Zeszyty Naukowe
Wydziału Zarządzania GWSH
Nr 20/2023, s. 23 - 32
DOI: 10.53259/2023.20.02

ISSN 2451-4535

Aleksandra Ferens
Uniwersytet Ekonomiczny w Katowicach,
Katowice, Polska
e-mail: aleksandra.ferens@ue.katowice.pl

UJAWNIENIE SZCZEGÓLNYCH OBSZARÓW RYZYKA W WYBRANYCH SPRAWOZDANIACH W DOBIE KRYZYSU

DISCLOSURE OF SPECIFIC RISK AREAS IN SELECTED REPORTS DURING CRISIS

Słowa kluczowe: pandemia Covid, wojna na Ukrainie, cyberbezpieczeństwo, zarządzanie ryzykiem
Keywords: *COVID-19 pandemic, war in Ukraine, cybersecurity, risk management*

Streszczenie

Celem artykułu jest identyfikacja szczególnych obszarów ryzyka wynikających z istniejącego kryzysu, ocena zakresu ich ujawnień w raportach zintegrowanych i innych sprawozdaniach wybranych spółek notowanych na GPW w Warszawie.
Metodyka: Przedmiotem badania są sprawozdania zintegrowane oraz sprawozdania zarządu wybranych spółek należących do branży paliwowej. W badaniach wykorzystano metodę analizy literatury, regulacji prawnych, dedukcji, analizę struktury i zakresu raportowanych informacji o ryzyku.
Wyniki przeprowadzonej analizy pokazały, że ujawnienia szczególnych obszarów ryzyka w analizowanych przedsiębiorstwach są stosunkowo niewielkie, informacje te są rozproszone w różnych częściach sprawozdań, a także nieporównywalne ze względu na brak jednolitej struktury danych.

Abstract

The aim of the article *is to identify specific risk areas resulting from the current crisis, assess the scope of these disclosures in integrated reports and other reports of selected companies listed on the Warsaw Stock Exchange.*
Methodology*: The subject of the study are integrated reports and management reports of selected companies belong to the fuel industry. The research used the method of literature analysis, legal regulations, deduction, analysis of the structure and scope of the reported risk information.*
The results *of the analysis showed that the disclosures about risk in the analysed companies are relatively small, the information is scattered in different parts of the reports, and also incomparable due to the lack of a uniform data structure.*

WPROWADZENIE

Trudna sytuacja związana z pandemią wirusa COVID – 19 i konfliktem zbrojnym na Ukrainie spowodowała istotne zmiany w globalnej gospodarce. Wiele przedsiębiorstw doświadczyło z tego powodu spadku przychodów, pogorszenia płynności, rentowności oraz drastycznego ograniczenia działalności. Efekty pandemii i trwające działania na Ukrainie to sytuacja nadzwyczajna, której konsekwencje są przewidywalne tylko w niewielkiej części, wymuszają na menadżerach ciągłego monitorowania zachodzących zmian oraz dużej elastyczności działania i umiejętności szybkiej reakcji na pojawiające się sygnały z otoczenia. Organizacje funkcjonują pod presją konieczności wykazania, że zarządzają

ryzykiem, a więc dysponują skutecznymi procesami i metodami identyfikacji obszarów ryzyka, jego pomiaru, oceny, reagowania na nie, ciągłego sterowania łącznie z odpowiednią sprawozdawczością.

Wśród szczególnych obszarów ryzyka związanego m.in. z dużym zakresem interaktywnych informacji przetwarzanych i wymienianych obecnie w cyberprzestrzeni jest cyberbezpieczeństwo. Zagadnienie to jest priorytetem dla najwyższych szczebli organizacji rządowych, a także członków zarządów firm, którzy upatrują w niedostępności infrastruktury informatyczno-sieciowej oraz narażeniu na ataki cybernetyczne duże zagrożenie. W tym kontekście firmy podejmują liczne inicjatywy w celu ochrony danych, ochrony krytycznych procesów biznesowych, dostępności i integralności informacji i systemów informatycznych.

Oznacza to, że obecnie coraz większą rolę w systemie informacyjnym rachunkowości odgrywa raportowanie na temat nowych obszarów związanych z ryzykiem w celu udostępnienia interesariuszom zewnętrznym informacji o efektach i metodach jego zarządzania, a interesariuszom wewnętrznym informacji niezbędnych do podejmowania decyzji zorientowanych na sterowanie ryzykiem. Narzędziem do komunikowania podejścia do zarządzania ryzykiem przedsiębiorstwa jest przede wszystkim raport zintegrowany oraz sprawozdanie zarządu. Jednym z podstawowych celów raportu zintegrowanego jest bowiem przedstawienie pełnego obrazu firmy, uwzględniającego powiązania oraz współzależność wszystkich czynników ryzyka istotnych dla spółki i jej zdolności do kreowania wartości. Opis ryzyka i zagrożeń jest jednym z wymaganych elementów składowych raportu zintegrowanego [Raulinajtys-Grzybek i in., 2018]. Sprawozdanie zarządu powinno natomiast przedstawiać istotne informacje o stanie majątkowym i finansowym, w tym ocenę uzyskiwanych efektów oraz wskazanie czynników ryzyka i opis zagrożeń [UoR, art. 49, ust.2].

Celem artykułu jest próba identyfikacji nowych obszarów ryzyka wynikających z pandemii COVID – 19, konfliktu na Ukrainie oraz cyberbezpieczeństwa, ocena zakresu tych ujawnień w raportach zintegrowanych i sprawozdaniach zarządu spółek branży paliwowej notowanych na GPW w Warszawie za lata 2020 i 2021. Spółki te dobrano celowo, gdyż należą do branży wskazanej jako operatora usług kluczowych zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa [Dz. U. 2020, poz.1369].

Artykuł koncentruje się na porównaniu zakresu narracyjnych ujawnień obszarów i czynników ryzyka, uzupełnia dorobek naukowy z zakresu raportowania niefinansowego. W badaniach wykorzystano metodę analizy: literatury, struktury i zakresu raportowanych przez badane spółki informacji o ryzyku wynikającym z pandemii COVID, wojny na Ukrainie z uwzględnieniem cyberbezpieczeństwa i cyberryzyka.

SPRAWOZDAWCZOŚĆ BIZNESOWA JAKO ŹRÓDŁO INFORMACJI NA POTRZEBY OCENY RYZYKA PRZEDSIĘBIORSTWA W WARUNKACH KRYZYSU

W literaturze z zakresu ekonomii, finansów i rachunkowości ryzyko jest różnie definiowane [Iwaszczuk, 2021, Bochenek, 2012, Klimczak, 2008, Jajuga, 1998]. Szerokiego przeglądu pojęcia ryzyka: jego etymologii, filozoficznego, neoklasycznego znaczenia, nurtu definiowania ryzyka umiejscowionego w teorii podejmowania decyzji, nurtu ofensywnego i defensywnego dokonała A. Karmańska [2018]. Na podstawie przedstawionych kontekstów i podejść w.w. autorów do definiowania ryzyka w rachunkowości, a także w świetle występującego obecnie kryzysu, w artykule przyjmuje się, że ryzyko jest kategorią obiektywną występującą zawsze niezależnie od stopnia ludzkiej świadomości, uświadomione, staje się kluczowym kryterium decyzyjnym w każdym obszarze funkcjonowania człowieka i jednostki gospodarczej, zmierzone – poddaje się zarządzaniu [por. Karmańska, Łada, 2019]. Współczesna nauka i wydarzenia takie jak pojawienie się Covid i wybuch wojny pozbawiły nas złudzeń, co do istnienia w świecie stałych i niezmiennych reguł. Ryzyko jest wkomponowane w dynamiczny, ewolucyjny model świata i dlatego jest czymś obiektywnym. Ryzyko związane jest nie tylko z realizacją określonych zamierzeń, ale dotyczy także chęci zachowania istniejącego stanu rzeczy, czyli z niepodjęciem lub zaniechaniem określonych działań. Każde przedsiębiorstwo działające na rynku musi zdać sobie sprawę, iż dzisiejsza, bieżąca decyzja może nie przynieść oczekiwanych rezultatów w przyszłości [por. Marcinek, 2001, Tarczyński, Mojsiewicz, 2001]. Ryzyko to zatem skumulowany efekt prawdopodobieństwa niepewnych zdarzeń, które mogą korzystnie lub niekorzystnie wpływać na realizację projektu czy funkcjonowanie przedsię-

biorstwa jako całości, a jego zidentyfikowanie i oszacowanie jest procesem wieloetapowym i złożonym. Inaczej jest z niepewnością, która odnosi się do zdarzenia lub zmian trudnych do oszacowania, a prawdopodobieństwo jest całkowicie nieznane [Pritchanel, 2002, Janasz i in. 2007].

Proces zarządzania ryzykiem przedsiębiorstwa dzieli się na cztery fazy [Poniatowska i in., 2022]. Pierwszą jest identyfikacja ryzyka, której celem jest rozpoznanie źródeł pochodzenia ryzyka oraz określenie jego podstawowych czynników [Nita, 2013, s.141]. Za drugą fazę uważa się analizę i ocenę ryzyka, polegającą na oszacowaniu ryzyka i ustaleniu poziomu wpływu poszczególnych ryzyk na przedsiębiorstwo. Kolejną fazą jest reakcja na ryzyko, czyli wybór i opracowanie metod przeciwdziałania ryzyku [Tworek, Cziura, 2017]. Skuteczne zarządzanie ryzykiem powinno także obejmować systematyczne monitorowanie ryzyka, co wymaga dokonywania ciągłych obserwacji faktów, zdarzeń, źródeł ryzyka występujących w przedsiębiorstwie oraz jego otoczeniu [por. Nowak, 2013]. Z punktu widzenia jednostki gospodarczej ryzykiem jest obarczone angażowanie w działalność wszystkich zasobów: rzeczowych, finansowych, ludzkich i kapitałów, dlatego za ważne narzędzie zarządzania ryzykiem uważa się rachunkowość, w ramach której dokonuje się pomiaru ich wartości [por. Nowak, 2013]. Współczesna rachunkowość jest ukierunkowana nie tylko na retrospektywny pomiar dokonań i ich raportowanie, ale także na pomiar prospektywny, dotyczący przewidywanych rezultatów działalności. Oznacza to, że w ramach systemu informacyjnego rachunkowości możliwa jest ocena poziomu ryzyka towarzyszącego działalności jednostek gospodarczych oraz ustalenie istotności wpływu ryzyka na przyszłe rezultaty. Ponadto, rachunkowość dysponuje odpowiednimi instrumentami, które w pewnych sytuacjach są skutecznymi sposobami zabezpieczenia przed ryzykiem [por. Nowak, 2013].

Szczególną rolę w prezentowaniu obszarów ryzyka i metodach jego zarządzania dla różnych grup interesariuszy ma sprawozdawczość, nie można bowiem zarządzać ryzykiem bez informacji [Kaczmarek, 2008]. Informacja z tego zakresu pełni obecnie rolę wspierającą inicjatywy w zakresie realizowanych działań z zakresu zarządzania ryzykiem mające na celu także złagodzenie skutków pandemii Covid – 19 i wojny na Ukrainie.

W 2021 roku Komitet Standardów Rachunkowości opracował projekt nowego standardu „Kontynuacja działalności oraz rachunkowość jednostek przy braku kontynuowania działalności". Największą uwagę zwrócono w nim na właściwą ocenę zdolności do kontynuacji działalności oraz wycenę majątku w warunkach kryzysu spowodowanego pandemią koronawirusa. Jako przesłankę wskazującą na znaczącą niepewność co do zdolności jednostki do kontynuacji działalności przyjęto m.in. niezdolność kierownika do zarządzania znaczącym ryzykiem biznesowym lub radzenia sobie ze zwiększoną odpowiedzialnością (art. 4.8). W standardzie tym postuluje się, aby wnioski z przedstawionych analiz dotyczących kontynuacji działania publikować we wprowadzeniu do sprawozdania finansowego. Brak jest natomiast jednoznacznego stanowiska prezentującego, gdzie i w jakim zakresie należy umieścić w sprawozdaniu jednostki zagadnienie dotyczące zarządzania ryzykiem w warunkach kryzysu spowodowanego pandemią.

W kwietniu 2022 Komitet Standardów Rachunkowości opracował rekomendacje dotyczące sporządzenia sprawozdania finansowego i sprawozdania z działalności w warunkach rosyjskiej agresji na Ukrainę. Według Komitetu, okoliczności związane z rosyjską agresją powinny zostać w odpowiedni sposób uwzględnione w sprawozdaniu finansowym, skonsolidowanym sprawozdaniu finansowym oraz w sprawozdaniu z działalności. Jako szczególne aspekty związane z ryzykiem rosyjskiej agresji Komitet Standardów przyjął:

1. potrzebę oceny możliwości przyjęcia przez jednostkę założenia kontynuacji działalności w zakresie m.in. identyfikacji ryzyka mogącego mieć charakter finansowy, operacyjny lub pozostały,
2. występowanie przesłanek na utratę wartości w odniesieniu do ryzyka utraty oraz zniszczenia rzeczowych aktywów trwałych, wartości niematerialnych i prawnych, zapasów, ryzyka utraty środków pieniężnych i ich ekwiwalentów, materializację ryzyka kursowego,
3. brak wiarygodności uznania wszelkich wartości szacunkowych.

Postuluje się, aby możliwe skutki agresji przedstawić w sposób przejrzysty i umożliwiający użytkownikom całościowy osąd, co do sytuacji jednostki, jej rozwoju, ryzyk i niepewności w tym zakresie. Informacje te zaleca się prezentować w sprawozdaniu z działalności (SzD). W szczególności w sprawozdaniu tym rozważyć należy przedstawienie rosyjskiej agresji na Ukrainę zarówno, jako istotnego

czynnika ryzyka, jak i czynnik determinujący kształtowanie się wyniku finansowego, a także płynności finansowej jednostki w przyszłości. W SzD należy przedstawić w sposób obiektywny i wyważony możliwe negatywne konsekwencje, tj. ryzyko związane z dalszym przebiegiem konfliktu na Ukrainie i opis jego możliwych skutków pod kątem wpływu na przewidywaną przyszłą sytuację finansową, majątkową i płynność jednostki oraz jej przewidywany rozwój, w tym także realizację celów i działań strategicznych oraz działalność operacyjną (Rekomendacje Komitetu Standardów Rachunkowości).

RAPORT ZINTEGROWANY JAKO SZCZEGÓLNE MIEJSCE PREZENTOWANIA INFORMACJI Z ZAKRESU ZARZĄDZANIA RYZYKIEM

W raportowaniu aspektów związanych z zarządzaniem ryzykiem duże znaczenie oprócz sprawozdania zarządu, ma raport zintegrowany. Jego rolą jest bowiem wyraźne i zwięzłe komunikowanie o tym, w jaki sposób strategia organizacji, przyjęty system zarządzania, wyniki działalności i perspektywy – wraz z czynnikami zewnętrznymi środowiska – prowadzą do tworzenia wartości organizacji w perspektywie krótko -, średnio – i długoterminowej. Zagrożenia mogą wynikać zarówno z czynników wewnętrznych, jak i zewnętrznych dla organizacji [IIRC, 2013]. Zgodnie z dobrymi praktykami raportowania zintegrowanego (Dobre Praktyki) raport powinien przedstawiać wszystkie kluczowe ryzyka specyficzne dla organizacji, całościowy opis podejścia do zarządzania ryzykiem w tym: podejście do identyfikacji ryzyka, zasady zarządzania ryzykiem i nadzór nad tym procesem. W procesie identyfikacji ryzyka należy uwzględnić: zewnętrzne i wewnętrzne źródła zagrożeń, ocenę ryzyk ze względu na prawdopodobieństwo ich wystąpienia oraz potencjalny wpływ materializacji danego ryzyka na działalność organizacji oraz zarządzanie ryzykiem [IIRC, 2013].

Informacje o zarządzaniu ryzykiem w tym raporcie powinny być sformułowane pod względem wpływu na przyszłe tworzenie wartości, które prezentuje zarówno aspekty ekonomiczne, społeczne i środowiskowe [Stubbs, Higgins, 2014]. Raport ten spełnia także warunki użytecznego dla interesariuszy raportu biznesowego, gdyż prezentuje zarówno informacje finansowe jak i niefinansowe [Kannenberg, Schreck, 2019]. Zgodnie z zaproponowaną przez IIRC ogólną strukturą raportu zintegrowanego, ma on składać się z ośmiu elementów, związanych ze sobą i niewykluczających się wzajemnie [IIRC, 2013], które obejmują: informacje ogólne o organizacji i otoczeniu zewnętrznym, ład korporacyjny, model biznesu, szanse i zagrożenia, strategię i alokację zasobów, dokonania, perspektywy, podstawy sporządzenia i prezentacji.

Obecnie nie ma wytycznych, które wskazywałyby raport zintegrowany jako istotny raport biznesowy prezentujący skutki pandemii Covid i konfliktu zbrojnego na Ukrainie. Biorąc pod uwagę jego strukturę ramową i rolę jaką pełni, autorka rekomenduje, aby uwzględnić w nim wybrane zagadnienia, a także odpowiedzi na pytania związane z zarządzaniem ryzykiem. Przykłady takich zagadnień oraz zestaw pytań przedstawia tabela 1.

Tabela 1. Elementy raportu zintegrowanego

Table 1. Integrated report elements

Elementy raportu zintegrowanego	Zagadnienia (wybrane)
Informacje ogólne o organizacji i otoczeniu zewnętrznym	Co organizacja robi, czym się zajmuje i w jakich warunkach funkcjonuje? W jakim stopniu pandemia i wojna wpływają na bieżącą działalność spółki i kształtowanie wartości przez przedsiębiorstwo w krótkim, średnim i długim okresie?
Ład korporacyjny	Jakie procesy są realizowane do podejmowania strategicznych decyzji w tym do przeciwdziałania skutkom pandemii COVID i konfliktowi zbrojnemu? Jakie szczególne działania podejmują osoby sprawujące nadzór w celu monitorowania strategicznego kierunku organizacji i podejścia do zarządzania ryzykiem?
Model biznesu	Jaki jest model biznesowy organizacji? Czy uwzględnia aspekty obecnego kryzysu wywołanego COVID i wojną w kluczowych jego elementach?

Szanse i zagrożenia	Jakie są zagrożenia (ryzyko) oraz szanse (o charakterze zewnętrznym i wewnętrznym), mające wpływ na zdolność organizacji do tworzenia wartości? Jak jednostka radzi sobie z tymi zagrożeniami? Jakie konsekwencje niosą za sobą Covid 19 i wojna na Ukrainie? Jakie działania podejmuje przedsiębiorstwo mające na celu złagodzenie zagrożeń i wykorzystanie szans?
Strategia i alokacja zasobów	Jakie są kierunki rozwoju organizacji? Jaki organizacja ma sposób na osiągnięcie wyznaczonego celu? Czy uwzględnia aspekty covidu i wojny? W jaki sposób strategia odpowiada na zidentyfikowane ryzyka i szanse? W jaki sposób strategia uwzględnia uwarunkowania zewnętrzne i zmiany w otoczeniu? W jaki sposób podejście do zarządzania wspiera zarządzanie zidentyfikowanym ryzykiem?
Dokonania	W jakim stopniu organizacja osiąga swoje cele strategiczne i jakie są ich wpływy na kapitały jednostki? Jaki jest związek pomiędzy przeszłymi i obecnymi wynikami, jak również między wynikami obecnymi i przyszłymi uwarunkowaniami związanymi z kryzysem?
Perspektywy	Jakie wyzwania i niepewności może napotkać organizacja w realizacji strategii uwzględniając skutki pandemii i wojny? Jakie są potencjalne skutki kryzysu dla modelu biznesowego i przyszłych wyników?
Podstawa sporządzenia i prezentacji	W jaki sposób organizacja określa, jakie kwestie należy uwzględnić w zintegrowanym raporcie i jak mierzy i ocenia kwestie skutków Covid i wojny na Ukrainie?

Źródło/Source: opracowanie własne na podstawie/own elaboration based on: IIRC (2013)

Uważa się, że sposób zarządzania ryzykiem może być opisany w różnych częściach raportu zintegrowanego, zidentyfikowane czynniki ryzyka mogą bowiem pojawić się we wszystkich aspektach towarzyszących działalności gospodarczej. Zagadnienia dotyczące ryzyka spowodowanego pandemią i wojną mogą być wpisane we wszystkie elementy raportu zintegrowanego lub tylko w wybrane, ważnym jest, aby zarządy spółek były skłonne do podejmowania działań w warunkach istniejącego kryzysu. Należy mieć także na uwadze, że skłonność zarządów do informowania interesariuszy zewnętrznych o obszarach i czynnikach ryzyka będzie się różnił w zależności od przyjętej polityki zarządzania ryzykiem. Na zakres prezentowanej informacji wpływ mają także czynniki behawioralne i prawdziwą może okazać się hipoteza postawiona przez A. Karmańską [Karmańska, Łada, 2019], że im większa skłonność zarządów do działania w warunkach niepewności i ryzyka, tym mniejsza skłonność do ujawnienia obszarów i czynników ryzyka lub przy wyższej odporności psychicznej na uświadomione czynniki ryzyka i – w konsekwencji – akceptacji wyższych poziomów ryzyka.

CYBERBEZPIECZEŃSTWO W SPRAWOZDAWCZOŚCI PRZEDSIĘBIORSTW

Pandemia Covid - 19 spowodowała, że w cyberprzestrzeni ilość pozyskiwanej, generowanej i udostępnianej informacji zdecydowanie wzrosła. Zjawisko to spowodowało, że liczba i dotkliwość cyberzagrożeń była w ostatnich latach bezprecedensowa, a koszty cyberataków dla zarządów firm i pozostałych interesariuszy zewnętrznych i wewnętrznych ogromne. Skutki wyrządzone w cyberprzestrzeni przez nieuprawnionych użytkowników, szczególnie w jednostkach uznanych za operatorów usług kluczowych[1], prowadzą do groźnych w skutkach konsekwencji społecznych i ekonomicznych. Firmy podejmują więc liczne inicjatywy w celu ochrony danych, krytycznych procesów biznesowych oraz dostępności i integralności systemów informatycznych. Stale ewoluujące cyberzagrożenia związane m.in. z konfliktem zbrojnym na Ukrainie i przyśpieszona w ostatnim czasie cyfryzacja to kluczowe czynniki powodujące potrzebę wypracowania odpowiednich narzędzi mających na celu zwiększenie

[1] Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do ustawy

zdolności organizacji w zakresie zarządzania ryzykiem cyberbezpieczeństwa[2] [Haapamäki, Sihvonen, 2019]. Uważa się, że konieczne jest wpisanie cyberbezpieczeństwa w całościowy łańcuch wartości firmy tj. zarówno w procesy operacyjne jak i wspomagające, czyli we wszystkich poziomach modelu biznesowego firmy.

Propozycja ram modelu zarządzania bezpieczeństwem systemu informacyjnego organizacji obejmuje 3 główne procesy: proces planowania, proces wdrażania (ustalenie założeń i metod nowego modelu) oraz proces prewencji - stosowanie środków zapobiegających i ograniczających wpływ incydentów. Wśród działań składających się na proces prewencji wyróżnia się m.in. raportowanie z tego zakresu [Ferens, 2021]. W Polsce istotnym aktem prawnym regulującym aspekty cyberbezpieczeństwa jest ustawa o krajowym systemie cyberbezpieczeństwa. Nowe wytyczne wprowadziły obowiązek szacowania ryzyka cyberbezpieczeństwa przez operatorów usług kluczowych, ale nie ma w nich informacji o konieczności raportowania informacji z tego zakresu. Także ustawa o rachunkowości nie wskazuje wprost konieczności ujęcia tych informacji, zważając jednak na rolę raportowania zintegrowanego i zakresu informacji koniecznych i zalecanych do prezentowania w tym raporcie, uważa się za konieczne uwzględnienie w sprawozdawczości zintegrowanej m.in. informacji o zagrożeniach i szansach związanych z cyberbezpieczeństwem.

SZCZEGÓLNE GRUPY RYZYKA W RAPORTACH ZINTEGROWANYCH SPÓŁEK ENERGETYCZNYCH

W celu zidentyfikowania ujawnień na temat ryzyka związanego ze skutkami pandemii COVID-19, agresji na Ukrainę oraz cyberbezpieczeństwa autorka przeanalizowała treść wybranych raportów biznesowych - zintegrowanych (RI) i sprawozdania zarządu (SZ) publikowanych przez spółki branży paliwowej notowane na GPW w ramach indeksu WIG -Paliwa za rok 2020, 2021. Wybór tego sektora podyktowany był faktem, że branża ta należy obecnie do tzw. operatorów usług kluczowych, które po spełnieniu określonych warunków obejmują przepisy Ustawy o KSC (ustawa o krajowym, 2018). Spółki należące do tego indeksu to sześć spółek, w tym cztery spółki polskie (Grupa Lotos, Grupa PGNiG, Grupa Orlen, Grupa Unimot), jedna węgierska (Grupa MOL) oraz jedna rumuńsko-tunezyjska (Grupa Serinus Energy). Badaniem zostały objęte spółki polskie. Zidentyfikowane przykładowe obszary ujawnień na temat ryzyk związanych z pandemią COVID, agresją na Ukrainę oraz cyberbezpieczeństwem w wybranych spółkach prezentuje tabela 2, 3 i 4.

Tabela 2. Segmenty sprawozdania dotyczące ryzyka związanego z Pandemią COVID w przedsiębiorstwach branży paliwowej w latach 2020-2021.

Table 2. Reporting segments on the risks associated with the COVID pandemic in companies in the fuel industry in 2020-2021.

Przedsiębiorstwo	Kategoria ujawnień o COVID - 19	Miejsce ujawnień
Lotos 2020	Optymalizacja przerobu ropy w warunkach pandemii Otoczenie zewnętrzne grupy - wpływ pandemii na światowy rynek paliw Strategia grupy Aktywne zarządzanie szansami i ryzykami CSR	SZ

[2] Definicją wyznaczającą zakres cyberbezpieczeństwa oraz jej połączenie z cyberprzestrzenią prezentują Yang, Lau, Gan [2019]. Cyberbezpieczeństwo to ochrona cyberprzestrzeni, tzn. informacji elektronicznych, technologii informacyjno-komunikacyjnych oraz użytkowników cyberprzestrzeni w zakresie ich osobistych, społecznych i krajowych możliwości, w tym ich interesów, materialnych lub niematerialnych, którzy są podatni na ataki z cyberprzestrzeni.

Lotos 2021	Bezpieczeństwo i higiena pracy Wpływ pandemii na światowy rynek paliw, podaż ropy naftowej Otoczenie regulacyjne Przewidywane kształtowanie się czynników zewnętrznych w 2022 roku Stan realizacji strategii Efektywnie wykorzystane aktywa w całym łańcuchu wartości Aktywne zarządzanie szansami i ryzykami CSR	SZ
PGNIG 2020	Strategia grupy Otoczenie konkurencyjne Opis wyników zaangażowania kapitałowego Sytuacja finansowa Grupy	SZ
PGNIG 2021	Działalność operacyjna Ryzyka aspektów pracowniczych	SZ, RI
Orlen 2020	Strategia działania – realizacja celów Procesy kadrowe CSR Trendy rynkowe, sprzedaż Rynki zbytu i udziały rynkowe Czynniki wpływające na zmianę EBITDA Perspektywy rozwoju działalności	RI
Orlen 2021	Otoczenie regulacyjne Czynniki wpływające na zmianę EBITDA Wyniki segmentowe Grupy Funkcje korporacyjne Działalność operacyjna	RI
Unimot 2020	Szacunek wpływu pandemii na działalność i sytuację finansową Główne czynniki i zdarzenia wpływające na działalność grupy kapitałowej Kierunki rozwoju grupy kapitałowe	SZ
Unimot 2021	Szacunek wpływu pandemii na działalność i sytuację finansową Otoczenie rynkowe Społeczna Odpowiedzialność Biznesu (CSR)	SZ

Źródło/Source: opracowanie własne na podstawie//own elaboration based on raportów Spółek

Tabela 3. Kategorie ujawnień dotyczących ryzyka wpływu wojny na Ukrainie.

Table 3. Report segments on the risk of the impact of the war in Ukraine.

Przedsiębiorstwo	**Kategoria ujawnień o COVID - 19**	**Miejsce ujawnień**
Lotos 2021	Otoczenie zewnętrzne grupy – wpływ wojny na grupę Ryzyko w działalności grupy	SZ
PGNIG 2021	Otoczenie – sytuacja na rynku w wyniku agresji Perspektywy rozwoju i wyzwania na przyszłość	SZ, RI
Orlen 2021	Trendy rynkowe Perspektywy rozwoju działalności	SZ
Unimot 2021	Wydarzenia po dniu bilansowym Główne czynniki wpływające na działalność grupy Charakterystyka wewnętrznych i zewnętrznych czynników istotnych dla rozwoju firmy Czynniki ryzyka i zagrożenia	SZ

Źródło/Source: opracowanie własne na podstawie//own elaboration based on raportów Spółek

Tabela 4. Ujawnienia dotyczące cyberryzyka i cyberbezpieczeństwa w przedsiębiorstwach branży paliwowej w latach 2020–2021.

Table 4. Disclosures regarding cybersecurity and cybersecurity in companies in the fuel industry in 2020–2021.

Przedsiębiorstwo	Kategoria ujawnień na temat cyberryzyka i cyberbezpieczeństwa	Miejsce ujawnień
Lotos 2020	Ryzyko systemów IT: Zewnętrzna lub wewnętrzna ingerencja (cyberatak) w systemy informatyczne (IT) i sterowania (OT) oraz awarie w wyniku braku wystarczających zasobów i nieefektywnych procesów w obszarze IT. Implementacja wymagań systemu ISO 27001 oraz ustawy o cyberbezpieczeństwie Podnoszenie świadomości pracowników w zakresie cyberbezpieczeństwa	SZ (Ryzyko bezpieczeństwa)
Lotos 2021	j.w.	j.w.
PGNIG 2020	brak	SZ; RI
PGNIG 2021	brak	SZ; RI
Orlen 2020	brak	RI; SZ
Orlen 2021	Zaktualizowano i wydano Zarządzenie w sprawie wprowadzenia „Polityki Bezpieczeństwa Teleinformatycznego w Koncernie", wyznaczając tym samym standardy w zakresie zarządzania cyberbezpieczeństwem Prowadzone jest ciągłe podnoszenie świadomości w zakresie zagrożeń, szczególnie teleinformatycznych oraz cyberzagrożeń. Cyberbezpieczeństwo systemów OT, IT, kontrola skuteczności działania cyberzabepieczeń	RI (Dokumentacja ZSZ) oraz Zarządzanie korporacyjne SZ (zarządzanie ryzykiem)
Unimot 2020	brak	SZ
Unimot 2021	brak	SZ

Źródło/Source: opracowanie własne/own elaboration

Informacje na temat skutków kryzysu spowodowanego Covid-19 oraz tych na jakie narażona jest obecnie spółka, sposobów ich monitorowania, reagowania na nie, należą do ważnych aspektów prezentowanych w sprawozdaniach zarządu i raportach zintegrowanych. Są akcentowane m.in. jako najważniejsze wydarzenia 2020 roku, powodujące istotne perturbacje na rynku paliw na świecie. Podkreśla się także ich wpływ na strategię grupy, poziom sprzedaży, kosztów, przepływy pieniężne, wskaźniki finansowe, realizowaną społeczną odpowiedzialność biznesu (CSR), realizowane inwestycje. Pandemia spowodowała także zdefiniowanie w 2020 nowego ryzyka związanego z potencjalnym ograniczeniem wydobycia. Ryzyka związane z Covid są prezentowane najczęściej w sekcji: zarządzanie ryzykiem, szanse i zagrożenia, strategia jednostki i działania z zakresu CSR. Ujawnienia dotyczące Covid – 19 i agresji na Ukrainę można znaleźć w różnych częściach sprawozdań, różnią się poziomem jakości, zakresem i sposobem ujęcia, spółki nie zastosowały zatem rekomendacji Komitetu Standardów Rachunkowości.

Wśród analizowanych spółek UNIMOT, PGNIG nie zamieściło informacji odnośnie cyberzagrożeń i cyberbezpieczeństwa. W sprawozdaniu zarządu w części dotyczącej przyjętych przez jednostkę celów i metod zarządzania ryzykiem spółka Lotos wyodrębniła kategorię cyberryzyka. Prezentowane przez spółkę informacje dotyczące cyberzagrożeń pozwalają ustalić zakres cyberryzyka. Spóła ta zwraca uwagę na aspekt ciągłego niedostatecznego dostosowania się do wymogów nowych przepisów prawa i podejmuje w tym celu konkretne działania. Spółka Lotos utworzyła m.in. Biuro Security Operation Center (SOC), które odpowiada za budowę centralnego systemu zgłaszania, monitorowania i koordynacji poważnych incydentów bezpieczeństwa, nadzoruje całokształt działań związanych z monitorowaniem, wykrywaniem oraz koordynacją i obsługą incydentów bezpieczeństwa informacji w Grupie, a także prowadzi szereg działań związanych z podnoszeniem świadomości pracowników w zakresie cyberbezpieczeństwa. Można zatem stwierdzić, że w.w. spółki nie podchodzą w sposób interaktywny do cyberryzyka, ponieważ w swoich planowanych działaniach uwzględniają tylko wybrane aspekty, a powinny uwzględnić zarówno część technologiczną, operacyjną, relacje z interesariuszami oraz wymianę informacji.

PODSUMOWANIE

Pandemia Covid – 19 oraz rosyjska agresja na Ukrainę wymusiła drastyczną zmianę zachowań w kwestiach społecznych, gospodarczych, prawnych, finansowych, a co za tym idzie zmianie uległa także sprawozdawczość podmiotów gospodarczych. Kluczową sprawą staje się zatem ocena sytuacji jednostki i jej otoczenia w warunkach niepewności i ryzyka. Jedną z podstawowych potrzeb informacyjnych interesariuszy zewnętrznych w dobie kryzysu jest możliwość oceny sposobu zarządzania ryzykiem, które pozwoli zabezpieczyć się przed jego skutkami. Przedsiębiorstwa powinny nieustannie modyfikować swoją dotychczasową strategię i prezentować ją w raportach biznesowych, co jest ściśle powiązane z zaufaniem do sposobu zarządzania bezpieczeństwem informacji i procesów oraz informowaniem o prowadzonych działaniach.

Przedstawione badania pokazały, że ujawnienia dotyczące zarządzania ryzykiem w odniesieniu do pandemii Covid, wojny na Ukrainie i cyberbezpieczeństwa w przedsiębiorstwach branży paliwowej są stosunkowo niewielkie, mimo, że sprawozdania zintegrowane i raporty zarządu są bardzo obszerne. Trudno zatem stwierdzić czy w przedsiębiorstwach tych funkcjonuje system zarządzania tymi ryzykami. Informacje te są rozproszone w różnych częściach tych sprawozdań, różnią się zakresem i formą prezentacji, taki stan powoduje, że informacje z tego zakresu nie mogą być porównywane ze względu na brak jednolitej struktury danych, co uniemożliwia dokonanie wieloaspektowej i wielosektorowej oceny podejmowanych działań przez badane jednostki raportujące.

Autorka proponuje uzupełnienie i ustrukturyzowanie dotychczas raportowanych informacji niefinansowych o informacje dotyczące zarządzania ryzykiem, a także rekomenduje zbudowanie „modelu biznesowego" przedsiębiorstwa, który obejmowałby aspekty zarządzania tymi ryzykami z uwzględnieniem zabezpieczeń przed cyber atakami. Zaleca się także uwzględnienie tych aspektów w modelu biznesowym firmy, a następnie raportowanie o nich. Propozycja, ta zapewni szereg korzyści w postaci podwyższenia transparentności koncepcji tworzenia wartości, zarówno dla klienta oraz dla właścicieli przedsiębiorstwa, osiągnięcie przewagi konkurencyjnej, wzmocnienie istniejących i budowanie nowych, trwałych relacji z interesariuszami.

BIBLIOGRAFIA

Bochenek M., 2012: *Ryzyko i niepewność w naukach ekonomicznych– rozważania semantyczne*, Ekonomia, (21), s. 46–63.

Carl L. Pritchanel., 2002: *Zarządzanie ryzykiem w projektach*, WIG-PRESS, Warszawa, s.7.

Ferens A., 2021: *Cyberbezpieczeństwo i cyberryzyko w raportach zintegrowanych i sprawozdaniach zarządu operatorów usług kluczowych*, Zeszyty Teoretyczne Rachunkowości, (45 (2), s. 31–50.

Haapamäki E., Sihvonen J., 2019: *Cybersecurity in accounting research* Managerial Auditing Journal, 34(7), s. 808–834.

IIRC (2013), https://integratedreporting.org/wp-content/uploads/2013/12/13–12–08-THE INTERNATIONAL-IR-FRAMEWORK-2–1.pdf [dostęp 25.09.2022].

Iwaszczuk N., 2021: *Ryzyko w działalności gospodarczej: definicje, klasyfikacje, zarządzanie*, IGSMiE PAN, Kraków.

Jajuga K., Jajuga T., 1998: *Inwestycje. Instrumenty finansowe. Ryzyko finansowe, Inżynieria finansowa*, PWN, Warszawa.

Janasz K., Janasz W., Wiśniewska J., 2007: *Zarządzanie kapitałem w przedsiębiorstwie*, Difin, Warszawa.

Kaczmarek T., 2008: *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa.

Kannenberg L., Schreck P., (2019): *Integrated reporting: boon or bane? A review of empirical research on its determinants and implications*, Journal of Business Economics, 89, s.515–567.

Karmańska A., Łada M., 2019: *Ujawnianie obszarów i czynników ryzyka w sprawozdaniach z działalności spółek giełdowych–obserwacje wobec zmian regulacji prawnych*, Zeszyty Teoretyczne Rachunkowości, 103 (159), s.42-43.

Karmańska A., red. 2008: *Ryzyko w rachunkowości*, Difin, Warszawa.

Klimczak K. M., 2008: *Dylematy ujęcia ryzyka w teorii ekonomii*, Acta Universitatis, Łódz.

Marcinek K., 2001: *Ryzyko projektów inwestycyjnych*. AE, Katowice, s.80.

Nita B., 2013: *Sprawozdawczość wewnętrzna w procesie zarządzania ryzykiem*. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, (287).

Nowak E., 2013, *Pomiar dokonań przedsiębiorstwa jako zadanie rachunkowości*. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, (289), s.430-436.

Poniatowska E., Regulanty K., Bagieńska A., 2022: *Sprawozdanie finansowe jako narzędzie pozyskania informacji o zarządzaniu ryzykiem w przedsiębiorstwie*, Akademia Zarządzania, 6(2), s.93.

Tworek P., Cziura P., 2017: *Wybrane problemy zarządzania ryzykiem w działalności przedsiębiorstw społecznych*, Zeszyty Naukowe Politechniki Częstochowskiej, Zarządzanie, 25(1), s. 101.

Raulinajtys-Grzybek M., Karwowski M., Świderska G. K., 2018: *Raport zintegrowany jako źródło informacji o podejściu przedsiębiorstwa do zarządzania ryzykiem*, Zeszyty Teoretyczne Rachunkowości, 98 (154), s. 203-224.

Rekomendacje Komitetu Standardów Rachunkowości, Sprawozdanie finansowe i sprawozdanie z działalności w warunkach rosyjskiej agresji na Ukrainę, Załącznik do Uchwały 6/2022 z 4 kwietnia 2022 r.

Stubbs W., Higgins C., 2014: *Integrated reporting and internal mechanisms of change*, Accounting, Auditing & Accountability Journal, 27 (7), s. 1068–1089

Tarczyński W., Mojsiewicz M., 2001: *Zarządzanie ryzykiem*, PWE, Warszawa, s.11.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2020, poz.1369.

Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2022 r., poz. 1488).

Yang L., Lau L., Gan H., 2020: *Investors' perceptions of the cybersecurity risk management reporting framework*, International Journal of Accounting & Information Management, 28 (1), s.167– 183.

https://www.gpw.pl/pub/GPW/pdf/Dobre_praktyki_raportowania_zintegrowanego.pdf