczególności może określać rodzaj dokumentów lub oświadczeń jakie powinny być w tej sprawie złożone. Wkład finansowy na rachunku powierniczym jest wolny od zajęcia w postepowaniu egzekucyjnym i podlega wyłączeniu z masy upadłościowej, a także nie wchodzi do spadku w razie śmierci posiadacza rachunku. Zastosowanie takiej formy zabezpieczenia wyklucza kredytowanie działalności pośrednika turystycznego lub organizatora turystyki z przedpłat klientów[81].

II filar zabezpieczenia finansowego stanowią środki zgromadzone w Turystycznym Funduszu Gwarancyjnym. Środki Funduszu są gromadzone na wyodrębnionym rachunku w Ubezpieczeniowym Funduszu Gwarancyjnym. Środki te mogą pochodzić z[82]:

- wpłat przedsiębiorców,
- odsetek od środków pieniężnych zgromadzonych na rachunku bankowym,
- przychodów z lokat środków Funduszu realizowanych z zachowaniem najwyższego stopnia bezpieczeństwa, jakości oraz rentowności środków, przy równoczesnym zachowaniu ich płynności,
- środków uzyskanych przez Ubezpieczeniowy Fundusz Gwarancyjny w ramach pożyczek i kredytów na rzecz Funduszu,
- innych wpływów.

Ze środków Turystycznego Funduszu Gwarancyjnego[83]:

- pokrywa się koszty powrotu klientów z imprezy turystycznej do miejsca wyjazdu lub do miejsca planowanego powrotu, w przypadku gdy organizator turystyki lub pośrednik turystyczny nie wywiązuje się z obowiązku i nie zapewnia tego powrotu,
- dokonuje się zwrotu środków klientom, którzy wnieśli wpłaty tytułem zapłaty za imprezę turystyczną, w przypadku gdy z winy organizatora turystyki bądź pośrednika turystycznego impreza nie została lub nie zostanie zorganizowana,

[81] J. Raciborski, *System zabezpieczeń finansowych na rzecz klientów, organizatorów imprez turystycznych i pośredników*, Ministerstwo Gospodarki i pracy, (www.sot.org.pl/web_documents/publikacja_13.pdf), dostęp: 25.03.2018 r.
[82] Ustawa z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz.U. 1997 Nr 133 poz. 884, z późn. zm.).
[83] *Turystyczny Fundusz Gwarancyjny, op. cit.*

– zapewnia się klientom zwrot części wpłat, którą wnieśli tytułem zapłaty za imprezę turystyczną, w przypadku gdy z winy organizatora turystyki bądź pośrednika turystycznego impreza nie została lub nie zostanie zorganizowana.

4.4. Ryzyka w turystyce

Działalność związana z turystyką i rekreacją wiąże się z ryzykiem, które może zagrażać zarówno podmiotom gospodarczym, jak i osobom fizycznym. Ryzyko może przyjmować rozmaite formy, a jego skutki potrafią być odczuwane przez bardzo długi czas. Z punktu widzenia działalności ubezpieczeniowej istotna jest klasyfikacja ryzyka, która została przedstawiona w Tabeli 4.1[84].

Tabela 4.1. Klasyfikacja ryzyka w działalności turystycznej.

Kryterium podziału	Rodzaje ryzyka
Charakter strat	• Finansowe • Niefinansowe
Wpływ czasu na ryzyko	• Statyczne • Dynamiczne
Źródła ryzyka (ilościowe i jakościowe)	• Fundamentalne • Partykularne
Konsekwencje ryzyka	• Czyste • Spekulatywne
Możliwość kwantyfikacji ryzyka	• Probabilistyczne • Estymacyjne
Źródła niebezpieczeństwa	• Przyrodnicze • Społeczne
Przedmiot ubezpieczenia	• Osobowe • Majątkowe
Sytuacja turysty	• Statystyczne • Technogenne • Antropogenne

Źródło: opracowanie własne na podstawie M. Sobczyk, *Ubezpieczenia w turystyce i rekreacji*, Difin, Warszawa 2013, s. 226.

Ryzyko finansowe generuje straty, które da się ocenić wartościowo. Najczęściej występuje w ubezpieczeniach majątkowych (np. zaginięcie bagażu podczas podróży). Ryzyko

[84] M. Sobczyk, *Ubezpieczenia w turystyce i rekreacji*, Warszawa Difin, Warszawa 2013, s. 224.

niefinansowe to takie, którego skutków nie można oszacować w sposób bezpośredni. Przykładowo, nieszczęśliwy wypadek, który spotkał turystę można zaliczyć do ryzyka finansowego (w przypadku, gdy wystąpił uszczerbek na zdrowiu np. złamanie ręki, nogi, wstrząs mózgu) lub niefinansowego (jeśli nie spowodował żadnych szkód)[85].

Ryzyko statyczne występuje niezależnie od czasu. Wiąże się z brakiem postępu ekonomicznego, technologicznego czy cywilizacyjnego. Jest to sytuacja raczej hipotetyczna np. zejście lawiny, wynikające z naturalnych procesów zachodzących w środowisku. Natomiast ryzyko dynamiczne może generować straty w skali jednostki, a także w całej zbiorowości. Jest ono kreowane przez modę, zachowania nabywców produktów turystycznych, zmiany cen itp.

Ryzyko fundamentalne dotyczy większych zbiorowości ludzkich lub całego społeczeństwa. Człowiek jest pośrednim adresatem tego ryzyka. Przykładem ryzyk fundamentalnych są trzęsienia ziemi, powodzie, pożary, huragany, wojny, rozruchy społeczne[86]. Skutkiem ryzyka fundamentalnego ostatnich czasów jest zmniejszona ilość wyjazdów turystycznych w rejony Turcji ze względu na panujące tam działania wojenne[87]. Ryzyko partykularne powoduje natomiast straty o charakterze indywidualnym, a źródłem jego powstania jest najczęściej aktywność poszczególnych jednostek np. podpalenie, rabunek, kradzież itp.

Ryzyko czyste powoduje stratę (gdy zostanie zrealizowane) lub nie dostarcza żadnych korzyści (jeśli nie zostanie zrealizowane). W praktyce tylko ryzyka czyste mogą być objęte ochroną ubezpieczeniową. Poza tym są one w wysokim stopniu mierzalne, a co się z tym wiąże przewidywalne z wysokim prawdopodobieństwem. Ryzyko spekulatywne odnosi się za to do tzw. wariancji potrójnej. Realizacja tego ryzyka uzasadnia oczekiwane korzyści lub poniesienie straty. Natomiast ryzyko niezrealizowane to brak straty lub zysku.

Ryzyko probabilistyczne ocenia się z wykorzystaniem metod matematycznych lub statystycznych opierając się o informacje liczbowe pochodzące z przeszłości. Takie szacunki można zastosować w przypadku wypadków samochodowych, złamań kończyn itp. Ryzyko estymacyjne jest nieubezpieczalne, ponieważ bardzo trudno jest oszacować

[85] *Ibidem*, s. 225.
[86] *Ibidem*, s. 226.
[87] *Turcja traci turystów przez politykę*, (http://wyborcza.pl/7,75399,22009657,turcja-traci-turystow-przez-polityke-w-ciagu-dwoch-lat-ich.html), dostęp: 01.05.2018 r.

prawdopodobieństwo z jakim się zrealizuje. Uznaje się, że ryzyko estymacyjne jest nieprzewidywalne, a tym samym niedające się ubezpieczyć.

Ryzyko przyrodnicze kreuje natura. Wiąże się z działaniem sił przyrody (np. ryzyko burzy śnieżnej, gwałtownego pogorszenia się pogody podczas wędrówki górskiej, zejście lawiny śnieżnej podczas jazdy na nartach). W przypadku ryzyka społecznego ryzyko związane jest z człowiekiem lub społeczeństwem np. zagrożenie skażeniem związane ze składowaniem toksycznych substancji.

Ryzyko osobowe wyrządza uszczerbek w dobrach osobistych turysty np. w życiu lub zdrowiu. Ryzyko majątkowe zaliczane jest do tzw. ryzyk pozostałych, które zagrażają mieniu np. kradzież walizki, pożar w wyniku, którego turysta traci sprzęt sportowy itp.

Ostatnie kryterium podziału wyróżnia ryzyko statystyczne, które wiąże się ze złożonością przyrody oraz brakiem możliwości prognozowania przyszłych wydarzeń z odpowiednią dokładnością[88]. Ryzyko technogenne związane jest z wykorzystywaniem przez turystę sprzętu oraz urządzeń technicznych (np. katastrofa kolejki linowej). Ostatnim typem ryzyka jest ryzyko antropogenne, które uwarunkowane jest decyzjami podejmowanymi przez turystę, a także jego poczuciem odpowiedzialności np. lekkomyślność, brawura czy nieliczenie się z własnymi siłami np. podczas skoków do wody z dużej wysokości)[89].

4.5. Możliwości ograniczenia niektórych rodzajów ryzyka w turystyce wynikające z ustanowienia Unii Europejskiej.

Ochronę przed kosztami leczenia za granicą może zapewnić turyście karta EKUZ. Z związku z akcesją Polski do Unii Europejskiej pojawiła się Europejska Karta Ubezpieczenia Zdrowotnego (EKUZ). Na jej podstawie turyści otrzymują prawo do bezpłatnych podstawowych świadczeń zdrowotnych w krajach UE oraz na obszarze EFTA (Europejskie Stowarzyszenie Wolnego Handlu). EKUZ stanowi dowód, że podróżujący jest uprawniony do świadczeń zdrowotnych w ramach systemu zabezpieczenia społecznego w swoim kraju,

[88] Ryzyko ubezpieczeniowe, (http://www.gu.com.pl/index.php?option=com_content&view=article&id=8913&catid=129:rynek-ubezpieczeniowy&Itemid=151) dostęp: 01.05.2018 r.
[89] M. Sobczyk, *op.cit.*, s. 228.

a także zapewnia zgodę ubezpieczyciela na pokrycie kosztów leczenia w trakcie pobytu za granicą.

Osoby posiadające Europejską Kartę Ubezpieczenia Zdrowotnego są uprawnione do otrzymania świadczeń zdrowotnych, które okażą się niezbędne z medycznego punktu widzenia podczas pobytu na terenie innego państwa członkowskiego, uwzględniając przy tym charakter świadczeń oraz przewidywany czas trwania pobytu. Zakres niezbędnych dla danej osoby świadczeń ustala każdorazowo lekarz. Podróżującemu należy udzielić niezbędnej pomocy medycznej, która umożliwi mu kontunuowanie wyjazdu bez konieczności powrotu do kraju w celu leczenia. Innymi słowy, oznacza to, że nie można stawiać pacjenta w sytuacji, w której byłby zmuszony do powrotu do swojego państwa na leczenie[90].

EKUZ przysługuje wszystkim ubezpieczonym w Narodowym Funduszu Zdrowia. Próbując porównać ją jednak z komercyjnym ubezpieczeniem turystycznych, należy wskazać kilka jej słabości[91]:

- EKUZ obowiązuje jedynie na terenie państw UE oraz w obszarze EFTA, dlatego osoby wyjeżdzające do innych krajów są pozbawione możliwości korzystania z niej,
- EKUZ uprawnia jedynie do korzystania z opieki medycznej w placówkach, które działają w ramach publicznego systemu opieki zdrowotnej w danym kraju,
- EKUZ nie zapewnia całości zwrotu poniesionych kosztów. W większości państw Unii Europejskiej pacjenci publicznej służby zdrowia uczestniczą w kosztach leczenia, dlatego podróżujący posiadający EKUZ muszą uwzględniać ewentualność częściowej partycypacji w kosztach leczenia,
- Zakres komercyjnego ubezpieczenia jest o wiele szerszy niż możliwości, które daje Europejska Karta Ubezpieczenia Zdrowotnego. Przykładowo EKUZ nie obejmuje usługi assistance medycznego czy sposobności skorzystania z telefonu alarmowego, który w ubezpieczeniach komercyjnych działa całą dobę.

Pewne ograniczenia i trudności EKUZ m.in. długi czas oczekiwania na pomoc, konieczność odpłatnego nabycia leków, brak pokrycia kosztów transportu chorego itp. stworzyły potrzebę

[90] *Wypoczynek w państwach członkowskich UE/EFTA*, (https://www.ekuz.nfz.gov.pl/faq/wypoczynek-w-panstwach-czlonkowskich-ue-efta), dostęp: 01.05.2018 r.
[91] A. Bera, *Analiza rynku ubezpieczeń turystycznych wybrane aspekty*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2008, Nr 521.

zawierania prywatnych ubezpieczeń KLZ (kosztów leczenia za granicą). Posiadanie prywatnego ubezpieczenia KLZ pozwala na uniknięcie konieczności poniesienia wysokich kosztów opieki medycznej (oraz kosztów z nią związanych), które nie są refundowane w ramach Europejskiej Karty Ubezpieczenia Zdrowotnego[92]. Przykładowe koszty leczenia w wybranych krajach Unii Europejskiej zostały przedstawione w Tabeli 4.2.

Tabela 4.2. Przykładowe koszty leczenia w wybranych krajach Unii Europejskiej (w EUR) według stanu na 08.2016.

Kraj	Złamanie ręki/nogi	Poparzenie słoneczne	Drobny zabieg chirurgiczny	Zatrucie pokarmowe	Dzienny pobyt w szpitalu na oddziale chirurgicznym	Dzienny pobyt w szpitalu na intensywnej terapii
Austria	100-3500	100-200	300-1500	100-250	500-1500	1 000-2000
Chorwacja	50-300	15-50	50-500	20-50	70-500	300 -1000
Francja	100-1500	50-200	200-1000	50-200	500-1500	1 000-2000
Grecja	100-1000	50-200	50-1000	50-250	200-800	300-1000
Hiszpania	100-1000	50-200	200-1000	50-250	250-800	500-1000
Niemcy	100-1000	50-200	200-1000	50-250	500-1500	1 000-2000
Wielka Brytania	150-1200	50-200	200-1000	50-250	500-1500	1 000-2000
Włochy	75-1000	50-200	200-1000	50-250	300-1000	800-1500

Źródło: opracowanie własne na podstawie *Koszty leczenia ambulatoryjnego za granicą,* (http://warta-ubezpieczenia.pl/wp-content/uploads/2016/08/Koszty-leczenia-ambulatoryjnego-za-granic%C4%85_lato.pdf), dostęp: 31.03.2018 r.

Tabela 4.2 przedstawia przykładowe koszty leczenia w wybranych krajach Unii Europejskiej wyrażone w euro. Najwyższe koszty leczenia dotyczą dziennego pobytu w szpitalu na oddziale intensywnej terapii, wynika to z zaangażowania drogiego sprzętu oraz personelu medycznego. Wśród analizowanych państw najwyższe koszty cechują Francję, Grecję i Wielką Brytanię, natomiast najtańsze koszty leczenia występują w Chorwacji.

Koszty transportu chorego przedstawia Tabela 4.3.

[92] E. Kowalewski, *Ubezpieczenia turystyczne*, Wyższa Szkoła Bankowa w Toruniu, (http://www.wsb.pl/sites/wsb.pl.torun/files/biblioteka/10.pdf), dostęp: 24.03.2018 r.

Tabela 4.3. Przykładowe koszty transportu chorego w wybranych krajach Unii Europejskiej (w EUR i PLN) według stanu na 08.2016.

Kraj	Transport sanitarny za granicą z miejsca zdarzenia do palcówki medycznej – w zależności od odległości (w EUR)	Repatriacja ambulansem – w zależności od wyposażenia ambulansu, odległości oraz kwalifikacji załogi (w PLN)	Repatriacja samolotem – w zależności od: bez asysty, z asystą cywilną, z asystą medyczną (w PLN)
Austria	100-800	3 000-8 000	2 000-12 000
Chorwacja	40-300	6 000-12 000	2 000-12 000
Francja	100-500	6 000-12 000	2 000-12 000
Grecja	50-300	7 000-15 000	2 000-12 000
Hiszpania	80-400	9 000-20 000	2 000-12 000
Niemcy	80-600	1 000-10 000	1 000-10 000
Wielka Brytania	100-400	5 000-18 000	2 000-12 000
Włochy	80-500	6 000-15 000	2 000-12 000

Źródło: opracowanie własne na podstawie *Koszty leczenia ambulatoryjnego za granicą,* (http://warta-ubezpieczenia.pl/wp-content/uploads/2016/08/Koszty-leczenia-ambulatoryjnego-za-granic%C4%85_lato.pdf), dostęp: 31.03.2018 r.

Tabela 4.3 przedstawia przykładowe koszty transportu chorego w wybranych krajach Unii Europejskiej wyrażone w euro oraz polskich złotych. Z powyższych danych wynika, że powyższe koszty cechuje duży przedział cenowy. Uwarunkowane jest to wieloma czynnikami np. w przypadku repatriacji ambulansem koszt transportu chorego zależy od wyposażenia ambulansu, odległości, a także kwalifikacji załogi. W przypadku kosztu transportu chorego ambulansem najwyższa górna granica występuje w Hiszpanii. Natomiast w przypadku transportu sanitarnego do placówki medycznej najwyższe koszty można ponieść w Austrii. Analizując repatriację samolotem można zauważyć, że w przypadku wszystkich krajów przedziały kosztów są do siebie zbliżone.

4.6. Ubezpieczenia turystyczne

Nauka o ubezpieczeniach nie określa definicji ubezpieczeń turystycznych. Również w przepisach, które tworzą kanon prawa ubezpieczeniowego nie została wyodrębniona ta grupa ubezpieczeń. W praktyce można najogólniej stwierdzić, iż ubezpieczenia turystyczne to

te, które służą zaspokojeniu potrzeb finansowych (zarówno gospodarstw domowych jak i przedsiębiorstw) oraz powstają w związku z realizacją ryzyka specyficznego dla podmiotu, który podejmuje aktywność w ramach turystyki i rekreacji[93].

Ubezpieczenia turystyczne chronią wszystkie dobra, które są narażone na uszczerbek w związku z podróżą (w tym amatorskim uprawianiem sportów). Dobra te to życie, a także środki finansowe i majątek towarzyszący podróżnym podczas wyjazdu (bagaż, sprzęt, samochód) lub w niego zaangażowany (np. zaliczka). Ubezpieczenia turystyczne nie są produktem standardowym, bowiem ich zakres, okres i przedmiot są dostosowywane indywidualnie do potrzeb ubezpieczeniowych klienta. Są one szczególnie ważne dla osób, które planują wyjazd za granicę.

Przedmiotem ubezpieczeń mogą być wydatki powstałe po stronie podróżującego, takie jak:

- koszty związane z nagłą chorobą lub powypadkowym leczeniem obrażeń,
- koszty związane z transportem wyniku nagłej choroby do kraju lub miejsca zamieszkania w celu dalszego leczenia, a także z powypadkowym transportem medycznym,
- wydatki poniesione na akcję ratowniczą lub poszukiwawczą,
- koszty pomocny prawnej w przypadku wejścia w konflikt z miejscowym prawem,
- koszty naprawy uszkodzonego sprzętu lub koszty korzystania z wypożyczalni sprzętu,
- wydatki na kupno nowego sprzętu, utraconego bagażu bądź jego składników na skutek ich trwałej utraty lub uszkodzenia, a także kradzieży,
- inne wydatki, które ubezpieczony musiałby ponieść na skutek wyrządzonej przez niego szkody innej osobie (np. gdy ze swojej winy uszkodzi sprzęt innej osoby).

Należy również pamiętać, że szkoda finansowa może powstać w przypadku utraty wpłaconej zaliczki, dokonanych przedpłat lub wydatków związanych z koniecznością wcześniejszego powrotu do kraju. Wymienione wydarzenia mogą powstać na skutek jednego wypadku, a dodatkowo także generować większe i bardziej dotkliwe straty.

[93] M. Gasińska, *Ubezpieczenia turystyczne w systemie ubezpieczeń gospodarczych*, „Zeszyty Naukowe Uczelni Vistula" 2013, Nr 32, s. 54.

Oferty ubezpieczycieli w ramach turystyki są zróżnicowane pod względem zakresu udzielanej ochrony, przedmiotu ubezpieczenia, a co się z tym wiąże także wysokości składki. Niektóre produkty zawierają podstawowy zakres ryzyka, inne natomiast oferują opcje dodatkowe i włączają w zakres ochrony ryzyka mniej typowe. Zakłady ubezpieczeń dostosowują oferty ubezpieczeniowe do rodzaju wypoczynku (np. związane z uprawianiem narciarstwa), wieku uczestników (np. pakiety dla studentów wyjeżdzających za granicę), specjalizacji programu (np. pielgrzymki) lub częstotliwości wyjazdów (tzw. pakiety business)[94]. Wybierając ofertę ubezpieczeniową należy zwrócić uwagę na rządzące nimi zasady, tzn. sytuacje w jakich można ubiegać się o odszkodowanie, wysokość sumy ubezpieczenia (kwot do których odpowiada ubezpieczyciel), katalog wyłączeń z zakresu ochrony ubezpieczeniowej oraz zakres terytorialny, w ramach którego obowiązuje ubezpieczenie. Z tego powodu kluczowe jest zapoznanie się z OWU (Ogólne Warunki Ubezpieczenia). Zawierając umowę ubezpieczenia należy wiedzieć, iż ubezpieczyciel nie pokryje wszystkich kosztów w każdym zdarzeniu (np. stan po spożyciu alkoholu skutkuje brakiem ochrony ubezpieczeniowej). Szczególnie ważne powinno być uważne czytanie warunków ubezpieczenia dotyczących kosztów leczenia i NNW (Następstwa Nieszczęśliwych Wypadków) przez osoby cierpiące na przewlekłe schodzenia. W razie potrzeby mogą one wykupić wariant z rozszerzeniem ochrony ubezpieczeniowej.

W przypadku ubezpieczeń turystycznych bardzo ważne jest zbieranie wszystkich dowodów potwierdzających zdarzenie wypadkowe oraz jego skutki takich jak: oryginalne rachunki, zaświadczenia medyczne oraz dowody opłat za udzieloną pomoc zdrowotną[95].

Najczęściej oferta dla wyjeżdzających osób konstruowana jest w formie pakietowej. Oznacza to objęcie jedną polisą kilku odmian i rodzajów ubezpieczeń, często odbiegających od siebie zasadniczo przedmiotem ochrony (np. Assistance, OC, mienia). Ubezpieczenia te oferowane są łącznie, a przyjęcie oferty skutkuje zawarciem jednej umowy ubezpieczenia. Ubezpieczenie pakietowe najczęściej oferuje atrakcyjniejsze składki, z reguły niższe, aniżeli suma składek należnych z tytułu zawarcia osobno każdej umowy wchodzącej w skład pakietu.

[94] A. Jędrzychowska, *op. cit.*, s. 441.
[95] *Ibidem*, s. 442.

Ponadto ubezpieczenia pakietowe upraszczają proces zawierania umów, które nie muszą być z osobna negocjowane i opłacane przez ubezpieczającego[96].

W dalszej części artykułu zostaną omówione najczęstsze składowe ubezpieczeń pakietowych, takie jak: ubezpieczenie NNW, ubezpieczenie odpowiedzialności cywilnej – komunikacyjnej i w życiu prywatnym, ubezpieczenie assistance – świadczenia pomocowe, ubezpieczenie kosztów leczenia za granicą, ubezpieczenie kosztów akcji ratowniczej i poszukiwawczej, ubezpieczenie sprzętu sportowego i bagażu oraz ubezpieczenie kosztów rezygnacji z uczestnictwa w wyjeździe lub wcześniejszego powrotu.

Ubezpieczenie następstw nieszczęśliwych wypadków najczęściej znajduje się w pakietach ubezpieczeń turystycznych. Jego przedmiotem są następstwa nieszczęśliwych wypadków powodujące uszkodzenie ciała, rozstrój zdrowia, trwały uszczerbek lub śmierć ubezpieczonego w trakcie wyjazdu. Podstawowymi świadczeniami wypłacanymi w przypadku trwałego uszczerbku na zdrowiu są: przy uszczerbku wynoszącym 100% oraz w wypadku śmierci – pełna suma ubezpieczenia, a w sytuacji częściowego uszczerbku na zdrowiu (np. złamanie ręki) – ustalony procent sumy ubezpieczenia odpowiadający procentowi trwałego uszczerbku[97]. Produkt ten jest szczególnie ważny przy podróżach związanych z turystyką sportową np. wyjazd na narty, wspinaczkę lub rejs. Każdorazowo należy wtedy ustalić z ubezpieczycielem czy wypadek związany z uprawianiem tej dyscypliny sportu jest objęty ochroną czy podlega wyłączeniu jako sport ekstremalny[98].

Zakupienie ubezpieczenia NNW w ramach pakietu nie koliduje z posiadaniem tego ubezpieczenia w miejscu nauki (np. ubezpieczenie NNW w ramach karty Euro21) lub w ramach ubezpieczenia do polisy na życie. Jest to bowiem produkt ubezpieczenia osobowego, w którym nie występuje program związany z ograniczeniem świadczenia limitem wartości przedmiotu ubezpieczenia. Innymi słowy w sytuacji zaistnienia wypadku wypłacone mogą być świadczenia z każdej polisy, która mieściła to zdarzenie w swojej definicji ubezpieczonego wypadku.

[96] E. Kowalewski, *op. cit.*
[97] A. Jędrzychowska, *op. cit.*, s. 442.
[98] Sporty ekstremalne to sporty, których uprawianie wiąże się z większym ryzykiem niż w przypadku uprawiania innych dyscyplin sportowych. Zazwyczaj wymagają od sportowca ponad przeciętnych zdolności fizycznych oraz psychicznych, a także odpowiedniego przygotowania. M. Sekida, *Turystyka ekstremalna vs. sporty ekstremalne*, (ojs.ukw.edu.pl/index.php/johs/article/download/4112/pdf), dostęp: 24.03.2018 r.

Kolejnym rodzajem ubezpieczenia wchodzącego w skład ubezpieczenia pakietowego jest ubezpieczenie odpowiedzialności cywilnej – komunikacyjnej i w życiu prywatnym. Mówiąc o odpowiedzialności cywilnej w trakcje wyjazdu, ma się na myśli odpowiedzialność wynikającą z prowadzenia pojazdu w czasie wyjazdu oraz odpowiedzialność za postępowanie w trakcie tego wyjazdu np. spowodowanie uszczerbku na czyimś ciele lub majątku (zamierzone lub wynikłe z nieuwagi)[99].

Wysokość zadośćuczynienia zależy nie tylko od rzeczywiście poniesionej szkody przez poszkodowanego, ale również od zwrotu tzw. utraconych korzyści (np. utracone zarobki w skutek pobytu w szpitalu). W przypadku szkody na osobie kwota należnego odszkodowania obejmuje także zwrot wszelkich wynikłych z tego powodu kosztów (np. koszty leczenia w szpitalu, koszty rehabilitacji). Dodatkowy koszt, z którym musi się liczyć sprawca stanowi również zadośćuczynienie dla poszkodowanego za doznaną krzywdę[100]. Należy również mieć na uwadze, że w granicy odpowiedzialności rodziców mieszczą się szkody, które powstały z winy ich nieletnich dzieci (np. podczas zabaw na plaży czy przy basenie). W przypadku uszkodzenia przez dzieci bądź osoby dorosłe czyjegoś ciała, spowodowania inwalidztwa lub śmierci (tzw. szkody na osobie), a także w razie zniszczenia czyjejś własności (tzw. szkody rzeczowe), zakład ubezpieczeń wypłaci tej osobie odszkodowanie.

Kolejnym przykładem ubezpieczenia wchodzącego w skład pakietu jest ubezpieczenie assistance - świadczenia pomocowe. Świadczenia te są dokładnie opisywane w Ogólnych Warunkach Ubezpieczenia, w których znajdują się wymogi na jakich ubezpieczony może z tych świadczeń skorzystać, a także zasady ich przyznawania – należy pamiętać, że są one ograniczone różnorodnie kształtowanymi limitami kwotowymi. W zależności od rodzaju umowy najczęściej występują następujące świadczenia[101]:

- pokrycie kosztów pobytu osoby towarzyszącej poszkodowanego w razie jego wypadku lub pobytu w szpitalu,
- koszty związane z podróżą, zakwaterowaniem, wyżywieniem osoby wskazanej przez ubezpieczonego, czy też jego opiekuna prawnego,

[99] A. Jędrzychowska, *op. cit.*, s. 443.
[100] *Ibidem*, s. 443.
[101] *Ubezpieczenia* turystyczne, (https://www.rf.gov.pl/vademecum-klienta/abc-ubezpieczen/Ubezpieczenia_turystyczne__20070#klz), dostęp: 02.05.2018 r.

- zwrotna pożyczka na kaucję – w sytuacji aresztowania ubezpieczonego,
- opieka nad nieletnimi dziećmi – w sytuacji, gdy podróżujący przebywał z dziećmi. W takich wypadkach ubezpieczyciel zapewnia dzieciom opiekę, a w uzasadnionych przypadkach pokrywa koszty ich transportu do miejsca zamieszkania,
- pomoc w razie kradzieży lub zgubienia dokumentów, środków pieniężnych bądź kart płatniczych,
- pokrycie kosztów zastępczego kierowcy – w przypadku, gdy stan zdrowia ubezpieczonego nie pozwala na prowadzenie pojazdu, którym podróżował,
- przekazanie osobom wskazanym przez ubezpieczonego istotnych wiadomości dotyczących przebiegu wyjazdu, nieprzewidzianych zdarzeń, choroby lub wypadków,
- sprowadzenie niezbędnych przedmiotów osobistych oraz leków,
- transport zwłok ubezpieczonego do miejsca pochówku w kraju.

Następnym przykładem ubezpieczenia turystycznego jest ubezpieczenie kosztów leczenia za granicą. Zapewnia ono pokrycie przez ubezpieczyciela kosztów związanych z leczeniem szpitalnym lub ambulatoryjnym podróżującego, a także zwrot wydatków poniesionych na leki lub inne świadczenia opieki medycznej. Należy szczególnie podkreślić, że koszty te muszą wystąpić w związku z zaistniałym wypadkiem lub w połączeniu z nagłym zachorowaniem. Ważnym elementem tego typu produktu, jest ustalenie odpowiedniej maksymalnej kwoty (sumy ubezpieczenia), do której zakład ubezpieczeń ponosi odpowiedzialność. Limit ten powinien stanowić sumę, która rzeczywiście zabezpieczy pełne pokrycie kosztów leczenia bez konieczności wkładu własnych środków pieniężnych. Jest to związane z faktem, że koszty leczenia w krajach, do których udają się polscy podróżni, w znacznej części nie należą do niskich, a ich pokrycie z własnej kieszeni byłoby uciążliwe lub niemożliwe.

Istotna jest także forma, w jakiej ubezpieczyciel dokona pokrycia wyżej wymienionych kosztów. Najwygodniejszym rozwiązaniem jest automatyczne pokrycie kosztów leczenia poszkodowanego, bez konieczności ponoszenia przez niego własnych nakładów finansowych, a następnie ubiegania się o ich refundację. W tego rodzaju ubezpieczeniach często wprowadzany jest minimalny limit od którego zaczyna działać ubezpieczenie (np. równowartość 100 euro). Bardzo ważna jest również możliwość skorzystania przez poszkodowanego z centrum alarmowego, które w razie wypadku koordynuje całą pomoc

medyczną, wybiera szpital oraz zapewnia transport medyczny. Zwykle w ramach ubezpieczenia kosztów leczenia za granicą lub jako odrębne ubezpieczenie, oferuje się wspomniane wcześniej dodatkowe świadczenia pomocowe (assistance)[102].

Kolejnym przykładem ubezpieczenia może być ubezpieczenie kosztów akcji ratowniczej i poszukiwawczej. Koszty takich działań pojawiają się jako część pakietów assistance, ubezpieczeń związanych ze zwrotem kosztów leczenia lub jako odrębna forma ubezpieczenia. Ubezpieczenie to ma na celu pokrycie kosztów związanych z przeprowadzeniem akcji ratowniczej i poszukiwawczej w celu ratowania życia i zdrowia podróżującego, a także udzielenia doraźnej pomocy medycznej na miejscu wypadku. Do działań ratowniczych często zaangażowany jest ciężki i drogi sprzęt, przez co koszty takich akcji mogą osiągać wysokie kwoty. To ubezpieczenie jest więc szczególnie istotne w przypadku wypoczynku w górach lub na morzu.

W trakcie wyjazdu równie ważnym może okazać się ubezpieczenie sprzętu sportowego i bagażu. Obejmuje ono ryzyko ich zniszczenia, uszkodzenia lub utraty w wyniku zdarzeń losowych (np. lawina, pożar, huragan). W momencie ustalania sumy ubezpieczenia bardzo ważne jest wzięcie pod uwagę wartości bagażu i sprzętu. Warto również zaznaczyć, że najczęściej zakres ochrony ubezpieczeniowej jest ograniczony do sytuacji, w których kradzież jest mało prawdopodobna (np. gdy bagaż znajduje się pod opieką właściciela lub w zamkniętym sejfie). W przypadku skradzionego sprzętu, po wypłacie odszkodowania zakład ubezpieczeń może pomniejszyć świadczenie pieniężne o stopień amortyzacji utraconej rzeczy.

W skład ochrony ubezpieczeniowej często nie wchodzą pieniądze w gotówce, papiery wartościowe, karty płatnicze, bilety, biżuteria, dzieła sztuki, sprzęt komputerowy, lekarstwa itp. Ponadto ubezpieczyciel nie odpowiada za szkody wynikające za uszkodzenia rzeczy związane z ich używaniem, powstałe na skutek kradzieży z użyciem dorabianych kluczy, polegające wyłącznie na uszkodzeniu bagażu, a także powstałe na skutek konfiskaty lub zatrzymania przez służby celne.

Ostatnim z omawianych ubezpieczeń jest ubezpieczenie kosztów rezygnacji z uczestnictwa w wyjeździe lub wcześniejszego powrotu. Gwarantuje ono rekompensatę wydatków poniesionych przez turystę w związku z podróżą (np. zaliczka, rata wpłaty),

[102] A. Jędrzychowska, *op.cit*., s. 446.

w przypadku gdy jest on zmuszony do rezygnacji z udziału w wyjeździe z powodu określonych zdarzeń. Powody te należy odpowiednio i szczegółowo udokumentować.

Szczególne przypadku, w których można skorzystać z tej formy ubezpieczenia są precyzyjnie określone w OWU. Do przykładowych należą: ciężki wypadek, śmierć bliskiego krewnego, kradzież dokumentów uprawniających do podróży itp. W ramach tego ubezpieczenia można także zapewnić sobie zwrot środków za niewykorzystany okres podróży, jeżeli ze wskazanych w OWU powodów nastąpiła konieczność wcześniejszego powrotu do kraju[103].

4.7. Identyfikacja kluczowych czynników różnicujących zakres ubezpieczenia i ich wpływ na koszty ubezpieczenia na przykładzie PZU Wojażer

Zakłady ubezpieczeń posiadają szeroką ofertę ubezpieczeń turystycznych, które pozwalają na finansowe zabezpieczenie podróży. Do analizy ubezpieczeń turystycznych wybrano ofertę firmy PZU SA, która jest najstarszą, najbardziej doświadczoną, a także największą firmą ubezpieczeniową w Polsce[104]. Ubezpieczenie turystyczne można zakupić stacjonarnie, a także przez stronę internetową np. na dedykowanej witrynie https://www.pzu.pl/produkty/ubezpieczenie-wojazer. Ubezpieczenie PZU Wojażer dopasowuje ofertę odpowiednio do potrzeb podróżującego. Najpierw należy jednak uzupełnić podstawowe dane, takie jak[105]:

1. Kierunek wyjazdu:
   - Polska – tylko wyjazdy zorganizowane,
   - Europa i kraje basenu Morza Śródziemnego,
   - Świat oprócz USA,
   - Świat.
2. Cel wyjazdu:
   - Wypoczynek, zwiedzanie, sporty rekreacyjne,

[103] *Ubezpieczenia turystyczne, op.cit.*
[104] *Firma ubezpieczeniowa PZU – informacje*, (https://www.pzu.pl/grupa-pzu/pzu-sa), dostęp: 26.04.2018 r.
[105] *PZU Wojażer,* (https://moje.pzu.pl/pzu/travel?mcid=p_pzu_pl&_ga=2.82721490.559090199.1522682237-606227484.1522682237), dostęp: 02.04.2018 r.

- Nauka, delegacja, praca biurowa,
- Praca fizyczna,
- Narty, snowboard rekreacyjnie,
- Sporty wysokiego ryzyka,
- Wyczynowe uprawianie sportu.

3. Podróżujący:

- Liczba wyjeżdzających osób,
- Choroba przewlekła,
- Uczeń lub student.

4. Termin wyjazdu.

W dalszej części artykułu zaprezentowano warianty ubezpieczenia biorąc pod uwagę cztery kryteria: kierunek wyjazdu, cel wyjazdu, podróżujący oraz termin wyjazdu. Dane mają charakter szacunkowy i posłużą do dalszej analizy tematu.

Tabela 4.4 przedstawia ofertę ubezpieczeniową PZU Wojażer z uwzględnieniem kryterium kierunku wyjazdu.

Tabela 4.4. Oferta ubezpieczeniowa PZU Wojażer z uwzględnieniem kryterium kierunku wyjazdu według stanu na dzień 02.04.2018 r.

Kierunek wyjazdu	Oferta 1	Oferta 2	Oferta 3
Polska	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 10 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: brak Ubezpieczenie bagażu: brak **Cena pakietu: 15,75 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 10 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 50 000 zł Ubezpieczenie bagażu: brak **Cena pakietu: 25,55 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 10 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony, Rowerzysta NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 70 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 2 000 zł **Cena pakietu: 37,94 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,16%**	**0,26%**	**0,38%**

Europa i kraje basenu Morza Śródziemnego	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 120 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: brak Ubezpieczenie bagażu: brak **Cena pakietu: 30,45 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 160 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 100 000 zł Ubezpieczenie bagażu: brak **Cena pakietu: 47,25 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 200 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony, Rowerzysta NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 100 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 3 000 zł **Cena pakietu: 69,30 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,03%**	**0,03%**	**0,03%**
Świat oprócz USA	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 160 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: brak Ubezpieczenie bagażu: brak **Cena pakietu: 45,85 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 180 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 150 000 zł Ubezpieczenie bagażu: brak **Cena pakietu: 69,16 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 200 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 300 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 5 000 zł **Cena pakietu: 98,21 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,03%**	**0,04%**	**0,05%**
Świat	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 300 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: brak	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 400 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 150 000 zł	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 500 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 350 000 zł

	Ubezpieczenie bagażu: brak **Cena pakietu: 71,05 zł**	Ubezpieczenie bagażu: brak **Cena pakietu: 110,60 zł**	Ubezpieczenie bagażu: suma ubezpieczenia 5 000 zł **Cena pakietu: 158,55 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,02%**	**0,03%**	**0,03%**

Źródło: opracowanie własne na podstawie *PZU Wojażer,* (https://moje.pzu.pl/pzu/travel?mcid=p_pzu_pl&_ga=2.82721490.559090199.1522682237-606227484.1522682237), dostęp: 02.04.2018 r.

Ubezpieczenie przedstawione w Tabeli 4.4 zostało przygotowane dla 23 letniej osoby, która zamierza wyjechać na 7 dniowy urlop z początkiem lipca w celu wypoczynku, zwiedzania oraz uprawiania sportów rekreacyjnych. Podróżujący nie choruje przewlekle oraz nie jest uczniem/studentem. Z powyższych danych wynika, że najdroższa cena pakietu ubezpieczeniowego dotyczy podróży na cały świat (zakres terytorialny obejmuje cały świat oraz terytorium Polski w związku z bezpośrednią podróżą z domu poza granice Rzeczypospolitej Polski i z powrotem)[106]. Wysoka cena ubezpieczenia wynika z wysokich kosztów leczenia.

Warto również zauważyć, że ubezpieczyciel, w każdym przypadku proponuje trzy oferty ubezpieczeniowe. Propozycje te różnią się skalą rozbudowania oferty, a co się z tym wiąże sumą ubezpieczenia poszczególnych ryzyk. Każda z ofert została zbadana pod względem procentowego udziału kosztu pakietu w sumie ubezpieczenia kosztów leczenia, które to stanowią główny składnik ubezpieczeń turystycznych. Z analizowanych danych wynika, że największe różnice można zauważyć w przypadku podróży na terenie kraju. Udział ten zwiększa się bowiem o około 0,1 punktu procentowego w przypadku każdej z ofert. Biorąc pod uwagę pozostałe kierunki wyjazdu różnice między danymi procentowymi są znikome, bądź w ogóle nie występują.

Tabela 4.5 przedstawia ofertę ubezpieczeniową PZU Wojażer z uwzględnieniem kryterium celu wyjazdu.

[106] *PZU Wojażer, op. cit.*

Tabela 4.5. Oferta ubezpieczeniowa PZU Wojażer z uwzględnieniem kryterium celu wyjazdu według stanu na dzień 02.04.2018 r.

Cel wyjazdu	Oferta 1	Oferta 2	Oferta 3
Wypoczynek, zwiedzanie, sporty rekreacyjne	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 120 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: brak Ubezpieczenie bagażu: brak **Cena pakietu: 30,45 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 160 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 100 000 zł Ubezpieczenie bagażu: brak **Cena pakietu: 47,25 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 200 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony, Rowerzysta NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 100 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 3 000 zł **Cena pakietu: 69,30 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,03%**	**0,03%**	**0,03%**
Nauka, delegacja, praca biurowa	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 120 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: brak Ubezpieczenie bagażu: suma ubezpieczenia 1 000 zł **Cena pakietu: 35,35 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 160 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 70 000 zł OC: suma gwarancyjna 50 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 3 000 zł **Cena pakietu: 58,10 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 200 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 100 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 5 000 zł **Cena pakietu: 75,95 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,03%**	**0,04%**	**0,04%**
Praca fizyczna	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 120 000 zł Pomoc w podróży (Assistance): Podstawowy	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 160 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 200 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony

	NNW: suma ubezpieczenia 50 000 zł OC: brak Ubezpieczenie bagażu: suma ubezpieczenia 2 000 zł **Cena pakietu: 47,86 zł**	NNW: suma ubezpieczenia 70 000 zł OC: brak Ubezpieczenie bagażu: suma ubezpieczenia 3 000 zł **Cena pakietu: 66,33 zł**	NNW: suma ubezpieczenia 100 000 zł OC: brak Ubezpieczenie bagażu: suma ubezpieczenia 5 000 zł **Cena pakietu: 85,32 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,04%**	**0,04%**	**0,04%**
Narty, snowboard rekreacyjnie	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 120 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: suma gwarancyjna 50 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 1 000 zł **Cena pakietu: 53,73 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 160 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 70 000 zł OC: suma gwarancyjna 100 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 3 000 zł **Cena pakietu: 80,86 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 250 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony, Sport NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 200 000 zł Ubezpieczenie bagażu: sprzęt sportowy suma ubezpieczenia 5 000 zł **Cena pakietu: 136,68 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,04%**	**0,05%**	**0,05%**
Sporty wysokiego ryzyka	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 120 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: suma gwarancyjna 50 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 1 000 zł **Cena pakietu: 70,00 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 200 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 70 000 zł OC: suma gwarancyjna 150 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 3 000 zł **Cena pakietu: 112,70 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 250 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony, Sport, Rowerzysta NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 200 000 zł Ubezpieczenie bagażu: sprzęt sportowy suma ubezpieczenia 5 000 zł **Cena pakietu: 179,55 zł**

Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,06%**	**0,06%**	**0,07%**
Wyczynowe uprawianie sportu	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 120 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: suma gwarancyjna 50 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 1 000 zł Klasa ryzyka sportu wyczynowego: klasa 1 **Cena pakietu: 37,45 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 200 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 70 000 zł OC: suma gwarancyjna 150 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 3 000 zł Klasa ryzyka sportu wyczynowego: klasa 1 **Cena pakietu: 63,70 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 250 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony, Sport, Rowerzysta NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 200 000 zł Ubezpieczenie bagażu: sprzęt sportowy suma ubezpieczenia 5 000 zł Klasa ryzyka sportu wyczynowego: klasa 1 **Cena pakietu: 103,25 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,03%**	**0,03%**	**0,04%**

Źródło: opracowanie własne na podstawie *PZU Wojażer,*(https://moje.pzu.pl/pzu/travel?mcid=p_pzu_pl&_ga=2.82721490.559090199.1522682237-606227484.1522682237), dostęp: 02.04.2018 r.

Ubezpieczenie przedstawione w Tabeli 5.5 zostało przygotowane dla 23 letniej osoby, która zamierza wyjechać na 7 dniowy urlop z początkiem lipca do Europy lub kraju Morza Śródziemnego. Podróżujący nie choruje przewlekle oraz nie jest uczniem/studentem. Z powyższych danych wynika, że uprawianie sportów odgrywa ważną rolę przy tworzeniu pakietu ubezpieczeniowego. Najdroższe propozycje wiążą się z wyjazdami podczas których turysta ma zamiar uprawiać sporty wysokiego ryzyka np. bungee jumping, sporty motorowodne, żeglarstwo morskie lub surfing[107]. Wynika to z dużego ryzyka towarzyszącemu uprawianiu tych dyscyplin sportowych. Warto również nadmienić, że cele wyjazdu można łączyć odpowiednio dostosowując ofertę.

W każdym przypadku procentowy udział kosztu pakietu w sumie ubezpieczenia kosztów leczenia oscyluje na podobnym poziomie między 0,03% - 0,07%. Najwyższe wskaźniki dotyczą

[107] *PZU Wojażer, op. cit.*

ofert, w przypadku których turysta ma zamiar uprawiać sporty wysokiego ryzyka 0,06% - 0,07%. Pozostałe oferty charakteryzują się podobnym wskaźnikiem względem siebie.

Tabela 4.6 przedstawia ofertę ubezpieczeniową PZU Wojażer z uwzględnieniem kryterium podróżującego.

Tabela 4.6. Oferta ubezpieczeniowa PZU Wojażer z uwzględnieniem kryterium podróżującego według stanu na dzień 02.04.2018 r.

Podróżujący	Oferta 1	Oferta 2	Oferta 3
1 osoba	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 120 000 zł Pomoc w podróży (Assistance): Podstawowy NNW: suma ubezpieczenia 50 000 zł OC: brak Ubezpieczenie bagażu: brak **Cena pakietu: 30,45 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 160 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 100 000 zł Ubezpieczenie bagażu: brak **Cena pakietu: 47,25 zł**	Ubezpieczenie kosztów leczenia: suma ubezpieczenia 200 000 zł Pomoc w podróży (Assistance): Podstawowy, Rozszerzony, Rowerzysta NNW: suma ubezpieczenia 100 000 zł OC: suma gwarancyjna 100 000 zł Ubezpieczenie bagażu: suma ubezpieczenia 3 000 zł **Cena pakietu: 69,30 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,03%**	**0,03%**	**0,03%**
2 osoby niespokrewnione	Oferta oraz cena pakietu jak w przypadku wyjazdu jednej osoby.	Oferta oraz cena pakietu jak w przypadku wyjazdu jednej osoby.	Oferta oraz cena pakietu jak w przypadku wyjazdu jednej osoby.
2 osoby spokrewnione	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. pakietu za osobę: 28 zł**	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. pakietu za osobę: 41,44 zł**	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. pakietu za osobę: 59,08 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,02%**	**0,03%**	**0,03%**
1 osoba – choroba przewlekła	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. Cena pakietu: 55,65 zł**	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. Cena pakietu: 81,20 zł**	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. Cena pakietu: 110,60 zł**

Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,05%**	**0,05%**	**0,06%**
1 osoba – uczeń lub student	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. Cena pakietu: 24,36 zł**	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. Cena pakietu: 39,27 zł**	Oferta jak w przypadku wyjazdu jednej osoby. Zmianie ulega jedynie **cena. Cena pakietu: 60,48 zł**
Koszt pakietu w sumie ubezpieczenia kosztów leczenia	**0,02%**	**0,02%**	**0,03%**

Źródło: opracowanie własne na podstawie *PZU Wojażer,* (https://moje.pzu.pl/pzu/travel?mcid=p_pzu_pl&_ga=2.82721490.559090199.1522682237-606227484.1522682237), dostęp: 02.04.2018 r.

Oferta została przygotowana dla 23 letniego podróżującego na 7 dniowy urlop z początkiem lipca do Europy lub kraju Morza Śródziemnego w celu wypoczynku, zwiedzania oraz uprawiania sportów rekreacyjnych. Analizując powyższe dane można zauważyć, że podróżując z osobą spokrewnioną można liczyć na zniżkę przy zakupie pakietu ubezpieczeniowego. Upusty dotyczą również podróży uczniów lub studentów do 26 roku życia. W przypadku zaznaczenia pola „choroba przewlekła" (do takich chorób zalicza się np. astma i cukrzyca) oferta ubezpieczeniowa nie ulega zmianie, podwyższone zostają za to ceny pakietów[108]. Wynika to z większego prawdopodobieństwa, że osoba podróżująca podczas wyjazdu będzie wymagała pomocy lekarskiej.

Procentowy udział kosztu pakietu w sumie ubezpieczenia kosztów leczenia jest najwyższy w przypadku podróżującego, który cierpi na przewlekłą chorobę. W przypadku trzeciej oferty wynosi nawet 0,06%. Pozostałe oferty określa wskaźnik w granicy 0,02%-0,03%, co stanowi znikomą zmienność między analizowanymi danymi.

Analizując pakiety ubezpieczeniowe oraz ich ceny biorąc pod uwagę miesiąc wyjazdu, a także jego długość nie można stwierdzić wpływu tych czynników na koszty oferty ubezpieczeniowej. W każdym przypadku cena ubezpieczenia turystycznego w przeliczeniu na jeden dzień wyniosła tyle samo, a zakres ubezpieczeniowy nie ulegał zmianie.

[108] *PZU Wojażer, op. cit.*

4.8. Zakończenie

Troska o bezpieczny wyjazd towarzyszy każdemu podróżującemu. Ubezpieczenia turystyczne zapewniają zwrot kosztów leczenia, a także szeroki zakres pomocy w sytuacjach, które mogą przytrafić się w podróży. Powstały one w związku z realizacją ryzyka w ramach podejmowanej aktywności w turystyce i rekreacji. Ubezpieczenie turystyczne chroni dobra, które są narażone na uszczerbek w związku z wyjazdem, a jego zakres jest indywidualnie dostosowywany do potrzeb turysty. W zależności od wybranego wariantu może on obejmować: pokrycie kosztów leczenia za granicą, możliwość odzyskania wpłaconych pieniędzy w przypadku rezygnacji z imprezy turystycznej, uzyskanie pomocy medycznej w każdym zakątku świata, transport medyczny, pokrycie kosztów ratownictwa i poszukiwania górskiego przez ubezpieczyciela, a także odszkodowanie w razie kradzieży bagażu lub sprzętu sportowego.

W toku przeprowadzonych badań przedstawiono ustawę o usługach turystycznych jako kluczowy akt prawny regulujący tę tematykę. Ponadto omówiono zagadnienia związane z systemem bezpieczeństwa finansowego biur podróży. Dokonano także charakterystyki ryzyk na jakie narażeni są podróżujący oraz szczegółowo omówiono ubezpieczenia turystyczne. Oprócz tego scharakteryzowano dostępną na rynku ofertę ubezpieczenia turystycznego PZU Wojażer z uwzględnieniem kryterium kierunku wyjazdu, celu wyjazdu, podróżującego oraz terminu wyjazdu. Na podstawie analizy można stwierdzić, że wyżej wymienione kryteria istotnie wpływają na koszty ubezpieczenia turystycznego.

Na zakończenie warto także dodać, że temat ubezpieczeń turystycznych jest bardzo szeroki i w przyszłości może stanowić bazę do wielu innych badan naukowych. Szczególnej analizie mogą zostać poddane również oferty innych zakładów ubezpieczeń. Poza tym ciekawą tematyką wydaje się kwestia ubezpieczenia wyjeżdzających do sfery tropikalnej lub katalog wyłączeń z zakresu ochrony ubezpieczeniowej w ramach ubezpieczeń turystycznych.

Rozdział 5.
Samochody autonomiczne a sektor ubezpieczeń

Karolina Urbaczka*

5.1. Wprowadzenie

Pod wpływem postępu technologicznego środki transportu, wykorzystywane przez społeczeństwo do przemieszczania się z miejsca na miejsce, ulegają nieustannym przemianom. Szybkie zmiany w tym obszarze rozpoczęły się w 1908 roku, gdy wprowadzono do seryjnej produkcji pierwszy samochód. Przemiany, które mają miejsce od początku drugiej dekady XXI w. wynikają z wykorzystywania nowych rozwiązań informatycznych do poprawy bezpieczeństwa na drogach. Większość nowych samochodów, które trafiają do sprzedaży, jest wyposażona w inteligentne systemy umożliwiające parkowanie bez udziału kierowcy, kontrolę utrzymania pasa ruchu w czasie jazdy czy też zachowanie stałej prędkości i bezpiecznej odległości od poprzedzającego pojazdu na autostradzie. Obecność chociaż jednego z tych rozwiązań pozwala na zaliczenie samochodu do grona samochodów zautomatyzowanych. Jednak prawdziwa rewolucja w transporcie nadejdzie wraz z wprowadzeniem na drogi samochodów w pełni autonomicznych, które będą w stanie poruszać się w każdych warunkach bez udziału kierowcy.

Artykuł ten ma na celu znalezienie odpowiedzi na pytanie, czy powszechna obecność samochodów autonomicznych na drogach spowoduje konieczność wprowadzenia zmian w działalności ubezpieczycieli. Aby zbadać tę kwestię przeprowadzono przegląd literatury krajowej i zagranicznej. W pierwszej kolejności dokonano charakterystyki samochodów autonomicznych oraz sklasyfikowano je z uwzględnieniem kryteriów różnych światowych organizacji. Następnie przedstawiono szanse i zagrożenia wynikające z wykorzystywania tego

* Koło Naukowe Ubezpieczeń „Risk Management", Katedra Zarządzania Ryzykiem i Ubezpieczeń, Uniwersytet Ekonomiczny w Krakowie.

rodzaju pojazdów, ze szczególnym uwzględnieniem nowych rodzajów ryzyka, które zmaterializują się wraz z postępującą automatyzacją samochodów. W dalszej części artykułu skupiono się na aktach prawnych wprowadzanych w różnych krajach, które określają podstawowe zasady dotyczące sposobu programowania systemów tych pojazdów, a także wprowadzają ramowe zasady ustalające sposób przypisywania odpowiedzialności za ewentualne szkody oraz podstawowy zakres ubezpieczenia samochodu autonomicznego. Ostatni podrozdział poświęcono opisowi przewidywań osób zarządzających firmami ubezpieczeniowymi co do wpływu samochodów autonomicznych na ich działalność, nowych rodzajów ubezpieczeń, a także działań, które powinni podjąć ubezpieczyciele w celu lepszej odpowiedzi na potrzeby rynku.

5.2. Charakterystyka i klasyfikacje samochodów autonomicznych

Jednoznaczne zdefiniowanie pojęcia „samochód autonomiczny" nie jest zadaniem łatwym. Na całym świecie podejmowane były liczne próby stworzenia klasyfikacji, która w sposób pełny i niepozostawiający wątpliwości określiłaby kryteria konieczne do spełnienia, by dany samochód został zaliczony do wybranego poziomu automatyzacji. W 2012 roku podjął się tego niemiecki Federalny Instytut ds. Badań nad Autostradami (*Die Bundesanstalt für Straßenwesen – BASt*), w 2013 roku amerykański Urząd ds. Bezpieczeństwa Ruchu Drogowego (*National Highway Traffic Safety Administration – NHTSA*), a w 2014 Stowarzyszenie Inżynierów Motoryzacji (*Society of Automotive Engineers – SAE*).

BASt przygotowało dokument pt. „*Definitions of Automation and Legal Issues in Germany*", w którym wyróżnił 5 poziomów automatyzacji pojazdów:

- brak automatyzacji (tylko kierowca),
- wspomagany,
- częściowo zautomatyzowany,
- wysoce zautomatyzowany,
- w pełni zautomatyzowany[109].

[109] T. M. Gasser, D. Westhoff, *BASt-study: Definitions of Automation and Legal Issues in Germany*, German Federal Highway Research Institute 2012, (http://onlinepubs.trb.org/onlinepubs/conferences/2012/Automation/presentations/Gasser.pdf), dostęp: 7.03.2018 r.

W przygotowanym przed NHTSA dokumencie „*Preliminary Statement of Policy Concerning Automated Vehicles*" wyróżniono następujące poziomy automatyzacji:

- poziom 0 – brak automatyzacji, kierowca obsługuje wszystkie systemy pokładowe, system może dostarczać jedynie ostrzeżenia, np. o zagrożeniu zderzeniem czołowym czy opuszczeniu właściwego pasa ruchu,
- poziom 1 – automatyka wybranych układów, samochód jest wyposażony w systemy wspomagające kierowcę oraz technologie zapobiegające zderzeniom, jednak nie zastępują one czujności kierowcy i nie przejmują od niego kontroli nad prowadzeniem pojazdu, system może uzupełniać kierowcę w zakresie sterowania pojazdem albo kontroli prędkości, jednak nie w zakresie obu tych czynności jednocześnie, np. adaptacyjny tempomat, automatyczne hamowanie, zachowanie toru jazdy,
- poziom 2 – łączna automatyzacja kilku układów, co najmniej dwie podstawowe funkcje kontroli nad pojazdem mogą być równocześnie przejęte przez system w określonych sytuacjach drogowych, kierowca jest odpowiedzialny za monitorowanie otoczenia i musi być w każdej chwili przygotowany do przejęcia kontroli nad pojazdem, np. adaptacyjny tempomat w połączeniu z systemem utrzymania pojazdu w pasie ruchu,
- poziom 3 – tzw. „automatyzacja samojezdna", kierowca może w określonych warunkach przekazać systemowi pełną kontrolę nad prowadzeniem pojazdu, system będzie samodzielnie monitorował otoczenie i oceni, kiedy kierowca powinien przejąć kontrolę ze względów bezpieczeństwa, o czym powiadomi kierowcę z odpowiednim wyprzedzeniem czasowym,
- poziom 4 – pełna automatyzacja, samochód jest zaprojektowany w taki sposób, że system jest w stanie kontrolować pojazd i jego otoczenie w trakcie całej podróży, kierowca nie musi nadzorować działania systemu, odpowiada jedynie za wprowadzenie adresu miejsca docelowego[110].

Klasyfikacje przygotowane przez BASt oraz NHTSA mają wiele cech wspólnych, jednak ich największą wadą był ograniczony terytorialnie zakres obowiązywania, a brak ujednoliconego zespołu kryteriów mógł prowadzić do nieporozumień między osobami posługującymi się

[110] *Preliminary Statement of Policy Concerning Automated Vehicles*, National Highway Traffic Safety Administration 2013, (https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf). dostęp: 7.03.2018 r.

klasyfikacją niemiecką a wykorzystującymi podział amerykański. Sytuacja uległa zmianie w 2014 roku, gdy SAE opublikowało dokument „*Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*”[111]. Zawarty w tym opracowaniu podział jest powszechnie stosowany na całym świecie.

Klasyfikacja ta zakłada wyodrębnienie 6 poziomów automatyzacji samochodów:

- poziom 0 – brak automatyzacji, stała kontrola kierowcy nad prowadzeniem pojazdu, system jest w stanie jedynie informować o zagrożeniach na drodze,
- poziom 1 – wspomaganie kierowcy, w określonych sytuacjach system jest w stanie przejąć kontrolę nad jednym z dwóch aspektów: sterowaniem lub kontrolą prędkości, pozostałe czynności związane z prowadzeniem pojazdu wykonuje kierowca,
- poziom 2 – częściowa automatyzacja, w określonych sytuacjach system może kontrolować zarówno sterowanie jak i prędkość pojazdu, kierowca odpowiada za nadzór nad sprawnym działaniem systemu oraz realizację pozostałych elementów prowadzenia pojazdu,
- poziom 3 – warunkowa automatyzacja, w określonych sytuacjach system może przejąć kontrolę nad wszystkimi aspektami jazdy, przy założeniu, że kierowca w każdej chwili musi być gotowy do przejęcia kontroli nad samochodem,
- poziom 4 – wysoka automatyzacja, w określonych sytuacjach system jest w stanie kontrolować wszystkie aspekty jazdy, nawet jeśli kierowca nie odpowiada na wezwanie do przejęcia kontroli,
- poziom 5 – pełna automatyzacja, system kontroluje wszystkie aspekty prowadzenia pojazdu przez cały czas trwania podróży w każdych warunkach drogowych.

Tabela 5.1 zawiera podsumowanie najważniejszych kryteriów decydujących o zakwalifikowaniu danego pojazdu do konkretnego poziomu automatyzacji oraz porównanie z odpowiadającymi poziomami z klasyfikacji BASt oraz NHTSA.

[111] *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*, Society of Automotive Engineers 2014, (https://www.sae.org/standards/content/j3016_201401), dostęp: 7.03.2018 r.

Tabela 5.1. Podsumowanie poziomów automatyzacji wg kryteriów SAE oraz porównanie z klasyfikacjami BASt i NHTSA (według stanu na dzień 7.03.2018)

Poziom SAE	Nazwa	Sterowanie i kontrola prędkości	Monitorowanie otoczenia	Kierowanie w sytuacjach awaryjnych	Dostępność trybu automatycznego	Poziom BASt	Poziom NHTSA
Kierowca jest odpowiedzialny za monitorowanie otoczenia							
0	Brak automatyzacji	Kierowca	Kierowca	Kierowca	Brak	Tylko kierowca	0
1	Wspomaganie kierowcy	Kierowca i system	Kierowca	Kierowca	Niektóre warunki	Wspomagany	1
2	Częściowa automatyzacja	System	Kierowca	Kierowca	Niektóre warunki	Częściowo zautomatyzowany	2
Zautomatyzowany system kierujący jest odpowiedzialny za monitorowanie otoczenia							
3	Warunkowa automatyzacja	System	System	Kierowca	Niektóre warunki	Wysoce zautomatyzowany	3
4	Wysoka automatyzacja	System	System	System	Niektóre warunki	W pełni zautomatyzowany	3/4
5	Pełna automatyzacja	System	System	System	Każde warunki	-	

Źródło: opracowanie własne na podstawie *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*, Society of Automotive Engineers 2014, (https://www.sae.org/standards/content/j3016_201401), dostęp: 7.03.2018 r.

Jak można zauważyć, w żadnej z tych klasyfikacji nie występuje określenie „samochód autonomiczny", które jednak jest powszechnie wykorzystywane w publikacjach oraz przez opinię publiczną. Należy zatem zastanowić się nad tym, na którym poziomie automatyzacji samochód można określić jako w pełni autonomiczny. Odpowiedzi na to pytanie dostarcza dokument „*Automated vehicles in the EU*" sporządzony w styczniu 2016 roku[112]. Wyróżnione zostały w nim dwa pojęcia – pojazd zautomatyzowany (*automated vehicle*) oraz pojazd autonomiczny (*autonomous vehicle*). Pojazd zautomatyzowany to pojazd wyposażony w technologię pozwalającą kierowcy przekazać systemom pokładowym część obowiązków związanych z jazdą, natomiast pojazd autonomiczny to w pełni zautomatyzowany pojazd

[112] S. Pillath, *Automated vehicles in the EU*, European Parliamentary Research Service 2016, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573902/EPRS_BRI(2016)573902_EN.pdf (dostęp: 7.03.2018).

wyposażony w technologie pozwalające systemowi wykonywać wszystkie funkcje związane z jazdą, bez jakiejkolwiek interwencji ze strony człowieka. Zgodnie z tą definicją, do pojazdów autonomicznych można zaliczyć jedynie pojazdy zakwalifikowane do 5 poziomu automatyzacji wg SAE. Jednak w praktyce pojęcie to jest wykorzystywane również w odniesieniu do pojazdów z 3 i 4 poziomu, co może prowadzić do mylnych przekonań kierowców co do ich odpowiedzialności za prowadzenie takich samochodów, a w efekcie do niebezpiecznych sytuacji na drogach wynikających z nieodpowiedniego poziomu uwagi.

Rozważając wpływ samochodów autonomicznych na ubezpieczenia należy zastanowić się, jakie samochody są już dostępne na rynku oraz kiedy pojawią się pojazdy o najwyższym poziomie automatyzacji. Samochody wspomagające kierowcę (poziom 1) są już obecnie bardzo rozpowszechnione, większość samochodów nowej produkcji posiada w wyposażeniu systemy takie jak adaptacyjny tempomat czy system kontroli pasa ruchu. Pojazdy z częściową automatyzacją (poziom 2) są mniej liczne, niż te zaliczane do pierwszego poziomu automatyzacji. Na rynku istnieje kilka głównych producentów posiadających w swojej ofercie tego typu samochody. Wszystkie modele Tesli, z wyjątkiem Roadstera, można wyposażyć w odpowiedni pakiet, który zapewnia drugi poziom automatyzacji, jednak zgodnie z zapewnieniami producenta oferowane wyposażenie jest przygotowane do pracy w trybie pełnej autonomii, wymaga jedynie dopracowania oprogramowania. Volvo oferuje częściową automatyzację w modelach S90, XC90, XC60 oraz XC40, Mercedes w samochodach klasy E oraz S, BMW w serii 5, a Lexus w modelu LS[113]. Wymagania niezbędne do zaliczenia do poziomu 3 automatyzacji spełnia obecnie tylko jeden seryjnie produkowany samochód – Audi A8[114]. Jest to zarazem pierwszy samochód wyposażony w LiDAR (*Light Detection and Ranging*)[115]. Samochody reprezentujące poziom 4 i 5 są obecnie jedynie w wersjach prototypowych lub koncepcyjnych. Przewiduje się, że na rynek trafią najwcześniej w 2020 roku[116].

[113] P. Barycki, *Zdejmujesz ręce z kierownicy i nie musisz się niczym przejmować. Tak, takie samochody są już na rynku*, (https://www.spidersweb.pl/2018/01/samochody-autonomiczne-poziomy.html), dostęp: 7.03.2018 r.
[114] T. Domański, *Oto nowe Audi A8. Pierwsza limuzyna, która nie potrzebuje kierowcy*, (https://www.spidersweb.pl/2017/07/nowe-audi-a8.html), dostęp: 7.03.2018 r.
[115] Metoda badania odległości od obiektów oparta na wykorzystaniu światła lasera, *Light Detection and Ranging (LIDAR)*, National Geodetic Survey, (https://www.ngs.noaa.gov/RESEARCH/RSD/main/lidar/lidar.shtml), dostęp: 7.03.2018 r.
[116] P. Barycki, *Zdejmujesz ręce z kierownicy…*, *op. cit.*

5.3. Szanse i zagrożenia związane z samochodami autonomicznymi

Jako jedną z głównych zalet samochodów autonomicznych podaje się wyeliminowanie najbardziej zawodnego elementu – człowieka. Samochód prowadzony przez system nie będzie zmęczony, rozkojarzony czy pod wpływem alkoholu, co wpłynie na zwiększenie bezpieczeństwa na drogach. Statystyki policyjne z wielu krajów potwierdzają, że do wypadków komunikacyjnych najczęściej dochodzi z winy kierowcy.

Tabela 5.2. Struktura wypadków komunikacyjnych w Polsce wg sprawców (% ogółu wypadków) oraz liczba zabitych z uwzględnieniem sprawstwa wypadków w latach 2012-2016

Sprawstwo wypadków	2012		2013		2014		2015		2016	
	wypadki	zabici	wypadki	zabici	wypadki	zabici	wypadki	zabici	wypadki	Zabici
Wina kierujących	81,5	70,3	81,9	67,6	82,1	68,4	82,8	68,4	86,4	75,5
Wina pieszych	10,1	17,5	8,9	17,2	8,7	17,6	7,9	15,3	7,3	13,2
Wina pasażerów	0,3	0,1	0,4	0,1	0,4	0,1	0,4	0,1	0,4	0,0
Współwina	1,4	2,3	1,5	2,3	1,3	1,5	1,1	2,1	1,1	1,3
Pozostałe przyczyny	6,7	9,8	7,4	12,8	7,5	12,4	7,7	14,1	4,8	10,0

Źródło: opracowanie własne na podstawie: *Wypadki drogowe w Polsce w 2012 roku,* Komenda Główna Policji, Warszawa 2013; *Wypadki drogowe w Polsce w 2013 roku,* Komenda Główna Policji, Warszawa 2014; *Wypadki drogowe w Polsce w 2014 roku,* Komenda Główna Policji, Warszawa 2015; *Wypadki drogowe w Polsce w 2015 roku,* Komenda Główna Policji, Warszawa 2016; *Wypadki drogowe w Polsce w 2016 roku,* Komenda Główna Policji, Warszawa 2017

Z przedstawionej w tabeli 2 struktury wypadków komunikacyjnych wynika, że w Polsce ponad 80% wypadków jest powodowanych przez kierujących. W USA ponad 90% wypadków wynika z błędów popełnionych przez kierowców[117], natomiast w Wielkiej Brytanii odsetek ten wynosi około 85%[118]. Na tej podstawie można wyciągnąć wniosek, że wprowadzenie na rynek

[117] D. J. Fagnant, K. M. Kockelman, *Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations*, Eno Foundation 2013, (https://www.enotrans.org/etl-material/preparing-a-nation-for-autonomous-vehicles-opportunities-barriers-and-policy-recommendations/), dostęp: 7.03.2018 r.
[118] *Table RAS50002: Contributory factors allocated to vehicles or pedestrians in reported accidents, Great Britain, 2012-2016*, (https://www.gov.uk/government/statistical-data-sets/ras50-contributory-factors#table-ras50002), dostęp: 7.03.2018 r.

samochodów w pełni autonomicznych przyniesie spadek liczby wypadków drogowych o co najmniej 80%. Już obecnie zauważalny jest wpływ wprowadzanej stopniowo automatyzacji samochodów na zmniejszenie liczby wypadków. Z raportu przygotowanego przez amerykański Urząd ds. Bezpieczeństwa Ruchu Drogowego (NHTSA) wynika, że w latach 2014-2016 wskaźnik wypadkowości samochodów Tesla Model S oraz Model X po zainstalowaniu funkcji autopilota (poziom 2 automatyzacji) spadł o niemal 40% w porównaniu do wskaźnika sprzed dokonania modyfikacji[119]. Przewiduje się, że przeciętna liczba wypadków na samochód w ciągu roku spadnie z poziomu ok. 0,043 w 2013 roku do ok. 0,009 w 2040 roku, co stanowi spadek o ok 80%. Jednak jednocześnie średni koszt naprawy szkód z pojedynczego wypadku wzrośnie z ok. 14000 dolarów w 2013 roku do ok. 35000 dolarów w 2040 roku, co wynika z większej wartości wyposażenia wykorzystywanego w samochodach autonomicznych[120].

Samochody autonomiczne uczestniczą w wypadkach rzadziej niż tradycyjne pojazdy, lecz praktycznie każdy taki wypadek jest nagłaśniany przez media i szeroko komentowany przez opinię publiczną. Może to zwiększać niechęć użytkowników dróg do wprowadzania samochodów o co raz to wyższych poziomach automatyzacji oraz wpływać negatywnie na reputację producentów tych samochodów. Znaczna większość takich wypadków powodowana jest jednak przez ludzi kierujących innymi samochodami na drodze lub przez niedostateczną uwagę kierowców pojazdów zautomatyzowanych. Z danych opublikowanych przez Google w maju 2015 roku wynika, że w czasie testów przeprowadzanych przez koncern w ciągu 6 lat miało miejsce 11 drobnych kolizji z udziałem ich samochodów, przy czym wszystkie zdarzenia były spowodowane przez ludzi, system autonomicznej jazdy nie spowodował ani jednego[121].

Jako że wskaźniki wypadkowości są jednym z podstawowych kryteriów branych pod uwagę przy obliczaniu składki ubezpieczeniowej można wysunąć wniosek, że spadek liczby wypadków o około 80% spowodowany pojawieniem się na drogach samochodów autonomicznych, wywoła obniżenie kosztów ubezpieczeń tych samochodów również o 80%.

---

[119] *ODI resume of investigation PE 16-007*, Office of Defects Investigation, (https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF), dostęp: 7.03.2018 r.

[120] *Automobile insurance in the era of autonomous vehicles. Survey results*, KPMG 2015, s. 6-7, (https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/kpmg-automobile-insurance-in-era-autonomous.pdf), dostęp: 7.03.2018 r.

[121] P. Barycki, *Jeśli usłyszysz o wypadku autonomicznego auta, możesz być niemal pewny, że spowodował go… człowiek*, (https://www.spidersweb.pl/2015/05/autonomiczne-auta-wypadki.html), dostęp: 7.03.2018 r.

Należy jednak pamiętać także o nowych rodzajach ryzyka, które pojawią się wraz z rozwojem technologii i wzrostem popularności samochodów autonomicznych, do których należą:

- ryzyko awarii oprogramowania i wyposażenia,
- niebezpieczeństwo zhakowania systemu sterowania,
- zwiększona skłonność do ryzyka,
- ryzyko związane z jazdą w kolumnie pojazdów,
- zwiększony ruch samochodowy[122].

Złożone systemy elektroniczne, jakimi niewątpliwie są samochody autonomiczne, zbudowane są z wielu powiązanych ze sobą podsystemów, a wraz z liczbą powiązań i poziomem skomplikowania zwiększa się liczba potencjalnych źródeł błędów. Niesie to za sobą zwiększone ryzyko awarii, a nawet z pozoru niewielka nieprawidłowość (np. fałszywe wskazanie czujnika, błąd obliczeniowy w oprogramowaniu czy chwilowe zakłócenie sygnału nawigacji) doprowadzić do wypadku. Dodatkowo przewiduje się, że takie wypadki, w razie wystąpienia, mogą być znacznie bardziej poważne, niż wypadki powstające z powodu błędów ludzkich. Rzadko zdarza się, by kierowca świadomie dopuścił się rażącego naruszenia bezpieczeństwa ruchu drogowego, jak np. jazda pod prąd autostradą, gdyż instynktownie zdaje sobie sprawę z tego, jak wielkie niebezpieczeństwo jest związane z takim manewrem. W przypadku samochodów autonomicznych awaria czujnika lub błąd w obliczeniach może doprowadzić do zdarzenia, które ludzki kierowca rozpoznałby za niewłaściwe i podjął kroki zmierzające do zapobiegnięcia wypadkowi. Z tego powodu, wypadki wynikające z błędów systemu mogą być trudne do przewidzenia oraz bardziej tragiczne w skutkach[123].

Oprogramowanie sterujące samochodów autonomicznych, jak każdy system komputerowy, może być podatne na ataki hakerskie i nieautoryzowane przejęcie kontroli nad pojazdem. Niesie to za sobą ryzyko wypadków spowodowanych zarówno z czystej ciekawości i chęci udowodnienia swoich umiejętności hakerskich, jak i powodów kryminalnych. Mogą być dokonywane próby zabójstw, gdzie narzędziem zbrodni będzie samochód autonomiczny, a

[122] T. Litman, *Autonomous Vehicle Implementation Predictions. Implications for Transport Planning,* Victoria Transport Policy Institute 2018, (https://www.vtpi.org/avip.pdf), s. 10 dostęp: 20.03.2018 r.
[123] G. Yeomans, *Autonomous Vehicles. Handing over control: opportunities and risks for insurance*, Lloyd's 2014, (https://www.lloyds.com/~/media/lloyds/reports/emerging-risk-reports/autonomous-vehicles-final.pdf), s. 15 dostęp: 20.03.2018 r.

także próby ataków terrorystycznych, gdzie nie będzie potrzebny kierowca-samobójca w samochodach-pułapkach[124].

Pojawienie się na drogach pojazdów autonomicznych, które z założenia są bezpieczniejsze od tych tradycyjnych, może spowodować zmniejszenie uwagi pozostałych uczestników ruchu drogowego i zwiększenie skłonności do podejmowania przez nich ryzyka. Pasażerowie, nie obawiając się skutków wypadku, mogą nie zapinać pasów bezpieczeństwa czy też nie przywiązywać uwagi do przewożenia ładunków w prawidłowy sposób. Kierowcy samochodów tradycyjnych mogą wykonywać manewry w sposób bardziej gwałtowny i bez uprzedniego upewnienia się co do możliwości ich bezpiecznego przeprowadzenia, wychodząc z założenia, że samochód autonomiczny tak czy inaczej zapobiegnie wypadkowi. Podobny wpływ może to mieć na pieszych, którzy będą wchodzić na jezdnię bez zachowania odpowiedniej ostrożności[125].

Pojazdy autonomiczne będą potrafiły komunikować się między sobą, co stworzy możliwość do łączenia się w kolumny (ang. *platooning*) i wspólnego pokonywania poszczególnych odcinków trasy, najczęściej po wydzielonych do tego pasach na drogach szybkiego ruchu czy autostradach, w celu zmniejszenia oporów powietrza i zużycia energii, a więc zwiększenia ekonomiczności jazdy. Jednak istnieje ryzyko, że również kierowcy pojazdów tradycyjnych będą się przyłączać do takich kolumn i zakłócą porządek ruchu przez np. nagłą zmianę pasa ruchu, nieprzewidywalne hamowanie czy przyśpieszanie, co może spowodować kolizje czy wypadki[126].

Brak konieczności posiadania uprawnień do kierowania pojazdu, większa wygoda oraz bezpieczeństwo autonomicznych samochodów może spowodować częstsze korzystanie z tych samochodów w porównaniu do tradycyjnych. Dodatkowym aspektem przyczyniającym się do zwiększonego ruchu ulicznego wynikającego z wprowadzenia samochodów autonomicznych jest fakt, że ludzie dojeżdżający do pracy w centrach miast nie będą zostawiać swoich samochodów na pobliskich parkingach, ale samochody te będą wracać do domów na przedmieściach, skąd znów przyjadą do centrum, gdy ich właściciele skończą pracę. W ten sposób zarówno poranny jak i popołudniowy szczyt komunikacyjny będzie się składał z dwóch

[124] T. Litman, *op. cit.*
[125] *Ibidem.*
[126] *Ibidem.*

fal. Z tych dwóch powodów, zwiększony ruch drogowy niesie za sobą zwiększone ryzyko wypadków[127].

Biorąc pod uwagę nowe rodzaje ryzyka, wskaźnik wypadkowości oraz koszty ubezpieczenia samochodów autonomicznych mogą zmniejszyć się nie o ok 80%, jak wynikałoby z wyeliminowania zawodnego i popełniającego błędy kierowcy, lecz w mniejszym stopniu. Zwłaszcza w początkowej fazie wprowadzania samochodów autonomicznych, gdy wciąż większość pojazdów na drogach będzie kierowana w sposób tradycyjny, spadek wskaźnika wypadkowości oraz kosztów ubezpieczenia może być znikomy.

5.4. Wybrane uregulowania prawne dotyczące samochodów autonomicznych

Z uwagi na co raz większy postęp technologiczny oraz zbliżającą się perspektywę powszechnego wykorzystywania samochodów autonomicznych na drogach publicznych niezbędne jest podjęcie kroków zmierzających do wprowadzenia uregulowań prawnych dotyczących takich samochodów. W Unii Europejskiej pierwszym dokumentem, który poruszał tę kwestię, był „*Amsterdam Declaration on Cooperation in the field of connected and automated driving*" podpisany 14 kwietnia 2016 roku przez ministrów transportu wszystkich krajów UE. Deklaracja zawierała porozumienie krajów członkowskich, Komisji Europejskiej oraz sektora prywatnego określające wspólne cele oraz działania zmierzające do ułatwienia wprowadzenia samochodów autonomicznych na rynek europejski[128]. Kolejnym krokiem podjętym przez Komisję Europejską była publikacja dokumentu „*A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*". Celem przyjętej strategii było umożliwienie wdrożenia samochodów połączonych, komunikujących się między sobą oraz z infrastrukturą drogową, przed rokiem 2019[129].

[127] *Ibidem.*
[128] *Declaration of Amsterdam. Cooperation in the field of connected and automated driving*, The Netherlands EU Presidency 2016, (https://www.regjeringen.no/contentassets/ba7ab6e2a0e14e39baa77f5b76f59d14/2016-04-08-declaration-of-amsterdam---final1400661.pdf), dostęp: 28.03.2018 r.
[129] Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, COM/2016/0766.

Oprócz prac na szczeblu unijnym, prace nad uregulowaniem funkcjonowania samochodów autonomicznych w przestrzeni publicznej podjęto także na szczeblu krajowym w Niemczech oraz w Wielkiej Brytanii.

W Niemczech w czerwcu 2017 roku Komisja Etyki działająca przy Federalnym Ministerstwie Transportu i Infrastruktury Cyfrowej (*Bundesministerium für Verkehr und digitale Infrastruktur* – BMVI) przygotowała raport „*Automated and Connected Driving*" zawierający wskazówki dotyczące sposobu programowania samochodów zautomatyzowanych, w tym normy etyczne. Prace prowadzono w pięciu wyodrębnionych grupach roboczych zajmujących się następującymi obszarami:

- sytuacje wiążące się z zagrożeniami nie do uniknięcia,
- dostępność i bezpieczeństwo danych,
- warunki interakcji między człowiekiem a maszyną,
- uwzględnienie kontekstu etycznego poza ruchem ulicznym,
- zakres odpowiedzialności za oprogramowanie oraz infrastrukturę[130].

W dokumencie zaznaczono, że najważniejszym celem przyświecającym wprowadzeniu samochodów częściowo oraz w pełni zautomatyzowanych jest poprawa bezpieczeństwa wszystkich użytkowników dróg oraz zwiększenie mobilności osób, które dotychczas były wykluczone z samodzielnego poruszania się samochodami z uwagi na stan zdrowia czy wiek. Dopuszczanie do ruchu samochodów zautomatyzowanych jest możliwe jedynie wtedy, gdy zapewniają zmniejszenie wypadkowości w porównaniu z samochodami tradycyjnymi, prowadzonymi przez ludzi. Dopuszczone do ruchu powinny być jedynie te pojazdy, które potrafią poruszać się w sposób asekuracyjny oraz przewidywalny, stwarzając minimalne zagrożenie dla najmniej chronionych uczestników ruchu, takich jak piesi czy rowerzyści. Odpowiedzialność za gwarantowanie bezpieczeństwa pojazdów wprowadzanych na rynek spoczywa na instytucjach publicznych, a więc powinien zostać powołany organ zajmujący się licencjonowaniem oraz monitorowaniem działania systemów kierujących wykorzystywanych w samochodach. Systemy te powinny zapobiegać krytycznym sytuacjom zawsze, gdy jest to możliwe, a także być wyposażone w oprogramowanie zdolne do dokonania wyboru

[130] *Automated and Connected Driving*, Ethics Commission Appointed by the Federal Minister of Transport and Digital Infrastructure 2017, (https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile), dostęp: 28.03.2018 r.

„mniejszego zła” w sytuacji, gdy niemożliwe jest całkowite wyeliminowanie zagrożenia. System powinien być zaprogramowany w taki sposób, by w razie zaistnienia sytuacji, w której zderzenie jest nieuniknione, ochronić zdrowie i życie ludzkie, nawet kosztem zaistnienia szkody na zwierzętach lub innym mieniu. Jednakże zabronione jest dokonywanie w takich sytuacjach wyborów, kto ma zostać ocalony a kto poszkodowany, na podstawie cech osobistych zagrożonych osób, takich jak wiek, płeć, kolor skóry, wygląd, kondycja fizyczna czy psychiczna. Głównym kryterium, którym ma kierować się system w takich wypadkach, jest kryterium minimalizacji szkód. W raporcie zaznaczono także fakt, że w przypadku samochodów zautomatyzowanych, odpowiedzialność, która dotychczas spoczywała w całości na kierującym, przenosi się na producentów pojazdów, dostawców oprogramowania, służby odpowiedzialne za utrzymanie inteligentnej infrastruktury drogowej, operatorów sieci komunikacyjnych, czy też dostawców usług informatycznych (np. w zakresie utrzymania serwerów). Odpowiedzialność za szkody spowodowane przez samochód z aktywowanym trybem automatycznej jazdy spoczywa na producencie samochodu i podlega zasadom właściwym dla odpowiedzialności produktowej. Zastosowane rozwiązania technologiczne muszą umożliwiać jednoznaczne określenie, czy w danej sytuacji aktywowany był tryb automatycznej jazdy, czy kierowca przejął manualną kontrolę nad pojazdem oraz odpowiedzialność za jego prowadzenie. Informacje na ten temat powinny być dokumentowane oraz przechowywane, dzięki czemu będzie można we właściwy sposób przypisać odpowiedzialność za powstałe szkody. W razie zaistnienia sytuacji awaryjnych, system musi automatycznie przejść w „bezpieczny tryb”, w którym ryzyko związane z przemieszczaniem się pojazdu będzie ograniczone do minimum. Autorzy dokumentu podkreślili także konieczność odpowiedniego szkolenia w zakresie korzystania z zautomatyzowanych pojazdów, a umiejętności te powinny podlegać sprawdzeniu na zasadach podobnych do obecnych egzaminów na prawo jazdy. Decyzja o wykorzystaniu przez zewnętrzne instytucje danych generowanych przez samochody autonomiczne w celach badawczych lub statystycznych należeć będzie do właściciela oraz użytkownika samochodu. Podkreślono rolę ustawodawców w zapewnieniu równowagi między gromadzeniem danych potrzebnych do zapewnienia bezpieczeństwa, a interesami jednostki oraz jej prawem do prywatności.

W Wielkiej Brytanii zagadnieniami związanymi z samochodami autonomicznymi zajęła się Komisja Specjalna ds. Nauki i Technologii powołana przez Izbę Lordów. W marcu 2017 roku opublikowano raport „*Connected and Autonomous Vehicles: The future?*", w którym przedstawiono działania w zakresie koordynacji oraz nadzoru konieczne do podjęcia przez rząd, wyszczególniono potencjalne korzyści społeczne i ekonomiczne związane z wprowadzeniem na rynek samochodów autonomicznych, podkreślono konieczność przeprowadzenia dalszych badań nad technologiami wykorzystywanymi w tego rodzaju samochodach oraz nad sposobem, w jaki upowszechnienie autonomicznych pojazdów wpłynie na zachowania kierowców, pieszych, rowerzystów oraz pozostałych użytkowników dróg, a także zwrócono uwagę na konieczność podjęcia międzynarodowej współpracy w celu ustanowienia spójnych standardów oraz ram prawnych odnoszących się do samochodów autonomicznych[131]. Podobnie jak w dokumencie opublikowanym przez niemiecki urząd, jako potencjalne źródło problemów wskazano kwestię gromadzenia oraz wykorzystywania danych generowanych przez samochody autonomiczne, a także sposób rozwiązywania dylematów natury etycznej w razie zaistnienia śmiertelnego zagrożenia, którego nie można uniknąć. W raporcie zaznaczono konieczność dokonania zmian w reżimie ubezpieczeń komunikacyjnych w taki sposób, aby zakresem ubezpieczenia objąć również pojazdy z włączonym trybem autonomicznym. Obecnie w razie zaistnienia wypadku komunikacyjnego ubezpieczyciel kierowcy-sprawcy wypłaca odszkodowanie poszkodowanym stronom. Jednak wraz z wprowadzeniem samochodów autonomicznych pojawia się możliwość, że do wypadku dojdzie w czasie działania trybu autonomicznego. W takim przypadku osoba siedząca za kierownicą nie musi być odpowiedzialna za spowodowanie szkody, a odpowiedzialność może spoczywać na producencie pojazdu. W wyniku konsultacji przeprowadzonych przez rząd Wielkiej Brytanii w 2016 roku zasugerowano, że dotychczasowy zakres ubezpieczenia komunikacyjnego powinien zostać rozszerzony. Zaproponowano stworzenie modelu jednego ubezpieczyciela, dzięki czemu poszkodowany byłby chroniony również w razie wypadku z udziałem samochodu w trybie autonomicznym. Poszkodowanemu przysługiwałoby roszczenie w stosunku do ubezpieczyciela komunikacyjnego, natomiast po wypłaceniu odszkodowania

[131] *Connected and Autonomous Vehicles: The future?*, House of Lords Science and Technology Select Committee 2017, (https://publications.parliament.uk/pa/ld201617/ldselect/ldsctech/115/115.pdf), dostęp: 28.03.2018 r.

ubezpieczycielowi przysługiwać będzie roszczenie regresowe w stosunku do strony odpowiedzialnej za spowodowanie wypadku, głównie w ramach odpowiedzialności produktowej. Osobą objętą ochroną ubezpieczeniową byłaby także osoba siedząca za kierownicą, gdyż ona również może zostać poszkodowana w wyniku wypadku zaistniałego w trybie autonomicznym. Zaznaczono, że niezbędne jest podjęcie dalszych prac nad uregulowaniem ubezpieczenia obejmującego samochody autonomiczne.

W celu określenia zasad ubezpieczenia pojazdów autonomicznych w Wielkiej Brytanii w październiku 2017 roku przygotowano projekt ustawy „*Automated and Electric Vehicles Bill*"[132]. Nowy akt prawny ma umożliwić konsumentom korzystanie z nowych rozwiązań technologicznych wykorzystywanych w transporcie. Ustawa zapewnia stworzenie nowego systemu odpowiedzialności w ubezpieczeniach odnoszących się do samochodów autonomicznych oraz opracowanie regulacji dotyczących instalacji oraz obsługi punktów ładowania pojazdów elektrycznych. Obecnie zakończono prace w Izbie Gmin i projekt oczekuje na wyznaczenie terminu posiedzenia komisji w Izbie Lordów. Ze względu na temat tego opracowania, część dotycząca samochodów elektrycznych nie zostanie omówiona.

W projekcie ustawy zaznaczono, że Sekretarz Stanu jest odpowiedzialny za przygotowanie listy wszystkich pojazdów, które są lub mogą być wykorzystywane na drogach lub w innych miejscach publicznych w Wielkiej Brytanii oraz są przystosowane do samodzielnego poruszania się przez chociaż część podróży bez konieczności monitorowania działania systemu oraz obserwowania otoczenia przez osobę siedzącą za kierownicą. Lista musi być podana do publicznej wiadomości po pierwszym sporządzeniu oraz po każdej aktualizacji. Przez pojęcie „samochód autonomiczny" rozumie się jedynie samochody znajdujące się w wykazie przygotowanym przez Sekretarza Stanu. Podstawowa odpowiedzialność za pokrycie szkód powstałych wskutek wypadku spowodowanego przez ubezpieczony samochód autonomiczny spoczywa na ubezpieczycielu. Jeśli jednak samochód nie podlega obowiązkowemu ubezpieczeniu odpowiedzialności cywilnej (zgodnie z przepisami ustawy o ruchu drogowym z 1988 roku są to samochody znajdujące się w posiadaniu m.in. władz lokalnych oraz jednostek policji), takie zobowiązanie spoczywa na właścicielu pojazdu. W porównaniu do zakresu

[132] Automated and Electric Vehicles Bill, HL Bill 82 57/1, (https://publications.parliament.uk/pa/bills/lbill/2017-2019/0082/lbill_2017-20190082_en_1.htm), dostęp: 28.03.2018 r.

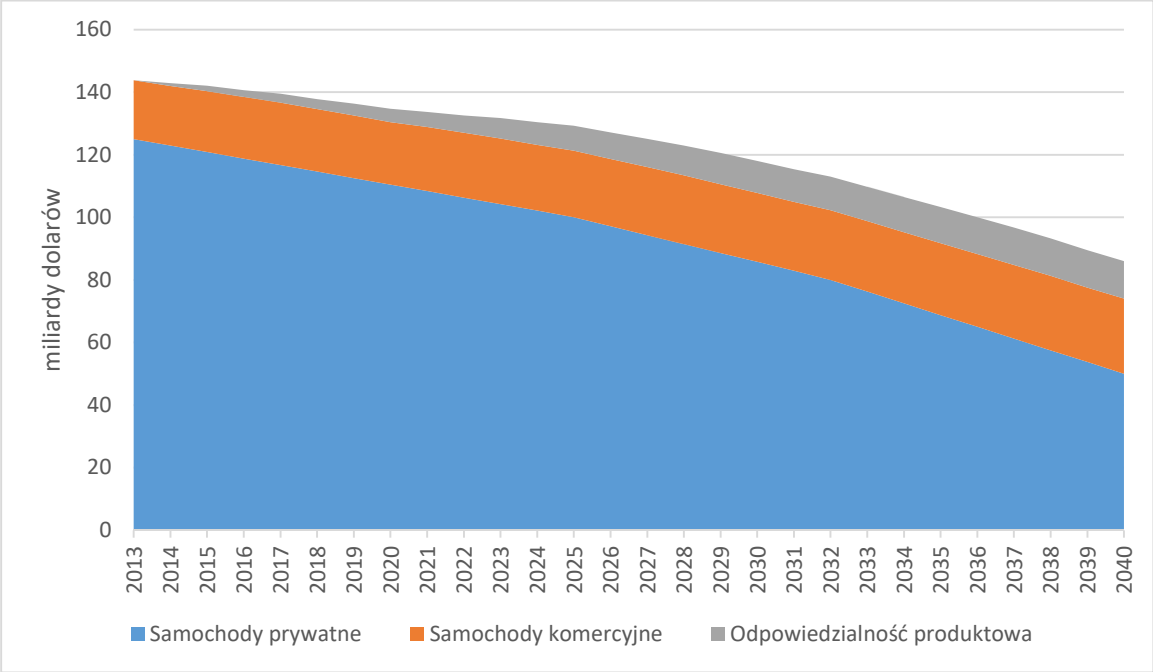
obowiązkowego ubezpieczenia samochodów tradycyjnych, odpowiedzialność ubezpieczyciela została poszerzona o szkody odniesione przez kierowcę w czasie, gdy samochód znajdował się w trybie autonomicznej jazdy. Odpowiedzialność ubezpieczyciela nie może zostać ograniczona lub wyłączona, z wyjątkiem przypadków wymienionych w dalszej części ustawy. Zaznaczono także, że zobowiązanie ubezpieczyciela do wypłaty odszkodowania nie wyklucza jego prawa do wystąpienia z roszczeniem regresowym w stosunku do osoby odpowiedzialnej za wypadek. Jeśli wypadek z udziałem pojazdu autonomicznego został w części spowodowany przez inną osobę poszkodowaną w jego wyniku, odpowiedzialność jest dzielona z uwzględnieniem zasad odnoszących się do wspólnych zaniedbań wynikających z ustawy z 1945 roku[133]. Właściciel oraz ubezpieczyciel samochodu nie ponosi odpowiedzialności za szkody odniesione przez osobę siedzącą za kierownicą, jeśli wypadek w całości wynikał z zaniedbania tej osoby polegającego na aktywowaniu trybu autonomicznego w warunkach, które na to nie pozwalały (np. w okolicy, która nie została poprawnie zmapowana oraz wgrana do systemu). Ustawa dopuszcza określone w polisie ograniczenie odpowiedzialności ubezpieczyciela, jeśli szkoda odniesiona przez ubezpieczonego powstała w wyniku wypadku będącego bezpośrednim następstwem wprowadzenia przez ubezpieczonego lub za jego wiedzą zabronionych przez warunki ubezpieczenia poprawek oprogramowania, a także niedopełnienia przez niego obowiązku zainstalowania aktualizacji niezbędnych do zapewnienia bezpiecznego poruszania się pojazdu. W razie odniesienia szkody przez osoby trzecie w wyniku takiego wypadku, ubezpieczycielowi przysługuje roszczenie regresowe w stosunku do ubezpieczonego, który wprowadził niedozwolone poprawki lub nie zaktualizował systemu. Ubezpieczyciel lub właściciel pojazdu, który pokrył szkody osób poszkodowanych, jest uprawniony do roszczeń regresowych w stosunku do osoby trzeciej odpowiedzialnej za wypadek, do kwoty odszkodowania wypłaconego poszkodowanemu. Kolejny paragraf zapewnia zgodność wprowadzanych przepisów z wcześniejszymi ustawami, np. ustawą o wypadkach śmiertelnych z 1976 roku czy też szkocką ustawą o szkodach z 2011 roku. Określa się także, że odpowiedzialność uregulowana w tej ustawie jest odpowiedzialnością deliktową, a nie kontraktową czy karną.

[133] Law Reform (Contributory Negligence) Act, 1945 Chapter 28 8 and 9 Geo 6, (https://www.legislation.gov.uk/ukpga/Geo6/8-9/28), dostęp: 3.04.2018 r.

5.5. Wypływ samochodów autonomicznych na sektor ubezpieczeń

Jak już zaznaczono w poprzedniej części artykułu, wprowadzenie samochodów autonomicznych wpłynie na zmniejszenie wskaźników wypadkowości, co powinno skutkować obniżeniem składek ubezpieczeniowych, jednak z drugiej strony wprowadzi nowe rodzaje ryzyka, które ubezpieczyciele powinni uwzględnić w oferowanych przez siebie produktach.

Wprowadzenie samochodów autonomicznych spowoduje zmniejszenie rynku klasycznych ubezpieczeń samochodowych. Przewidywane zmiany na tym rynku w Stanach Zjednoczonych obrazuje rysunek 5.1.



Rysunek 5.1. Wartość ubezpieczanych szkód w podziale na ubezpieczenia samochodów prywatnych, komercyjnych oraz odpowiedzialności produktowej w USA w latach 2013-2040 (w mld dolarów)

Źródło: opracowanie własne na podstawie: *Automobile insurance in the era of autonomous vehicles. Survey results*, KPMG 2015, s. 9.

W samych Stanach Zjednoczonych przewiduje się spadek skumulowanej sumy ubezpieczenia z tytułu klasycznych ubezpieczeń samochodowych z ok. 145 mld dolarów w 2013 roku do ok. 86 mld dolarów w roku 2040, co stanowi ok. 40% spadek. Najbardziej dotknięty zostanie sektor ubezpieczeń samochodów prywatnych, w przypadku którego dojdzie do zmniejszenia wartości ubezpieczanych szkód o ok. 60% - ze 125 mld dolarów do 50 mld dolarów. Dojdzie do nieznacznego zwiększenia sumy ubezpieczeniowej z ubezpieczeń

samochodów komercyjnych - z ok. 19 mld dolarów do ok. 24 mld dolarów. Pojawi się nowy rodzaj ubezpieczeń samochodowych – ubezpieczenie odpowiedzialności za produkt, który w 2040 roku będzie odpowiadał za ok. 12 mld dolarów potencjalnych szkód.

W 2015 roku przeprowadzono badanie wśród kadry zarządzającej największych firm ubezpieczeniowych zajmujących się ubezpieczeniami samochodów prywatnych oraz komercyjnych, które miało na celu poznanie poglądów oraz stopnia przygotowania tych firm na upowszechnienie samochodów autonomicznych[134]. Z badań opublikowanych przez KPMG wynika, że jedynie 29% badanych osób kierujących firmami ubezpieczeniowymi posiada szeroką wiedzę na temat pojazdów autonomicznych, natomiast 23% nie posiada praktycznie żadnej wiedzy na ten temat. Pokazuje to, że większość zarządzających nie zdaje sobie sprawy z zalet oraz wad samochodów autonomicznych oraz z ich możliwego wpływu na działalność ubezpieczeniową. Badani wskazali, że wraz z wprowadzaniem samochodów autonomicznych zwiększą swoje zaangażowanie w ubezpieczenia samochodów prywatnych (35% badanych) oraz nie zmienią zaangażowania w ubezpieczenia samochodów komercyjnych (48%). Wynika z tego, że osoby te nie doceniają możliwych zmian w modelu własności samochodów. Wraz z wdrożeniem samochodów autonomicznych bardziej powszechne staną się floty samochodów na wynajem oferowane przez producentów samochodów lub inne podmioty, które zmniejszą zapotrzebowanie społeczeństwa na posiadanie własnego samochodu. Badani przewidują obniżenie składek zarówno w ubezpieczeniach prywatnych (45% zarządzających zdecydowałoby się na taki ruch) oraz komercyjnych (35%), a także wprowadzenie nowych rodzajów produktów do swojej oferty (61% badanych w przypadku ubezpieczeń prywatnych i 45% badanych w przypadku ubezpieczeń komercyjnych). Większość respondentów uważa, że w ciągu najbliższych 10 lat wprowadzenie samochodów autonomicznych nie będzie miało znaczącego wpływu na działalność ubezpieczeniową ich firm. Jednak szybki postęp techniczny może już wcześniej wymusić zmiany w sposobie działania ubezpieczycieli, na które nie będą oni przygotowani. Ponad 70% ankietowanych uważa, że ich przedsiębiorstwo nie jest gotowe na powszechne wprowadzenie samochodów autonomicznych, natomiast jedynie 10% osób zarządzających ubezpieczycielami wskazało, że są na to dobrze przygotowani. Obecnie aż 68% badanych firm nie przeznacza żadnych środków finansowych na działania, które mają

[134] *Automobile insurance…*, *op. cit.*

zwiększyć ich gotowość na nadchodzące zmiany, a jedynie 3% z nich przeznacza na ten cel powyżej 1% swojego budżetu. Firmy, które zdecydowały się podjąć tego typu działania, w większości ograniczyły się do przeprowadzenia rozmów wśród osób pracujących w danej firmie lub z osobami spoza swojej organizacji. Na opracowanie planów operacyjnych lub strategicznych, uwzględniających potencjalny wpływ pojazdów autonomicznych, zdecydowało się jedynie 16%. Pokazuje to, że kwestia pojazdów autonomicznych oraz skala zmian, jakie wywołają one w sposobie przemieszczania się społeczeństwa oraz w zapotrzebowaniu na konkretne produkty ubezpieczeniowe, jest niedoceniana przez ubezpieczycieli. Większość kadry zarządzającej uważa, że do prawidłowego odnalezienia się w zmienionych warunkach, niezbędne będzie właściwe uwzględnienie wpływu wprowadzonych technologii w wycenie składki ubezpieczeniowej. W opinii badanych głównymi usługodawcami oferującymi ubezpieczenia samochodów autonomicznych, oprócz firm ubezpieczeniowych, będą producenci sprzętu (np. Ford, Mercedes Benz), start-upy oraz znane firmy z branży technologicznej (np. Google, Intel).

Jak już wspomniano we wcześniejszej części artykułu, wprowadzenie samochodów autonomicznych do powszechnego użytku oraz związane z tym powstanie nowych rodzajów ryzyka, wykreuje zapotrzebowanie na nowe rodzaje produktów ubezpieczeniowych. Szacuje się, że wartość skumulowanych składek z tego tytułu wyniesie w 2025 roku w Stanach Zjednoczonych 15 mld dolarów, natomiast w 2050 roku ok. 34 mld dolarów[135]. Wśród najważniejszych obszarów, w których ubezpieczyciele powinni rozwinąć swoją działalność, należy wymienić:

- cyberbezpieczeństwo,
- odpowiedzialność produktowa,
- infrastruktura publiczna dla samochodów autonomicznych.

Ubezpieczenie w obszarze cyberbezpieczeństwa powinno obejmować swoim zakresem kradzież pojazdu, nieautoryzowane wejście do pojazdu poprzez wprowadzenie zmian w oprogramowaniu zabezpieczającym zamki oraz wykorzystanie „*ransomware*" do uniemożliwienia korzystania z samochodu do czasu zapłacenia żądanego okupu.

[135] *Insuring autonomous vehicles*, Accenture, Stevens Institute of Technology 2017, (https://www.accenture.com/t20170530T040532__w__/pl-en/_acnmedia/PDF-53/Accenture-Autonomous_Vehicles.pdf), dostęp: 4.04.2018 r.

Opracowane zostaną także polisy ubezpieczeniowe chroniące przed przejęciem kontroli nad pojazdem poprzez *hacking*, a następnie wykorzystaniem przejętego pojazdu do celów kryminalnych lub terrorystycznych. Ubezpieczyciele oferować będą również produkty chroniące przed naruszeniem prywatności, kradzieżą tożsamości lub danych osobowych dokonanym z wykorzystaniem istniejącej zdalnej komunikacji między kilkoma samochodami. Rozwiązania proponowane w zakresie ubezpieczeń związanych z cyberbezpieczeństwem były wzorowane na wzorcach zaczerpniętych z amerykańskiego sektora informatycznego[136].

Ubezpieczyciele będą oferować polisy pokrywające zobowiązania producentów pojazdów autonomicznych wynikające z potencjalnych awarii wyposażenia (np. awaria czujników, kamery monitorującej otoczenie, urządzeń LIDAR oraz radarów), awarii oprogramowania (np. błędów w kodzie, przepełnienia pamięci, wad algorytmów), a także błędów powodujących utratę komunikacji z innymi pojazdami czy też utratę połączenia internetowego. Ubezpieczenie od odpowiedzialności za produkt będzie niezbędne nie tylko ostatecznemu producentowi pojazdu, ale także jego dostawcom bezpośrednim i pośrednim, gdyż w razie awarii wytworzonego przez nich elementu mogą zostać pociągnięci do odpowiedzialności przez ostatecznego wytwórcę, któremu przysługiwać będzie prawo do roszczeń regresowych[137].

Ubezpieczenie w zakresie infrastruktury publicznej dla samochodów autonomicznych powinno gwarantować ochronę podmiotów odpowiedzialnych na wypadek awarii urządzeń umożliwiających kontrolę przemieszczania się pojazdów oraz natężenia ruchu publicznego. Do urządzeń tych zalicza się czujniki oraz sygnalizatory zewnętrzne, podzespoły odpowiedzialne za komunikację między elementami infrastruktury, a także serwery oparte na chmurze, które mogą działać nieprawidłowo lub zostać przeciążone, a ich działanie może być zakłócone przez czynniki zewnętrzne[138].

Przystosowanie się do nowej rzeczywistości, w której samochody autonomiczne będą stanowiły główny środek transportu indywidualnego, będzie wymagało od ubezpieczycieli podjęcia w niedalekiej przyszłości szeregu różnorodnych działań. Samochody autonomiczne będą generowały bardzo liczne dane na temat sposobu jazdy, najczęściej wybieranych tras czy

[136] *Ibidem.*
[137] *Ibidem.*
[138] *Ibidem.*

też wykrywanych zagrożeń. Dostęp do tego typu danych będzie znacznie ograniczony, jednak ze względu na bogactwo informacji, których one dostarczą, warto podjąć kroki zmierzające do uzyskania prawa do wykorzystywania tych danych dla celów ubezpieczeniowych. Jednak samo otrzymanie dostępu do danych nie zapewni sukcesu, niezbędne będzie również przeszkolenie personelu oraz opracowanie niezbędnego oprogramowania umożliwiającego przetwarzanie oraz analizowanie *big data*. Ubezpieczyciele będą musieli także opracować nowe modele aktuarialne uwzględniające zmieniony profil ryzyka. Z każdym kolejnym poziomem automatyzacji zmniejsza się wpływ osoby siedzącej za kierownicą na prowadzenie pojazdu, a więc zmniejsza się ryzyko wynikające z błędów popełnianych przez ludzi. Jednak równocześnie pojawiają się także nowe rodzaje ryzyka związane z wykorzystywaną technologią. Zmodyfikowane modele powinny uwzględniać te dwa aspekty i zapewniać właściwe oszacowanie ryzyka oraz obliczenie adekwatnej do niego składki ubezpieczeniowej. Należy również wziąć pod uwagę rozszerzenie współpracy z producentami wyposażenia, twórcami oprogramowania, rządami oraz innymi podmiotami z branży motoryzacyjnej. Wzajemna wymiana wiedzy oraz doświadczeń tych organizacji w obszarze pojazdów autonomicznych może przynieść znaczne korzyści dla ubezpieczycieli, zwłaszcza w zakresie odpowiedniego przygotowania się do wdrożenia rozwiązań, które dopiero zostaną wprowadzone przez producentów w przyszłości. Ubezpieczyciele, których głównym źródłem przychodów są składki pozyskane z indywidualnych ubezpieczeń komunikacyjnych, powinni rozważyć zmianę modelu biznesowego oraz gamy oferowanych produktów i skupienie swojej uwagi na ubezpieczeniach komercyjnych. Wynika to z faktu, że wraz z upowszechnieniem samochodów autonomicznych zmianie ulegnie model własności samochodów. Straci na znaczeniu posiadanie własnego środka transportu, natomiast zyska na popularności korzystanie z flot samochodów do wynajęcia. Zwiększy się więc zapotrzebowanie na grupowe ubezpieczenia samochodów wykorzystywanych w działalności gospodarczej, a zmniejszeniu ulegnie popyt na indywidualne ubezpieczenia komunikacyjne[139].

5.6. Zakończenie

[139] *Ibidem.*

Po dokonaniu analizy klasyfikacji samochodów autonomicznych, ocenie szans oraz zagrożeń związanych z ich wprowadzeniem na drogi można wyciągnąć wniosek, że wywrą one znaczny wpływ na sektor ubezpieczeń. Dojdzie do skurczenia się rozmiarów tradycyjnego rynku ubezpieczeń komunikacyjnych za sprawą zmniejszenia wypadkowości samochodów autonomicznych i idącym za tym spadkiem składek ubezpieczeniowych. Firmy ubezpieczeniowe będą musiały przystosować się do zmienionego modelu odpowiedzialności, w którym wraz z postępującą automatyzacją samochodów oraz wypieraniem pojazdów tradycyjnych, zanikać będzie odpowiedzialność kierowcy za spowodowane szkody, a zwiększać się będzie zakres odpowiedzialności producentów tych samochodów. Zmiana ta znajdzie swoje odzwierciedlenie w nowych rodzajach produktów oferowanych przez ubezpieczycieli. Ważną rolę w ustalaniu zakresu ubezpieczenia komunikacyjnego samochodów częściowo oraz w pełni autonomicznych odegrają rządy poszczególnych państw oraz instytucje o ponadnarodowym zasięgu. Rozwiązania wprowadzone w Niemczech oraz Wielkiej Brytanii niewątpliwie będą podstawą do opracowania podobnych uregulowań w pozostałych krajach. Niepokojące są wyniki badań wskazujące na niedocenianie przez ubezpieczycieli wpływu samochodów autonomicznych na ich działalność, słabe przygotowanie na powszechne występowanie takich samochodów na drogach oraz niechęć do podejmowania i finansowania działań zmierzających do łatwiejszego odnalezienia się w nowej rzeczywistości, w której samochody autonomiczne będą podstawowym środkiem komunikacji.

Rozdział 6.
Cyberterroryzm we współczesnym świecie i możliwość jego ubezpieczenia

Marta Stokłosa*

6.1. Wprowadzenie

We współczesnych czasach Internet stwarza ogromne szanse rozwoju dla społeczeństwa, jednak niesie ze sobą także wiele zagrożeń. W XXI wieku funkcjonowanie społeczeństw jest coraz bardziej uzależnione od systemów informatycznych. Zwiększenie możliwości wykorzystania zaawansowanej technologii sprawia, iż pojawia się nowy obszar nielegalnej działalności. Można zatem dostrzec, że Internet może być doskonałym narzędziem wykorzystywanym także przez terrorystów. Dzięki rozwojowi technologii informacyjnej z klasycznego terroryzmu wyewoluował jego obecnie najgroźniejszy rodzaj, tzn. cyberterroryzm. W związku z tym zapewnienie bezpieczeństwa w tej dziedzinie stanowi bardzo ważną gałąź bezpieczeństwa narodowego, a także jest jednym z najważniejszych wyzwań XXI wieku.

W związku ze zidentyfikowanym problemem autor postawił następujące pytania badawcze: Jakie są zagrożenia związane z funkcjonowaniem cyberprzestrzeni? Jaka jest skala zagrożenia cyberterroryzmem na świecie? Czy cyberterroryzm zastąpi tradycyjne działania terrorystyczne? Czy istnieją akty prawne, które regulują sferę cyberprzestrzeni w Polsce, a także w zakresie międzynarodowym? Czy można się ubezpieczyć przed cyberterroryzmem?

Z tak postawionych pytań można sformułować następującą hipotezę badawczą: cyberterroryzm stanowi zagrożenie dla funkcjonowania państw, a także jest ryzykiem niespełniającym warunku ubezpieczalności ze względu na potencjalnie katastrofalne rozmiary strat.

* Koło Naukowe Ubezpieczeń „Risk Management”, Katedra Zarządzania Ryzykiem i Ubezpieczeń, Uniwersytet Ekonomiczny w Krakowie.

W celu weryfikacji powyższej hipotezy badawczej dokonano analizy krajowych publikacji naukowych uzupełnionych publikacjami anglojęzycznymi, literaturą z zakresu ubezpieczeń, polskimi i międzynarodowymi aktami prawnymi, a także raportami na temat cyberataków.

Niniejszy artykuł składa się z pięciu części. W pierwszej części scharakteryzowano cyberzagrożenia, a wśród nich cyberterroryzm, będący głównym problemem rozważań artykułu. Następnie opisano skalę cyberterroryzmu poprzez przytoczenie historycznych ataków terrorystycznych w sieci. W trzecim punkcie przeanalizowano akty prawne służące zwalczaniu cyberterroryzmu. Następnie przedstawiono dostępne na rynku ubezpieczenia cybernetyczne. W ostatnim punkcie scharakteryzowano warunki ubezpieczalności ryzyka.

6.2. Miejsce cyberterroryzmu wśród innych cyberzagrożeń

Cyberzagrożenie można zdefiniować jako zagrożenie związane z działalnością w sieci internetowej, handlem online, systemami elektronicznymi oraz przechowywaniem danych osobowych[140]. Do potrzeb analizy rodzajów cyberzagrożeń niezbędne jest zdefiniowanie obszaru, w którym występują, czyli cyberprzestrzeni. Istnieje wiele różnych definicji, jednak w literaturze przedmiotu cyberprzestrzeń jest zdefiniowana jako ogół wirtualnych powiązań („nieprzestrzennych" w sensie fizycznym, niematerialnych), które powstały i istnieją dzięki ich fizycznym manifestacjom (komputery, infrastruktura telekomunikacyjna)[141]. Natomiast w prawie polskim cyberprzestrzeń jest określona ustawowo jako przestrzeń przetwarzania oraz wymiany informacji, tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych wraz z oprogramowaniem), które zapewniają przetwarzanie i przechowywanie oraz wysyłanie i odbieranie danych przez sieci telekomunikacyjne[142].

Istotną kwestią we współczesnym świecie jest zapewnienie bezpieczeństwa w cyberprzestrzeni, co jest zadaniem niewątpliwie trudnym. Wynika to głównie z tego, że cyberprzestrzeń jest zjawiskiem stosunkowo nowym oraz ciężkim do jednoznacznego

[140] T. Olsen, *Cyber Risk*, Willis 2013, s. 6, (https://www.pwc.dk), data dostępu: 02.03.2018 r.
[141] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009, s. 28.
[142] Art. 2 ust. 1b *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (tekst jednolity: Dz.U. 2002, Nr 156 poz. 1301, ze zm.)

zdefiniowania ze względu na jej cechy charakterystyczne, które stanowią w wielu przypadkach swoiste novum[143]. Stanowi to przeszkodę na drodze formalno-prawnego uregulowania kwestii bezpieczeństwa cyberprzestrzeni na poziomie państwowym oraz międzynarodowym. Dlatego przestępcy, nieskrępowani ograniczeniami prawa, sprawnie wymyślają coraz to nowsze formy wykorzystania cyberprzestrzeni w celu prowadzenia nielegalnej działalności, co ułatwia im także szybka dynamika zmian w tym środowisku[144].

Istnieje zatem wiele rodzajów cyberzagrożeń, które można różnie klasyfikować, a ich podstawowy podział przedstawia tabela 6.1.

Tabela 6.1. Rodzaje cyberzagrożeń

Rodzaj cyberzagrożenia	Cechy charakterystyczne
Cyberprzestępstwo	Wykorzystanie cyberprzestrzeni w celu dokonania pospolitych oraz zorganizowanych aktów kryminalnych skierowanych na zasoby osób prywatnych lub organizacji.
Cyberprzemoc	Wykorzystanie cyberprzestrzeni do wymuszania odbioru niepożądanych komunikatów zawierających informacje sprzeczne z wartościami adresata, np. obrazy, dane, treści.
Cyberinwigilacja	Wykorzystanie cyberprzestrzeni w celu kontroli lub pozyskania informacji o zachowaniach oraz działaniach obywateli .
Cyberautorytaryzm	Wykorzystanie cyberprzestrzeni w życiu politycznym państwa sprzeczne z zadami demokracji liberalnej, przeciwieństwo cyberdemokracji.
Cyberterroryzm	Wykorzystanie cyberprzestrzeni w celu dokonywania działań terrorystycznych, pozapaństwowych oraz państwowych.
Cyberwojna	Wykorzystanie cyberprzestrzeni do realizowania działań politycznych z wykorzystaniem sił zbrojnych, skierowanych na struktury i zasoby państwa przeciwnika.

Źródło: K. Węderska, *Cybernetyczny Pearl Harbor- mit czy rzeczywistość?*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka, Diffin, Warszawa 2014, s. 71-72.

Wszystkie wyżej wymienione cyberzagrożenia stanowią istotny problem XXI wieku. Jednakże jako, że po 11 września 2001 roku problem związany z terroryzmem nabrał znaczenia globalnego oraz stał się jedynym z głównych zagrożeń bezpieczeństwa międzynarodowego[145], można stwierdzić, że wraz z postępem technologii informacyjnej oraz upowszechnieniem

[143] T. R. Aleksandrowicz*, Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego,* s. 11, (www.abw.gov.pl/pl/pbw), data dostępu: 02.03.2017 r.
[144] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* Zeszyty Naukowe UEK nr 22/2012, S. Koziej, s. 129.
[145] A. Podraza, P. Potakowski, K. Wiak, *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013, s. 86.

Internetu obecnie to cyberterroryzm jest niewątpliwie jednym z większych zagrożeń dla funkcjonowania państw, gdyż współczesne organizacje terrorystyczne wykorzystują sieci teleinformatyczne do ataków terrorystycznych. Dodatkowo sieć pozwala im zdobyć międzynarodowy rozgłos, co sprawia że odznaczają się wysokim stopniem zorganizowania, a także mają znaczne zasoby środków ekonomicznych oraz technicznych. Duże znaczenie ma również działalność propagandowa, która służy, jak w przypadku Al-Kaidy, do rekrutacji nowych członków, czy też dostarczania instrukcji wykonania bomb bądź do przeprowadzania zamachów terrorystycznych wykorzystujących inne metody i środki działania[146].

Definicja cyberterroryzmu nie jest jednak łatwa do określenia. Specjaliści, którzy zajmują się tym zagrożeniem mają trudności z wskazaniem, jakie działania można określić mianem cyberterroryzmu, a jakie nie[147].

Za twórcę pojęcia cyberterroryzm uznawany jest Barry Collin, pracownik *Institute for Security and Intelligence* z Kalifornii, który użył go dla określenia połączenia cyberprzestrzeni oraz terroryzmu w latach 80 ubiegłego wieku. Zgodnie z B. Collinem, cyberterroryzm jest to świadome wykorzystanie systemu informacyjnego, sieci komputerowej bądź jej składowych części w celu wsparcia albo ułatwienia akcji terrorystycznej[148].

D. Denning podaje węższą definicję stwierdzając, że cyberterroryzm jest bezprawnym atakiem lub groźbą ataku na komputery, sieci bądź systemy informacyjne w celu zastraszenia albo wymuszenia na rządzie bądź ludziach daleko idących politycznych oraz społecznych celów. Dodatkowo dodaje, że za atak cyberterrorystyczny można uznać jedynie taki akt, który spowoduje bezpośrednie szkody człowiekowi oraz jego mieniu albo przynajmniej jest na tyle znaczący, iż budzi strach[149]. Dodatkowo jest przy tym najmniej przewidywalnym z uwagi na fakt powszechności korzystania z sieci internetowej, a także instrumentem wpływania zorganizowanych grup terrorystycznych na funkcjonowanie infrastruktury krytycznej państwa, czyli na krajowe systemy: łączności, transportu, energetyki, zaopatrzenia w wodę, itd.[150].

---

[146] M. Pala, *Wybrane aspekty bezpieczeństwa w cyberprzestrzeni*, [w:] *De Securitate et Defensione. O Bezpieczeństwie i Obronności* nr 1/ 2015, s. 120.

[147] W. Smolski, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa,* [w:] *Repozytorium Uniwersytetu Wrocławskiego,* Wrocław 2015, s. 481.

[148] D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 79

[149] J. Kisielnicki, *MIS. Systemy informatyczne zarządzania*, Wydawnictwo Placet, Warszawa 2008, s. 413.

[150] A. Bógdoł-Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003, s. 203.

Robert Kośla definiuje cyberterroryzm jako działania, które blokują, niszczą albo zniekształcają informacje przetwarzane, przechowywane oraz przekazywane w systemach teleinformatycznych, a także niszczą te systemy[151]. Według R. Kośli, w pojęciu cyberterroryzm mieści się również wykorzystywanie systemów teleinformatycznych do dezinformacji, czy walki psychologicznej. Celem ataku jest jednak najczęściej informacja przetwarzana, a nie cały system jako taki.

Jeszcze inną definicję podaje M. Pollit, który uważa cyberterroryzm za zaplanowany i politycznie umotywowany atak przeciwko systemom, programom komputerowym, a także bazom danych, skutkujący przemocą wobec celów niewojskowych; popełniany przez grupy ponadnarodowe albo tajnych agentów[152].

Wyróżnia się dwa typy cyberterroryzmu w oparciu o kryterium przedmiotowe oraz podmiotowe[153]. Kryterium przedmiotowe dotyczy jedynie skutków ataków cyberterrorystycznych, które mogą mieć charakter militarny, gospodarczy oraz polityczny. Natomiast zgodnie z kryterium podmiotowym można mówić o cyberterrorystach oraz ich ofiarach, czyli o podmiotach działań oraz podmiotach ataku. Patrząc przez pryzmat stosunków międzynarodowych, podmioty ataku stanowią zarówno uczestnicy państwowi jak i niepaństwowi. Natomiast wśród podmiotów działań można wyróżnić grupy zorganizowane oraz cyberterrorystów indywidualnych. Do grup zorganizowanych można zaliczyć zarówno klasyczne organizacje terrorystyczne takie jak np. Tamilskie Tygrysy, czy Al Kaida, które wykorzystują w swoich działaniach oprócz środków konwencjonalnych także cyberprzestrzeń, jak i takie grupy terrorystyczne, które składają się z hakerów komputerowych działających tylko w cyberprzestrzeni. Istnieje kilka tysięcy osób należących do cyberterrorystów indywidualnych, których można określić mianem profesjonalnych hakerów. Są to osoby posiadający ścisłe, wysokie kwalifikacje, które za odpowiednią opłatą mogą wykonywać zadania o charakterze politycznym zlecone przez zorganizowane grupy terrorystyczne[154].

---

[151] R. Kośla, *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski. Wystąpienie na konferencji w Bemowie*, 29 listopada 2002.
[152] M.M. Pollit, *Cyberterrorism – Fact or a Fancy?*, [w:] *Focus on Terrorism*, ed. E.V. Linden, New York 2007, s. 67.
[153] W. Smolski, *Cyberterroryzm…,op. cit.,* s. 482.
[154] *Ibidem.*

Kolejnym aspektem dotyczącym cyberzagrożeń są narzędzia służące do przeprowadzania cyberataków. Można wyróżnić 20 podstawowych narzędzi, które są wykorzystywane do przeprowadzania ataków na systemy informatyczne, a są to[155]:

- wirusy, robaki oraz bakterie (złośliwe oprogramowanie – *malware*) – programy, które rozprzestrzeniając się w systemie informatycznym zmieniają sposób jego działania lub reprodukując się zajmują pamięć procesora, przestrzeń dyskową oraz inne zasoby, a w konsekwencji – blokują dostęp do danych,
- złośliwe podzespoły – umieszczanie w komputerach chipów zawierających programy, które umożliwiają nieuprawniony dostęp do systemu bądź tworzą wady konstrukcyjne,
- konie trojańskie – programy pozwalające na podejmowanie w systemie komputerowym działań bez zgody i wiedzy jego prawowitego użytkownika, np. formatowanie dysków, usuwanie plików, kopiowanie danych itd.,
- uwierzytelnianie – podszywanie się pod osobę, która ma dostęp do systemu,
- próbkowanie – dostęp do komputera poprzez analizę jego charakterystyki,
- ominięcie – ominięcie procesu zabezpieczającego dany system,
- kopiowanie – nieuprawnione kopiowanie plików,
- czytanie – nieuprawniony dostęp do informacji,
- kradzież – przejęcie zasobów systemu przez nieuprawnioną osobę bez pozostawiania kopii,
- modyfikacja – zmiana zawartości danych bądź charakterystyki obiektu ataku,
- usunięcie – zniszczenie obiektu ataku,
- bomby logiczne – aktywizują nowe funkcje elementów logicznych komputera oraz prowadzą do zniszczenia sprzętu i/lub oprogramowania,
- tylne drzwi – pozostawiona przez twórców oprogramowania „furtka" nieznanej użytkownikowi; za ich pomocą można uzyskać nieuprawniony dostęp do systemu,
- przechwycenie transmisji – uzyskanie dostępu do przesyłanych między komputerami treści,

[155] T. R. Aleksandrowicz*, Bezpieczeństwo…, op.cit*., s. 15-16.

- maskarada – udawanie przez atakującego jednego z pełnoprawnych użytkowników systemu poprzez np. modyfikację pakietów w czasie połączenia,
- podsłuchiwanie – śledzenie ruchów występujących w sieci,
- receptor van Ecka – oglądanie przez napastnika na osobnym monitorze repliki obrazów pojawiających się na monitorze komputera atakowanego użytkownika,
- *e-mail bombing* – przesyłanie na skrzynkę pocztową wielkiej ilości danych, co powoduje jej przepełnienie,
- *DDoS (Distributed Denial of Service)* – blokowanie dostępu do strony internetowej poprzez przesyłanie pod jej adresem bardzo dużego pakietu danych z różnych źródeł, co prowadzi do zawieszenia się serwera,
- *electromagnetic pulse* – emisja promieniowania elektromagnetycznego należącego do widma radiowego, co prowadzi do zniszczenia urządzenia elektronicznego i danych.

Często pojęcia cyberatak oraz cyberterroryzm są mylone ze sobą, co może prowadzić do wielu nieporozumień. Warto jednak zaznaczyć, że według D. E. Denning cyberatak, który jest politycznie umotywowany może być przejawem cyberterroryzmu. Musi to jednak dotyczyć przypadku, który nie tylko zakłóca porządek ekonomiczny oraz prawny, ale także pociąga za sobą bardzo duże straty[156].

6.3. Skala zagrożenia cyberterroryzmem na świecie

W XXI rządy państw na całym świecie stoją w obliczu bezprecedensowego poziomu cyberataków i zagrożeń, które mogą podważyć bezpieczeństwo narodowe oraz krytyczną infrastrukturę, a firmy, które przechowują poufne dane klientów walczą o utrzymanie swojej reputacji w wyniku masowych naruszeń danych[157].

Przedsiębiorstwa z różnych sektorów przemysłu narażone są na potencjalnie ogromne straty fizyczne, a także na zobowiązania i koszty w wyniku cyberataków i naruszeń bezpieczeństwa danych[158]. Od roku 2013 do 2018 liczba tych naruszeń wyniosła ponad 7,9

[156] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego,* „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1, 2005, s. 103.
[157] R. P. Hartwig, *Cyber risks: The growing threat*, Insurance information Institute, June 2014, (www.iii.org) data dostępu: 02.03.2018 r., s. 2.
[158] *Global Risks 2014, Ninth Edition, by the World Economic Forum*, (www.weforum.org/risks), data dostępu: 07.03.2018 r.

mld, z czego jedynie 4% dotyczyło tzw. "bezpiecznych naruszeń", czyli takich w których zastosowano szyfrowanie, a skradzione dane stały się bezużyteczne[159]. W tabeli 2 przedstawiono przykłady największych naruszeń danych w ostatnich latach na świecie.

Tabela 6.2. Przykłady największych naruszeń bezpieczeństwa danych osobowych na świecie w latach 2013-2017

Nazwa firmy	Rok ataku	Liczba wykradzionych danych osobowych
MySpace	2013	360 000 000
Target	2013	110 000 000
eBay	2014	145 000 000
CyberVor	2014	1 200 000 000
Friend Finder Networks	2016	412 214 295
Equifax	2017	143 000 000
Reliance Jio	2017	120 000 000

Źródło: Opracowanie własne na podstawie: *Top Scoring Data Breaches*, (www.breachlevelindex.com), data dostępu: 07.03.2018 r.

Skala różnego rodzaju ataków w cyberprzestrzeni jest ogromna, choć nie wszystkie z nich to ataki terrorystyczne. Można wysnuć wniosek, iż cyberterroryzm ma bardzo duży potencjał rozwoju, co potwierdzają również liczne przykłady jego wykorzystania.

Pierwszym z nich była operacja „Pustynna burza" w latach 90 XX wieku w Zatoce Perskiej. Hakerzy złamali zabezpieczenia amerykańskie zdobywając w ten sposób strategiczne dane dotyczące ich ataku na Irak. Natomiast pracownicy wojskowi USA umieszczali wirusy komputerowe w kserokopiarkach oraz drukarkach, które dostarczali do Iraku jeszcze przed konfliktem w Zatoce Perskiej, co doprowadziło do zniszczenia nawet około 50% irackich układów scalonych. Pokazało to już wtedy, że odchodzi się od tradycyjnych metod terroryzmu na rzecz cyberterroryzmu[160].

W 1999 roku podczas walk w Kosowie, obie strony konfliktu korzystały z Internetu. Nie tylko wspierał on oficjalną propagandę natowską i jugosłowiańską, ale także służył do komunikacji, demonizowania przeciwnika, włamywania się na strony internetowe oraz atakowania za pomocą wirusów. Serbowie wysyłali tysiące e-maili do różnego rodzaju

[159] Data Breach Statistic, (www.breachlevelindex.com), data dostępu: 07.03.2018 r.
[160] K. Węderska, *Cybernetyczny…, op. cit.,* s. 74.

organizacji, np. prasy, telewizji, radia, czy rządów państw NATO z apelem o zaprzestanie bombardowania. Skupiały się one przede wszystkim na masakrach, które powodowały naloty natowskie. Natomiast NATO, Brytyjczycy oraz Amerykanie używali Internetu do celów propagandowych[161]. NATO tydzień po rozpoczęciu operacji poniosło istotną porażkę, ponieważ hakerzy z Serbii i Czarnogóry zdołali zablokować oficjalny serwer www sojuszu poprzez wysłanie przez pocztę elektroniczną kilkadziesiąt tysięcy listów z protestem przeciwko operacji NATO w Jugosławii. Przykład ten dowodzi na to, że konfliktowi konwencjonalnemu mogą także towarzyszyć konflikty elektroniczne[162].

W 2000 roku miał miejsce internetowy konflikt arabsko – izraelski, zwany przez Palestyńczyków *elektronicznym dżihadem*. Wszystko zaczęło się od uprowadzenia do Libanu trzech izraelskich żołnierzy przez libański Hezbollah, co spowodowało ponowne wkroczenie sił zbrojnych Izraela do Libanu. Towarzyszyły temu ataki cybernetyczne obu stron, które dotyczyły przede wszystkim stron rządowych i finansowych. Hakerzy będący po stronie Izraela włamali się na stronę organizacji terrorystycznej, gdzie umieścili gwiazdę Dawida, hebrajskie napisy oraz izraelski hymn. Z kolei palestyńscy hakerzy zaatakowali strony Kancelarii Prezesa Rady Ministrów i Ministerstwa Obrony. Byli wśród nich m.in. terroryści z Al. Kaidy, Hezbollahu oraz Hamasu[163].

W 2001 roku Chińczycy przechwycili amerykański samolot zwiadowczy, który przymusowo lądował w Chinach po zderzeniu z myśliwcem chińskim. Waszyngton został oskarżony przez Pekin o szpiegostwo, co doprowadziło do wybuchu wojny elektronicznej między USA a Chinami. Hakerzy amerykańscy umieścili na stronach chińskich instytucji oraz firm pornograficzne obrazki, a także obraźliwe hasła. Ponadto dokonali kilkuset ataków np. na *China Nuclear Information Center*, *China Telecom* i strony rządowe. Hakerzy chińscy odpowiedzieli od razu. Utworzyli stronę internetową www.killusa.com, z której każda osoba chcąca wziąć udział w antyamerykańskiej krucjacie, mogła znaleźć potrzebne oprogramowanie. Zaatakowany został Biały Dom, Departamenty Zdrowia, Pracy, Energetyki i

[161] M. F. Gawrycki, *Cyberterroryzm*, Fundacja Studiów Międzynarodowych, Warszawa 2003, s.166-167.
[162] *E-Terroryzm.pl*, Internetowy Biuletyn Instytutu Studiów nad Terroryzmem, Listopad 2013, s. 6.
[163] *Ibidem*, s. 6-7.

Spraw Wewnętrznych, a także Izba Reprezentantów oraz Dowództwo Marynarki Wojennej. W wyniku obustronnych działań zdobyto 1500 stron amerykańskich i ponad 300 chińskich[164].

W 2007 roku w Estonii został przeniesiony z centrum Tallina na przedmieścia pomnik Żołnierzy Armii Czerwonej. Spowodowało to liczne zamieszki, a także doprowadziło do masowych cyberataków. Polegały one na przesyłaniu dużej ilości danych, co zablokowało strony oraz serwery rządowe, kancelarii prezydenta i największych gazet. Dodatkowo zawiesiły się systemy bankowe oraz wewnętrzna sieć policji Estonii. Mieszkańcy byli odcięci od Internetu, a co za tym idzie również od pieniędzy zdeponowanych w bankach. Nie działały bankomaty, sieci komórkowe, a także poczta elektroniczna[165]. Podczas tego ataku wykorzystano *DDoS*, czyli metodę, która polega na zarzucaniu określonych serwerów olbrzymią ilością danych, co prowadzi do ich przeciążenia i zablokowania. O atak oskarżono Rosję, jednak ostatecznie nie udało się im udowodnić winy[166].

Następną ofiarą cyberataku była w 2008 roku Gruzja. Zastosowano wtedy, podobnie jak w przypadku Estonii, ataki *DDoS*, a także podmieniono niektóre strony rządowe i wysyłano sfałszowane komunikaty CNN oraz BBC, które infekowały komputery. Nie działały nie tylko strony rządowe, ale także strony niektórych ambasad i banków. W tych cyberprzestępstwach brały udział serwery rosyjskie takie, jak *Russian Business Network*, czy *StopGeorgia.ru*[167].

W 2010 roku w konflikcie pakistańsko-indyjskim używano cyberprzestrzeni do trwających ponad pół roku wzajemnych włamań hakerów obu stron na strony internetowe m.in. mediów, wyższych uczelni, służb bezpieczeństwa, wojska czy korporacji[168].

Również w 2010 roku celem ataku cybernetycznego zostały irańskie systemy obsługujące prawie całą infrastrukturę państwa, łącznie blisko 30 tysięcy komputerów. Przypuszcza się, że atak miał za zadanie zniszczyć, uszkodzić albo zlikwidować reaktor jądrowy Iranu. Trojan

[164] *Ibidem*, s.7.
[165] S. Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, Journal of Strategic Security, Number 2 Volume 4, No. 2, Federation of American Scientists, Washington, D.C., Summer 2011, s. 50.
[166] *Ibidem*, s. 51.
[167] S. W. Korns, J. E. Kastenberg, *Georgia's Cyber Left Hook, (*http://ssi.armywarcollege.edu) data dostępu: 09.03.2018 r.
[168] *Indyjsko-pakistański konflikt o Kaszmir*, (www.psz.pl) data dostępu: 09.03.2018 r.

którego użyto – *Stuxnet23*, skutecznie sparaliżował irański system elektrowni atomowych w Natanz i Buszehr, co opóźniło uruchomienie elektrowni jądrowej w Buszehr o dwa miesiące[169].

6.4. Zwalczanie cyberterroryzmu - aspekt prawny

Ze względu na szczególną szkodliwość społeczną cyberterroryzmu oraz coraz większe zagrożenie, które stwarza dla współczesnego świata, zaczęto ustanawiać nowe przepisy prawne regulujące sferę cyberprzestrzeni, nie tylko w prawodawstwie poszczególnych krajów, ale także na gruncie międzynarodowym.

W Polsce przestępstwa o charakterze cyberterrorystycznym są uregulowane w Kodeksie Karnym[170] i podlegają odpowiedzialności karnej jako tzw. czyny noszące znamiona klasycznych przestępstw terrorystycznych albo jako „przestępstwa komputerowe". W rozdziale XXXIII Kodeksu Karnego pt. „Przestępstwa przeciwko ochronie informacji" ustawodawca pogrupował przestępstwa, które należy uznać za wykroczenia przeciwko ochronie informacji w cyberprzestrzeni, a są to:

- bezprawny dostęp do informacji, do całości lub części systemu informatycznego poprzez otwieranie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej lub przełamanie albo omijanie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia - kara ograniczenia wolności albo pozbawienia wolności do lat 2; ta sama kara grozi za zakładanie lub posługiwanie się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem w celu uzyskania bezprawnej informacji, bądź ujawnienie takiej informacji innej osobie (art. 267),
- bezprawne zniszczenie, uszkadzanie, usuwanie lub zmienianie zapisu istotnej informacji albo w inny sposób udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznania się z nią - kara ograniczenia wolności albo pozbawienia wolności do lat 2; jeśli dotyczy to zapisu na informatycznym nośniku danych – kara pozbawienia wolności do lat 3; natomiast jeżeli sprawca wyrządza przy tym znaczną szkodę majątkową – kara pozbawienia wolności od 3 miesięcy do lat 5 (art. 268),

[169] K. Węderska, *Cybernetyczny, op. cit.,* s. 77.
[170] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*, (Dz. U. 1997, Nr 88, poz. 553, ze zm.).

- bezprawne zniszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych albo w istotnym stopniu zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych - kara pozbawienia wolności do lat 3; jeśli następuje przy tym wyrządzenie znacznej szkody majątkowej - kara pozbawienia wolności od 3 miesięcy do lat 5 (art. 268a),
- niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych - kara pozbawienia wolności od 6 miesięcy do lat 8; ta sama kara za niszczenie albo wymienianie informatycznych nośników danych lub niszczenie albo uszkadzanie urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych (art. 269),
- bezprawne zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej w istotnym stopniu przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych -kara pozbawienia wolności od 3 miesięcy do lat 5 (art. 269a),
- wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej - kara pozbawienia wolności do lat 3 (art. 269b).

Dodatkowo kwestie cyberzagrożeń porusza również dokument pod tytułem Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022[171], który jest następstwem działań podejmowanych w przeszłości przez administrację rządową. Jest to dokument wykonawczy w stosunku do Strategii Bezpieczeństwa Narodowego RP– Doktryną cyberbezpieczeństwa RP wydaną przez Biuro Bezpieczeństwa Narodowego w 2015 r[172].

[171] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*, Ministerstwo Cyfryzacji, Warszawa 2017, (www.gov.pl) data dostępu: 18.04.2018 r.
[172] *Doktryna cyberbezpieczeństwa RP,* BBN, 2015, (https://www.bbn.gov.pl) data dostępu: 18.04.2018 r.

Założeniem Strategii jest określenie ramowych działań, które mają na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów infrastruktury krytycznej, operatorów usług kluczowych, dostawców usług cyfrowych, a także administracji publicznej na incydenty w cyberprzestrzeni. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu, a także zwalczaniu przestępstw i działań o charakterze terrorystycznym oraz szpiegowskim w cyberprzestrzeni. Strategia ta jest spójna z prowadzonymi działaniami dotyczącymi operatorów infrastruktury krytycznej, które wykorzystują systemy teleinformatyczne i uwzględniają potrzeby zaangażowania Sił Zbrojnych Rzeczypospolitej Polskiej[173].

Natomiast na gruncie międzynarodowym w Europie pierwszą próbę zdefiniowania czynów stwarzających zagrożenia w cyberprzestrzeni podjęła Rada Europy, która w 2001 r. w Budapeszcie przyjęła Konwencję o cyberprzestępczości[174]. Konwencja budapesztańska dzieli przestępstwa popełniane w cyberprzestrzeni na cztery kategorie:

- przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów,
- przestępstwa komputerowe,
- przestępstwa ze względu na charakter zawartych informacji,
- przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Do pierwszej kategorii zalicza się:

- nielegalny dostęp (art. 2), będący umyślnym, bezprawnym dostępem do całości lub części systemu informatycznego; można jednak wprowadzić wymóg, że przestępstwo musi zostać popełnione przez naruszenie zabezpieczeń i z zamiarem pozyskania danych informatycznych albo z innym nieuczciwym zamiarem bądź w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym,
- nielegalne przechwytywanie danych (art. 3), czyli umyślne, bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych z, do, lub w ramach systemu informatycznego, łącznie z emisjami

[173] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, op. cit.,* s. 6.
[174] *Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.*, (Dz. U. 2015 poz. 728, z późn. zm.).

elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Można wprowadzić wymóg, że przestępstwo musi zostać popełnione z nieuczciwym zamiarem albo w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym,

- naruszenie integralności danych (art. 4), definiowane jako umyślne, bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian albo usuwanie danych informatycznych. Można zastrzec sobie prawo wprowadzenia wymogu, że zachowanie opisane w ustępie l musi skutkować poważną szkodą,
- naruszenie integralności systemu (art. 5), rozumiane jako umyślne, bezprawne, poważne zakłócanie funkcjonowania systemu informatycznego przez wprowadzanie, wykasowywanie, transmisję, niszczenie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych,
- niewłaściwe wykorzystywanie urządzeń (art. 6), czyli umyślne oraz bezprawne działania polegające na produkcji, sprzedaży, pozyskiwaniu z zamiarem wykorzystania, dystrybucji, importowania, lub innego udostępniania: - urządzenia, w tym także programu komputerowego, przeznaczonego albo przystosowanego przede wszystkim do popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5, - hasła komputerowego, kodu dostępu albo podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna.

Drugą kategorię stanowią przestępstwa komputerowe takie jak:

- fałszerstwo komputerowe (art. 7), rozumiane jako umyślne, bezprawne wprowadzanie oraz dokonywanie zmian, wykasowywanie albo usuwanie danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne, bez względu na to, czy są one zrozumiałe oraz czy można je bezpośrednio odczytać. Można wprowadzić wymóg, że odpowiedzialność karna dotyczy działania w zamiarze oszustwa lub w podobnym nieuczciwym zamiarze,
- oszustwo komputerowe (art. 8), które jest umyślnym, bezprawnym spowodowaniem utraty majątku przez inną osobę spowodowane: wprowadzeniem, dokonaniem zmian, wykasowaniem lub usunięciem danych informatycznych bądź każdą ingerencją w

funkcjonowanie systemu komputerowego z zamiarem oszustwa albo nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.

Trzecią kategorią przestępstw w cyberprzestrzeni są przestępstwa ze względu na charakter zawartych informacji. Dotyczą one czynów związanych z bezprawnym oraz umyślnym produkowaniem, oferowaniem, udostępnianiem, pozyskiwaniem i posiadaniem pornografii dziecięcej za pomocą systemu informatycznego (art. 9).

Do ostatniej, czwartej kategorii przestępstwa należą wszelkie naruszania praw autorskich oraz pokrewnych z wykorzystaniem systemu informatycznego.

Kolejnym aktem prawnym na gruncie międzynarodowym jest prawo Unii Europejskiej, które definiuje przestępstwa cybernetyczne w dyrektywie o atakach na systemy informatyczne[175]. Jej treść jest obowiązującym aktem prawotwórczym dla wszystkich członków Unii Europejskiej i zobowiązuje ich do podjęcia kroków, które umożliwią karanie jako przestępstw:

- niezgodnego z prawem dostępu do systemów informatycznych (art. 3), czyli umyślnego oraz bezprawnego uzyskiwania dostępu do całości albo jakiejkolwiek części systemu informatycznego, gdy zostało ono popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi,
- niezgodnej z prawem ingerencji w systemy (art. 4), a zatem umyślnego oraz bezprawnego uzyskiwania dostępu do całości albo jakiejkolwiek części systemu informatycznego, gdy to przestępstwo zostało popełnione z naruszeniem środków bezpieczeństwa, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi,
- niezgodnej z prawem ingerencji w dane (art. 5), definiowanej jako umyślne oraz bezprawne usuwanie, pogarszanie, uszkadzanie, zmienianie albo eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi,
- niezgodnego z prawem przechwytywania (art. 6), a więc umyślnego oraz bezprawnego przechwytywania za pomocą środków technicznych niepublicznych przekazów danych komputerowych z, do, lub w ramach systemu informatycznego, w tym emisji

[175] *Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiS,* (Dz. Urz. UE L 218 z 14 VIII 2013 r. poz. 8.).

elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi.

W art. 7 pod tytułem *Narzędzia do popełniania przestępstw* przedstawiono czyny polegające na umyślnym wytwarzaniu, dostarczaniu, sprzedaży w celu użycia oraz przywozu, rozpowszechnianiu albo udostępnianiu w inny sposób: programu komputerowego, zaprojektowanego albo przystosowanego głównie do popełnienia jednego z wymienionych przestępstw, kodu dostępu, hasła komputerowego lub podobnych danych umożliwiających dostęp do całości bądź części systemu informatycznego. Tak, jak w przypadku pozostałych czynów, warunkiem uznania tych czynów za przestępstwa jest bezprawność oraz umyślność działania sprawcy, a także to, że czyn nie stanowi przypadku mniejszej wagi.

Istotną kwestią w walce z cyberterroryzmem jest współpraca w wymiarze międzynarodowym. Polskie organizacje, które reagują na incydenty w cyberprzestrzeni, współpracują oraz należą do międzynarodowych organizacji przeciwdziałających zagrożeniom w cyberprzestrzeni, a są to[176]:

- *European Network and Information Security Agency* (ENISA), działająca w ramach państw członkowskich UE;
- *Cooperative Cyber Defence Centre of Excellence* (CCDCoE), które działa w ramach Sojuszu Północnoatlantyckiego;
- *NATO Cyber Defence Management Authority*;
- *Forum of Incident Response and Security Teams* (FIRST) zrzeszająca zespoły CERT (Computer Emergency Response Team) z całego świata.

Istnienie organizacji międzynarodowych umożliwia szybką wymianę potrzebnych informacji, co z kolei umożliwia bardzo szybkie reagowanie na nowe zagrożenia generowane poprzez Internet. Funkcjonowanie tego typu organizacji umożliwia również porównywanie rozwiązań technologicznych miedzy państwami, a także powstawanie ujednoliconego systemu zabezpieczeń, gwarantującego wysoki jego poziom we wszystkich krajach zrzeszonych[177].

[176] M. Pala, *Wybrane…, op. cit.,* s. 126.
[177] K. Żukrowska, M. Grącik, *Bezpieczeństwo międzynarodowe*, Szkoła Główna Handlowa ,Warszawa 2006, s. 187.

6.5. Cyberterroryzm jako przedmiot ubezpieczenia

Według raportu sporządzanego przez Allianz Global Corporate & Specialty[178], wśród 10 największych zagrożeń dla przedsiębiorstw w 2017 roku wyróżnia na pierwszym, bądź drugim miejscu, ryzyka związane z cyberprzestrzenią. Dodatkowo, według badań Allianz, cyberryzyko z pozycji 15 miejsca w 2013 roku awansowało na 3 największe zagrożenie dla funkcjonowania biznesu w 2017 roku. Zdaniem Michaela Bruch'a, szefa Emerging Trends w AGCS[179], zwiększenie wzajemnych połączeń i wyrafinowanie cyberataków stwarza nie tylko ogromne bezpośrednie ryzyko dla klientów korporacyjnych i komercyjnych, ale także pośrednio poprzez narażone krytyczne infrastruktury, takie jak IT, woda lub zasilanie. Cyberataki mogą poważniej wpłynąć na firmy i społeczeństwa poprzez długotrwałe i powszechne przerwy w działaniu tych krytycznych infrastruktur. Natomiast z danych opracowanych przez Allbroker[180] roczny globalny koszt związany z cyberatakami wynosi 1780 mld zł, z czego w Polsce jest to 7 mld zł, co stanowi około 0,4% PKB. W związku z tym należałoby się zastanowić, czy cyberubezpieczenia nie zmniejszyłyby znacząco ryzyka związanego z cyberprzestrzenią, w szczególności z cyberterroryzmem oraz czy nie mogłyby obniżyć kosztów występowania cyberterroryzmu.

W 2018 roku na polskim rynku ubezpieczeń, ubezpieczenia cybernetyczne dostępne są w ofercie pięciu towarzystw ubezpieczeń[181]:

- STU Ergo Hestia S.A. – ubezpieczenie danych elektronicznych od ryzyka cybernetycznego,
- Chubb European Group Limited Oddział w Polsce – ubezpieczenie DataGuard Advantage,
- AIG Europe Limited Sp. z o.o. Oddział w Polsce – ubezpieczenie CyberEdge,
- Leadenhall Polska S.A. – ubezpieczenie Leadenhall Cyber,
- TUiR Allianz Polska S.A. – ubezpieczenie Cyber Protect.

[178] Allianz Risk Barometer 2018: Appendix , Allianz Global Corporate & Specialty, (www.agcs.allianz.com), data dostępu: 23.03.2018 r., s. 28.
[179] *Allianz Risk Barometer 2017 - Top risks in focus: Cyber* incidents, **Allianz Global Corporate & Specialty,** (www.agcs.allianz.com) data dostępu: 23.03.2018 r.
[180] *Cyber ubezpieczenia,* Allbroker Sp z.o.o., (www.allbroker.pl) data dostępu: 23.03.2018 r.
[181] G. Strupczewski, *Zagrożenia cybernetyczne instytucji finansowych* [w:] *Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych*, nr 24 (2/2017), s. 78.

Wymienione wyżej ubezpieczenia, oprócz ubezpieczenia Leadenhall Cyber, mają konstrukcję pakietową. Jest ona oparta na podziale na trzy sekcje, które obejmują różne rodzaje ryzyka cybernetycznego. Pierwsza sekcja jest traktowana z reguły jako wariant podstawowy, a pozostałe dwie sekcje i opcjonalne klauzule dodatkowe przedstawiają możliwe rozszerzenia zakresu ochrony ubezpieczeniowej.

W ubezpieczeniu Chubb w zakresie podstawowym (sekcja I) występuje ochrona danych elektronicznych przed ryzykiem cybernetycznym. Sekcja II rozszerza ochronę o inne ryzyka, w tzw. w systemie *all risk*, na które są narażone dane komputerowe. Natomiast sekcja III przewiduje dodatkowo ubezpieczenie ryzyka utraty zysków przedsiębiorstwa oraz powstania kosztów dodatkowych na skutek realizacji jednego z wymienionych ryzyk cybernetycznych w ramach sekcji I lub II[182].

Ubezpieczenie cybernetyczne w Ergo Hestii w ramach sekcji I jest porównywalne do ubezpieczenia w Chubb. W sekcji II jednak proponuje dodatkowo ubezpieczenie od zwiększonych kosztów działalności przedsiębiorstwa wynikających z utraty bądź uszkodzenia danych elektronicznych. Są to koszty: porad prawnych, public relations w celu przywrócenia reputacji, przeniesienia nieutraconych danych na inne serwery, ograniczenia skutków utraty danych). W sekcji III natomiast jest oferowane ubezpieczenie odpowiedzialności cywilnej za szkody wyrządzone osobom trzecim na skutek zaistniałego ataku komputerowego albo hakerskiego. Są to m.in. koszty: odtworzenia i przywrócenia danych lub systemu u poszkodowanych; działania specjalistów z zakresu informatyki śledczej poniesione w związku z poszukiwaniem sprawcy ataku komputerowego; postępowań administracyjnych związanych z ochroną danych osobowych (GiODO), a także ochroną prawa własności intelektualnej (Urząd Patentowy); czy także utracone korzyści poniesione przez osoby trzecie powstałe wskutek uszkodzenia, utraty danych lub powstałych w wyniku wycieku danych personalnych osób trzecich. W ramach dodatkowej klauzuli możliwe jest także ubezpieczenie danych w chmurze obliczeniowej[183].

W ubezpieczeniu AIG w sekcji I jest zawarte ryzyko odpowiedzialności cywilnej ubezpieczonego za wszystkie szkody wyrządzone działalnością gospodarczą w sferze

[182] *Ubezpieczenie w zakresie ryzyk cybernetycznych (Cyber),* Chubb European Group Limited Sp. z o.o., (www.chubb.com) data dostępu 23.03.2018 r.
[183] *Ubezpieczenia cybernetyczne*, Ergo Hestia S.A.,(www.ergohestia.pl) data dostępu 23.03.2018 r.

przechowywania oraz wykorzystania danych elektronicznych, również danych osobowych. W sekcji II ubezpieczenie jest rozszerzone o koszty kar administracyjnych nałożonych przez uprawnione do tego instytucje oraz organy publiczne, a także koszty reprezentowania ubezpieczonego w postępowaniach przed tymi organami. W sekcji III natomiast istnieje możliwość wykupienia ochrony na wypadek powstania innych kosztów dodatkowych związanych z wystąpieniem cyberzagrożenia, a są to np.: zawiadomienie poszkodowanych o naruszeniu bezpieczeństwa danych, zatrudnienie specjalistów z zakresu informatyki śledczej, ochrona reputacji, odzyskanie utraconych danych. Dodatkowo do zakresu ochrony ubezpieczeniowej mogą zostać włączone: działalność multimedialna, próby wymuszenia, a także utrata zysku w wyniku zakłócenia działania sieci[184].

Ubezpieczenie Allianz w sekcji I jest podobne do AIG, gdyż także oferuje ubezpieczenie OC, natomiast w sekcji II obejmuje ochronę w trakcie przerwy w prowadzeniu działalności, spowodowanej awarią systemu komputerowego przedsiębiorstwa oraz cyberwymuszenia. Sekcja III rozszerza dodatkowo ubezpieczenie o koszty wsparcia PR oraz koszty doradztwa eksperta IT[185].

Ostatnim z dostępnych na polskim rynku ubezpieczeń cybernetycznych jest ubezpieczenie Leadenhall Cyber. Jest ono inaczej skonstruowane od tych wcześniej wymienionych, ponieważ zakres ochrony jest podzielony na sekcje od A do G. Sekcje A i D obejmują ubezpieczenie odpowiedzialności cywilnej oraz kosztów obrony w sprawach o naruszenie prywatności, sekcja B - koszty kar za naruszenie prywatności, sekcja C - koszty naruszenia bezpieczeństwa informacji, sekcja E - odpowiedzialność multimedialną, czyli odpowiedzialność za publikacje np. w mediach społecznościowych, czy stronach internetowych, sekcja F - pokrycie kosztów i wymuszonych płatności w związku z atakiem hakerskim, a sekcja G - koszty odtworzenia danych oraz utracony zysk związany z przestojem wywołanym np. włamaniem do systemu informatycznego ubezpieczonego[186].

Mimo iż opisane ubezpieczenia cybernetyczne obejmują ochronę przed wieloma aspektami zagrożeń w cyberprzestrzeni, należy zauważyć, iż analizując ogólne warunki

[184] *Ubezpieczenie Cyber Edge*, AIG Europe Limited Oddział w Polsce, (www.aig.pl) data dostępu: 23.03.2018 r.
[185] *Ubezpieczenie technologii cyfrowych i ochrony danych (Cyber Protect),* Allianz SE, (www.allianz.pl) data dostępu: 23.03.2018 r.
[186] *Ubezpieczenie Cyber,* Leadenhall Polska S.A., (www.leadenhall.pl) data dostępu: 23.03.2018 r.

ubezpieczenia, we wszystkich z wymienionych ofert widnieje zapis, że z ochrony ubezpieczeniowej wyłączone są wszelkie koszty wynikające z ataków cybernetycznych związanych z: terroryzmem, działaniami wojennymi, zamieszkami, wojną, czy działaniem władz.

6.6. Cyberterroryzm a warunki ubezpieczalności ryzyka

Skoro wszystkie dostępne ubezpieczenia cybernetyczne nie obejmują swoim zakresem cyberterroryzmu, można zadać pytanie, dlaczego mimo wzrastającej groźby cyberterroryzmu żadna z firm ubezpieczeniowych nie oferuje ubezpieczenia obejmującego to zagrożenie. W celu uzyskania odpowiedzi na to pytanie należy przypomnieć, czym jest ubezpieczalność ryzyka oraz jakie są jej zasady.

Ubezpieczalność ryzyka z definicji polega na możliwości jego transferu do zakładu ubezpieczeń[187]. Ryzyko jest ubezpieczalne wtedy, gdy powsiada takie cechy, jak[188]:

- definiowalność oraz mierzalność, tzn., że szkody winny być jasno, a także w miarę precyzyjnie określone, powinna zaistnieć łatwość stwierdzenia, czy i kiedy dana szkoda wystąpiła, a także czy można określić jej wartość,
- powtarzalność, czyli występowanie dużej liczby jednorodnych zdarzeń, które generują szkody, co w konsekwencji pozwala korzystać z prawa wielkich liczb w celu prognozowania wielkości szkody,
- losowość, która oznacza, że występowanie szkód powinno być wynikiem pewnych zdarzeń, które mogą, ale nie muszą zajść; nie mogą to być więc zdarzenia, które na pewno się wydarzą w określonym wcześniej czasie,
- brak szkód katastroficznych, czyli brak sytuacji, w której jedną szkodą w tym samym czasie dotkniętych został duży procent ubezpieczonych obiektów bądź ludzi.

Z kolei Berliner w 1982 roku wprowadził proste, ale rygorystyczne i kompleksowe podejście do różnicowania między ryzykami ubezpieczalnymi i nieubezpieczalnymi. To podejście, które opiera się na dziewięciu kryteriach ubezpieczalności jest często

[187] M. Fedor, *Granice ubezpieczalności cz. 1*, Gazeta Ubezpieczeniowa- Pismo Środowisk ubezpieczeniowych i fananswych 2004, (www.gu.com.pl), data dostępu: 20.04.2018 r.
[188]P. Kowalczyk, E. Poprawska, W. Ronka-Chmielowiec, *Metody aktuarialne*, Wydawnictwo PWN, Warszawa 2006, s. 13.

wykorzystywane do analizy rynków i produktów ubezpieczeniowych. Kryteria te są podzielone na trzy szerokie kategorie, które klasyfikują ryzyko pod względem aktuarialnym, rynkowym i i społecznym (patrz Tabela 6.3)[189].

Ryzyko kwalifikujące się jako ubezpieczalne w kategorii aktuarialnej wymaga niezależności wystąpienia i wiarygodności oszacowania prawdopodobieństwa straty (losowość wystąpienia straty). Dodatkowo zakłady ubezpieczeń muszą mieć możliwość zarządzania suma ubezpieczeniową, tak by gwarantowało to ich wypłacalność (maksymalna możliwa strata), a średnia strata na zdarzenie powinna być umiarkowana. Liczba zdarzeń rocznie musi być wystarczająco duża (masowość zdarzeń), a także nie powinna występować nadmierna asymetria informacji (tj. pokusa nadużycia, selekcja negatywna). Kryteria aktuarialne obejmują prawo wielkich liczb, które jest centralnym paradygmatem w teorii ubezpieczeń i oznacza, że im większa liczba wzajemnie niezależnych i identycznie rozłożonych ryzyk w portfelu ryzyka, tym niższa wariancja łącznej wartości strat[190].

Kryteria rynkowe odnoszą się do adekwatności składek ubezpieczeniowych, których wysokość powinna zapewnić wystarczający zwrot kapitału dla ubezpieczyciela. Odpowiednia składka ubezpieczeniowa jest ustalana w wysokości zapewniającej środki finansowe na wypłatę odszkodowań oraz świadczeń, na tworzenie rezerwy techniczno - ubezpieczeniowej i funduszów rezerwowych, a także na pokrycie kosztów działalności ubezpieczeniowej[191]. Składka składa się z premii za ryzyko pokrywającej oczekiwane straty, narzutu na koszty zapewniającego zwrot kosztów działalności zakładu ubezpieczeń, a także narzutu bezpieczeństwa na ryzyka procesowe i parametryczne[192] oraz z narzutu na wydatki nieprzewidziane, czyli tzw. składnik losowy, który jest niezależny od zakładu ubezpieczeń. Aby ubezpieczyciel mógł osiągnąć dany poziom bezpieczeństwa, a jednocześnie oferować wartościowy produkt ubezpieczeniowy, niezbędne jest odpowiednie określenie sumy

[189] C. Biener, M. Eling, J. Hendrik, *Insurability of Cyber Risk: An Empirical Analysis, Institute of Insurance Economics,* Working Papers on Finance No. 2015/03, s. 9.
[190] *Ibidem,* s. 9.
[191] E. Spigarska, *Zasady kalkulacji składki ubezpieczeniowej w zakładach ubezpieczeń* [w:] *Prace i Materiały Wydziału Zarządzania Uniwersytetu Gdańskiego*, 4/2007, s. 79.
[192] Opisuje niepewność w oszacowaniu dokładnej natury procesu straty, w którym stosuje się modele statystyczne do opisania losowości procesu straty. Wybór i specyfikacja tych modeli są narażone na potencjalne błędy w oszacowaniu.

ubezpieczeniowej, której wysokość zależy m.in. od rodzaju przedmiotu objętego ubezpieczeniem, czy od potencjalnej straty.

Tabela 6.3. Kryteria ubezpieczalności ryzyka i powiązane z nimi wymagania według Berlinera

Kryteria ubezpieczalności		Wymagania
Aktuarialne	Losowość występowania strat	Ryzyko musi być niezależne, a wystąpienie straty przewidywalne.
	Maksymalna możliwa strata	Możliwość zarządzania sumą ubezpieczeniową przez zakłady ubezpieczeń tak, aby były wypłacalne
	Średnia strata na zdarzenie	Jej wielkość powinna być umiarkowana.
	Masowość zdarzeń	Zdarzenia muszą się powtarzać i być podobne.
	Asymetria informacji	Ryzyko moralne oraz negatywna selekcja nie występują, bądź występują w niewielkim stopniu
Rynkowe	Składka ubezpieczeniowa	Można ją oszacować w wielkości pozwalającej na otrzymanie odpowiedniej rekompensaty przez zakład ubezpieczeń, a jednocześnie niestanowiącej nadmiernego kosztu dla ubezpieczonego.
	Limity na pokrycie	Są do zaakceptowania przez zakład ubezpieczeń.
Społeczne	Polityka publiczna	Ubezpieczenie ryzyka nie może być motywatorem do popełniania przestępstw.
	Ograniczenia prawne	Stabilność systemu prawnego powinna ułatwiać rozwój rynku ubezpieczeniowego.

Źródło: C. Biener, M. Eling, J. Hendrik, *Insurability…*, *op. cit*., s. 9.

Aby spełnić kryteria społeczne ubezpieczalności ryzyka wymagane jest natomiast, aby dane ryzyko można było ubezpieczyć zgodnie z zasadami polityki publicznej oraz szeroko pojętymi wartościami społecznymi. W związku z tym, ubezpieczenie danego ryzyka nie może zachęcać do dokonywania oszustw, ani też nie powinno prowadzić do negatywnych zjawisk społecznych. Do kryteriów społecznych należy również kryterium ograniczeń prawnych, dotyczy ono m.in. obowiązujących ograniczeń prawnych rodzajów działalności, w które towarzystwo ubezpieczeniowe może się angażować i które zakazują ubezpieczania niektórych rodzajów ryzyka. Stabilność ram prawnych w danym kraju jest innym ważnym warunkiem, który musi zostać spełniony, aby ryzyko było ubezpieczalne[193].

Głównym wymogiem ubezpieczenia od określonego ryzyka jest niezależność ryzyka. Według Denisa Kesslera, „ryzyko musi być losowe, aby mogło być ubezpieczalne, czyli

[193] *Ibidem.*

prawdopodobieństwo zrealizowania się ryzyka musi być równe liczbie z przedziału obustronnie otwartego od 0 do 1"[194]. W przypadku ryzyka cyberterrorystycznego ten wymóg nie jest spełniony. Baer i Parkinson twierdzą, że istniejące systemy cybernetyczne są zaprojektowane w podobny sposób i w związku z tym są wrażliwe na te same incydenty, co uzasadnia hipotezę, że incydenty mogą być bardzo wysoko skorelowane między firmami (np. w przypadku *DDoS*)[195].

Kryteria maksymalnej straty oraz umiarkowanej średniej straty są spełnione, jeżeli możliwe jest ograniczenie maksymalnej możliwej straty na zdarzenie, co warunkuje wypłacalność, a średnia strata jest do zaakceptowania przez zakład ubezpieczeń. W przypadku wystąpienia cyberterroryzmu oszacowanie możliwej straty jest bardzo trudne, ponieważ jedno zdarzenie może objąć swym zasięgiem nawet cały kraj i wygenerować ogromne koszty. Przykładowo według statystyk w 2018 roku średni koszt cyberataku na przedsiębiorstwo w celu kradzieży danych wyniesie 3,8 mln $, natomiast w 2020 roku jest szacowany na 150 mln $[196]. Statystyki te pokazują, jak szybko sfera cyberprzestępstw się będzie rozwijać, a co za tym idzie również cyberterroryzmu. Jednakże cyberterroryzm niesie ze sobą większe potencjalne straty.

Następnym kryterium aktuarialnym warunkującym ubezpieczalność ryzyka jest masowość zdarzeń. Liczba ataków cyberterrorystycznych ciągle wzrasta. Według badań FBI w 2017 roku codziennie na świecie dochodziło do 4000 ataków cybernetycznych[197], co w stosunku do 860 ataków w 2011 roku stanowi ponad 4,5 krotny wzrost[198]. Ataki cybernetyczne można uznać za masowe ze względu na ich coraz większą skalę, jednakże nie są one do siebie podobne, gdyż każdy atak należy traktować bezprecedensowo, ponieważ wiąże się z innymi działaniami. W związku z tym nie można uznać tego kryterium za spełnione.

---

[194] M. Fedor, *Bezwzględne kryteria ubezpieczalności*, Gazeta Ubezpieczeniowa Pismo Środowisk Ubezpieczeniowych i Finansowych, 08/ 2004, (www.gu.com.pl) data dostępu: 21.04.2018 r.

[195] J. H. Wirfs, *Essays on ciber risk and efficency in the insurance industry*, The University of St. Gallen, Difo-Druck GmbH, Bamberg, 2016, s. 88.

[196] J. Mason, *Cyber Security Statistics,* Honest, In-Depth & Transparent VPN Reviews from Real Users, (thebestvpn.com) data dostępu: 21.04.2018 r.

[197] *Ibidem.*

[198] *Internet Crime Reaport 2011*, Internet Crime Compliant Center, (www.pdf.ic3.gov) data dostępu: 21.04.2018 r.

Kryterium asymetrii informacji wynika z kolei ze zróżnicowania zakresu informacji jakimi dysponują strony transakcji. W związku z tym w ubezpieczeniach może występować ryzyko moralne, a także selekcja negatywna, które są często postrzegane jako podstawowe utrudnienia rozwój rynku. Ryzyko moralne wynika z braku motywacji ubezpieczonego do podjęcia środków, które zmniejszyłyby prawdopodobieństwo wystąpienia straty bądź zredukowałyby rozmiar straty po zakupie ubezpieczenia. Natomiast selekcja negatywna może powodować wypieranie lepszego produktu ubezpieczeniowego przez gorszy. Jest to związane z dużą zależnością między współczesnymi systemami informacyjnymi, która sprawia, że zwiększa się znacząco podatność na ryzyko cybernetyczne, mimo że pojedyncze firmy inwestują w cyberubezpieczenia. Dodatkowo zależność ta utrudnia odkrywanie, a tym bardziej dowodzenie źródeł straty i tożsamości sprawców, co potencjalnie zwiększa niechęć firm do inwestowania w środki zapobiegawcze. W związku z tym ryzyko cyberterrorystyczne nie spełnia tego kryterium[199].

Wśród kryteriów rynkowych ubezpieczalności ryzyka występują składka ubezpieczeniowa i limity na pokrycie. Pierwsze z kryterium odnosi się do wysokości składek, które powinny być odpowiednio oszacowane, tak aby zakład ubezpieczeń mógł otrzymać należną rekompensatę, a ubezpieczający nie ponosił nadmiernego kosztu z tytułu ubezpieczenia. W przypadku cyberterroryzmu określenie sumy, która byłaby wystarczająca dla często nawet katastrofalnych strat, jest bardzo trudne. Jest to spowodowane m.in. niewielką liczbą uczestników rynku, niewielkim rozmiarem puli ryzyka, ograniczonymi danymi, a także istotną asymetrią informacji, która wymaga kosztownej weryfikacji[200].

Ostatnimi kryteriami ubezpieczalności ryzyka są kryteria społeczne, czyli polityka publiczna i ograniczenia prawne. By dane ryzyko spełniało pierwsze z tych nich, ubezpieczenie nie może uatrakcyjniać popełniania przestępstw, ani nie powinno być motywatorem do oszustw. W przypadku przestępstw cybernetycznych istnieje duża możliwość, iż przedsiębiorstwa posiadające ubezpieczenie będą chciały wyłudzić pieniądze ze względu na trudną wykrywalność sprawców włamań hakerskich i innych wykroczeń w sieci. Dodatkowo duża dostępność do ubezpieczeń cybernetycznych może obniżyć bariery popełniania

[199] J. H. Wirfs, *Essays…, op. cit.,* s. 92-93.
[200] *Ibidem*, s. 93-94.

przestępstw. Firmy mogą mieć także mniejszą motywację do angażowania się w samoochronę, a to z kolei może prowadzić do ogólnego narażenia przemysłu i dużych strat. Natomiast kryterium ograniczeń prawnych należy rozumieć dwojako, jako ryzyko zmian aktów prawnych obowiązujących w danym kraju i powiązanymi z tym, zmianami produktów ubezpieczeniowych, a także jako ograniczenia, co do rodzaju działalności, którą można ubezpieczyć. Niepewność zmiany przepisów prawnych może również stanowić istotną barierę rozwoju rynku ubezpieczeń cybernetycznych, a ze względu na szybko rozwijający się sektor Technologii Informacyjnej taka niepewność występuje[201].

Zatem można zauważyć, że ryzyko związane z cyberterroryzmem nie spełnia warunków ubezpieczalności i w związku z tym zakłady ubezpieczeń mogą odmówić ubezpieczenia takiego ryzyka.

6.7. Zakończenie

Podsumowując rozważania na temat cyberterroryzmu można zauważyć, że jest to poważny problem obecnych czasów. Rozwój Internetu daje użytkownikom wiele korzyści, jednak niesie za sobą także wiele zagrożeń. Odpowiadając na pytanie, jakie są zagrożenia związane z funkcjonowaniem cyberprzestrzeni można wymienić: cyberprzestępstwa, cyberprzemoc, cyberautorytaryzm, cyberinwigilacje, cyberterroryzm oraz cyberwojny. Zagrożenia te są coraz większe, dlatego istotne są wszelkiego rodzaju zabezpieczenia stosowane w sieci, które utrudniają hakerom przeprowadzanie ataków.

Po dokonaniu analizy skali zagrożenia cyberterroryzmem na świecie, autor określił ją jako dużą. Świadczy o tym chociażby ilość ataków terrorystycznych, która wydarzyła się w ciągu ostatnich lat za pośrednictwem sieci. Od roku 2013 do 2018 liczba naruszeń danych osobowych wyniosła ponad 7,9 mld. Ataki te spowodowały duże szkody i doprowadzały nawet do paraliżu całego kraju, czego przykładem może być Estonia, gdzie normalne funkcjonowanie państwa zostało prawie wstrzymane, powodując tym samym panikę wśród obywateli.

Odpowiadając na pytanie, czy cyberterroryzm zastąpi w przyszłości terroryzm, można przypuszczać, że się tak nie stanie. Prawdopodobnie oba rodzaje przestępczości będą się uzupełniały i w ten sposób będą mogły poważnie zagrozić bezpieczeństwu państwa, a przede

[201] *Ibidem.*

wszystkim jego infrastrukturze krytycznej. Odpowiedź można argumentować historycznymi działaniami wojennymi, które funkcjonowały na dwóch płaszczyznach: rzeczywistej oraz internetowej, takich jaki np. operacja „Pustynna burza", czy walki w Kosowie w 1999 roku.

Po dokonaniu analizy aktów prawnych autor zauważył, że cyberprzestrzeń jest uregulowana zarówno w krajowych przepisach prawnych, jak i w międzynarodowych. W Polsce Kodeks Karny reguluje kwestie dotyczące sprawców przestępstw z użyciem systemów teleinformatycznych, natomiast w Unii Europejskiej obowiązują takie akty prawne, jak Konwencja o cyberprzestępczości, a także Dyrektywa o atakach na systemy informatyczne, które ujednolicają działania prowadzące do zatrzymania przestępców w cyberprzestrzeni dla wszystkich państw członkowskich. Problemem jest jednak ciągle brak jednej definicji cyberterroryzmu, co utrudnia współpracę międzynarodową, a wykrycie cyberprzestępców jest utrudnione ze względu na fakt, iż mogą oni przeprowadzać atak z każdego punktu na ziemi.

Podstawowym celem pracy było zbadanie, czy można się ubezpieczyć przed cyberterroryzmem. Autor zauważył, że na rynku polskim istnieją towarzystwa ubezpieczeń, które oferują cyberubezpieczenia. Jednak są to ubezpieczenia dla przedsiębiorstw z tytułu przede wszystkim utraty danych. Natomiast żadne towarzystwo nie oferuje ubezpieczeń od cyberterroryzmu. Jest to spowodowane tym, że cyberterroryzm nie spełnia warunków ubezpieczalności, ponieważ skutki jego wystąpienia mogą być katastrofalne. Dodatkowo ciężko zdefiniować możliwe szkody, a także nie występuje powtarzalność aktów cyberterrorystycznych, która umożliwiałaby kalkulacje ryzyka i wyliczenie odpowiedniej składki.

Rozdział 7.
Ubezpieczenia cybernetyczne – charakterystyka i analiza rynku globalnego

Katarzyna Żelichowska, Joanna Żelichowska*

7.1. Wprowadzenie

W dobie globalizacji i wszechobecnej cyfryzacji połączonej z dominującą rolą internetu jako platformy wymiany informacji, ryzyka związane z cyberprzestrzenią awansowały do grona najważniejszych zagrożeń dla gospodarki światowej. Każda organizacja wykorzystująca w swojej działalności dane osobowe, zbiory danych, patenty, tajemnice handlowe czy techniczne jest realnie narażona na wystąpienie takich zdarzeń jak: wyciek informacji, ujawnienie tajemnicy przedsiębiorstwa lub danych wrażliwych, awaria systemów informatycznych. Skutki takich incydentów mają z roku na rok coraz większy wymiar finansowy. Straty bezpośrednie i koszty następcze mają wpływ na sytuację ekonomiczną zarówno całych gospodarek, jak i pojedynczych przedsiębiorstw. Powodują utratę reputacji, wywołują wzrost poziomu kosztów i spadek przychodów, a w efekcie obniżenie wartości przedsiębiorstwa i utratę pozycji. W wyniku pojawienia się różnego rodzaju wirusów oraz złośliwych programów powstało zagrożenie uszczerbku w mieniu oraz ryzyko obowiązku prawnego pokrycia strat poniesionych przez innych. Brak możliwości uniknięcia lub wyeliminowania zagrożeń cybernetycznych zrodził konieczność zapewnienia źródeł finansowania ich potencjalnych skutków. Zapotrzebowanie na metody finansowania cyberryzyka legło u podstaw powstania nowej linii ubezpieczeń utworzonej z myślą o szeroko rozumianej aktywności gospodarczej w cyberprzestrzeni, zwanej ubezpieczeniami cybernetycznymi.

Celem artykułu jest charakterystyka ubezpieczeń cybernetycznych oraz ich analiza na rynku globalnym. W niniejszym artykule wykorzystano specjalistyczne raporty branżowe, w

* Koło Naukowe Ubezpieczeń „Risk Management", Katedra Zarządzania Ryzykiem i Ubezpieczeń, Uniwersytet Ekonomiczny w Krakowie.

tym również anglojęzyczne, publikowane przez instytucje ubezpieczeniowe oraz podmioty zajmujące się badaniem bezpieczeństwa IT. Tekst składa się z ośmiu części. Na początku omówiono genezę ubezpieczeń cybernetycznych oraz podjęto próbę zdefiniowania i sklasyfikowania ryzyka cybernetycznego. W kolejnej części poruszono temat skali zagrożeń na świecie oraz regulacji prawnych dotyczących cyberzagrożeń. Następnie przedstawiono najważniejsze cechy charakterystyczne dla ubezpieczeń cybernetycznych oraz ich pozycję na rynku światowym omówioną głównie na podstawie badań opublikowanych przez Allianz. W ostatniej część artykułu zobrazowano szkodowość wynikającą z realizacji incydentów cybernetycznych, natomiast w podsumowaniu zawarto ogólne wnioski, dotyczące m.in. barier rozwoju ubezpieczeń cybernetycznych oraz korzyści z nich wynikających.

Pierwsze ubezpieczenia obejmujące ryzyko cybernetyczne pojawiły się pod koniec lat 90. w odpowiedzi na Y2K (*year 2 kilo bug*), tzw. pluskwę milenijną i towarzyszące jej problemy związane z przełomem stulecia. W wyniku katastroficznych skutków, które miały nastąpić z nastaniem roku 2000 poprzez błąd wywołany chęcią zaoszczędzenia przez programistów dwóch bajtów na zapisie daty, spowodowały, że po raz pierwszy pojawiła się świadomość skali ryzyka, jakiej musi sprostać gospodarka w obliczu awarii systemów komputerowych. Pierwsze produkty ubezpieczeniowe dotyczące odpowiedzialności cywilnej oraz nieruchomości były oferowane w bardzo ograniczonym zakresie. Drugim etapem rozwoju ubezpieczeń cybernetycznych było pokrycie ochrony prawnej poufnych danych osobowych. Polityka ta koncentruje się na kosztach wynikających z niekontrolowanego naruszenia chronionych informacji. Dla obecnego trzeciego etapu rozwoju charakterystyczna jest świadomość zagrożeń cybernetycznych[202]. Bez wątpienia XXI wiek został zdominowany nowoczesnymi rozwiązaniami technologicznymi (telefon komórkowy, GPS, robotyka, automatyka, poczta elektroniczna), tym samym przyczyniając się do rozwoju cyberprzestrzeni.

[202] G.Strupczewski *The cyber-insurance market in Poland and determinants of its development from the insurance broker's perspective*, "Economics and Business Review" 2017, Vol. 3 (17), Nr 2, s. 36, (http://www.ebr.edu.pl/pub/2017_2_33.pdf), dostęp: 22.03.2018 r.

7.2. Definicja, systematyka ryzyka cybernetycznego oraz identyfikacja czynników determinujących jego wzrost

Ryzyko cybernetyczne jest nieodłącznym elementem świata systemów informatycznych. Do tej pory nie powstała powszechnie uznawana definicja ryzyka cybernetycznego, która ujmowałaby wszystkie jego aspekty. Chociaż podjęto znaczące wysiłki w celu zbadania tego rodzaju ryzyka, Międzynarodowy Fundusz Walutowy zaobserwował, że jest to termin powszechnie używany, ale bardzo trudny do zdefiniowania i określenia pod względem ilościowym.

Jedna z podstawowych definicji mówi, że cyberryzyko jest to rodzaj ryzyka gospodarczego związanego z posiadaniem, działaniem, wykorzystywaniem i oddziaływaniem urządzeń oraz technologii IT w przedsiębiorstwie[203]. Z kolei według Światowego Forum Ekonomicznego cyberryzyko to ryzyko związane z niepożądanym zdarzeniem, czy też atakiem na poszczególne elementy ekosystemu, który wywołać może negatywne skutki dla zdrowia publicznego, bezpieczeństwa ekonomicznego, a nawet bezpieczeństwa narodowego[204]. Natomiast według MFW ryzyko cybernetyczne jest podręcznikowym przykładem ryzyka systemowego, którego źródłem jest wykorzystywanie technologii informatycznych i elektroniczne przetwarzanie danych. Ekspozycje na ryzyko są powszechne dla przedsiębiorstw. Istnienie asymetrii informacji, niewłaściwie dostosowane systemy motywacyjne czy też powiązania strategiczne mogą doprowadzić do nieprawidłowego oszacowania ryzyka. Wymienione niedoskonałości mogą sprawić, że rynek transferu ryzyka związanego z cyberprzestępczością może zawieść, co będzie skutkowało nieefektywną alokacją ryzyka w całym kraju[205]. Zdaniem M. Eling i J.H. Wirfs termin "ryzyko cybernetyczne" obejmuje wiele źródeł ryzyka wpływających na informacyjne i technologiczne aktywa firmy, rządów lub osób prywatnych. Przykładami takiego ryzyka są kradzież tożsamości, ujawnienie poufnych informacji oraz przerwa w działalności[206]. Jak widać

---

[2] G. Strupczewski*, Zagrożenia cybernetyczne instytucji finansowych, „*Rozprawy Ubezpieczeniowe" 2017, nr 2, s. 67, http://www.knfpan.pan.pl/images/Fin._110-17_15-G.Strupczewski.pdf (dostęp: 22.03.2018).

[204] *Understanding Systemic Cyber Risk,Global Agenda Council on Risk & Resilience,* October 2016,World Economic Forum, s. 5, http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf (dostęp: 22.03.2018 r.).

[205] E. Kopp, L. Kaffenberger, C. Wilson*, Cyber Risk, Market Failures, and Financial Stability,* WP/17/185, August 2017, s. 7, https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104 (dostęp: 22.03.2018 r.).

[206] M. Eling,J. Wirfs Hendrik, 2016, *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class,*s.5,

zdefiniowanie ryzyka cybernetycznego stanowi duże wyzwanie, co jest następstwem wielu składowych, a z których najistotniejsze to postęp techniczny oraz powiązania z wieloma dyscyplinami naukowymi.

Ryzyko cybernetyczne najczęściej klasyfikuje się według kryterium rodzaju szkodliwych działań prowadzących do strat. Jest to więc podział ze względu na przyczyny szkód, w którym wyróżnia się działania celowe oraz niecelowe, nazywane także przypadkowymi. Do działań celowych należą:

- infekcja złośliwego oprogramowania, np. wirusy, robaki sieciowe, koń trojański, dialer, botnet,
- przełamanie zabezpieczeń, np. nieuprawnione logowanie, włamanie na konto, ataki sieciowe, włamanie do aplikacji,
- publikacje w sieci internet, np. obraźliwe treści, zniesławienie, naruszenie praw autorskich, dezinformacja,
- nielegalne gromadzenie informacji, np. skanowanie, podsłuch, inżynieria społeczna, szpiegostwo spam,
- sabotaż komputerowy, np. nieuprawniona zmiana informacji, nieuprawniony dostęp, nieuprawnione wykorzystanie informacji, atak odmowy dostępu DDoS, skanowanie danych, wykorzystanie podatności w urządzeniach, wykorzystanie podatności aplikacji,
- czynnik ludzki, np. naruszenie procedur bezpieczeństwa, naruszenie obowiązujących przepisów prawa,
- cyberterroryzm, np. przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni.

Natomiast do działań przypadkowych można zaliczyć:

- wypadki i zdarzenia losowe, np. awarie sprzętu, awarie łącza, błędy oprogramowania,
- czynnik ludzki, np. naruszenie procedur, zaniedbanie, błędna konfiguracja urządzenia, brak wiedzy, naruszenie praw autorskich[207].

Należy również wspomnieć o klasyfikacji opisanej w taksonomii operacyjnych zagrożeń cyberbezpieczeństwa, której autorami są James J. Cebula oraz Lisa R. Young. Biorąc pod uwagę

https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf (dostęp: 22.03.2018 r.).

[207] G. Strupczewski, *Zagrożenia..., s. 68.*

źródła cyberryzyka, wyróżnili oni cztery klasy ryzyka, do których zaliczyli 13 podklas, a następnie 56 ich elementów. Do głównych źródeł cyberryzyka należą:

- działania ludzkie, które opisują klasę ryzyka operacyjnego, charakteryzującą się problemami spowodowanymi przez działania podejmowane lub niepodejmowane przez ludzi w danej sytuacji. Ta klasa obejmuje działania zarówno osób wewnętrznych, jak i osób z zewnątrz. Zawarte w niej podklasy dotyczą działań celowych (oszustwa, kradzieże, sabotaże, wandalizm), nieumyślnych (błędy, pomyłki, zaniedbania) oraz niepodjęcia odpowiednich czynności (wynikających np. z braku wiedzy czy umiejętności);
- zakłócenia w pracy systemów i urządzeń IT, charakteryzujące się problematycznym, nieprawidłowym lub nieoczekiwanym funkcjonowaniem urządzeń technicznych. Do podklas należą m.in. awarie sprzętu (obniżające jego wydajność, pojemność oraz powodujące problemy w zapewnieniu odpowiedniego funkcjonowania), awarie oprogramowania (problemy dotyczące kompatybilności, konfiguracji, utrzymania prawidłowego poziomu zabezpieczeń) oraz awarie systemów zintegrowanych (których skutkiem jest nieprawidłowe działanie polegające na braku spójności i kompleksowości);
- niewydolność procesów wewnętrznych w organizacji, będąca klasą ryzyka związaną z problematycznymi awariami procesów wewnętrznych. Podklasy obejmują projektowanie i realizację procesów, sterowanie nimi oraz wsparcie;
- wypadki zewnętrzne, związane z wydarzeniami, na ogół poza kontrolą organizacji. Często nie można zaplanować ani przewidzieć czasu wystąpienia tych zdarzeń. Do podklas zaliczyć można katastrofy naturalne, problemy prawne, zmiany w otoczeniu biznesowym oraz uzależnienie od zewnętrznych dostawców[208].

W publikacji Indyjskiego Instytutu Zarządzania w Kalkucie dotyczącej ubezpieczeń od cyberryzyka autorzy również podjęli się próby jego sklasyfikowania. Wyróżnili oni dwie klasyfikacje, z których pierwsza zawiera następujące typy:

[208] J. Cebula, L.R. Young, *A Taxonomy of Operational Cyber Security Risks,* December 2010, s. 2, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf (dostęp: 22.03.2018 r.).

- naruszenie poszczególnych elementów bezpieczeństwa sieci, takich jak zapora sieciowa, serwery proxy, oprogramowania antywirusowe, infekcja serwera złośliwym oprogramowaniem lub nieautoryzowany dostęp,
- naruszenie serwera sieci organizacji i wyświetlanie nieodpowiednich treści na stronie internetowej,
- problemy z dostawcami usług internetowych i aplikacji, np. Application Service Provider (ASP), Internet Service Provider (ISP),
- kradzież tożsamości, np. kradzież poufnych danych o klientach z bazy danych organizacji,
- ataki niezadowolonych pracowników wewnątrz organizacji,
- cyber wymuszenia,
- odmowa dostępu (Denial of Service), polegająca na zablokowaniu łącza lub serwisu internetowego.

Druga klasyfikacja została dokonana ze względu na wpływ ryzyka cybernetycznego na przedsiębiorstwa. W tym przypadku wyróżniono straty bezpośrednie oraz pośrednie (patrz tabela 7.1)[209].

Tabela 7.1. Klasyfikacja ryzyka cybernetycznego ze względu na jego wpływ na przedsiębiorstwa

Rodzaj straty	Przykłady
Bezpośrednia	Brak dostępu do sieci korporacyjnych
	Włamanie do sieci oraz niszczenie zasobów informacyjnych przez hakerów
	Ujawnianie tajemnic przedsiębiorstwa, planów lub innych poufnych informacji firmy
	Nieautoryzowany dostęp do danych
	Odmowa transakcji elektronicznych
Pośrednia	Pogorszenie kapitalizacji rynkowej
	Nieumyślne naruszenie prywatności klientów poprzez ujawnienie danych osobowych

[209] A. Mukhopadhyay, D. Saha, B.B Chakrabarti, A. Mahanti, A. Podder, *Insurance for Cyber-risk: A Utility Model,* Indian Institute of Management Calcutta, 2005, Vol. 32, No. 1, *s. 156,* https://www.researchgate.net/profile/Arunabha_Mukhopadhyay/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model/links/00b7d518016c99e908000000.pdf (dostęp: 20.03.2018 r.).

	Nieprzestrzeganie przepisów dotyczących transakcji
	Sprawy sądowe i roszczenia z tytułu odpowiedzialności cywilnej

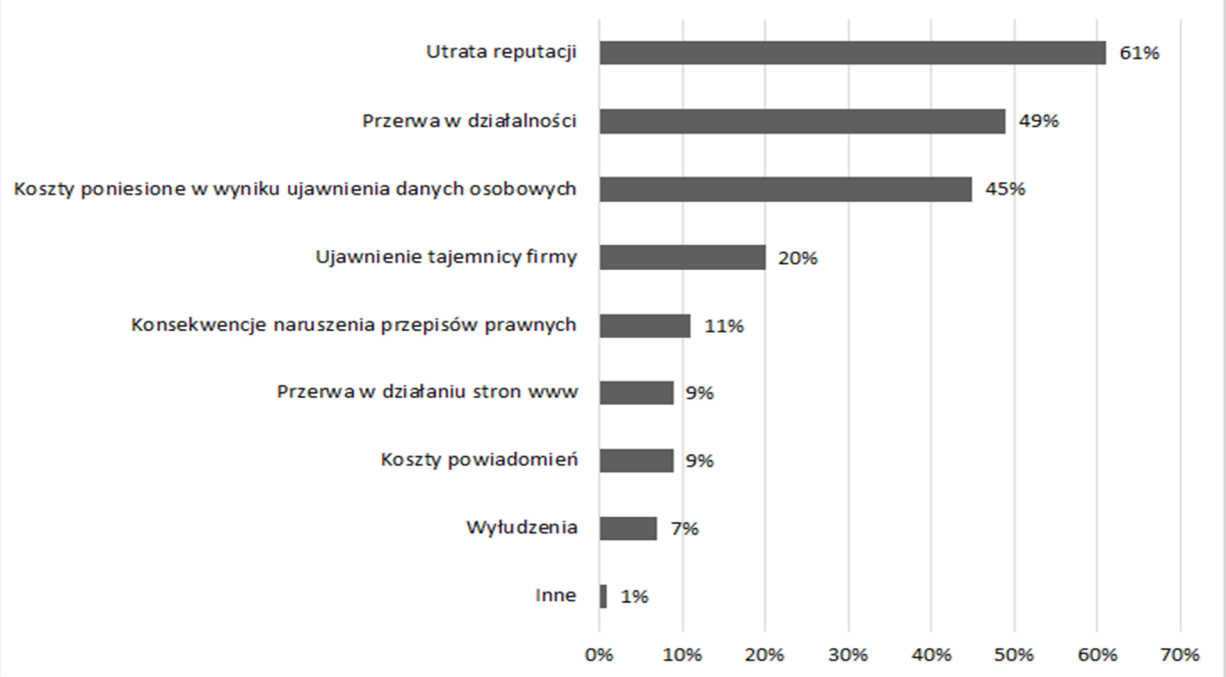
Źródło: opracowanie własne na podstawie *Insurance for Cyber-risk: A Utility Model*, Mukhopadhyay A., Saha D., Chakrabarti B.B., Mahanti A., Podder A., Indian Institute of Management Calcutta, 2005, Vol. 32, No. 1., (https://www.researchgate.net/profile/Arunabha_Mukhopadhyay/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model/links/00b7d518016c99e908000000.pdf), dostęp: 20.03.2018 r.

Ryzyko cybernetyczne obejmuje: wpływ klęsk żywiołowych na centra danych i infrastrukturę łączności, awarie systemu, działania przestępców mające na celu kradzież danych bankowości internetowej lub dokonywanie wymuszeń (cyberprzestępczość) oraz sponsorowane przez korporacje i państwa szpiegostwo mające na celu kradzież własności intelektualnej. Obejmuje ono również przenikanie lub zakłócanie infrastruktury komputerowej kraju (cyberataki), internetową działalność terrorystyczną (cyberterroryzm) i grupy aktywistów wykorzystujące Internet do realizacji swoich celów (cyberaktywność). Według publikacji Lloyd's dotyczącej zarządzania ryzykiem cybernetycznym zagrożenia te mogą doprowadzić do szeregu szerszych zagrożeń dla biznesu, takich jak:

- ryzyko operacyjne, dotyczące strat wynikających z nieodpowiednich lub nieudanych procesów wewnętrznych, działań ludzkich, awarii systemów lub ze zdarzeń wewnętrznych. Do tej kategorii należy większość zagrożeń cyfrowych, których skutkami mogą okazać się utrata klientów, utrata danych, przerwanie łańcucha dostaw oraz wyłączenie wewnętrznej sieci komputerowej;
- ryzyko finansowe, obejmujące straty wynikające z niemożności prowadzenia działań biznesowych, takich jak przyjmowanie i realizacja zamówień lub prowadzenie produkcji, jak również z oszustw i kradzieży;
- ryzyko własności intelektualnej, dotyczące utraty planów produkcji, planów marketingowych oraz dostanie się ich w ręce konkurencji, które mogą poważnie zaszkodzić przedsiębiorstwu oraz doprowadzić do zmniejszenia jego przewagi konkurencyjnej;
- ryzyko regulacyjne, dotyczące naruszenia przez organizację regulacyjnych wymogów w obszarze ochrony danych osobowych, które stają się coraz bardziej uciążliwe, w wyniku czego może zostać nałożona sankcja lub grzywna;

– ryzyko utraty reputacji, bowiem publiczna widoczność incydentów może zaszkodzić wizerunkowi, marce i reputacji firmy. Ta szkoda może wynikać nawet z drobnych incydentów, takich jak utrata usługi lub naruszenie tylko kilku przepisów. W skrajnych przypadkach incydenty związane z bezpieczeństwem mogą spowodować utratę zaufania do spółki przez akcjonariuszy i potencjalnie wpłynąć na jej cenę[210].

Badania Allianz Risk Barometer 2015 przedstawiają główne przyczyny strat ekonomicznych spowodowanych ryzykami cybernetycznymi w wybranych przedsiębiorstwach w 2015 roku[211] (patrz rys. 7.1).



Rysunek 7.1. Główne przyczyny strat ekonomicznych wywołanych ryzykami cybernetycznymi w wybranych przedsiębiorstwach w 2015 roku (w %)

Źródło: Allianz Risk Barometer, (*Top Business Risks 2015*, Allianz Global Corporate & Specialty, s. 12, https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2015_EN.pdf), dostęp:15.03.2018 r.

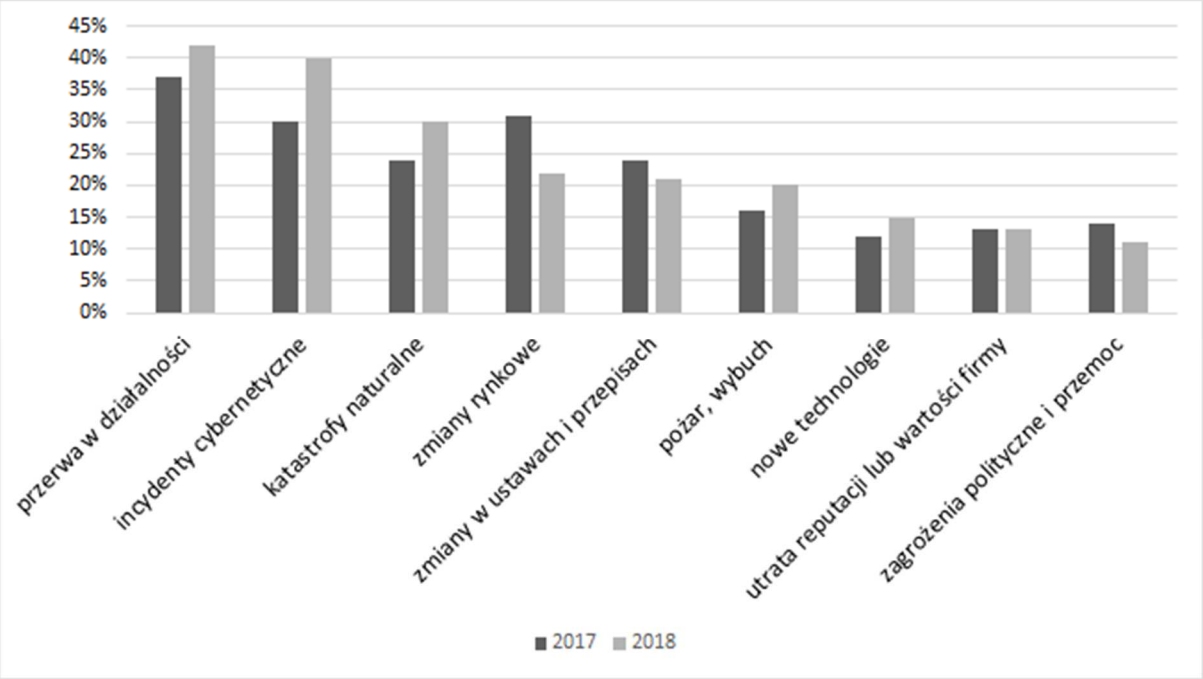
[210] *Managing digital risk Trends, issues and implications for business,* Lloyd's 2010, s. 5, https://www.lloyds.com/~/media/lloyds/reports/360/360-digital/lloyds_360_digital_risk_report-(2).pdf (dostęp: 22.03.2018 r.).

[211] *A guide to cyber risk. managing the impact of increasing interconnectivity* Allianz Global Corporate & Specialty, Allianz 2015, s. 12, https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf (dostęp: 22.03.2018 r.).

Wyniki przeprowadzonych badań wskazują, że najważniejsze ryzyko cybernetyczne wywołujące straty ekonomiczne stanowi utrata reputacji (61%), przerwa w działalności (49%) oraz koszty poniesione w wyniku ujawnienia danych osobowych (45%)[212].

7.3. Opis skali cyberzagrożeń

Według badań opublikowanych przez Allianz (2018) najbardziej istotne zagrożenia dla przedsiębiorstw to przerwa w działalności oraz incydenty cybernetyczne, które kontynuują tendencję wzrostową do drugiego najważniejszego ryzyka biznesowego (40%), natomiast jeszcze 5 lat temu incydenty te zajmowały 15 miejsce. Podobnie jak klęska żywiołowa, atak cybernetyczny może potencjalnie wpłynąć na setki firm, co z kolei może być tragiczne w skutkach[213] (patrz Rysunek 7.2).



Rysunek 7.2. Najważniejsze rodzaje zagrożeń dla przedsiębiorstw na świecie w latach 2017 i 2018 (w %)

Źródło: opracowanie własne na podstawie Allianz Risk Barometer: Appendix 2018, (Allianz Global Corporate & Specialty, http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_APPENDIX.pdf), dostęp: 15.03.2018 r.

[212] *Ibidem,* s. 12.

[213] *Allianz Risk Barometer, Top Business Risk* 2018, Allianz Global Corporate & Specialty, s. 6, http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf (dostęp: 15.03.2018 r.).

Coraz częściej można usłyszeć o różnego rodzaju atakach w cyberprzestrzeni. Pod koniec 2013 r. miał miejsce jeden z największych i najbardziej rozpoznawalnych ataków cybernetycznych o nazwie Carbanak. Niezidentyfikowana grupa przestępcza zaatakowała wówczas wiele banków oraz instytucji finansowych. Według badań było to ok. 100 podmiotów bankowych, skoncentrowanych głównie w Rosji, Stanach Zjednoczonych, Niemczech, Chinach i na Ukrainie. Straty wynikające z tego ataku oszacowano na ok. 1 mld USD. Atak polegał początkowo na wysłaniu do instytucji e-maili z załącznikami, których otwarcie skutkowało infekcją komputerów użytkowników programami szpiegowskimi, które umożliwiały przestępcom dostęp do sieci bankomatów, rachunków bankowych, kart kredytowych i przelewów bankowych[214]. Natomiast w Polsce jednym z bardziej rozpoznawalnych był atak na Polskie Linie Lotnicze LOT dnia 21 czerwca 2015 roku, kiedy to przez 4 godziny LOT nie wykonywał zaplanowanych rejsów z lotniska im. Fryderyka Chopina w Warszawie. W wyniku przeprowadzonego śledztwa pod koniec września 2015 roku okazało się, że LOT padł ofiarą ataku DDoS z wykorzystaniem wzmocnienia przez odbicie pakietów DNS (*reflected amplification*) w celu generowania dużego ruchu wychodzącego. Atak ten skutkował brakiem możliwości komunikacji z Eurocontrol[215], przez co niemożliwe było przesyłanie planów lotu, bez których rejsy nie mogły się odbywać[216]. Stosunkowo niedawno, bo dnia 12 maja 2017 roku, miał miejsce cyberatak z wykorzystaniem WannaCry, czyli złośliwego oprogramowania mającego na celu zablokowanie dostępu do komputera z systemem Windows. W ciągu kilku dni wirus zainfekował ponad 230 000 komputerów w 150 krajach. Aby odblokować zainfekowane urządzenie należało zapłacić odpowiedni okup. Atak dotyczył wielu sektorów, m.in. energetyki, transportu, żeglugi, telekomunikacji oraz opieki zdrowotnej. *Britain's National Health Service* (NHS) poinformował wówczas, że wszystkie urządzenia technologiczne, w tym wyposażenie sali operacyjnej, mogły zostać naruszone, przez co opieka nad pacjentami mogła być utrudniona. Jak się później okazało, ataku można było uniknąć,

[214] Kaspersky, *Carbanak APT. The great bank robbery, Kaspersky Lab, February 2015, Version 2.1, s. 3, https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf (dostęp: 29.03.2018 r.)*

[215] Eurocontrol to Europejska Organizacja ds. Bezpieczeństwa Żeglugi Powietrznej, http://www.eurocontrol.int/articles/who-we-are.

[216] CERT Polska 201, Raport roczny z działalności CERT Polska*, Krajobraz bezpieczeństwa polskiego internetu*, s. 27, https://www.cert.pl/PDF/Raport_CP_2015.pdf (dostęp: 13.03.2018 r.).

gdyby wszystkie przedsiębiorstwa zastosowały specjalną łatę wydaną 14 marca 2017 roku przez Microsoft, która usunęłaby wszystkie luki w zabezpieczeniach[217].

Z danych opublikowanych przez Allianz (tabela 7.2) wynika, że wśród 10 największych gospodarek świata to Stany Zjednoczone ponoszą największe straty wynikające z ataków cybernetycznych (108 mld USD), następnie Chiny (60 mld USD) i Niemcy (59 mld USD). Gdyby jednak uwzględnić stosunek tych strat do PKB, okazuje się, że skutki cyberprzestępczości są najbardziej dotkliwe dla Niemiec ponieważ w porównaniu do pozostałych państw ich wskaźnik wynosi aż 1,6%[218].

Tabela 7.2. Wielkość strat wynikających z cyberprzestępczości w 10 największych gospodarkach świata w 2013 roku

Lp.	Państwo	PKB (bln USD)	Koszty poniesione w wyniku cyberprzestępczości (mld USD)	Koszty wynikające z cyberprzestępczości w relacji do PKB
1	USA	16,8	108	0,64%
2	Chiny	9,5	60	0,63%
3	Japonia	4,9	0,9	0,02%
4	Niemcy	3,7	59	1,60%
5	Francja	2,8	3	0,11%
6	Wielka Brytania	2,7	4,3	0,16%
7	Brazylia	2,4	7,7	0,32%
8	Rosja	2,1	2	0,10%
9	Włochy	2,1	0,9	0,04%
10	Indie	1,9	4	0,21%

Źródło: *A guide to cyber risk. Managing the impact of increasing interconnectivity.,* Allianz Global Corporate & Specialty, Allianz 2015, s. 7, (https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf), dostęp: 22.03.2018 r.

[217] J. M. Ehrenfeld, WannaCry, *Cybersecurity and Health Information Technology: A Time to Act,* 24 May 2017, (https://link.springer.com/content/pdf/10.1007%2Fs10916-017-0752-1.pdf), dostęp: 20.03.2018 r.
[218] Allianz 2015, *A guide to cyber risk*…, s. 7.

Badania skali ataków cybernetycznych uwzględniające kryterium geograficzne (w ujęciu kontynentów) pokazują, że firmy północnoamerykańskie doświadczają około dwukrotnie więcej (52,6%) incydentów związanych z cyberatakami niż firmy europejskie (24,9%), a nawet ponad dwa razy więcej niż firmy zlokalizowane na innych kontynentach. Wynik ten może być powodem wprowadzonych obowiązkowych amerykańskich standardów sprawozdawczości, których jeszcze nie ma na innych kontynentach. Jeśli chodzi o skalę strat to Azja wykazuje najwyższą średnią stratę, podczas gdy Europa i Ameryka Północna mają znacznie mniejsze straty. Może być to spowodowane tym, że firmy północnoamerykańskie i europejskie są bardziej zdolne i chętne do inwestowania w ograniczanie cyberryzyka w przypadku dużych strat. Ustalono również, że aż 75,9% wszystkich incydentów związanych z cyberatakami dotyka instytucji finansowych, co nie jest zaskakujące, ponieważ firmy świadczące usługi finansowe, takie jak banki i firmy ubezpieczeniowe przechowują znaczną ilość danych osobowych. Ważnym aspektem różnicującym skalę zagrożenia cybernetycznego jest uwzględnienie rozmiaru firmy. Zatem według danych wraz ze wzrostem wielkości firmy liczba incydentów wzrasta. W przedsiębiorstwach zatrudniających ponad 250 pracowników odnotowano aż 87% wszystkich wypadków, podczas gdy w małych i średnich firmach odsetek ten wynosił po ok. 4%[219].

7.4. Regulacje prawne zagrożeń w cyberprzestrzeni

Dynamiczny rozwój technologii teleinformatycznych przyczynił się do powstania nowego pola aktywności, jakim jest cyberprzestrzeń. Zgodnie z polską definicją zawartą w projekcie Rządowego Programu Obrony Cyberprzestrzeni, cyberprzestrzeń to „cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami”[220]. Cyberprzestrzeń stanowi zatem nowy wymiar istotny z punktu widzenia bezpieczeństwa państw. Jest także źródłem nowych wyzwań i zagrożeń wiążących się z koniecznością ustanowienia nowych uregulowań,

[219] M. Eling, J. Wirfs Hendrik*, op. cit., s. 15.*
[220] N. Stępnicka, *Cyberprzestrzeń i zagrożenia z nią związane*, [w:] *Bezpieczeństwo i zarządzanie kryzysowe, bezpieczeństwo społeczności lokalnych*, pod red. Z.Wilk-Woś,”Przedsiębiorczość i Zarządzanie”, Wydawnictwo SAN, Warszawa 2017, Tom 18, cz.3, nr 5, s. 192.

podjęcia niezbędnych zabezpieczeń i informacji celem zapewnienia bezpieczeństwa państwa, instytucji i osób korzystających z cyberprzestrzeni[221].

Cyberprzestępstwa można rozpatrywać zarówno w wąskim (sensu stricto) jak i szerokim zakresie (sensu largo). Cyberprzestępczość w znaczeniu sensu largo obejmuje wszelkie typy czynów zabronionych, przy których popełnieniu wykorzystywane są technologie informatyczne oraz czyny skierowane przeciwko danym i systemom informatycznym. Natomiast cyberprzestępczość sensu stricto obejmuje przestępczość komputerową, która już od początku była nieodłącznym elementem rozwoju nowoczesnych technologii stopniowo zyskując na znaczeniu w policyjnych statystykach. Początkowo kwestia ta była problemem marginalnym[222]. Pod koniec XX wieku komputery zaczęto powszechnie wykorzystywać jako narzędzie służące do dokonywania czynów zabronionych. W konsekwencji pojawiły się nowe przestępstwa, jak również nowe formy znanych już przestępstw. Zagrożenia w cyberprzestrzeni dotyczą głównie:

- infrastruktury krytycznej państwa,
- operatorów świadczących usługi teleinformatyczne,
- usług finansowych (w tym operacji bankowych),
- wysokich technologii,
- systemów energetycznych,
- różnych form świadczonych usług transportowych, zdrowia publicznego,
- zakłóceń funkcjonowania instytucji państwowych (głównie stanowisk kierowania bezpieczeństwem państwa, a także sektora prywatnego),
- wszystkiego tego, co narusza żywotne interesy państwa i jego obywateli[223].

Zagrożenia występujące w cyberprzestrzeni można podzielić na takie, których źródłem jest technika (np. awarie sprzętu, zasilania itp.) i takie, których źródłem są ludzie. Do drugiej z tych grup oprócz zagrożeń spowodowanych przez ludzkie błędy (wynikające np. z

[221] *Ibidem,* s. 193.
[222] A.Golonka, *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne,* Rozprawy i Materiały 2016, nr 1(18), s. 64, (https://sp.ka.edu.pl/numery/2016-1/studia-prawnicze-rim-2016-1-golonka.pdf), dostęp: 22.03.2018 r.
[223] J. Zawisza *Cyberprzestępczość i jej wpływ na bezpieczeństwo człowieka,* [w:] *Bezpieczeństwo zewnętrzne i wewnętrzne wobec współczesnych wyzwań-wybrana problematyka,* pod red. A. Stępień., "Przedsiębiorczość i Zarządzanie", Wydawnictwo SAN, Warszawa 2017, Tom 18, nr 5, cz.2, s. 54.

nieświadomości użytkowników lub lekceważenia obowiązków przez personel przedsiębiorstw i instytucji), zalicza się również wiele rodzajów działań mających różny stopień zasięgu i szkodliwości[224]. Istotnym rodzajem cyberzagrożeń jest malware, oznaczający złośliwe, szkodliwe oprogramowanie a także program instalujący się w komputerze użytkownika bez jego zgody i wiedzy realizujący niepożądane funkcje. Do malware zaliczają się:

- wirusy komputerowe - programy komputerowe posiadające zdolność powielania się, wykorzystujące system operacyjny, aplikacje oraz tożsamość użytkownika komputera,
- robaki - samoreplikujące się programy, których celem jest zarażenie całej infrastruktury sieciowej. Rozprzestrzeniają się poprzez wykorzystywanie luk w systemach operacyjnych,
- trojany - służą do włamywania się do komputera, maskując szkodliwą zawartość i działając wewnątrz pozornie prawidłowego oprogramowania. Celem trojanów jest przejęcie kontroli nad funkcjami komputera lub dokonanie uszkodzeń[225].

Równie groźnym dla bezpieczeństwa systemu komputerowego jest inny rodzaj cyberzagrożenia, jakim jest bomba logiczna. Jest to program ze specjalnym kodem, który po uaktywnieniu się, dokonuje zniszczenia zawartości komputera. Następnym przykładem złośliwego oprogramowania jest dialer generujący nadzwyczaj wysokie koszty, będące zarazem zyskiem atakującego. Jest to możliwe poprzez połączenie się zainfekowanego komputera z internetem[226].

Przestępstwa komputerowe, jako składowa cyberprzestępstw dzielą się na: przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych, przestępstwa związane z naruszeniem praw autorskich, fałszerstwa i oszustwa komputerowe[227]. Specyficznym rodzajem zagrożeń występujących w sieci jest cyberterroryzm, czyli atak przeprowadzany przez organizacje terrorystyczne, które wykorzystują cyberprzestrzeń przede wszystkim do zdobywania informacji, manipulowania danymi, pozyskiwania środków,

[224] D. Byrska, K. Gawkowski, D. Liszkowska, *Unia Europejska. Geneza. Funkcjonowanie. Wyzwania.,* Monografia Naukowa współautorska, wyd. Exante, Wrocław 2017, s. 77.
[225] N. Stępnicka, *op. cit.,* s. 195.
[226] *Ibidem,* s. 195.
[227] *Ibidem*, s. 196.

blokowania usług sieciowych oraz prowadzenia bezpośrednich ataków na określone serwery, zwłaszcza rządowe[228].

Można zauważyć, że cyberprzestępczość obejmuje szeroką gamę czynów zabronionych, począwszy od przestępstw popełnianych przeciwko ochronie informacji takie jak: hacking, sabotaż komputerowy, spowodowanie szkody w bazach danych, aż po złożone przestępstwa gospodarcze. Ciągła dynamika tego zjawiska wymaga zatem stałego monitorowania rozwiązań prawnych, jak i podejmowania oraz dostosowywania działań do istniejących zagrożeń. Przykładem krajowych działań na rzecz przeciwdziałania cyberprzestępczości może być powołanie Wydziału do Walki z Cyberprzestępczością w 2014 roku, działającego przy Biurze Służby Kryminalnej Komendy Głównej Policji, której zadaniem jest zwalczanie zagrożeń cybernetycznych, jak również wsparcie w postępowaniach prowadzonych w tym zakresie[229]. Za bezpieczeństwo informatyczne w Polsce odpowiadają m.in. Agencja Bezpieczeństwa Wewnętrznego, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Wewnętrznych i Administracji, Służba Kontrwywiadu Wojskowego oraz zespoły, które podejmują działania w sytuacjach zagrożeń systemów teleinformatycznych. Są to m.in. CERT, Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej oraz CERT-y funkcjonujące w ramach operatorów telekomunikacyjnych[230].

Bezpieczeństwo jest nie tylko podstawową potrzebą człowieka, ale także niezbędnym elementem prawidłowego funkcjonowania przedsiębiorstwa. Ważne jest zapewnienie bezpieczeństwa przetwarzanych informacji firmy m.in. poprzez restrykcyjne przepisy. W Polsce istnieje ponad dwieście aktów prawnych dotyczących ochrony informacji. Do zapewnienia bezpieczeństwa przetwarzanych informacji firmy oraz urzędy są zobligowane przez ustawy m.in. takie jak:

- ustawa o ochronie danych osobowych,
- ustawa o ochronie informacji niejawnych,
- ustawa o dostępie do informacji publicznej,
- ustawa o prawie autorskim i prawach pokrewnych[231].

[228] J. Zawisza, *op. cit*., s. 57
[229] A.Golonka, *Cyberprzestępczość – międzynarodowe...*, s. 68.
[230] N. Stępnicka, *op. cit.,* s. 194.
[231] B.Hołyst, J.Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia,* Prokuratura i Prawo 1, 2011, s. 13, (http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2011/01/1holyst.pdf), dostęp: 24.03.2018 r.

Każda z właściwych ustaw (oraz towarzyszące im rozporządzenia) narzuca na instytucję określone obowiązki w zakresie bezpieczeństwa informacji. Obowiązki te dotyczą zarówno zachowania poufności określonych informacji, jak i ich dostępności i integralności. Stosuje się również odrębne wymagania dotyczące tajemnicy zawodowej zobowiązującej do zapewnienia ochrony pewnym danym. W obliczu postępującej informatyzacji społeczeństwa i ułatwionego dostępu do prywatnych informacji osób i podmiotów gospodarczych jednym z najważniejszych wymogów koniecznych dla prawidłowego funkcjonowania gospodarki stała się prawna ochrona poufnych danych prywatnych. W Polsce regulacje dotyczące ochrony danych osobowych wywodzą się z prawa międzynarodowego, wspólnotowego oraz polskiego. Szczególne znaczenie ma ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r., dzięki której standardy w tym zakresie zostały ujednolicone. Według ustawy koncepcja ochrony danych osobowych opiera się na balansowaniu interesów. Z jednej strony jest prawo do ochrony prywatności, a z drugiej - prawo do informacji o osobie, której dane dotyczą. Osobom tym zostały zapewnione instrumenty kontroli przetwarzania danych, natomiast na administratorów nałożono określone obowiązki[232].

Z uwagi na fakt, iż zapewnieniem bezpieczeństwa w cyberprzestrzeni jest zainteresowana cała społeczność międzynarodowa, niezbędne jest wypracowanie jednolitych standardów w tym obszarze. Wyłania się więc potrzeba podejmowania wspólnych inicjatyw, zwłaszcza przez pryzmat działalności organizacji międzynarodowych. W 2002 roku podjęto kroki przeciw przestępstwom cybernetycznym i przyjęto program obrony cybernetycznej w ramach struktur NATO. Ponadto, w 2004 r. powołano ENISA, czyli Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, której celem jest zwiększenie bezpieczeństwa w sieciach i systemach informatycznych[233]. Wskutek rosnącej liczby incydentów cybernetycznych w 2008 roku powstała Strategia Obrony Cybernetycznej, a w 2010 r. w Lizbonie przyjęto Koncepcję Strategiczną NATO. Istotnym elementem walki z cyberzagrożeniami jest ratyfikowana w 2015 roku Konwencja Rady Europy o cyberprzestępczości, w której uwzględniono odpowiedzialność karną za popełnienie czynów zabronionych przy wykorzystaniu technologii informatycznej.

[232] *Ibidem,* s. 14.
[233] J.Żuk, M.Żuk, *Zagrożenia w cyberprzestrzeni a bezpieczeństwo jednostki*, „Rozprawy Społeczne" 2016, Tom 10, nr 3, s. 72, (http://rozprawy-spoleczne.pswbp.pl/pdf/rs_nr_3_2016_top_druk_art_09.pdf), dostęp: 7.03.2018 r.

Ponadto wprowadzono odrębne przepisy dotyczące współpracy państw, w których zawarto zasady przeprowadzania postępowań przeciwko przestępcom. Kwestia zapewnienia bezpieczeństwa w cyberprzestrzeni jest także przedmiotem zainteresowania Unii Europejskiej. W związku z tym wielokrotnie wypracowywano wspólne stanowiska, m. in. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z 12 sierpnia 2013 roku dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222WSiSW [Dyrektywa Parlamentu Europejskiego i Rady 2013]. Dodatkowo powołano Europejskie Centrum ds. Walki z Cyberprzestępczością [Komisja Europejska 2014], które zajmuje się walką z przestępczością zorganizowaną w sieci oraz cyberatakami[234].

Dążenie do zapewnienia bezpieczeństwa stanowi podstawę funkcjonowania i priorytet każdego państwa. Powstawanie nowych kategorii zagrożeń wymaga ciągłej współpracy w obszarze bezpieczeństwa. W celu uzyskania większej ochrony i kontroli nad informacjami o użytkownikach internetu, 25 maja 2018 roku w krajach członkowskich Unii Europejskiej zaczną obowiązywać nowe unijne przepisy o ochronie danych osobowych. Unijne Rozporządzenie o Ochronie Danych Osobowych (RODO) zostało przyjęte przez Parlament Europejski i Radę Unii Europejskiej w kwietniu 2016 roku. Nowe przepisy będą dotyczyć wszystkich podmiotów niezależnie od ich wielkości, formy organizacyjnej czy struktury własności, które na terenie UE przetwarzają dane w sposób zautomatyzowany prowadzące rejestr np. klientów czy pracowników. Zatem polscy administratorzy danych będą zmuszeni stosować się do zunifikowanych zasad ochrony danych osobowych, tj.: zasady zgodności z prawem, zasady rzetelności i przejrzystości, zasady ograniczenia celu, zasady minimalizacji danych, ograniczenia przechowywania oraz zasady prawidłowości, integralności i poufności. Zgodnie z nową zasadą rozliczalności dodatkowo będą zobligowani tak prowadzić wewnętrzną politykę bezpieczeństwa informacji, aby móc dowieść przestrzegania powyższych zasad[235]. Wdrożenie RODO i jego aktywne stosowanie stawia na uprzywilejowanej pozycji osoby fizyczne, którym nadane zostaną nowe prawa. Podczas procesu podawania danych osobowych otrzymają one

[234] A Stępień, *Bezpieczeństwo w erze cyfryzacji,* [w:] *Bezpieczeństwo zewnętrzne i wewnętrzne wobec współczesnych wyzwań-wybrana problematyka,* pod red. Stępień A., "Przedsiębiorczość i Zarządzanie", Wydawnictwo SAN, Warszawa 2017, Tom 18, nr 5, cz.2, s. 87.

[235] K. Dąbek, A. Kamiński, *Czynniki rozwoju ubezpieczeń cybernetycznych na świecie i w Polsce - wybrane aspekty* [w:] *Kierunki rozwoju ubezpieczeń prywatnych i publicznych,* pod red. W.Sułkowska, M.Cycoń, Wydawnictwo poltext, Warszawa 2017, Rozdział 15, s. 208.

od firm bardziej transparentne informacje m.in. o celach, w ramach których dane będą wykorzystywane. To jeden z nowych obowiązków, które ustawa RODO wymusza na przedsiębiorstwach. Zbiór informacji o tych celach to rejestr czynności przetwarzania, który będzie jednym z kluczowych dokumentów w firmie. Rozporządzenie wprowadza też nowe procedury mające dbać o bezpieczeństwo[236]. Są to:

- ,,*privacy by design*" - wymagająca od przedsiębiorcy ochrony danych już na etapie projektowania dóbr i usług mających pojawić się na rynku,
- ,,*privacy by default*" - przepis według którego od użytkowników można wymagać podania tylko tych danych, które są niezbędne do przeprowadzenia konkretnej czynności[237].

Nowe przepisy regulują też warunki przetwarzania danych osób nieletnich w serwisach społecznościowych. Przewidziano także uproszczony mechanizm składania skarg przez konsumentów w przypadku naruszenia ich prywatności. Firmy, które mają do czynienia ze znaczącą liczbą danych osobowych, będą miały obowiązek powołać osobę odpowiedzialną za ochronę danych. Wdrożenie RODO eliminuje niektóre z obecnie obowiązujących przepisów, m.in. obowiązek zgłaszania zbioru danych osobowych do GIODO, w którego miejsce pojawi się PUEDO czyli Prezes Urzędu Ochrony Danych Osobowych. Organ ten będzie mógł przeprowadzać trzy formy kontroli:

- kontrola planowa zgodna ze stworzonym wcześniej planem kontroli,
- kontrola doraźna odbywająca się najczęściej z powodu doniesienia,
- kontrola prowadzona w toku postępowania administracyjnego o długości maksymalnie miesiąca.

Kolejną zmianą jest rejestr naruszeń, będący zapisem wszystkich przypadków naruszenia przez firmę bezpieczeństwa danych osobowych. Przepis ten wymusza na przedsiębiorcach poinformowanie przyszłego PUEDO o popełnionych błędach. Ponadto, standardowy obowiązek informacyjny zostanie rozszerzony. Rolą przedsiębiorstwa będzie podanie podstawy prawnej, zgodnie z którą przetwarzane są dane użytkownika, a także zawiadamianie

[236] *RODO-nowe obowiązki dla firm i dodatkowe prawa dla osób fizycznych* Fundacja rozwoju e-commerce (https://fundacja-ecommerce.pl/rodo-nowe-obowiazki-dla-firm-dodatkowe-prawa-dla-osob-fizycznych/?gclid=EAIaIQobChMIw7ry7Mzk2QIVll4YCh03LQAXEAMYAiAAEgKwcvD_BwE), dostęp: 22.03.2018 r.
[237] *RODO - nowe obowiązki dla firm…*

o przekazaniu danych do państwa trzeciego[238]. Rozporządzenie RODO ma zatem na celu zwiększenie ochrony osób prywatnych i zapewnienie im dostępu do informacji o stosowanym sposobie przetwarzania personaliów. Ewentualne stwierdzone braki w procesie przetwarzania danych osobowych mogą skutkować bardzo wysokimi karami finansowymi nakładanymi przez PUEDO, nawet do wysokości 20 mln euro lub 4% rocznego obrotu firmy w przypadku rażących naruszeń[239]. Zastosowanie będą miały środki prawne o charakterze administracyjnym oraz administracyjne kary pieniężne. W odróżnieniu od dotychczasowej ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, w RODO nie wyodrębniono sankcji karnych[240]. Najwyższe kary za niedostosowanie się do przepisów dotyczą korporacji i instytucji przetwarzających ogromne ilości danych ze względu na możliwość wyrządzenia poważniejszych szkód od małych firm. Wprowadzone zmiany prawne są wyzwaniem organizacyjnym, technicznym oraz finansowym dla organizacji prowadzących działalność na terenie UE. Niedopełnienie obowiązku notyfikacji oraz towarzyszące mu kary administracyjne, grzywny lub inne sankcje finansowe są fundamentalnym czynnikiem rozwoju ubezpieczeń cybernetycznych, które zapewnią ochronę przed roszczeniami poszkodowanych[241].

7.5. Charakterystyka ubezpieczeń cybernetycznych

Powołanie odpowiednich służb do walki z cyberprzestępczością nie jest wystarczającym zabezpieczeniem przed zagrożeniami związanymi z cyberprzestrzenią. Ze względu na ograniczone możliwości działań nakierowanych na przeciwdziałanie i zapobieganie atakom cybernetycznym, na znaczeniu zyskały metody oparte na ryzyku, koncentrujące się na najbardziej wartościowych aktywach podmiotów. Zarządzanie ryzykiem powinno być nieodłącznym elementem działalności każdej instytucji lub przedsiębiorstwa uwzględniającym czynniki zewnętrzne (hakerzy, przestępcy zorganizowani, byli pracownicy) oraz czynniki

[238] *Ibidem.*
[239] *Ibidem.*
[240] *Nie zastosujesz się do RODO, czekają cię kary* Prenumerata elektroniczna Dziennika Gazety Prawnej, (dostęp: 22.03.2018 r.) http://prawo.gazetaprawna.pl/artykuly/1098885,nadchodzi-rodo-jakie-kary-za-niedostosowanie-sie-do-przepisow.html
[241] G.Strupczewski *Wpływ ustawodawstwa amerykańskiego na rozwój rynku ubezpieczeń cybernetycznych w USA,* Zeszyty Naukowe, 10(958), s. 83, (https://www.researchgate.net/publication/315629601_Wplyw_ustawodawstwa_amerykanskiego_na_rozwoj_rynku_ubezpieczen_cybernetycznych_w_USA), dostęp: 13.03.2018 r.

wewnętrzne (pracownicy, zabezpieczenia, procedury, infrastruktura informatyczna). Równie ważne jest oszacowanie przez zewnętrznych ekspertów potencjalnych strat i kosztów dodatkowych a także przewidywanych następstw finansowych w przypadku kryzysu przedsiębiorstwa. Prognozowane wydatki wymagają zabezpieczenia relatywnie wysokich środków. W konsekwencji następuje wzmożone zainteresowanie alternatywnymi metodami finansowania cyberryzyka wobec podstawowych zabezpieczeń technicznych w postaci ubezpieczenia cybernetycznego. Może być ono częściowym rozwiązaniem problemu, jako niezbędnego elementu kompleksowego programu ochrony ubezpieczeniowej danego przedsiębiorstwa. W odpowiedzi na zgłaszane zapotrzebowanie i chęć zwiększania ochrony przed cyberryzykiem na rynkach pojawiły się wyspecjalizowane produkty ubezpieczeniowe[242]. Należy pamiętać, że ubezpieczenie cybernetyczne nie może stanowić alternatywy wobec zabezpieczeń techniczno-logicznych, które chronią informacje i dobre imię firmy, jednak może okazać się dobrym uzupełnieniem tych działań.

Pierwsze ubezpieczenia powiązane z technologiami komputerowymi pojawiły się w USA w latach 90. XX w. Początkowo były one rozszerzeniem standardowych linii ubezpieczeń majątkowych: technicznych i OC. Ubezpieczenia cybernetyczne jako oddzielny produkt ubezpieczeniowy dynamicznie rozwinęły się w drugiej dekadzie naszego wieku, po kryzysie finansowym z 2007-2008 roku. Aktualnie cyberpolisy stanowią pakiety modułowe składające się z kilku sekcji. Zostały one stworzone w oparciu o wiedzę i doświadczenie specjalistów z różnych dziedzin m.in. informatyki. Specjalistyczne ubezpieczenie cyberryzyk może wypełnić wiele luk w tradycyjnych ubezpieczeniach. Polisa przede wszystkim chroni przedsiębiorstwo i ogranicza szkody w przypadku roszczeń odszkodowawczych związanych z utratą lub ujawnieniem danych. Zapewnia również pokrycie kosztów specjalistów, ekspertów ds. informatyki śledczej, odzyskiwania danych, prawników oraz konsultantów PR, których zadaniem jest doradztwo i opracowanie odpowiedniego planu działania w sytuacji kryzysowej. Ponadto, ubezpieczenie ryzyka cybernetycznego pozwala ograniczyć dotkliwe i daleko sięgające skutki naruszenia bezpieczeństwa danych. Przedmiotem ubezpieczenia cybernetycznego mogą być niemal wszystkie najważniejsze skutki incydentów cybernetycznych takie jak np. awaria infrastruktury, kradzież danych, nieumyślne i złośliwe

[242] K.Dąbek, A.Kaminski, *Czynniki rozwoju ubezpieczeń...,* s. 210.

działanie pracowników, działalność cywilna z tytułu naruszenia prywatności, kary administracyjne i koszty w postępowaniach regulacyjnych, wycieki danych i poufnych informacji oraz koszty reakcji po naruszeniu bezpieczeństwa informacji, koszty przeciwdziałania sytuacji kryzysowej, przywracanie sprawności systemów i integralności danych, utrata reputacji oraz utrata zysku. Ponadto, ubezpieczenie pokrywa koszty profesjonalnej pomocy na etapie aranżowania ochrony jak i po wystąpieniu zdarzenia ubezpieczeniowego. Zakres polisy jest elastyczny, dzięki czemu indywidualny program ubezpieczenia może zostać dostosowany do kluczowych ekspozycji na ryzyko przedsiębiorstwa, uwzględniając specyfikę funkcjonowania instytucji finansowych[243].

Oferta ubezpieczeń cybernetycznych skierowana jest do wszystkich przedsiębiorstw, które przetwarzają dane elektroniczne. Największe zainteresowanie ubezpieczeniami występuje wśród przedsiębiorstw z sektora usług finansowych, telekomunikacyjnych, handlu hurtowego i detalicznego, ochrony zdrowia. Jednak kompozycja rodzajów cyberryzyka występującego w poszczególnych sektorach gospodarki może być bardzo różna. Przykładowo instytucje finansowe są narażone głównie na wyciek poufnych danych osobowych i finansowych, a także nieuprawniony dostęp do systemu informatycznego (co może skutkować utratą reputacji i przerwą w działalności), podczas gdy firmy z sektora zaawansowanych technologii, takie jak koncerny farmaceutyczne wrażliwe na kradzież własności intelektualnej. Z kolei zakłady przemysłowe, wytwórcy i dostawcy mediów powinni zwracać szczególną uwagę na ochronę elektronicznych systemów kontroli maszyn i urządzeń[244].

Od pierwotnej postaci prostego ubezpieczenia majątkowego zakres ochrony cyberpolis ewoluuje w kierunku rozszerzonego ubezpieczenia odpowiedzialności cywilnej i ochrony prawnej, a także wyspecjalizowanego assistance z wysokimi sumami ubezpieczeń. Warto zaznaczyć, że ubezpieczenie assistance obejmuje m.in. doradztwo przy wdrażaniu polityki bezpieczeństwa oraz optymalizacji zabezpieczeń, dostęp do specjalistów z zakresu ochrony reputacji, a także usługi monitoringu nadużyć kredytowych lub ochrony tożsamości ofiar wycieków danych. Zakres ochrony ubezpieczenia cybernetycznego ze względu na dominujący charakter prawno-finansowy pozwala zaliczyć je do ubezpieczeń finansowych. Produkt ten

[243] K.Dąbek, A.Kaminski, *Czynniki rozwoju ubezpieczeń...,* s. 211.
[244] G.Strupczewski *Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie*, 2017, s. 259, (http://www.knfpan.pan.pl/images/Fin._110-17_15-G.Strupczewski.pdf), dostęp: 20.03.2018 r.

daje możliwość zabezpieczenia się przed negatywnymi skutkami problemów finansowych wynikających m.in. z roszczeń od niezadowolonych klientów. W konsekwencji staje się niezbędnym dopełnieniem programu ochrony ubezpieczeniowej, często polecanym przez firmy doradcze i brokerskie[245].

Ze względu na fakt istnienia ryzyka cybernetycznego oraz rosnącej świadomości zagrożeń stymulowanych postępem technologicznym wśród podmiotów gospodarczych, a także innych istotnych czynników należy spodziewać się wzrostu zainteresowania ubezpieczeniami cybernetycznymi. Rosnąca liczba i częstotliwość cyberincydentów przyczyniła się do przekonania o słuszności aktywnego zarządzanie ryzykiem. Jednym z głównych czynników determinujących rozpowszechnienie się cyberubezpieczeń jest potrzeba ochrony prywatności, minimalizacja finansowych konsekwencji zrealizowania się zagrożenia cybernetycznego a także obawa przed utratą reputacji, która może okazać się dotkliwym elementem zwłaszcza dla przedsiębiorstw opierających się na zaufaniu klientów. Następnym czynnikiem jest zmiana norm prawnych dotyczących sposobu postępowania w razie cyberincydentu[246].

Rozwój rynku ubezpieczeń cybernetycznych może napotkać bariery wywołane zachowaniami klientów lub uwarunkowaniami płynącymi z makrootoczenia - czynniki popytowe, a także czynniki podażowe. Do czynników popytowych należy zaliczyć m.in. niewłaściwą postawę właścicieli i zarządzających wobec ryzyka cybernetycznego, którzy postrzegają je jako nieubezpieczalne. Przedsiębiorstwa rezygnują z oferowanej ochrony ubezpieczeniowej z powodu nierozumienia korzyści z niej płynącej lub obawy przed komplikacjami wynikającymi z wdrażania ubezpieczenia. Częstym powodem lekceważenia z tej ochrony jest inwestycja w techniczne środki bezpieczeństwa IT kosztem zakupu ubezpieczenia. Do czynników podażowych zależnych od towarzystw ubezpieczeń należy m.in. ostrożność przy wprowadzaniu do oferty produktowej ubezpieczeń cybernetycznych spostrzeganych jako nowość stanowiącą słabo rozpoznawalne ryzyko[247]. Wyróżnić tu można pięć obszarów problemowych, które stanowią bariery rozwoju rynku ubezpieczeń cybernetycznych. Są to:

[245] K.Dąbek, A.Kaminski, *ob. cit.,* Rozdział 15, s. 212.
[246] G.Strupczewski *Ryzyko cybernetyczne jako..,* s. 260.
[247] G.Strupczewski, *Ryzyko cybernetyczne jako...,* s. 261.

- procedury związane z opracowaniem formularzy wniosków ubezpieczeniowych,
- ryzyko prawne dotyczące zgodności z przepisami prawa,
- underwriting - niedostatek danych skutkujący brakiem możliwości różnicowania składek,
- technologia IT powiązana z pojawiającymi się nowymi zagrożeniami,
- kumulacja szkód[248].

Dynamiczny charakter cyberryzyka może powodować nieadekwatne prognozowanie. Ponadto towarzystwo ubezpieczeniowe musi brać pod uwagę trudność oszacowania zdarzeń katastroficznych a także ich rozkład strat. Niezwykle istotna jest zatem asymetria informacji, będąca źródłem hazardu moralnego oraz selekcji negatywnej objawiającej się w dysponowaniu pełniejszą informacją ubezpieczonego w stosunku do ubezpieczyciela. Niewystarczająca ilość danych historycznych oznacza zwiększoną niepewność odnośnie do underwritingu, kształtowania warunków ochrony, ekspozycji na ryzyko a nawet polityki rezerw techniczno-ubezpieczeniowych. Te wszystkie bariery mogą sprawić, że nadmierna rozbudowa portfela ubezpieczeń cybernetycznych może skutkować obniżeniem ratingu ubezpieczyciela. W konsekwencji towarzystwa ubezpieczeniowe często stosują wysokie udziały własne w szkodzie, a także wyłączenia odpowiedzialności[249]. Przykładowo, według Ogólnych Warunków Umowy w Leadenhall Polska S.A., wyłączenia te dotyczą jakichkolwiek okoliczności, działań, uchybień lub zaniechań popełnionego przed datą początku okresu ubezpieczenia (a w przypadku umowy stanowiącej kontynuację wcześniejszej, przed datą początku okresu z pierwszej tych umów) lub przed datą retroaktywną. Wyłączenie odpowiedzialności jest także stosowane w przypadku domniemanego lub rzeczywistego naruszenia praw własności przemysłowej, kradzieży, kopiowania, ujawnienia lub publikacji handlowych a także jakiegokolwiek umyślnego naruszenia praw, niedozwolonych praktyk biznesowych, uchybienia lub zaniechania popełnione przez ubezpieczonego z bezprawnym zamiarem[250].

[248] *Ibidem,* s. 263.
[249] *Ibidem,* s. 265.
[250] *Karta produktu Leadenhall cyber,* (https://www.leadenhall.pl/files/Karta_produktu_LH_CYBER.pdf), dostęp: 17.03.2018 r.

Na polskim rynku (według stanu na koniec lutego 2018 roku) ubezpieczenia cybernetyczne oferowane są przez:

- AIG Europe Limited Sp. z o.o Oddział w Polsce - ubezpieczenie CyberEdge,
- STU Ergo Hestia S.A - ubezpieczenie danych elektronicznych od ryzyk cybernetycznych,
- Chubb European Group Ltd Sp. z o.o Oddział w Polsce - ubezpieczenie Data Guard Advantage,
- Leadenhall Polska S.A. - ubezpieczenie Leadenhall Cyber,
- TUiR Allianz Polska S.A. - ubezpieczenie Allianz Cyber Protect.

Oferta powyższych zakładów jest na razie bardzo skromna, a rozwiązania mało elastyczne. W konsekwencji ubezpieczenia cybernetyczne w Polsce nie są jeszcze tak powszechne jak w innych krajach np. USA.

Składka ubezpieczeniowa musi odzwierciedlać ryzyko podejmowane przez ubezpieczyciela. Wstępna ocena ryzyka cybernetycznego oraz obliczenie stawki ubezpieczeniowej bazuje na danych underwritingowych odzwierciedlających skalę narażenia na ryzyko. Najczęściej stawka zależna jest od branży, przychodów, liczby pracowników a także od wybranej sumy ubezpieczenia. Ustalając wysokość składki ubezpieczeniowej, towarzystwa ubezpieczeń biorą pod uwagę również takie czynniki, jak ilość przechowywanych danych wrażliwych oraz wrażliwość na ryzyko utraty zysku w wyniku cyberataków lub awarii systemów IT. W zależności od towarzystwa ubezpieczeniowego, może być tych czynników więcej. W rzeczywistości ustalenie prawidłowej składki oraz zbudowanie wiarygodnego modelu cyberryzyka jest ograniczone z powodu braku danych o szkodach, lub niepełną informację, która jest kluczowym elementem oceny ryzyka oraz zakwotowania składki ubezpieczeniowej[251]. W publikacji Indyjskiego Instytutu Zarządzania w Kalkucie, autorzy poruszyli temat udoskonalenia obliczania składki, które odbywa się za pomocą parametrów takich jak czynniki ryzyka oraz czynniki oceny ryzyka. Czynniki ryzyka, jeśli są obecne, mogą stanowić poważne zagrożenie. Wpływają one zarówno na częstotliwość jak i wielkość roszczeń. W niektórych przypadkach czynniki te nie są obiektywnie mierzalne. Dlatego też

[251] G.Strupczewski, *Wymogi informacyjne towarzystw ubezpieczeń w zakresie prewencji i bezpieczeństwa IT jako metoda redukcji asymetrii informacji w ubezpieczeniach cybernetycznych,* [w:] *Kierunki rozwoju ubezpieczeń prywatnych i publicznych,* pod red. W.Sułkowska, M.Cycoń, Wydawnictwo poltext, 2017, Rozdział 16, s. 220.

wykorzystuje się tak zwane parametry proxy, czyli współczynniki oceny ryzyka używane do obliczania składki[252]. Czynnikami determinującymi wzrost ryzyka cybernetycznego są:

- liczba godzin transakcji online,
- łatwość zhakowania strony internetowej i koszty jej naprawy,
- luka w zabezpieczeniach sprzętu ISP / użytkowników (np. bramy routerów),
- ryzyko ataku wirusa oraz infekcji złośliwego oprogramowania,
- ryzyko awarii oprogramowania lub sprzętu,
- przepustowość serwera użytkownika / dostawcy usług internetowych,
- strony internetowe dostępne dla użytkownika.

Natomiast do czynników oceny ryzyka należą m.in.:

- rodzaj ochrony (w obszarze szkód własnych lub pakiet ubezpieczeń). Jest to istotny współczynnik, ponieważ użytkownicy posiadający kompleksową ochronę będą mieli większą skłonność do bycia nieostrożnym niż posiadający ubezpieczenie od szkód własnych,
- wielkość nadwyżki (tj. wartość wnoszonego ryzyka w stosunku do wspólnie ponoszonego ryzyka),
- wartość zawartości strony internetowej i jej znaczenie dla przychodów organizacji,
- wiek użytkownika,
- cel użytkowania będący zastępnikiem dla liczby godzin transakcji online oraz ryzyka ataku wirusa[253].

Towarzystwa ubezpieczeniowe pozyskują informację w postaci kwestionariuszy wypełnianych przez klientów, które w zależności od przyjętych formularzy przyjmują formę pytań otwartych jak i zamkniętych. W większości towarzystw ubezpieczeniowych struktura kwestionariusza obejmuje pięć sekcji: podstawowe dane underwritingowe, zabezpieczenia organizacyjne, zabezpieczenia techniczne, ochrona danych osobowych, zarządzanie cyberryzykiem[254]. Wiodącą rolę pełnią podstawowe dane underwritingowe, na których oparta jest wstępna ocena ryzyka. Najczęściej pozyskuje się następujące informacje:

[252] A. Mukhopadhyay, D. Saha, B.B Chakrabarti, A. Mahanti, A. Podder, *op. cit*., s. 167.
[253] *Ibidem,* s. 167.
[254] G.Strupczewski, *Wymogi informacyjne towarzystw ubezpieczeń...,* s. 220.

- roszczenia wynikające z naruszenia prywatności lub kradzieży i utraty danych osobowych, dochodzenia prowadzone przez organ regulacyjny,
- skargi od klientów, pracowników,
- ewentualne zawieszenia systemu w przeszłości na skutek cyberataku[255].

Również problem bezpieczeństwa systemu IT wchodzącego w skład zabezpieczeń organizacyjnych w przedsiębiorstwie należy do istotnych determinant cyberryzyka, często pojawiającej się w kwestionariuszach (szczególny nacisk na tę tematykę kładą zwłaszcza Hestia i Lloyd's).

7.6. Rynek światowy ubezpieczeń cybernetycznych

W związku z zakorzenieniem się nowoczesnych technologii w życiu codziennym, pojawiają się nowe niebezpieczeństwa. Wzrastająca świadomość zagrożeń cybernetycznych, takich jak wpływ zakłóceń w działalności gospodarczej, a także zmiany regulacyjne przyczyniają się do rozwoju rynku ubezpieczeń cybernetycznych ze względu na większe przywiązywanie wagi do cyberbezpieczeństwa. Ubezpieczenia cybernetyczne zyskują coraz szerszy zasięg. Według szacunków publikowanych przez różne instytucje branżowe i grupy ubezpieczeniowe wynika, że w 2015 roku łączna wartość światowego rynku ubezpieczeń cybernetycznych wynosiła 2 mld USD, z czego 90% tej kwoty przypada na Stany Zjednoczone. Do tak wysokiego wyniku przyczyniły się następujące czynniki:

- wprowadzenie przepisów dotyczących naruszenia danych w 47 stanach, Dystrykcie Kolumbii, Guam, Puerto Rico i na Wyspach Dziewiczych,
- umieszczenie w 2015 roku przez firmy amerykańskie ryzyka cybernetycznego jako jednego z pięciu najważniejszych zagrożeń,
- wzrost naruszenia danych (od 2006 roku zgłoszone naruszenia danych w USA wzrosły o 325%),
- wzrost średnich kosztów naruszenia danych o 60% w porównaniu do roku 2006[256].

[255] *Ibidem,* s. 221.
[256] *Global Cyber Market Overview. Uncovering the hidden opportunities*, Aon Inpoint, June 2017, s. 5, (http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf), dostęp: 28.03.2018 r.

Z kolei badania przeprowadzone przez Marsh sugerują ciągłe przyspieszenie popytu na cyberbezpieczeństwo. Według tych danych, liczba amerykańskich klientów Marsh kupujących samodzielne ubezpieczenie cybernetyczne wzrosła w 2014 roku o 32% w stosunku do 2013 roku. Współczynnik absorpcji w sieci, czyli odsetek obecnych klientów odpowiedzialnych za bezpieczeństwo finansowe i zawodowe Marsh, którzy kupili ubezpieczenia cybernetyczne wzrósł do 16%. Zgodnie z najnowszymi badaniami (2018 rok, Marsh) rola ubezpieczeń w zwiększaniu odporności cybernetycznej jest coraz większa i uznawana przez decydentów na całym świecie. Również Organizacja Współpracy Gospodarczej i Rozwoju (OECD) zaleca działania w kierunku zakupu ubezpieczeń cybernetycznych. Globalnie prognozuje się, że poziom popytu na cyberubezpieczenia będzie zależał od częstotliwości występowania incydentów cybernetycznych oraz ewolucji regulacji prawnych w zakresie ochrony prywatności w wielu krajach. Przykładowo w Indiach w 2017 roku nastąpił wzrost liczby firm kupujących ubezpieczenia o 50% w stosunku do 2016 roku[257].

Zdaniem M. Eling i J.H. Wirfs, jak dotąd zasięg rynku ubezpieczeniowego jest niewielki. Co więcej, poza Stanami Zjednoczonymi, ochrona ubezpieczeniowa związana z ryzykiem cybernetycznym nie jest zbyt dobrze znana i mało wykorzystywana. Na przykład w Europie około 25% korporacji nie zdaje sobie sprawy, że tego rodzaju ubezpieczenie istnieje, a jedyne 10% kupiło ubezpieczenie od cyberryzyka (Marsh, 2013)[258]. Korzystanie z oferty ubezpieczeń cybernetycznych jest uzależnione od postrzegania ryzyka cybernetycznego, które uwarunkowane jest wielkością firmy. Im większa jest firma, tym poważniej postrzega ryzyko cybernetyczne. W ciągu pięciu lat (2011-2015) średnio o 14,4% więcej dużych korporacji postrzegało cyberryzyko jako przynajmniej umiarkowane w porównaniu do mniejszych firm. Również w Polsce 76% ankietowanych potwierdza, że niski poziom postrzegania ryzyka cybernetycznego ogranicza zainteresowanie ubezpieczeniem cybernetycznym[259].

Aon podaje, że początkowo ubezpieczenia cybernetyczne były kupowane głównie przez firmy TMT (Technology, Media and Telecom). W latach 2011-2015 popyt na ubezpieczenia był napędzany przez duże korporacje przechowujące dane osobowe i przetwarzające ogromne

[257] *Cyber risk management. Response and recovery*, Marsh&McLennan Companis, Global Risk Center, 2018, s. 8, (https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/WCD%20MMC%20Cyber%20Risk%20Management.pdf), dostęp: 25.03.2018 r.
[258] M. Eling,J. Wirfs Hendrik, 2016, *op. cit., s. 20.*
[259] Strupczeski, *The cyber-insurance market... s. 40*.

transakcje finansowe dużych detalistów i silnie regulowanych instytucji finansowych. Firmy te w USA pokrywają prawie połowę składek ubezpieczeniowych, odpowiednio 21% i 29%. Ponadto, rosnącym segmentem amerykańskiego rynku cybernetycznego jest opieka zdrowotna. Szacuje się, że stanowi ona 15% składki ubezpieczeniowej. Ubezpieczenie to jest zabezpieczeniem przed naruszeniem ochrony danych, zwłaszcza informacji o pacjencie. Obecnie (2018 r.) ubezpieczenia dla firm opieki zdrowotnej są oferowane jako odrębny produkt (niezależne ubezpieczenie) przez ubezpieczycieli. Niepokój dotyczący narażenia szpitali i klinik na cyberataki, które mogłyby wpłynąć na sieciowe urządzenia podtrzymujące życie są kolejnym czynnikiem determinującym popyt na ubezpieczenia cybernetyczne[260]. Według danych z 2017 roku głównymi nabywcami ubezpieczeń są duże i średnie przedsiębiorstwa, które stanowią około 80% składki ubezpieczeniowej. Prognozuje się również wzrost popytu wśród mniejszych przedsiębiorstw ze względu na większą świadomość cyberzagrożeń. Według prognoz bazujących na danych historycznych i założeniu utrzymującego się wzrastającego trendu, wartość amerykańskiego rynku ubezpieczeń w 2020 roku wyniesie 5,6 mld USD[261].

Zgodnie z badaniami opublikowanymi przez Allianz w 2017 roku 30% respondentów potwierdza, że cyfryzacja stwarza firmom nowe możliwości, jednak zmienia także charakter aktywów korporacyjnych z przeważnie fizycznych na coraz bardziej nienamacalne, niosąc ze sobą nowe zagrożenia, przede wszystkim zagrożenia cybernetyczne. Najnowsze badania stanowią kontynuację trendu obserwowanego od 2015 roku. Zgodnie z Allianz Risk Barometer 2018, przerwa w działalności (BI) jest najważniejszym globalnym ryzykiem szósty rok z rzędu. Ryzyko cybernetyczne badane przez ekspertów ds ryzyka z 80 krajów, w dalszym ciągu znajduje się w czołówce. Zajmuje miejsce pierwsze w USA, a drugie na świecie. Jest to prawdopodobnie spowodowane niedawnymi cyberatakami takimi jak WannaCry i Petya / NotPetya, które spowodowały znaczne straty finansowe dla wielu firm[262].

Firmy, które najbardziej obawiają się ryzyka cybernetycznego i które najczęściej kupują cyberubezpieczenia, działają głównie w sektorze usług finansowych (22,8%), telekomunikacji (14,8%), handlu hurtowego i detalicznego (9,6%) oraz opieki zdrowotnej (11,7%). Jednak

[260] *Global Cyber Market Overview. Uncovering...,* s. 5.
[261] *Ibidem*, s. 6.
[262] Allianz Risk Barometer, *Top Business Risk 2018 r...*, s. 6.

rodzaje cyberryzyka w różnych sektorach gospodarki mogą się między sobą różnić. Na przykład instytucje finansowe są narażone przede wszystkim na wyciek poufnych danych osobowych i finansowych lub nieautoryzowany dostęp do systemu, co może skutkować m.in. kradzieżą pieniędzy, utratą reputacji oraz przerwami w działalności. Natomiast firmy z sektorów wysokich technologii, takie jak firmy farmaceutyczne, są znacznie bardziej narażone na kradzieże własności intelektualnej. Zakłady przemysłowe, producenci i dostawcy mediów powinni z kolei zwrócić szczególną uwagę na ochronę elektronicznych (w szczególności odległych) systemów kontrolowania maszyn i urządzeń[263].

W raporcie Allianz znajduje się 5 trendów rozwoju ubezpieczeń cybernetycznych:

- wyłączenia w klasycznych polisach ubezpieczeniowych oraz wzrost znaczenia specjalistycznych cyberubezpieczeń dotyczących odpowiedzialności cywilnej,
- weryfikacja adekwatności pokrycia ubezpieczeniowego w stosunku do roszczeń osób poszkodowanych oraz roszczeń odszkodowawczych,
- umożliwienie zakładom ubezpieczeń segmentacji klientów oraz oferowania produktów dostosowanych do specyficznych potrzeb w niektórych sektorach,
- poprawa znajomości ryzyka cybernetycznego w zakładach ubezpieczeń oraz zwiększenie świadomości ubezpieczeniowej wśród przedsiębiorców,
- szybkie reagowanie na incydenty cybernetyczne, co może ograniczyć szkody z nimi związane[264].

7.7. Szkodowość w ubezpieczeniach cybernetycznych

Od 2005 roku zjawisko naruszenia danych osobowych, stało się głównym problemem wielu organizacji, zarówno w sektorze prywatnym, jak i publicznym. Od 2005 r. odnotowano 5 029 przypadków naruszenia danych w Stanach Zjednoczonych, gdzie organizacje muszą zgłaszać wycieki danych organom regulacyjnym, obejmujące ponad 675 milionów szacunkowych danych, zgodnie z *Identity Theft Resource Center*. Statystyki spoza USA są niejednolite. Według szacunków the Center for Media, Data and Society na Uniwersytecie Środkowoeuropejskim w Europie odnotowano co najmniej 200 naruszeń, z czego 227

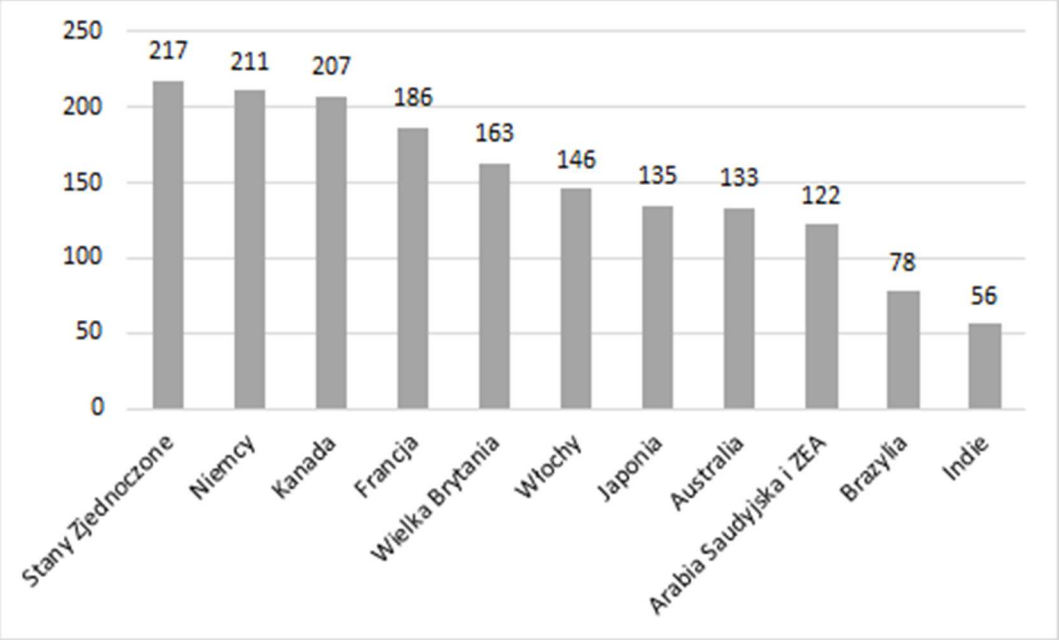
[263] G. Strupczewski, *The cyber-insurance market in Poland...,* s. 37.
[264] Allianz 2015*, A guide to cyber risk…,* s.18.

milionów danych odnotowano od 2005 r. Według Allianz (2015) przeciętny koszt naruszenia danych osobowych wzrasta dla przedsiębiorstw na całym świecie do 3,8 mln USD, w porównaniu do 3,5 mln USD roku poprzedniego[265].

W raporcie NetDiligence z 2017 roku dotyczącego szkód ubezpieczeniowych można znaleźć wyniki badań przeprowadzonych na podstawie danych opublikowanych w latach 2014-2017 zaczerpniętych głównie ze Stanów Zjednoczonych oraz Kanady. Według raportu łączne koszty poniesione w wyniku naruszenia ochrony danych osobowych dotyczące wniosków złożonych w latach 2014-2017 wyniosły 202 mln USD. Najmniejszy zanotowany koszt naruszenia wynosił 110 USD, a największy - 16,8 mln USD. Natomiast przeciętny koszt w okresie 2014-2017 wyniósł 394 000 USD[266].

Ponemon Institute przedstawił wyniki z badania przeprowadzonego w 2015 roku w wybranych 11 krajach, przedstawiające istotne różnice w przeciętnym koszcie naruszenia bezpieczeństwa danych osobowych w przeliczeniu na jednego mieszkańca. Jak pokazuje rysunek 3, koszty związane z wyciekiem danych są zróżnicowane pod względem terytorialnym, a więc najwyższe koszty per capita ponoszą Stany Zjednoczone i Niemcy – wynoszą one odpowiednio 217 USD i 211 USD. Natomiast Indie i Brazylia miały najniższe koszty na poziomie odpowiednio 56 USD i 78 USD[267].

[265] *Ibidem,* s. 6.
[266] *Cyber Claims Study*, NetDiligence 2017, s. 5, (https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition.pdf), dostęp: 10.03.2018 r.
[267] Ponemon Institute*, 2015 Cost of Data Breach Study: Global Analysis,* s. 5, Ponemon Institute, May 2015, (https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF), dostęp: 10.03.2018 r.

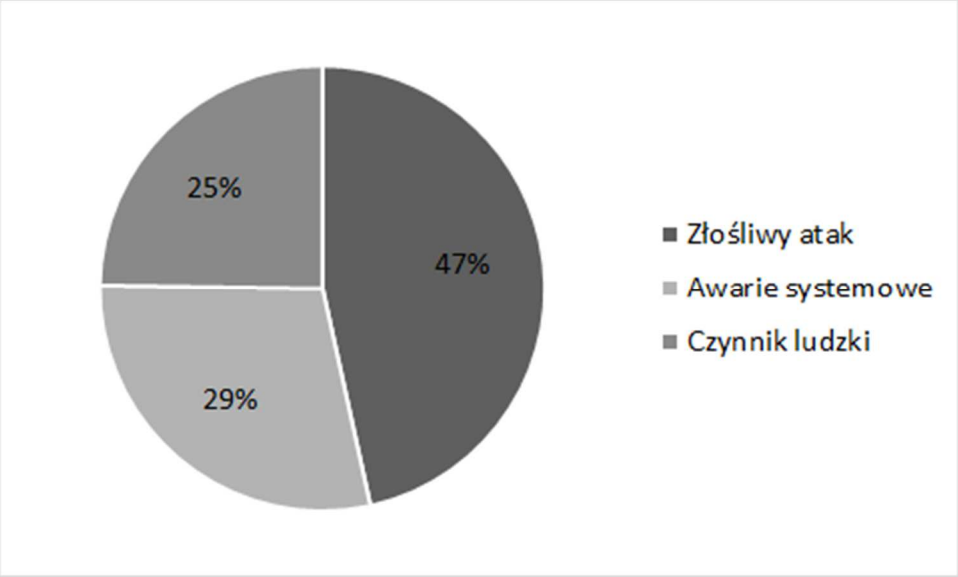


Rysunek 7.3. Przeciętny koszt naruszenia ochrony danych osobowych per capita w 11 wybranych krajach w 2015 roku (w USD)

Źródło: *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, May 2015, s. 5, (https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF), dostęp: 10.03.2018 r.

Jak podaje Ponemon Institute (2015) głównymi przyczynami globalnego naruszenia bezpieczeństwa danych są złośliwe i przestępcze ataki. Rysunek 7.4 zawiera najważniejsze przyczyny w ujęciu skonsolidowanym dla badanych, wcześniej wymienionych 11 krajów. Aż 47% incydentów obejmuje złośliwy atak, 25% dotyczy zaniedbania pracownika lub wykonawcy (czynnik ludzki), natomiast 29% obejmuje awarie i błędy systemu, które dotyczą zarówno awarii procesów informatycznych, jak i biznesowych. Co ważniejsze, to właśnie przestępcze ataki są najbardziej kosztowne na całym świecie[268].

[268] *Ibidem*, s. 10.



Rysunek 7.4. Udział głównych przyczyn naruszenia ochrony danych osobowych w badanych 11 krajach w 2015 roku (w %)

Źródło: *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, May 2015, s. 10, (https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF), dostęp: 10.03.2018 r.

Z danych wynika, że koszty naruszenia ochrony danych osobowych w przeliczeniu na jednego mieszkańca spowodowane atakami złośliwymi wzrosły ze średnio 159 USD w 2014 r. do 170 USD w 2015 r. Jest to znacznie więcej niż koszty per capita w przypadku naruszenia bezpieczeństwa danych wywołanego przez system i czynniki ludzkie wynoszące odpowiednio 142 USD i 137 USD. W roku 2014 natomiast, usterki systemowe wynosiły średnio 126 USD, zaś błąd ludzki 117 USD[269].

7.8. Zakończenie

W dobie globalizacji i w czasach postępu technologicznego, gdy dominującą rolę zaczął pełnić internet, ryzyka związane z cyberprzestrzenią awansowały do grona najważniejszych zagrożeń dla gospodarki światowej. Każda firma, która przechowuje dane elektroniczne na komputerze, serwerze lub w Internecie jest narażona na ataki cybernetyczne. W miarę wzrostu ryzyka cybernetycznego i jego rosnącego potencjalnego wpływu na gospodarkę, organizacje będą musiały stawić czoła rosnącej presji na wdrożenie solidnego rozwiązania i

[269] *Ibidem*, s. 10.

kompleksowego zarządzania ryzykiem cybernetycznym. Upowszechnienie się ryzyka w sferach życia prywatnego i gospodarczego jest jednym z czynników determinujących popyt na cyberpolisy. W konsekwencji cyberubezpieczenia są coraz częściej postrzegane jako kluczowy element zarządzania kosztami. Ze względu na szeroki zakres pokrycia ubezpieczeniowego zachęca się firmy do zaopatrzenia się w ten produkt, który pozwala na transfer ryzyka cybernetycznego łagodząc skutki jego działania.

Ograniczony charakter doświadczeń w zakresie roszczeń związanych z bezpieczeństwem cybernetycznym, jak i brak ostatecznych danych na temat kosztów związanych z różnymi rodzajami ryzyka i awariami bezpieczeństwa utrudnia rozwój branży ubezpieczeniowej i reasekuracyjnej. Jedną z kluczowych kwestii dotyczących ubezpieczenia od skutków cyberryzyka jest brak wiarygodnych danych, co przyczynia się do asymetrii informacji pomiędzy ubezpieczonymi a ubezpieczycielami. Ważny jest także problem określenia ubezpieczalnych rodzajów ryzyka, do którego mogą doprowadzać zmiany technologiczne. Barierę stanowi również brak odpowiedniej asekuracji, wywołanej brakiem wiarygodnych danych, oraz powstawaniem i rozwojem nowych form cyberprzestępstw, które stanowiąc nierozpoznawalne ryzyko, utrudniają prawidłowe oszacowanie faktycznych szkód powstałych w wyniku realizacji incydentów cybernetycznych[270].

Rynek ubezpieczeń cybernetycznych w Polsce nie jest jeszcze rozwinięty w porównaniu do innych krajów. Czynnikiem, który może wpłynąć na wzrost znaczenia ubezpieczeń cybernetycznych jest wejście w życie unijnego Rozporządzenia o Ochronie Danych Osobowych (RODO) w maju 2018 roku, będącego uzupełnieniem regulacji prawnych, których celem jest zwiększenie bezpieczeństwa w cyberprzestrzeni, a także ograniczenie szkód wynikających z cyberprzestępstw. Rozporządzenie to może również doprowadzić do wzrostu zainteresowania produktami ubezpieczeniowymi oraz ich rozwoju.

Według ostatniej edycji ćwiczeń „Cyber-EXE Polska" (2016 r.) polegających na zaaranżowaniu symulowanego ataku, który ma na celu zbadanie jak zachowają się uczestnicy ćwiczenia, polskie banki są coraz lepiej przygotowane na cyberzagrożenia i potrafią dobrze koordynować niezbędne działania podejmowane w chwili wystąpienia cyberataku. W

[270] *Incentives and barriers of the cyber insurance market in Europe,* Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, ENISA 2012, s. 19, (www.enisa.europa.eu), dostęp: 20.03.2018 r.

porównaniu do ćwiczenia przeprowadzonego dwa lata wcześniej, z najnowszego Cyber-EXE Polska (2016 r.) wynika, że sektor bankowy i ubezpieczeniowy zrobił duży postęp w obronie przed cyberatakami. Nadal jednak istnieje dość duży problem we współpracy pomiędzy bankami, które w ograniczonym stopniu informują się nawzajem o zaistniałych zagrożeniach[271].

Ubezpieczenie od cyberryzyka jest odpowiedzią na zapotrzebowanie rynku wobec konieczności pokrycia następstw cyberincydentów. Ponadto ma fundamentalne znaczenie dla ochrony przedsiębiorstw przed szkodami wynikającymi z roszczeń odszkodowawczych związanych z utratą danych. Główne stymulanty w dziedzinie cyberbezpieczeństwa można powiązać z oczekiwaniami lepszego określenia, co jest skuteczne w zmniejszaniu ryzyka (a tym samym zwiększaniu ryzyka dla użytkowników takich produktów i usług dla przewoźników ubezpieczeniowych). Miałoby to wpływ na pobudzenie zasięgu działania rynków wtórnych, zwiększając podaż i prawdopodobnie podnosząc świadomość klientów na temat wymagań dotyczących bezpieczeństwa cybernetycznego.

[271] *Cyber-EXE Polska: Banki są coraz lepiej przygotowane na cyberzagrożenia,* „Puls Biznesu" ISBNews, 2016, (https://www.pb.pl/cyber-exe-polska-banki-sa-coraz-lepiej-przygotowane-na-cyberzagrozenia-81882)

Literatura

Piśmiennictwo

Becella A., *Kierunki rozwoju ubezpieczenia kredytu kupieckiego w Polsce*, Studia Oeconomica Posnaniensia, 2015, vol. 3, nr 2.

Bera A., *Analiza rynku ubezpieczeń turystycznych wybrane aspekty*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, 2008, Nr 521.

Biener C., Eling M., Hendrik J., *Insurability of Cyber Risk: An Empirical Analysis*, Institute of Insurance Economics, Working Papers on Finance No. 2015/03.

Bógdoł-Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.

Broda M.Z., *Nowe wyzwania BI,* cz. 2, Dziennik Ubezpieczeniowy 2008, nr 2103.

Byrska D., Gawkowski K., Liszkowska D., *Unia Europejska. Geneza. Funkcjonowanie. Wyzwania.,* Monografia Naukowa współautorska, wyd. Exante, Wrocław 2017.

Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, COM/2016/0766.

Cycoń M., Jedynak T., *Ubezpieczenie utraty zysku jako metoda zarządzania ryzykiem w działalności gospodarczej*, Ekonomiczne Problemy Usług nr 63, Zeszyty Naukowe Uniwersytetu Szczecińskiego, 2011.

Dankiewicz R., Ubezpieczenia kredytu kupieckiego w procesie zarządzania ryzykiem utraty należności w okresach wahań koniunktury w gospodarce, „Zarządzanie i Finanse", 2012, Nr 4.

Dankiewicz R., Determinanty rozwoju rynku ubezpieczeń kredytu kupieckiego w Polsce, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 2011, Nr 228.

Dankiewicz R., *Odpowiedzialność ubezpieczyciela w ubezpieczeniu kredytu kupieckiego. Wybrane aspekty*, Wiadomości ubezpieczeniowe, Nauka dla praktyki, PIU nr 01/2009.

Dankiewicz R., *Składka a faktyczny koszt ubezpieczenia kredytu kupieckiego*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 2010, Nr 105.

Dąbek K., Kamiński A., *Czynniki rozwoju ubezpieczeń cybernetycznych na świecie i w Polsce - wybrane aspekty* [w:] *Kierunki rozwoju ubezpieczeń prywatnych i publicznych,* pod red. Sułkowska W., Cycoń M., Wydawnictwo Poltext, 2017

Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

E-Terroryzm.pl, Internetowy Biuletyn Instytutu Studiów nad Terroryzmem, Listopad 2013.

Fedor M., *Bezwzględne kryteria ubezpieczalności*, Gazeta Ubezpieczeniowa Pismo Środowisk Ubezpieczeniowych i Finansowych, 08/ 2004.

Fedor M., *Granice ubezpieczalności cz. 1*, Gazeta Ubezpieczeniowa Pismo Środowisk ubezpieczeniowych i finansowych 07/2004.

Gasińska M., *Ubezpieczenia turystyczne w systemie ubezpieczeń gospodarczych*, Zeszyty Naukowe Uczelni Vistula, 2013, Nr 32.

Gawrycki M. F., *Cyberterroryzm*, Fundacja Studiów Międzynarodowych, Warszawa 2003.

Gos W., Hońko S., *Branżowe problemy rachunkowości i podatków*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 373, pod red. Zbigniew Luty, Aleksandra Łakomiak, Alicja Mazur Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2014.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* Zeszyty Naukowe UEK nr 22/2012.

Herzog S., *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, Journal of Strategic Security, Number 2 Volume 4, No. 2, Federation of American Scientists, Washington, D.C., Summer 2011.

Iwanicz-Drozdowska M., *Ubezpieczenia*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2013.

Jagoda R., *Koszty i korzyści a ryzyko ubezpieczenia należności*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 2015, Nr 398.

Jędrzychowska A., *Ubezpieczenia turystyczne*, [w:] *Ubezpieczenia*, pod red. W. Ronka-Chmielowiec, Wydawnictwo C.H. Beck, Warszawa 2016.

Jęksa Z., *Ubezpieczenia majątku i zysku firmy*, Poltext, Warszawa 1999.

Kisielnicki J., *MIS. Systemy informatyczne zarządzania*, Wydawnictwo Placet, Warszawa 2008.

Kośla R., *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski. Wystąpienie na konferencji w Bemowie*, 29 listopada 2002.

Kowalczyk P., Poprawska E., Ronka-Chmielowiec W., *Metody aktuarialne*, Wydawnictwo PWN, Warszawa 2006.

Krajenta M. *Rozwój i znaczenie ubezpieczeń cybernetycznych na polskim rynku ubezpieczeniowym,* "Wybrane problemy ubezpieczeń tom 2 - ubezpieczenia gospodarcze, zdrowotne, rolnicze i inne zagadnienia", Monografia naukowa, Warszawa czerwiec 2016.

Kufel J., *Ubezpieczenia gospodarcze w orzecznictwie sądowym,* Wydawnictwo Branta, Bydgoszcz 2002.

Kukiełka J., *Ubezpieczenie kredytu*, Centrum Edukacji i Rozwoju Biznesu Olympus, Warszawa 1994.

Lewandowska K., *Zmiany klimatu a ryzyko dla przedsiębiorstwa, Wybrane problemy gospodarki światowej pierwszej dekady nowego wieku,* W. Michalczyka (red.), Uniwersytet Ekonomiczny we Wrocławiu. Katedra Międzynarodowych Stosunków Gospodarczych, Wrocław 2009.

Lisowski J., *Specyfika gospodarki finansowej ubezpieczycieli kredytu kupieckiego w Polsce,* Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010.

Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, Madej M., Terlikowski M. (red.), Warszawa 2009.

Miazek- Popłacz J., Dla kogo ubezpieczenie utraty zysku, Miesięcznik Ubezpieczeniowy, styczeń 2014.

Monkiewicz J., *Podstawy ubezpieczeń. Tom II – produkty*, Poltext, Warszawa 2001.

Nahotko S., *Ryzyko ekonomiczne w działalności gospodarczej*, TNOiK: Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego, Bydgoszcz 1997.

Pala M., *Wybrane aspekty bezpieczeństwa w cyberprzestrzeni*, [w:] *De Securitate et Defensione. O Bezpieczeństwie i Obronności* nr 1/ 2015.

Podraza A., Potakowski P., Wiak K., *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa 2013.

Pollit M. M., *Cyberterrorism – Fact or a Fancy?*, [w:] *Focus on Terrorism*, ed. E.V. Linden, New York 2007.

Putelbergier B., *Rezerwy techniczno-ubezpieczeniowe*, Gazeta Ubezpieczeniowa, 24 stycznia 2006

Radawiecka E., *Porównanie bilansu zakładów ubezpieczeń i zakładów reasekuracji do bilansu innych jednostek*, Zeszyty Naukowe Wydziału Nauk Ekonomicznych nr 17, Koszalin 2013.

Radawiecka E., *Rezerwy techniczno-ubezpieczeniowe warunkiem stabilności funkcjonowania zakładów ubezpieczeń*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 765 Finanse, Rynki Finansowe, Ubezpieczenia nr 61 (2013), pod red. Teresy Kiziukiewicz, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2013.

Ronka-Chmielowiec W., *Ubezpieczenia*, Wyd. C.H.Beck, Warszawa 2016.

Rybicka K., *Rezerwy w rachunkowości zakładu ubezpieczeń*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 765 Finanse, Rynki Finansowe, Ubezpieczenia nr 61 (2013), pod red. Teresy Kiziukiewicz, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2013

Rydzicki T., *Polisa na utracone zyski*, Gazeta Małych i Średnich Przedsiębiorstw, 2007 r., nr 61.

Ryzyko operacyjne w naukach o zarządzaniu, pod red. I. Staniec, J. Zawiła-Niedźwiecki, C. H. Beck, Warszawa 2015.

Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa,* [w:] *Repozytorium Uniwersytetu Wrocławskiego,* Wrocław 2015.

Sobczyk M., *Ubezpieczenia w turystyce i rekreacji*, Wydawnictwo Difin, Warszawa 2013.

Spigarska E., *Rezerwy techniczno-ubezpieczeniowe jako podstawa wypłacalności i stabilności finansowej zakładów ubezpieczeń*, Prace i Materiały Wydziału Zarządzania Uniwersytetu Gdańskiego 2009 nr 3/1, Gdańsk 2009.

Spigarska E., *Zasady kalkulacji składki ubezpieczeniowej w zakładach ubezpieczeń*, Prace i Materiały Wydziału Zarządzania Uniwersytetu Gdańskiego, 4/2007.

Stępień A. *Bezpieczeństwo w erze cyfryzacji,* [w:] *Bezpieczeństwo zewnętrzne i wewnętrzne wobec współczesnych wyzwań-wybrana problematyka,* pod red. Stępień A., "Przedsiębiorczość i Zarządzanie", Wydawnictwo SAN, Warszawa 2017, Tom 18, nr 5, cz.2.

Stępnicka N., *Cyberprzestrzeń i zagrożenia z nią związane*, [w:] *Bezpieczeństwo i zarządzanie kryzysowe, bezpieczeństwo społeczności lokalnych*, pod red. Wilk-Woś Z., "Przedsiębiorczość i Zarządzanie", Wydawnictwo SAN, Warszawa 2017, Tom 18, nr 5, cz.3.

Strupczewski G., *Wymogi informacyjne towarzystw ubezpieczeń w zakresie prewencji i bezpieczeństwa IT jako metoda redukcji asymetrii informacji w ubezpieczeniach cybernetycznych,* [w:] *Kierunki rozwoju ubezpieczeń prywatnych i publicznych,* pod red. Sułkowska W., Cycoń M., Wydawnictwo Poltext, Kraków 2017.

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

Sułkowska W., *Współczesne ubezpieczenia gospodarcze*, Wyd. Uniwersytetu Ekonomicznego w Krakowie, Kraków 2013.

Szewczuk A., *Business Interruption- Ewolucja kompleksowego programu ubezpieczeniowego dla sektora małych i średnich przedsiębiorstw*, Ekonomiczne Problemy Usług nr 50, Zeszyty Naukowe Uniwersytetu Szczecińskiego, 2010.

Szewczuk A*., Ubezpieczenie należności jako efektywny instrument zarządzania ryzykiem handlowym w warunkach kryzysu finansowego*, Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług, 2010, Nr 43.

Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego,* Zeszyty Naukowe Akademii Marynarki Wojennej, nr 1, 2005.

Ubezpieczenia dla przedsiębiorstw, pod. red. E. Wierzbickiej, Oficyna Wydawnicza Szkoła Główna Handlowa w Warszawie, Warszawa 2014.

Ubezpieczenia gospodarcze, pod. red. T. Sangowskiego, Poltext, Warszawa, 1998.

Ubezpieczenia non- life, pod. red. E. Wierzbickiej, CeDeWu, Warszawa 2010.

Ubezpieczenia wobec wyzwań XXI wieku, pod. red. W. Ronki-Chmielowiec, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2011.

Ubezpieczenia, pod. red. W. Ronki-Chmielowiec, C.H.Beck, Warszawa 2016.

Węderska K., *Cybernetyczny Pearl Harbor- mit czy rzeczywistość?*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka, Diffin, Warszawa 2014

Wierzbicka E., *Ubezpieczenie jako ekonomiczny instrument zarządzania należnościami małych i średnich przedsiębiorstw*, 2015, Nr 5/2015.

Wirfs J. H., *Essays on ciber risk and efficency in the insurance industry*, The University of St. Gallen, Difo-Druck GmbH, Bamberg, 2016.

Współczesne ubezpieczenia gospodarcze, pod red. W. Sułkowskiej, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2013.

Zawisza J. *Cyberprzestępczość i jej wpływ na bezpieczeństwo człowieka,* [w:] *Bezpieczeństwo zewnętrzne i wewnętrzne wobec współczesnych wyzwań-wybrana problematyka,* pod red. Stępień A., "Przedsiębiorczość i Zarządzanie", Wydawnictwo SAN, Warszawa 2017, Tom 18, nr 5, cz.2.

Żukrowska K., Grącik M., *Bezpieczeństwo międzynarodowe*, Szkoła Główna Handlowa, Warszawa 2006.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady 2006/43/WE z dnia 17 maja 2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiS (Dz. Urz. UE L 218 z 14 VIII 2013 r. poz. 8).

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. 2015 poz. 728, z późn. zm.)

Rozporządzenie Ministra Finansów z dnia 12 kwietnia 2016 r. w sprawie szczególnych zasad rachunkowości zakładów ubezpieczeń i zakładów reasekuracji (Dz.U. 2016 poz.562).

Ustawa z dnia 23 kwietnia 1964r. – Kodeks cywilny (Dz.U. 1964 nr 16 poz. 93).

Ustawa z dnia 7 lipca 1994 r. o gwarantowanych przez Skarb Państwa ubezpieczeniach kontraktów eksportowych (Dz.U. 1994 nr 86 poz. 398).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. 1997, Nr 88, poz. 553, z późn. zm.).

Ustawa z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz.U. 1997 Nr 133 poz. 884, z późn. zm.).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (tekst jednolity: Dz. U. 2002, Nr 156 poz. 1301, ze zm.)

Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (tekst jedn. Dz. U. z 2004 r., poz. 1807).

Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej.

Ustawa z dnia 24 listopada 2017 r. o imprezach turystycznych i powiązanych usługach turystycznych (Dz.U. 2017 poz. 2361).

Źródła internetowe

2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2015, (https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF), dostęp: 10.03.2018 r.

A guide to cyber risk. Managing the impact of increasing interconnectivity., Allianz Global Corporate & Specialty, Allianz 2015, (https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf), dostęp: 22.03.2018 r.

Aleksandrowicz T. R.*, Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego,* (www.abw.gov.pl/pl/pbw).

Allianz Risk Barometer, *Top Business Risk 2018*, Allianz Global Corporate & Specialty, (http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf) dostęp: 15.03.2018 r.

Allianz Risk Barometer 2017 - Top risks in focus: Cyber incidents, Allianz Global Corporate & Specialty, (www.agcs.allianz.com).

Allianz Risk Barometer, Top Business Risks 2015, Allianz Global Corporate & Specialty, (https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2015_EN.pdf), dostęp: 15.03.2018 r.

Allianz Risk Barometer: Appendix 2018, Allianz Global Corporate & Specialty, (http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_APPENDIX.pdf), dostęp: 15.03.2018 r.

Automated and Connected Driving, Ethics Commission Appointed by the Federal Minister of Transport and Digital Infrastructure 2017, (https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile).

Automated and Electric Vehicles Bill, HL Bill 82 57/1, (https://publications.parliament.uk/pa/bills/lbill/2017-2019/0082/lbill_2017-20190082_en_1.htm), dostęp: 28.03.2018 r.

Automobile insurance in the era of autonomous vehicles. Survey results, KPMG 2015, (https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/kpmg-automobile-insurance-in-era-autonomous.pdf), dostęp: 5.04.2018

Barycki P., *Jeśli usłyszysz o wypadku autonomicznego auta, możesz być niemal pewny, że spowodował go… człowiek*, (https://www.spidersweb.pl/2015/05/autonomiczne-auta-wypadki.html), dostęp: 20.03.2018.

Barycki P., *Zdejmujesz ręce z kierownicy i nie musisz się niczym przejmować. Tak, takie samochody są już na rynku*, (https://www.spidersweb.pl/2018/01/samochody-autonomiczne-poziomy.html), dostęp: 7.03.2018.

Business interruption Insurance Efficacy: Five Key Issues, Marsh & McLennan Companies, Marsh Risk Management Research, February, 2015, (https://www.marsh.com/us/insights/research/business-interruption-insurance-efficacy—five-key-issues.html), dostęp: 18.04.2018 r.

Cebula J. J., Young L. R., *A Taxonomy of Operational Cyber Security Risks*, Software Engineering Institute, December 2010, (https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf), dostęp: 22.03.2018 r.

Connected and Autonomous Vehicles: The future?, House of Lords Science and Technology Select Committee 2017, (https://publications.parliament.uk/pa/ld201617/ldselect/ldsctech/115/115.pdf), dostęp: 28.03.2018.

Cyber Claims Study, NetDiligence 2017, (https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition.pdf), dostęp 10.03.2018r.

Cyber-EXE Polska: Banki są coraz lepiej przygotowane na cyberzagrożenia, Puls Biznesu ISBNews, 19.01.2016, (https://www.pb.pl/cyber-exe-polska-banki-sa-coraz-lepiej-przygotowane-na-cyberzagrozenia-818827).

Cyber risk management. Response and recovery, Marsh&McLennan Companis, Global Risk Center, 2018, (https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/WCD%20MMC%20Cyber%20Risk%20Management.pdf), dostęp: 22.03.2018 r.

Cyber ubezpieczenia, Allbroker Sp z.o.o., (www.allbroker.pl).

Data Breach Statistic, (www.breachlevelindex.com).

Declaration of Amsterdam. Cooperation in the field of connected and automated driving, The Netherlands EU Presidency 2016, (https://www.regjeringen.no/contentassets/ba7ab6e2a0e14e39baa77f5b76f59d14/2016-04-08-declaration-of-amsterdam---final1400661.pdf), dostęp: 28.03.2018.

Doktryna cyberbezpieczeństwa RP, BBN, 2015, (https://www.bbn.gov.pl).

Domański T., *Oto nowe Audi A8. Pierwsza limuzyna, która nie potrzebuje kierowcy*, (https://www.spidersweb.pl/2017/07/nowe-audi-a8.html), dostęp: 7.03.2018.

Ehrenfeld Jesse M., *WannaCry, Cybersecurity and Health Information Technology: A Time to Act*, 24 May 2017, (https://link.springer.com/content/pdf/10.1007%2Fs10916-017-0752-1.pdf), dostęp: 20.03.2018 r.

Eling M., Wirfs J.H., *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class*,(Institute of Insurance Economics, University of St. Gallen, 2016, https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf), dostęp: 22.03.2018 r.

Fagnant D. J., Kockelman K. M., *Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations*, Eno Foundation 2013, (https://www.enotrans.org/etl-material/preparing-a-nation-for-autonomous-vehicles-opportunities-barriers-and-policy-recommendations/), dostęp: 7.03.2018.

Firma ubezpieczeniowa PZU – informacje, (https://www.pzu.pl/grupa-pzu/pzu-sa), dostęp: 26.04.2018 r.

Gasser T. M., Westhoff D., *BASt-study: Definitions of Automation and Legal Issues in Germany*, German Federal Highway Research Institute 2012, (http://onlinepubs.trb.org/onlinepubs/conferences/2012/Automation/presentations/Gasser.pdf), dostęp: 7.03.2018.

Global Claims Review 2015: Business Interruption in Focus. Global trends and development in business interruption claims, Allianz Global Corporate& Speciality, 2015, (https://www.agcs.allianz.com/assets/PDFs/Reports/AGCS-Global-Claims-Review-2015.pdf), dostęp: 01.03.2018 r.

Global Cyber Market Overview. Uncovering the hidden opportunities, Aon Inpoint, June 2017, (http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf), dostęp: 28.03.2018 r.

Global Risks 2014, Ninth Edition, by the World Economic Forum, (www.weforum.org/risks).

Golonka A., *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne,* Rozprawy i Materiały 2016, nr 1(18), (https://sp.ka.edu.pl/numery/2016-1/studia-prawnicze-rim-2016-1-golonka.pdf), dostęp: 22.03.2018 r.

Hartwig R. P., Cyber risks: The growing threat, Insurance information Institute, June 2014, (www.iii.org).

Hołyst B., Pomykała J., *Cyberprzestępczość, ochrona informacji i kryptologia,* Prokuratura i Prawo 1, 2011, s.13, (http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2011/01/1holyst.pdf), dostęp: 24.03.2018 r.

Incentives and barriers of the cyber insurance market in Europe, Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, ENISA, June 2012, (www.enisa.europa.eu), dostęp: 20.03.2018 r.

Indyjsko-pakistański konflikt o Kaszmir (www.psz.pl).

Insuring autonomous vehicles, Accenture, Stevens Institute of Technology 2017, (https://www.accenture.com/t20170530T040532__w__/pl-en/_acnmedia/PDF-53/Accenture-Autonomous_Vehicles.pdf), dostęp: 4.04.2018.

Internet Crime Reaport 2011, Internet Crime Compliant Center, (www.pdf.ic3.gov).

Karta produktu Leadenhall Cyber, (https://www.leadenhall.pl/files/Karta_produktu_LH_CYBER.pdf), dostęp 17.03.2018 r.

Kaspersky, *Carbanak APT. The great bank robbery*, Kaspersky Lab, February 2015, Version 2.1, s. 3, (https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf), dostęp: 29.03.2018 r.

Kopp E., Kaffenberger L., Wilson C*., Cyber Risk, Market Failures, and Financial Stability*, WP/17/185, August 2017, (https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104), dostęp: 22.03.2018 r.

Korns S. W., Kastenberg J. E*., Georgia's Cyber Left Hook, (*http://ssi.armywarcollege.edu).

Koszty leczenia ambulatoryjnego za granicą, (http://warta-ubezpieczenia.pl/wp-content/uploads/2016/08/Koszty-leczenia-ambulatoryjnego-za-granic%C4%85_lato.pdf), dostęp: 31.03.2018r.

Kowalewski E., *Ubezpieczenia turystyczne*, Wyższa Szkoła Bankowa w Toruniu, (http://www.wsb.pl/sites/wsb.pl.torun/files/biblioteka/10.pdf), dostęp: 24.03.2018 r.

Krajobraz bezpieczeństwa polskiego internetu, Raport roczny z działalności CERT Polska 2015, (https://www.cert.pl/PDF/Raport_CP_2015.pdf), dostęp: 13.03.2018 r.

Law Reform (Contributory Negligence) Act, 1945 Chapter 28 8 and 9 Geo 6, (https://www.legislation.gov.uk/ukpga/Geo6/8-9/28), dostęp: 3.04.2018 r.

Light Detection and Ranging (LIDAR), National Geodetic Survey, (https://www.ngs.noaa.gov/RESEARCH/RSD/main/lidar/lidar.shtml), dostęp: 7.03.2018.

Litman T., *Autonomous Vehicle Implementation Predictions. Implications for Transport Planning*, Victoria Transport Policy Institute 2018 (https://www.vtpi.org/avip.pdf), dostęp: 20.03.2018.

Managing digital risk. Trends, issues and implications for business, Lloyd's 360° Risk Insight, Lloyd's 2010, (https://www.lloyds.com/~/media/lloyds/reports/360/360-digital/lloyds_360_digital_risk_report-(2).pdf), dostęp: 22.03.2018 r.

Mason J., *Cyber Security Statistics,* Honest, In-Depth & Transparent VPN Reviews from Real Users, (www.thebestvpn.com).

Mukhopadhyay A., Saha D., Chakrabarti B.B., Mahanti A., Podder A., *Insurance for Cyber-risk: A Utility Model*, Indian Institute of Management Calcutta, 2005, Vol. 32, No. 1, (https://www.researchgate.net/profile/Arunabha_Mukhopadhyay/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model/links/00b7d518016c99e908000000.pdf), dostęp: 20.03.2018 r.

Nie zastosujesz się do RODO, czekają cię kary Prenumerata elektroniczna Dziennika Gazety Prawnej, (http://prawo.gazetaprawna.pl/artykuly/1098885,nadchodzi-rodo-jakie-kary-za-niedostosowanie-sie-do-przepisow.html), dostęp: 22.03.2018 r.

ODI resume of investigation PE 16-007, Office of Defects Investigation, (https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF), dostęp: 20.03.2018.

Olsen T., *Cyber Risk*, Willis, 2013, (https://www.pwc.dk).

Payment Practices Barometer Poland 2017, Atradius 2017, (https://atradius.pl/reports/payment-practices-barometer-poland-2017.html) dostęp:21.04.2018 r.

Payment Study 2017, CRIBIS D&B 2017 (https://www.dnb.ru/media/entry/54/Payment_Study_2017_Light.pdf) dostęp:31.03.2018 r.

Pillath S., *Automated vehicles in the EU*, European Parliamentary Research Service 2016, (http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573902/EPRS_BRI(2016)573902_EN.pdf), dostęp: 7.03.2018

Preliminary Statement of Policy Concerning Automated Vehicles, National Highway Traffic Safety Administration 2013, (https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf), dostęp: 7.03.2018.

Problemy sektora MSP i Budownictwa, Euler Hermes (http://www.eulerhermes.pl/euler-hermes-w-polsce/centrum-prasowe/wiadomosci/Pages/170823_Problemy-sektora-MSP-i-budownictwa.aspx) dostęp: 04.04.2018 r.

PZU Wojażer, (https://moje.pzu.pl/pzu/travel?mcid=p_pzu_pl&_ga=2.82721490.559090199.1522682237-606227484.1522682237), dostęp: 02.04.2018r.

Raciborski J., *System zabezpieczeń finansowych na rzecz klientów, organizatorów imprez turystycznych i pośredników*, Ministerstwo Gospodarki i pracy, (www.sot.org.pl/web_documents/publikacja_13.pdf), dostęp: 25.03.2018 r.

RODO - nowe obowiązki dla firm i dodatkowe prawa dla osób fizycznych, Fundacja rozwoju e-commerce, (https://fundacja-ecommerce.pl/rodo-nowe-obowiazki-dla-firm-dodatkowe-prawa-dla-osob-fizycznych/?gclid=EAIaIQobChMIw7ry7Mzk2QIVll4YCh03LQAXEAMYAiAAEgKwcvD_BwE), dostęp: 22.03.2018 r.

Ryzyko ubezpieczeniowe, (http://www.gu.com.pl/index.php?option=com_content&view=article&id=8913&catid=129:rynek-ubezpieczeniowy&Itemid=151) dostęp: 01.05.2018r.

Sekida M., *Turystyka ekstremalna vs. sporty ekstremalne*, (ojs.ukw.edu.pl/index.php/johs/article/download/4112/pdf) , dostęp: 24.03.2018 r.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, Ministerstwo Cyfryzacji, Warszawa 2017, (www.gov.pl).

Table RAS50002: Contributory factors allocated to vehicles or pedestrians in reported accidents, Great Britain, 2012-2016 (https://www.gov.uk/government/statistical-data-sets/ras50-contributory-factors#table-ras50002), dostęp: 7.03.2018.

Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, Society of Automotive Engineers 2014, (https://www.sae.org/standards/content/j3016_201401), dostęp: 7.03.2018.

Top Scoring Data Breaches, (www.breachlevelindex.com)

Turcja traci turystów przez politykę, (http://wyborcza.pl/7,75399,22009657,turcja-traci-turystow-przez-polityke-w-ciagu-dwoch-lat-ich.html), dostęp: 01.05.2018r.

Turystyczny Fundusz Gwarancyjny, (https://www.ufg.pl/infoportal/faces/pages_home-page/Page_3dc12681_156b6b90c42__7ff6/Page_3dc12681_156b6b90c42__7ff5/Page_3dc12681

_156b6b90c42__7ff2?_afrLoop=9143258310815940&_afrWindowMode=0&_adf.ctrl-state=k968gqp1s_38), dostęp: 28.04.2018 r.

Ubezpieczenie Cyber, Leadenhall Polska S.A., (www.leadenhall.pl).

Ubezpieczenie Cyber Edge, AIG Europe Limited Oddział w Polsce, (www.aig.pl).

Ubezpieczenia cybernetyczne, Ergo Hestia S.A.,(www.ergohestia.pl).

Ubezpieczenie technologii cyfrowych i ochrony danych (Cyber Protect), Allianz SE, (www.allianz.pl).

Ubezpieczenia turystyczne, (https://www.rf.gov.pl/vademecum-klienta/abc-ubezpieczen/Ubezpieczenia_turystyczne__20070#klz), dostęp: 02.05.2018 r.

Ubezpieczenie w zakresie ryzyk cybernetycznych (Cyber), Chubb European Group Limited Sp. z o.o., (www.chubb.com).

Understanding Systemic Cyber Risk, Global Agenda Council on Risk & Resilience, October 2016, World Economic Forum, (http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf), dostęp: 22.03.2018 r.

W 2017 roku ogłoszono niewypłacalność 900 firm w Polsce, (https://www.windykacja.pl/raporty,w-2017-roku-ogloszono-niewyplacalnosc-900-firm-w-polsce.html) dostęp:02.04.2018 r.

W *III kwartale 2017 roku najwyższa liczba niewypłacalności od 5 lat,*(https://www.windykacja.pl/raporty,w-iii-kwartale-2017-roku-najwyzsza-liczba-niewyplacalnosci-od-5-lat.html), dostęp: 04.04. 2018 r.

Wypadki drogowe w Polsce w 2012 roku, Komenda Główna Policji, Warszawa 2013, (http://statystyka.policja.pl/download/20/137021/Raport2012int.pdf), dostęp: 7.03.2018.

Wypadki drogowe w Polsce w 2013 roku, Komenda Główna Policji, Warszawa 2014, (http://statystyka.policja.pl/download/20/137223/WYPADKIDROGOWE2013.pdf), dostęp: 7.03.2018.

Wypadki drogowe w Polsce w 2014 roku, Komenda Główna Policji, Warszawa 2015, (http://statystyka.policja.pl/download/20/167907/raportrocznyruchdrogowy2014r.pdf), dostęp: 7.03.2018.

Wypadki drogowe w Polsce w 2015 roku, Komenda Główna Policji, Warszawa 2016, (http://statystyka.policja.pl/download/20/192140/Wypadki2015.pdf), dostęp: 7.03.2018.

Wypadki drogowe w Polsce w 2016 roku, Komenda Główna Policji, Warszawa 2017, (http://statystyka.policja.pl/download/20/236480/Wypadki2016.pdf), dostęp: 7.03.2018.

Wypoczynek w państwach członkowskich UE/EFTA, (https://www.ekuz.nfz.gov.pl/faq/wypoczynek-w-panstwach-czlonkowskich-ue-efta), dostęp: 01.05.2018 r.

Yeomans G., *Autonomous Vehicles. Handing over control: opportunities and risks for insurance*, Lloyd's 2014, (https://www.lloyds.com/~/media/lloyds/reports/emerging-risk-reports/autonomous-vehicles-final.pdf), dostęp: 20.03.2018 .

Żuk J., Żuk M., *Zagrożenia w cyberprzestrzeni a bezpieczeństwo jednostki*, „Rozprawy Społeczne" 2016, Tom 10, nr 3, (http://rozprawy-spoleczne.pswbp.pl/pdf/rs_nr_3_2016_top_druk_art_09.pdf), dostęp: 7.03.2018 r.

Spis tabel

Spis rysunków

UNIWERSYTET
EKONOMICZNY
W KRAKOWIE

RISK
MANAGEMENT
KOŁO NAUKOWE UBEZPIECZEŃ

KATEDRA ZARZĄDZANIA RYZYKIEM I UBEZPIECZEŃ

KU.UEK.KRAKOW.PL