

Warszawa, 10 kwietnia 2026 r.

Prof. dr hab. Mariusz Próchniak
Katedra Ekonomii II
Kolegium Gospodarki Światowej
Szkola Główna Handlowa w Warszawie
mproch@sgh.waw.pl

Recenzja pracy doktorskiej pt.

„Wpływ incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw”

autorstwa mgr. Konrada Sałka

1. Ogólna charakterystyka pracy i jej ocena

Przedmiotem recenzji jest praca doktorska autorstwa mgr. Konrada Sałka pod tytułem: *Wpływ incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw*. Praca zawiera 130 stron oraz składa się z czterech rozdziałów.

Przedłożona do recenzji rozprawa doktorska mgr. Konrada Sałka dotyczy bardzo aktualnego problemu badawczego. Jest to tematyka ważna dla współczesnej gospodarki cyfrowej. W ostatnich latach obserwujemy dynamiczny wzrost znaczenia technologii informatycznych w funkcjonowaniu przedsiębiorstw, instytucji finansowych oraz państwa, co prowadzi do wzrostu ryzyka związanego z cyberbezpieczeństwem. Zagadnienie wpływu incydentów cyberbezpieczeństwa na wartość rynkową przedsiębiorstw stanowi wobec powyższego nie tylko interesujący problem badawczy, ale także ważne wyzwanie praktyczne, mające implikacje dla inwestorów, menedżerów oraz regulatorów rynku.

We wstępie na stronie 10 Autor trafnie identyfikuje lukę badawczą, szczególnie w odniesieniu do literatury polskojęzycznej, gdzie nadal brakuje pogłębionych analiz empirycznych

wykorzystujących metody ilościowe do badania krótkoterminowych reakcji rynków finansowych na incydenty cyberbezpieczeństwa. Jak Autor słusznie zauważa „Luka ta wskazuje na potrzebę wprowadzenia ilościowych badań nad wpływem cyberzagrożeń na rynki finansowe do polskiego dyskursu naukowego, co stanowi jeden z kluczowych celów niniejszej pracy”. Wybór tematu należy zatem uznać za w pełni uzasadniony zarówno z perspektywy poznawczej, jak i aplikacyjnej.

Celem rozprawy jest zbadanie krótkoterminowego wpływu incydentów cyberbezpieczeństwa na wartość rynkową przedsiębiorstw notowanych na giełdzie, przy wykorzystaniu metody *event study*. Autor formułuje następującą hipotezę badawczą: „Cyberataki mają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm notowanych na giełdzie, co znajduje odzwierciedlenie w ujemnych wartościach skumulowanych nadzwyczajnych zwrotów (CAR) po ujawnieniu incydentu”. Hipoteza ta została sformułowana w sposób klarowny, precyzyjny oraz umożliwiający jej empiryczną weryfikację, co należy uznać za istotną zaletę pracy.

Już na etapie wstępu Autor wykazuje się dobrą orientacją w problematyce badawczej oraz umiejętnością osadzenia własnych rozważań w teorii ekonomii i finansów. W szczególności trafnie wskazuje, że cyberataki generują nie tylko bezpośrednie koszty finansowe, lecz także skutki pośrednie, takie jak utratą reputacji czy spadek zaufania inwestorów, które mogą mieć bezpośrednie przełożenie na wycenę rynkową przedsiębiorstw. Takie ujęcie problemu świadczy o dojrzałości naukowej Autora oraz jego zdolności do identyfikowania złożonych mechanizmów ekonomicznych.

Celowi pracy została podporządkowana struktura. Jest ona poprawna i nie budzi żadnych zastrzeżeń. Podział na cztery rozdziały odpowiada klasycznemu układowi rozpraw doktorskich w naukach społecznych w dyscyplinie ekonomia i finanse. Autor w umiejętny sposób przechodzi od podstaw teoretycznych, a następnie przeprowadza analizę empiryczną i na tej podstawie formułuje wnioski. Całość osadzona jest gruntownie w literaturze, o czym świadczy szeroki przegląd literatury (s. 112-123 rozprawy doktorskiej). Poszczególne rozdziały mają właściwą i logicznie uzasadnioną strukturę i tworzą spójną całość. Naturalnie jest, że pewne elementy zostały w rozprawie pominięte, ale temat jest szeroki i konieczne było zastosowanie przez Autora tzw. „Brzytwy Ockhama”, przypisywanej XIV-wiecznemu franciszkaninowi, Wilhelmowi z Ockham. Zgodnie z „Brzytwą Ockhama”, w wyjaśnianiu zjawisk należy dążyć do prostoty, wybierając takie wyjaśnienia, które opierają się na jak najmniejszej liczbie pojęć i

założeń. Autor w umiejętny sposób to czyni. Mógłby np. przeprowadzić bardziej zawile i skomplikowane badanie empiryczne, ale do weryfikacji hipotezy badawczej nie jest to konieczne.

Podsumowując, temat pracy jest bardzo aktualny i ciekawy. Analiza została przeprowadzona przez Autora na poprawnym poziomie metodologicznym. Całość jest szeroko osadzona w literaturze przedmiotu. Praca wykazuje wysoki wkład w dyscyplinę ekonomia i finanse.

2. Szczegółowa ocena poszczególnych rozdziałów

Pierwszy rozdział pracy poświęcony jest zagadnieniom cyberbezpieczeństwa oraz cyberataków i ich skutków gospodarczych. Bardzo wysoko należy ocenić fakt, że Autor rozpoczyna od przedstawienia precyzyjnych definicji najważniejszych pojęć wykorzystywanych w pracy (cyberatak i cyberbezpieczeństwo). W ekonomii precyzyjne definicje odgrywają duże znaczenie dla przejrzystości wyводу i dużym atutem jest zdefiniowanie głównych zagadnień omawianych w rozprawie.

Wartościowym elementem jest głębokie osadzenie tego rozdziału w literaturze przedmiotu. Autor odwołuje się do uznanych źródeł literaturowych, cytując zarówno przełomowe prace w tym zakresie (np. P. Cornish, *The Cybersecurity Lexicon*, Routledge, 2017; T. Rid, *Cyber War Will Not Take Place*, Oxford University Press, 2013), jak też najnowsze badania w tym temacie, opublikowane w ostatnich latach (np. Su Y., *A Comprehensive Survey of Distributed Denial of Service (DDoS) Attacks and Defenses*, „Electronics”, vol. 13(4), 2024)¹. Należy to ocenić pozytywnie.

W rozdziale pierwszym Autor podkreśla interdyscyplinarny charakter cyberbezpieczeństwa, obejmujący aspekty techniczne, organizacyjne, prawne oraz finansowe (ekonomiczne). Takie ujęcie problemu jest zgodne z aktualnymi trendami badawczymi i świadczy o szerokim spojrzeniu Autora na analizowaną problematykę.

¹ Namiary bibliograficzne tej pozycji, cytowanej według pracy, są nieprecyzyjnie zapisane. Powinno być: Su, Y., Xiong, D., Qian, K., & Wang, Y. (2024), *A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network*, „Electronics”, 13(4), 807, DOI: 10.3390/electronics13040807.

W dalszej części rozdziału Autor dokonuje klasyfikacji cyberataków, wyszczególniając phishing, ransomware, ataki DDoS (*Distributed Denial of Service*), wycieki danych, ataki związane z wykorzystaniem sztucznej inteligencji, czy też ataki oparte na socjotechnice. Taka klasyfikacja pozwala Czytelnikowi lepiej zrozumieć badane zjawisko. Opis ten ma charakter poprawny, ale niestety po lekturze Czytelnik czuje pewien niedosyt. Wywód mógłby być bardziej podparty danymi liczbowymi; rekomendowałbym także bardziej pogłębioną analizę ich ekonomicznych konsekwencji.

Szczególnie istotnym elementem pierwszego rozdziału jest analiza kosztów cyberataków oraz ich wpływu na zachowania konsumentów i zaufanie do przedsiębiorstw. Autor trafnie wskazuje, że skutki incydentów cybernetycznych wykraczają poza bezpośrednie straty finansowe i obejmują również utratę zaufania, spadek wartości marki oraz zakłócenia operacyjne. Takie ujęcie tematu jest poprawne z punktu widzenia weryfikacji hipotezy badawczej, co zostanie przeprowadzone w dalszej części pracy. Można jednak zgłosić zastrzeżenie, że analiza jest miejscami zbyt płytka. Szkoda, że Autor w rozdziale I nie odniósł się do konkretnych studiów przypadków lub – jak wcześniej wspomniałem – danych empirycznych.

Drugi rozdział recenzowanej pracy doktorskiej dotyczy funkcjonowania rynków finansowych oraz ich podatności na cyberataki. Autor przedstawia podstawowe mechanizmy działania rynków kapitałowych, a następnie analizuje ich wrażliwość na zakłócenia wynikające z incydentów cybernetycznych. Szczególnie interesujące są rozważania dotyczące roli technologii cyfrowych w funkcjonowaniu współczesnych rynków finansowych, w tym znaczenia handlu algorytmicznego oraz systemów płatniczych.

Autor słusznie zauważa, że rosnąca cyfryzacja rynków finansowych zwiększa ich efektywność, ale jednocześnie czyni je bardziej podatnymi na zakłócenia. Cyberataki mogą być zatem postrzegane jako zakłócenie w przepływie i dostępie do informacji, co wpływa na oczekiwania inwestorów oraz ich decyzje inwestycyjne. Interesującym dopełnieniem wywodu prowadzonego w rozdziale II jest analiza związana ze sztuczną inteligencją i jej rolą w sektorze finansowym. Autor właściwie konkluduje, że algorytmy AI, szczególnie te wykorzystywane w analizie rynkowej i tradingu, są atrakcyjnym celem dla cyberprzestępców. Moim zdaniem kwestie powiązania cyberbezpieczeństwa ze sztuczną inteligencją byłyby nawet ciekawym tematem odrębnej rozprawy.

Najważniejszą częścią rozprawy jest rozdział trzeci, w którym Autor przedstawia wyniki badań empirycznych przeprowadzonych z wykorzystaniem metody *event study*. Metodologia została opisana w sposób poprawny i zgodny ze standardami obowiązującymi w literaturze finansowej. Autor wyjaśnia sposób konstrukcji okna bazowego oraz okna zdarzenia, a także procedurę obliczania nadzwyczajnych stóp zwrotu i ich skumulowanych wartości.

Jak Autor pisze: „Okno bazowe, obejmujące 120 dni przed zdarzeniem, umożliwia oszacowanie normalnych zwrotów akcji, natomiast okno zdarzenia (-3, +3) pozwala uchwycić krótkoterminową reakcję rynku na ujawnienie cyberataku.” W tym aspekcie pewien niedosyt budzi brak przeprowadzonej szerokiej analizy odporności (wrażliwości) wyników na przyjęte założenia (parametry) (tzw. *robustness check*). Tym bardziej, że jak Autor słusznie wskazuje: „W literaturze dotyczącej metody *event study* długość okna bazowego zazwyczaj mieści się w przedziale od 100 do 250 dni obrotowych przed oknem zdarzenia. W niniejszej analizie przyjęto okno bazowe obejmujące 120 dni obrotowych poprzedzających okno zdarzenia. Wybór ten stanowi kompromis między dążeniem do precyzyjnego oszacowania parametrów a ograniczeniami wynikającymi z dostępności danych.” Biorąc pod uwagę powyższe, o ile brak analizy odporności można byłoby uznać za właściwy w pracy licencjackiej lub magisterskiej, o tyle w pracy doktorskiej warto byłoby zbadać, na ile wyniki byłyby inne, gdybyśmy wzięli pod uwagę inne długości okien.

Niemniej jednak, zastosowana przez Autora metoda badawcza jest właściwa. Pozwala na uchwycenie krótkoterminowych reakcji rynku na określone zdarzenia informacyjne. Autor prawidłowo wykorzystuje tę metodę do analizy wpływu cyberataków na wycenę przedsiębiorstw. Dodatkowo zastosowanie testu *t*-Studenta umożliwia ocenę istotności statystycznej uzyskanych wyników, co zwiększa wiarygodność przeprowadzonych analiz.

Wyniki badań wskazują jednoznacznie, że ujawnienie incydentów cyberbezpieczeństwa prowadzi do statystycznie istotnych ujemnych skumulowanych nadzwyczajnych stóp zwrotu. Oznacza to, że rynki finansowe reagują negatywnie na informacje o cyberatakach, co znajduje odzwierciedlenie w spadkach cen akcji analizowanych przedsiębiorstw. Wynik ten jest ekonomicznie uzasadniony i nie stoi w sprzeczności z teoretycznym modelem strukturalnym.

Interpretacja wyników jest spójna. Autor wskazuje, że negatywna reakcja rynku wynika przede wszystkim z utraty zaufania inwestorów oraz wzrostu postrzeganego ryzyka. Jednocześnie można zauważyć, że analiza mogłaby zostać rozszerzona o dodatkowe aspekty, takie jak zróżnicowanie reakcji w zależności od branży, wielkości przedsiębiorstwa czy rodzaju incydentu. Uwzględnienie tych czynników pozwoliłoby na bardziej pogłębioną interpretację wyników. Jak widać po wykonanej analizie i po przeprowadzonym wnioskowaniu, wyniki mają dużą wartość aplikacyjną m.in. z punktu widzenia polityki gospodarczej.

Rozdział czwarty ma charakter aplikacyjny i stanowi próbę przełożenia wyników badań na przedsiębiorstwa. Autor omawia sposoby zapewnienia cyberbezpieczeństwa oraz strategie ograniczania skutków incydentów dla wartości rynkowej przedsiębiorstw. W szczególności podkreśla znaczenie działań prewencyjnych, takich jak inwestycje w systemy ochrony, a także skutecznego reagowania na incydenty.

Ta część pracy stanowi istotne uzupełnienie analizy empirycznej i świadczy o dużym potencjale praktycznym pracy doktorskiej. Wnioski sformułowane w tym rozdziale mogą być wykorzystane przez przedsiębiorstwa oraz instytucje finansowe w procesie zarządzania ryzykiem cybernetycznym.

3. Usterki techniczne

Wysoka ocena merytoryczna pracy nie współgra ze słabą redakcją pracy. W pracy jest wiele błędów redakcyjnych, stylistycznych, literowych itp. Oznacza to, że praca nie została dokładnie przeczytana. Przed ewentualną publikacją niezbędne jest dokładne przeczytanie przez Autora całej pracy i wyeliminowanie błędów. Poniżej przedstawiam wybrane niedociągnięcia:

Str. 4-5 (spis treści): brak punktu 6 w rozdziale II, rozdział IV zapisany w inny sposób niż rozdziały I-III.

Str. 9: akapit zaczyna się od „teoretycznego kontekstu dla badania (...)” (urwany został początek akapitu).

Str. 30: akapit nie jest wyjustowany (jest wyrównany do lewej).

Str. 34-36: brak jest uzasadnienia do zapisywania tytułów wielką literą.

Str. 51: zła składnia w zdaniu „Jednak wraz ze wzrostem jej znaczenia pojawiają się wiele istotne wyzwania...”

Język jest w większości przypadków precyzyjny. Występują jednak pewne niedoskonałości stylistyczne, takie jak powtórzenia czy nadmiernie rozbudowane zdania.

4. Podsumowanie

Podsumowując, rozprawa doktorska mgr. Konrada Sałka stanowi wartościowe opracowanie naukowe, które wnosi istotny wkład do badań nad wpływem cyberataków na rynki finansowe. Autor wykazał się umiejętnością formułowania problemów badawczych, stosowania metod ilościowych oraz interpretacji wyników. Pomimo pewnych ograniczeń, praca spełnia wymagania stawiane rozprawom doktorskim w dziedzinie nauk społecznych w dyscyplinie ekonomia i finanse.

5. Konkluzja końcowa

Mimo moich pewnych uwag krytycznych, co jest naturalnym elementem recenzji, w ogólnym rozrachunku uważam, że **praca jest bardzo ciekawa, stanowi oryginalne rozwiązanie problemu naukowego i wnosi wiele nowego do literatury przedmiotu**. Rozprawa doktorska we właściwy sposób prezentuje ogólną wiedzę teoretyczną kandydata. Autor we właściwy sposób stawia i weryfikuje hipotezę badawczą, prezentuje oraz interpretuje wyniki, a także wyciąga wnioski. Nie mam do tego zastrzeżeń.

Praca stanowi ważny wkład w rozwój dziedziny nauk społecznych, dyscypliny ekonomia i finanse. Uważam że praca spełnia wszelkie wymogi ustawowe. W ujęciu całościowym oceniam ją bardzo wysoko. Wnoszę zatem o przyjęcie pracy, dopuszczenie mgr. Konrada Sałka do dalszych etapów postępowania doktorskiego i do publicznej obrony pracy doktorskiej.

Biorąc pod uwagę rangę tematu oraz zawartość analizy, **wnioskuję o wyróżnienie** niniejszej rozprawy. W szczególności, podstawą wyróżnienia są następujące elementy:

- wysoka aktualność podjętego tematu,
- jasno sformułowany cel badawczy oraz precyzyjna hipoteza,
- trafny dobór metody badawczej,

- spójność i przejrzystość struktury rozprawy,
- dogłębność analizy,
- wnikliwość badawcza podczas wnioskowania.

 Podpisano przez/ Signed by:
MARIUSZ
PRÓCHNIAK
Data/ Date: 11.04.2026 11:14
mSzofir

.....
prof. dr hab. Mariusz Próchniak