Dr hab. Łukasz Jabłoński, prof. UEK
Katedra Teorii Ekonomii
Kolegium Ekonomii, Finansów i Prawa
Uniwersytet Ekonomiczny w Krakowie

Kraków, 12. marca 2026r.

Recenzja rozprawy doktorskiej Pana mgr Konrada Sałka pt. „Wpływ incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw" napisanej pod kierunkiem naukowym Pana prof. dr hab. Sławomira I. Bukowskiego

1. Podstawy formalno-prawne sporządzenia recenzji

Podstawę prawną niniejszej recenzji stanowią ustawa z dnia 20 lipca 2018 r. prawo o szkolnictwie wyższym (Dz. U. 2024, poz. 1571) oraz rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 19 stycznia 2018 r. w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodzie doktorskim, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora (Dz. U. z 2018 r., poz. 261). Recenzję przygotowano w związku z pismem prof. dr hab. Sławomira I. Bukowskiego, Rektora Uniwersytetu Radomskiego im. Kazimierza Pułaskiego z dnia 10 lutego 2026 roku. *Rozprawa doktorska Pani mgr Magdaleny Wrońskiej została napisana na Wydziale Ekonomii i Finansów Uniwersytetu Radomskiego im. Kazimierza Pułaskiego.*

W ocenie merytorycznej szczególna uwaga została zwrócona na osiągnięte rezultaty, a także ich znaczenie dla nauki i praktyki. Ocenie poddano również poprawność sformułowania problemów i hipotez badawczych, trafność doboru metod i narzędzi badawczych oraz umiejętność ich zastosowania, prawidłowość układu pracy i jej struktura oraz sformułowanie wniosków końcowych. W recenzji odniesiono się także do kwestii formalno-językowych oraz doboru literatury i umiejętność wykorzystania źródeł, na których została oparta rozprawa.

2. Uwagi wstępne

Obszar badawczy, w którym została osadzona rozprawa doktorska mgr Konrada Sałka, należy do zagadnień wyraźnie zyskujących na znaczeniu we współczesnej ekonomii i finansach. Problematyka wpływu incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw sytuuje się na styku finansów przedsiębiorstw, rynku kapitałowego, zarządzania ryzykiem oraz ekonomicznych konsekwencji transformacji cyfrowej. Wraz z postępującą cyfryzacją działalności gospodarczej, rosnącą

zależnością przedsiębiorstw od infrastruktury teleinformatycznej oraz wzrostem znaczenia danych jako zasobu strategicznego, cyberbezpieczeństwo przestaje być zagadnieniem wyłącznie technicznym, a staje się istotnym czynnikiem determinującym bezpieczeństwo ekonomiczne przedsiębiorstw oraz stabilność rynku finansowego. Z tego względu wybór tematu rozprawy należy uznać za trafny zarówno z poznawczego, jak i aplikacyjnego punktu widzenia (Anderson 2020).

Aktualność podjętej problematyki wynika, po pierwsze, z rosnącej skali i złożoności zagrożeń cybernetycznych, które generują dla przedsiębiorstw nie tylko koszty bezpośrednie, lecz także koszty pośrednie, związane z utratą reputacji, spadkiem zaufania interesariuszy, zakłóceniami operacyjnymi oraz wzrostem postrzeganego ryzyka inwestycyjnego. W warunkach wysokiej wrażliwości rynków kapitałowych na nowe informacje szczególnego znaczenia nabiera pytanie o to, czy oraz w jakim stopniu ujawnienie cyberataku prowadzi do natychmiastowej rewizji wyceny rynkowej przedsiębiorstwa. Podjęcie tak sformułowanego problemu badawczego należy ocenić pozytywnie, ponieważ odnosi się on do mechanizmu transmisji informacji o charakterze pozafinansowym do cen aktywów finansowych, a zatem do jednego z ważniejszych zagadnień współczesnej ekonomii finansowej (Campbell et al. 2003; Gordon, Loeb, Zhou 2011; Cavusoglu, Mishra, Raghunathan 2004).

Po drugie, pomimo wyraźnego wzrostu zainteresowania ekonomicznymi konsekwencjami cyberataków, literatura przedmiotu nadal nie dostarcza jednoznacznego i wyczerpującego obrazu ich krótkookresowego wpływu na wycenę przedsiębiorstw. Znaczna część istniejących opracowań koncentruje się na szerszych konsekwencjach naruszeń bezpieczeństwa, takich jak wpływ na ujawnienia ryzyka cybernetycznego, reputację przedsiębiorstwa, odporność organizacyjną, koszty naruszeń czy długofalowe implikacje dla funkcjonowania spółki i jej interesariuszy, podczas gdy analizy odnoszące się bezpośrednio do reakcji rynku wokół momentu ujawnienia incydentu pozostają nadal relatywnie nieliczne i nie zawsze prowadzą do spójnych wniosków (Amani, Magnan, Moldovan 2025; Ali et al. 2021). Z nowszych badań wynika wprawdzie, że rynek kapitałowy reaguje negatywnie na wiadomości o cyberatakach, jednak skala, trwałość i statystyczna istotność tej reakcji zależą od rodzaju incydentu, jego dotkliwości, cech przedsiębiorstwa oraz zastosowanej procedury estymacyjnej. Tego rodzaju niejednoznaczność wyników wzmacnia zasadność wyboru problemu badawczego, zwłaszcza że badania oparte na metodzie *event study* pozostają podstawowym narzędziem identyfikacji krótkoterminowych efektów informacji rynkowej na ceny akcji i nadal znajdują rozwinięcie we współczesnych analizach cyberincydentów (Akyildirim et al. 2024; Mukit et al. 2025; Huygen, Beulen 2025).

Po trzecie, na pozytywną ocenę wyboru tematu wpływa jego użyteczność praktyczna. Ustalenie, czy incydenty cyberbezpieczeństwa wywołują statystycznie istotną, negatywną reakcję rynku, ma znaczenie nie tylko dla rozwoju wiedzy ekonomicznej, lecz również dla praktyki zarządzania przedsiębiorstwem, decyzji inwestycyjnych oraz polityki regulacyjnej. Wyniki tego rodzaju badań mogą

bowiem wspierać menedżerów w projektowaniu strategii ograniczania ryzyka cybernetycznego, inwestorów w lepszej ocenie ryzyka spółek, a regulatorów w doskonaleniu standardów raportowania incydentów i wymogów bezpieczeństwa. Takie ujęcie problemu badawczego należy uznać za cenne, ponieważ łączy walor poznawczy z wyraźnym potencjałem aplikacyjnym (Arcuri, Brogi, Gandolfi 2018; Gordon, Loeb, Zhou 2011).

Tytuł rozprawy w brzmieniu „Wpływ incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw" odpowiada jej treści. Zawiera on podstawowe kategorie pojęciowe, tj. incydenty cyberbezpieczeństwa, krótkoterminową wycenę oraz przedsiębiorstwa, a zarazem wskazuje kierunek analizowanej zależności, to jest od wystąpienia i ujawnienia incydentu do reakcji rynku odzwierciedlonej w wycenie przedsiębiorstwa. Zaletą tytułu jest jego komunikatywność i zgodność z rzeczywistym przedmiotem analizy. Można jedynie zauważyć, że tytuł ma charakter dość szeroki, podczas gdy większa precyzja mogłaby zostać osiągnięta przez wyeksponowanie giełdowego charakteru próby badawczej lub zakresu podmiotowego analizy. Nie zmienia to jednak faktu, że tytuł zasadniczo trafnie oddaje zawartość merytoryczną rozprawy.

Rozprawa doktorska mgr Konrada Sałka ma charakter teoretyczno-empiryczny. Cel badawczy rozprawy Autor osiągnął przy pomocy metod i technik badawczych właściwych dla analizy krótkookresowych reakcji rynku kapitałowego na określone zdarzenia. Część teoretyczną rozpoczęto od charakterystyki kluczowych kategorii pojęciowych, których dotyczy rozprawa, a więc cyberbezpieczeństwa, cyberataków oraz ich ekonomicznych implikacji (Rozdział I). W kolejnym rozdziale (Rozdział II) przedstawiono problematykę rynków finansowych, ich funkcjonowania w warunkach postępującej cyfryzacji oraz podatności na zagrożenia wynikające z rozwoju cyberprzestępczości. Empiryczną część rozprawy stanowi Rozdział III, w którym Autor zaprezentował metodę badawczą zastosowaną do analizy wpływu incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw notowanych na giełdzie. W rozdziale tym omówiono dobór próby badawczej, konstrukcję okna estymacyjnego i okna zdarzenia, a także wyniki badania uzyskane przy zastosowaniu metody *event study*. Rozdział IV poświęcono natomiast zagadnieniom związanym z zapewnieniem cyberbezpieczeństwa oraz ograniczaniem ryzyka cybernetycznego.

Rozprawę oparto na zróżnicowanym zbiorze piśmiennictwa, obejmującym monografie i opracowania zwarte, artykuły publikowane w periodykach naukowych, raporty i dokumenty instytucjonalne, akty prawne, a także materiały źródłowe odnoszące się do konkretnych incydentów cybernetycznych. Z pewnością walorem rozprawy jest wykorzystanie licznych źródeł obcojęzycznych, głównie anglojęzycznych, co wzmacnia jej osadzenie w międzynarodowej literaturze przedmiotu. Zastosowane w rozprawie metody badawcze oceniam pozytywnie, jako właściwie dobrane w kontekście celu i hipotezy badawczej. Jednocześnie problem badawczy podjęty przez Autora wpisuje się w dyscyplinę naukową: ekonomia i finanse.

3. Cel rozprawy i hipotezy badawcze

Głównym celem rozprawy doktorskiej Autor uczynił „zbadanie krótkoterminowego wpływu incydentów cyberbezpieczeństwa na wartość rynkową przedsiębiorstw notowanych na giełdzie"[1]. Cel ten został sformułowany poprawnie i pozostaje zgodny z tytułem rozprawy, który akcentuje wpływ incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw. Na pozytywną ocenę zasługuje to, że zarówno w tytule, jak i w opisie celu głównego wyraźnie wyeksponowano zasadnicze kategorie pojęciowe, tj. incydenty cyberbezpieczeństwa, krótkoterminowy okres analizy oraz wartość rynkową przedsiębiorstw. Co istotne, w samej formule celu głównego Autor doprecyzowuje również obiekt analizy, wskazując, że badanie dotyczy przedsiębiorstw notowanych na giełdzie. Niemniej brakuje bardziej precyzyjne zawężenie obiektów badania do firm notownych na konkretnych giełdach papierów wartościowych. W moim przekonaniu wskazanie tych informacji we Wstępie rozprawy, a być może nawet w celu głównym i hipotezie głównej precyzyjnie ukierunkowałoby uwagę czytelnika na *de facto* przedmioty badania. W szczególności we Wstępie pojawia się wskazanie, że chodzi o firmy notowane na giełdzie, natomiast pełniejsze doprecyzowanie próby badawczej następuje dopiero w części empirycznej pracy (s. 61).

Cel główny rozprawy należy uznać za trafny, jednak z recenzenckiego punktu widzenia można zgłosić do niego drobną uwagę. O ile jego ogólna konstrukcja odpowiada tytułowi pracy i logice podjętego badania, o tyle dla większej precyzji można byłoby rozważyć jeszcze wyraźniejsze wskazanie zakresu podmiotowego analiz, np. przez bezpośrednie zaznaczenie, że chodzi o spółki giełdowe objęte analizą zdarzeń w określonym przedziale czasowym. Tego rodzaju doprecyzowanie zwiększałoby przejrzystość celu badawczego już na etapie lektury Wstępu, bez konieczności oczekiwania na szczegóły metodologiczne przedstawione w dalszych partiach rozprawy. Nie zmienia to jednak faktu, że zasadniczy sens celu głównego został ujęty prawidłowo i odpowiada zarówno problemowi badawczemu, jak i przyjętej metodzie analizy.

Pewien niedosyt może natomiast budzić brak wyraźnie wyodrębnionych celów szczegółowych o charakterze teoretycznym i empirycznym. Konstrukcja pracy doktorskiej o charakterze teoretyczno-empirycznym powinna wynikać z logicznie uporządkowanego układu celów szczegółowych, powiązanych z poszczególnymi rozdziałami rozprawy. W recenzowanej pracy taki podział nie został dostatecznie wyeksponowany. Tymczasem cele teoretyczne mogłyby korespondować z rozdziałami poświęconymi cyberbezpieczeństwu oraz funkcjonowaniu rynków finansowych w warunkach cyfryzacji, natomiast cele empiryczne powinny zostać jednoznacznie przypisane rozdziałowi

[1] Takie sformułowanie znajdujemy w Abstrakcie rozprawy. Z Kolei we Wstępie rozprawy (str. 8) znajdujemy mniej udane sformułowanie celu rozprawy *„...weryfikacja, czy ujawnienie cyberataku powoduje istotnie negatywną reakcję rynku, co znajduje odzwierciedlenie w ujemnych skumulowanych nadzwyczajnych zwrotach (CAR - Cumulative Abnormal Returns) w okresie po incydencie."*

badawczemu, w którym Autor wykorzystuje metodę *event study* do analizy reakcji rynku na ujawnienie cyberataków. Brak takiej wyraźnej segmentacji nie uniemożliwia przeprowadzenia procesu badawczego, ale osłabia przejrzystość konstrukcji rozprawy oraz utrudnia ocenę, w jakim stopniu poszczególne części pracy służą realizacji celu głównego. W efekcie można odnieść wrażenie, że część teoretyczno-deskryptywna została potraktowana bardziej jako szerokie tło dla badań empirycznych niż jako komponent podporządkowany odrębnie sformułowanym celom cząstkowym.

W pracy została natomiast wskazana hipoteza badawcza, choć rzeczywiście nie jest ona szczególnie mocno wyeksponowana, co może utrudniać jej szybkie uchwycenie podczas lektury. Autor formułuje ją w następującym brzmieniu: „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". Hipotezę tę należy uznać za poprawnie sformułowaną. Zawiera ona bowiem zarówno wskazanie kierunku zależności, jak i sposób jej empirycznej operacjonalizacji przy użyciu skumulowanych nadzwyczajnych stóp zwrotu, właściwych dla metody event study. Jej zaletą jest spójność z celem głównym, tytułem rozprawy oraz zastosowaną procedurą badawczą. Można jedynie zauważyć, że dla większej przejrzystości konstrukcji pracy warto byłoby wyraźnie nazwać ją hipotezą główną i ewentualnie rozważyć uzupełnienie jej o hipotezy szczegółowe odnoszące się do rodzaju incydentu, siły reakcji rynku czy zróżnicowania skutków między badanymi przedsiębiorstwami.

Pomimo wskazanych powyżej wątpliwości, mających charakter polemiczny, cel główny i hipoteza badawcza rozprawy doktorskiej pana mgr Konrada Sałka zostały sformułowane prawidłowo, umożliwiając Autorowi przeprowadzenie procesu badawczego.

4. Ocena merytoryczna wartości rozprawy

Rozprawa doktorska pana mgr Konrada Sałka składa się z czterech rozdziałów poprzedzonych Wstępem i zamkniętych Wnioskami i podsumowaniem. Ze względu na objętość, tj. liczbę stron, względnie wyrównany charakter mają Rozdziały I i IV, których objętość wynosi odpowiednio 18 i 16 stron. Nieco większą objętością charakteryzuje się Rozdział II (25 stron), natomiast najbardziej rozbudowaną część pracy stanowi Rozdział III (33 strony), zawierający empiryczną część rozprawy.

Rozdział I rozprawy, zatytułowany „Cyberbezpieczeństwo i cyberataki – skutki gospodarcze", ma charakter wprowadzający i porządkujący podstawowe kategorie pojęciowe, na których oparto dalsze rozważania. Autor rozpoczyna go od omówienia definicji cyberataku i cyberbezpieczeństwa, następnie przedstawia rodzaje cyberataków, ewolucję technologii cyberbezpieczeństwa, koszty cyberataków dla gospodarki i przedsiębiorstw oraz wpływ incydentów cybernetycznych na zachowania konsumentów i zaufanie do firm. Układ rozdziału jest logiczny i przejrzysty. Autor wychodzi w nim od

kwestii definicyjnych i typologicznych do zagadnień o charakterze ekonomicznym i społecznym, tworząc tym samym punkt wyjścia do dalszych rozważań zawartych w rozprawie.

W rozdziale tym Autor trafnie dostrzega interdyscyplinarny charakter cyberbezpieczeństwa, sytuując je nie tylko w obszarze technologii informacyjnych, ale również w ekonomii, zarządzaniu i funkcjonowaniu przedsiębiorstw. Szczególnie cenne jest ujęcie w tym rozdziale gospodarczych skutków cyberataków, takich jak straty finansowe, zakłócenia działalności operacyjnej, utrata danych oraz osłabienie zaufania klientów i interesariuszy. Dzięki temu rozdział ten nie ogranicza się wyłącznie do technicznego opisu zagrożeń, lecz stanowi próbę osadzenia ich w realiach współczesnej gospodarki cyfrowej.

Rozdział I poprawnie porządkuje podstawowe pojęcia i przedstawia szerokie tło badanego problemu, jednak miejscami wywód ma bardziej charakter sprawozdawczy niż analityczny. Dotyczy to zwłaszcza fragmentów poświęconych typologii cyberataków oraz ewolucji technologii cyberbezpieczeństwa, gdzie można byłoby oczekiwać silniejszego powiązania prowadzonych rozważań z zasadniczym problemem rozprawy, tj. wpływem incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw. W tym celu lepszym rozwiązaniem przed omówieniem typów cyberataków i ewolucji technologii zastosować kryteria mich klasyfikacji, które powinny korespondować z celem głównym lub celami szczegółowymi (których w rozprawie niestety brak). Dzięki temu czytelnik miałby wrażenie, że w mnogości wyzwań, zagrożeń, incydentów itp. Związanych z cyberbezpieczeństwem na uwagę w kontekście celu rozprawy zasługują pewne ich grupy. Jednocześnie pewien niedosyt budzi natomiast relatywnie słabsze wyeksponowanie w Rozdziale I związku między omawianymi zagadnieniami a późniejszą analizą reakcji rynku kapitałowego.

Rozdział II rozprawy poświęcono problematyce rynków finansowych w warunkach postępującej cyfryzacji oraz ich podatności na zagrożenia cybernetyczne. Autor koncentruje się w nim na funkcjonowaniu współczesnego rynku finansowego, roli technologii cyfrowych w obrocie finansowym, a także na zagrożeniach wynikających z rosnącej zależności instytucji i uczestników rynku od infrastruktury teleinformatycznej. Rozdział ten pełni istotną funkcję w konstrukcji rozprawy, ponieważ stanowi pomost między ogólną charakterystyką cyberbezpieczeństwa, przedstawioną w Rozdziale I, a empiryczną analizą wpływu incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw zawartą w dalszej części pracy.

Na pozytywną ocenę zasługuje fakt, że Autor trafnie osadza analizowany problem w realiach współczesnych rynków finansowych, wskazując, iż rozwój cyfrowych kanałów komunikacji, automatyzacja procesów finansowych oraz wzrost znaczenia danych i systemów transakcyjnych zwiększają efektywność rynku, ale jednocześnie generują nowe źródła ryzyka. Rozdział ten słusznie akcentuje, że cyberzagrożenia nie są już wyłącznie problemem technologicznym, lecz stają się czynnikiem oddziałującym na stabilność instytucji finansowych, bezpieczeństwo obrotu oraz poziom

zaufania uczestników rynku. W tym sensie Rozdział II stanowi ważne rozwinięcie ekonomicznego kontekstu rozprawy.

Jednocześnie należy zauważyć, że przy omawianiu uwarunkowań funkcjonowania rynków finansowych oraz obszarów ich podatności na incydenty cybernetyczne Autor nie stosuje wyraźnych kryteriów klasyfikacji analizowanych zjawisk. W rezultacie wywód przybiera miejscami postać sekwencji opisów i wyliczeń, które – choć oparte na literaturze przedmiotu – nie zawsze są podporządkowane celowi badawczemu. Z tego względu czytelnik nie otrzymuje w pełni przejrzystych podstaw do analizy tych kwestii w bezpośrednim związku z celem badawczym rozprawy. Innymi słowy, część rozważań ma charakter bardziej kompilacyjny niż problemowy, przez co związek między omawianymi uwarunkowaniami rynku finansowego a późniejszą analizą reakcji wyceny przedsiębiorstw na incydenty cyberbezpieczeństwa nie zawsze zostaje dostatecznie silnie wyeksponowany.

Rozdział III stanowi zasadniczy rdzeń empiryczny rozprawy, gdzie Autor przedstawia procedurę badawczą służącą weryfikacji hipotezy, zgodnie z którą cyberataki wywierają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm notowanych na giełdzie. W badaniu zastosowano metodę *event study*, uzupełnioną testem t-Studenta, przy czym procedura obejmuje wyznaczenie okna bazowego liczącego 120 dni, określenie okna zdarzenia od -3 do +3 dni wokół ujawnienia incydentu, oszacowanie oczekiwanych stóp zwrotu przy użyciu modelu rynkowego oraz obliczenie nadzwyczajnych stóp zwrotu (AR) i skumulowanych nadzwyczajnych stóp zwrotu (CAR). Analizę oparto na 32 przypadkach cyberataków spełniających przyjęte kryteria doboru próby, tj. notowanie spółki na giełdzie, precyzyjnie określoną datę ujawnienia incydentu oraz istotność zdarzenia.

Na pozytywną ocenę zasługuje sam wybór metody badawczej, a więc *event study*, która należy do klasycznych i zarazem najbardziej adekwatnych narzędzi badania krótkookresowej reakcji rynku na analizowane incydenty. Pozwala ona porównać rzeczywiste stopy zwrotu z oczekiwanymi stopami zwrotu w warunkach braku danego incydentu, a następnie uchwycić reakcję rynku. Z punktu widzenia celu rozprawy zastosowanie tej metody należy uznać za trafne, ponieważ umożliwia ona bezpośrednią obserwację zmian w wycenie przedsiębiorstw wokół momentu ujawnienia cyberataku. Autor poprawnie wskazuje podstawowe elementy tej procedury oraz konsekwentnie wykorzystuje je w dalszej analizie wyników.

Jednocześnie należy zauważyć, że Autor stosunkowo słabo wyeksponował zalety metody event study na tle alternatywnych podejść empirycznych. Wprawdzie wskazuje, że jest to metoda powszechnie wykorzystywana do analizy krótkoterminowych reakcji na konkretne wydarzenia, jednak nie rozwija szerzej argumentacji, dlaczego właśnie to narzędzie badawcze jest w analizowanym problemie lepsze lub bardziej użyteczne niż inne możliwe podejścia. W rozdziale brakuje choćby krótkiego odniesienia do alternatywnych sposobów badania ekonomicznych skutków cyberataków,

takich jak analizy panelowe, modele regresyjne uwzględniające cechy przedsiębiorstw i zdarzeń, badania długookresowych efektów rynkowych czy studia porównawcze obejmujące grupy kontrolne. Z tego względu czytelnik nie otrzymuje pełnego obrazu metodologicznego uzasadnienia wyboru zastosowanego narzędzia, mimo że sam wybór metody należy uznać za trafny.

Pewien niedosyt budzi również sposób prezentacji próby badawczej. Poza zestawieniem przedsiębiorstw ujętych w badaniu, zawartym w tabeli 2 (s. 82), Autor nie przedstawia choćby skrótowej charakterystyki badanych firm w kontekście ich podstawowych podobieństw i różnic, które mogłyby mieć znaczenie dla skali reakcji rynku na analizowane incydenty. Tymczasem z punktu widzenia interpretacji wyników użyteczne byłoby choćby ogólne wskazanie, czy analizowane podmioty należą do podobnych czy odmiennych sektorów, czy różnią się wielkością, znaczeniem rynkowym, profilem ryzyka lub poziomem uzależnienia od technologii cyfrowych. Autor traktuje bowiem całą próbę w sposób homogeniczny, a momentami wręcz punktowy, koncentrując się na samym zdarzeniu i jego bezpośrednim odzwierciedleniu w CAR. Nie stanowi to istotnej wady z perspektywy samej efektywności procedury *event study*, która wymaga odpowiedniej liczebności próby i została tu zastosowana poprawnie, jednak krótka charakterystyka badanych przedsiębiorstw mogłoby wzbogacić interpretację wyników i pozwoliłoby czytelnikowi postawić pytanie, dlaczego niektóre spółki reagują silniej, a inne słabiej na incydenty cyberbezpieczeństwa, nawet jeśli rozprawa nie stawiała sobie za cel pełnego wyjaśnienia tych różnic.

W mojej ocenie Rozdział III należy uznać za najważniejszą i zarazem najlepiej podporządkowaną celowi rozprawy część pracy. Autor poprawnie konstruuje procedurę badawczą, przeprowadza analizę z wykorzystaniem właściwego narzędzia empirycznego i uzyskuje wyniki pozwalające na weryfikację hipotezy badawczej. Zastrzeżenia budzi przede wszystkim niewystarczające osadzenie wyboru metody event study na tle innych możliwych podejść badawczych oraz zbyt ograniczona charakterystyka próby badawczej. Uwagi te nie podważają jednak wartości samej analizy empirycznej, lecz wskazują na elementy, które mogłyby zwiększyć jej przejrzystość metodologiczną i pogłębić warstwę interpretacyjną rozprawy.

Rozdział IV poświęcono sposobom zapewnienia cyberbezpieczeństwa, w tym profilaktyce cybernetycznej, reagowaniu na incydenty oraz budowaniu odporności rynkowej przedsiębiorstw. Autor podejmuje w nim zagadnienia związane z ochroną organizacji przed skutkami cyberataków, wskazując zarówno na znaczenie rozwiązań technicznych i organizacyjnych, jak i na rolę regulacji, procedur oraz standardów bezpieczeństwa. Zawarte w tym rozdziale rozważania mają niewątpliwy walor praktyczny, ponieważ odnoszą się do metod ograniczania ryzyka cybernetycznego oraz minimalizowania strat wynikających z incydentów bezpieczeństwa. W tym sensie Rozdział IV stanowi próbę uzupełnienia części diagnostycznej o komponent bardziej aplikacyjny.

Jednocześnie można odnieść wrażenie, że treść tego rozdziału nie jest w pełni konieczna z punktu widzenia realizacji głównego celu rozprawy, którym jest zbadanie krótkoterminowego wpływu incydentów cyberbezpieczeństwa na wartość rynkową przedsiębiorstw notowanych na giełdzie. O ile bowiem Rozdział III pozostaje bezpośrednio podporządkowany weryfikacji hipotezy badawczej i zawiera zasadniczy rdzeń empiryczny pracy, o tyle Rozdział IV ma charakter bardziej postulatywny i praktyczny. Z tego względu jego związek z głównym problemem badawczym nie został dostatecznie silnie wyeksponowany. Czytelnik może odnieść wrażenie, że rozdział ten stanowi wartościowe, lecz tylko częściowo zintegrowane dopełnienie wcześniejszych analiz.

W mojej ocenie wrażenie to może wynikać również z braku wyraźnie wyodrębnionych celów szczegółowych rozprawy. Gdyby Autor sformułował obok celu głównego także cele cząstkowe, w tym np. cel aplikacyjny odnoszący się do sposobów ograniczania ryzyka cybernetycznego i ochrony wartości rynkowej przedsiębiorstw, łatwiej byłoby uzasadnić miejsce i funkcję Rozdziału IV w strukturze pracy. W obecnym układzie rozprawy rozdział ten sprawia bowiem wrażenie części dobudowanej do zasadniczego rdzenia badawczego, a jego rola w procesie dochodzenia do celu głównego nie została w pełni przekonująco uzasadniona.

Nie zmienia to jednak faktu, że Rozdział IV zawiera treści merytorycznie interesujące i użyteczne z praktycznego punktu widzenia. Jego walorem jest zwrócenie uwagi na to, że problem cyberbezpieczeństwa nie powinien być postrzegany wyłącznie jako źródło zagrożeń dla bieżącej wyceny przedsiębiorstwa, lecz również jako obszar zarządzania ryzykiem, wymagający odpowiednich działań prewencyjnych i reakcyjnych. Z tego względu rozdział ten należy ocenić pozytywnie pod względem aplikacyjnym, choć z zastrzeżeniem, że jego usytuowanie w strukturze rozprawy oraz związek z głównym celem badawczym mogłyby zostać lepiej ujete.

Część *Wnioski i podsumowanie* zamyka rozprawę i stanowi próbę syntetycznego ujęcia najważniejszych ustaleń wynikających z przeprowadzonych rozważań teoretycznych i empirycznych. Autor wskazuje w niej zasadnicze rezultaty badania, potwierdzając, że incydenty cyberbezpieczeństwa mogą wywierać negatywny wpływ na krótkoterminową wartość rynkową przedsiębiorstw notowanych na giełdzie. Ta część pracy spełnia zatem podstawową funkcję porządkującą, ponieważ zbiera najważniejsze wnioski płynące z analizy i domyka zasadniczy tok wywodu badawczego.

Na pozytywną ocenę zasługuje to, że w zakończeniu Autor podejmuje próbę odniesienia uzyskanych wyników do szerszego kontekstu funkcjonowania przedsiębiorstw i rynku finansowego w warunkach narastających zagrożeń cybernetycznych. Dzięki temu *Wnioski i podsumowanie* nie mają wyłącznie charakteru technicznego streszczenia wcześniejszych rozdziałów, lecz stanowią również próbę wskazania znaczenia przeprowadzonych badań dla praktyki gospodarczej i zarządzania ryzykiem. W tym sensie część ta koresponduje z aplikacyjnym wymiarem rozprawy.

W kontekście powyżej wskazanych wątpliwości o charakterze polemicznym, pragnę postawić Doktorantowi kilka pytań, na które chciałbym usłyszeć odpowiedzi w trakcie publicznej obrony rozprawy doktorskiej, tj.:

1. *Jakie alternatywne metody empiryczne mogłyby zostać zastosowane do badania wpływu incydentów cyberbezpieczeństwa na wartość rynkową przedsiębiorstw oraz uzasadnić? Jakie przesłanki zdecydowały o wyborze event study jako narzędzie badawcze zastosowane w rozprawie?*
2. *Proszę zaproponować zestaw celów szczegółowych oraz odpowiadających im hipotez szczegółowych, które — zdaniem Doktoranta — porządkowałyby strukturę rozprawy i w sposób bardziej przejrzysty prowadziły do realizacji celu głównego oraz weryfikacji hipotezy głównej.*
3. *Czy i w jakim zakresie zróżnicowanie badanych przedsiębiorstw pod względem branży, wielkości, pozycji rynkowej lub stopnia zależności od technologii cyfrowych mogło wpływać na zróżnicowanie reakcji kursów giełdowych na ujawnienie incydentów cyberbezpieczeństwa?*

1. Ocena formalnej strony pracy

Od strony formalnej rozprawa została przygotowana poprawnie. Nie jest ona wolna od uchybień redakcyjnych, językowych i bibliograficznych. W pracy występują pewne niefortunności polegające na m.in. urwany fragment zdania we Wstępie (s. 9), błąd techniczny w przypisów [161718] (np. zlane numery przypisów na s. 10). Zastrzeżenia budzi również staranność opracowania bibliografii, gdzie pojawiają się niekompletne lub błędnie zapisane opisy, np. urwany identyfikator DOI w przypisie na s. 58, brak nazwy wydawnictwa (Journal) w przypisie nr 73 na str. 31.

2. Wnioski końcowe

Recenzowana rozprawa doktorska mgr Konrada Sałka prezentuje oryginalne rozwiązanie zagadnienia naukowego i problemu badawczego. Pracę doktorską mgr Konrada Sałka oceniam pozytywnie. Rozprawa posiada walory naukowe, pragmatyczne oraz poznawcze. Doktorant wykazał się wiedzą teoretyczną w dyscyplinie naukowej ekonomia i finanse, które poszerzają dotychczasowy stan wiedzy. Zawarte w recenzji uwagi krytyczne oraz sugestie proponuję wykorzystać przez Doktoranta w jego dalszej pracy naukowej, zwłaszcza w przyszłych publikacjach naukowych.

Jednocześnie chciałbym podkreślić mocne strony rezultatów badawczych Autorki, zawartych w recenzowanej rozprawie doktorskiej:

1. Trafny i aktualny wybór problemu badawczego; rozprawa podejmuje temat istotny z punktu widzenia współczesnej gospodarki cyfrowej, rynku kapitałowego oraz bezpieczeństwa ekonomicznego przedsiębiorstw.
2. Interdyscyplinarne ujęcie analizowanej problematyki; Autor łączy zagadnienia z zakresu ekonomii i finansów, rynku kapitałowego, zarządzania ryzykiem oraz cyberbezpieczeństwa.
3. Poprawny dobór metody badawczej do celu rozprawy; zastosowane narzędzie analityczne jest adekwatne do badania krótkookresowej reakcji rynku na ujawnienie incydentów cyberbezpieczeństwa.
4. Aplikacyjny charakter wyników rozprawy; zawarte w pracy ustalenia mogą mieć znaczenie dla przedsiębiorstw, inwestorów oraz instytucji odpowiedzialnych za bezpieczeństwo i stabilność rynku.

Praca mgr Konrada Sałka spełnia wymogi ustawy z dnia 20 lipca 2018 r. prawo o szkolnictwie wyższym (Dz. U. 2024, poz. 1571). W związku z powyższym wnoszę do Senatu Uniwersytetu Radomskiego im. Kazimierza Pułaskiego o przyjęcie rozprawy doktorskiej mgr Konrada Sałka pt. „Wpływ incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw" oraz dopuszczenie jej do publicznej obrony.

Literatura przywołana w recenzji:

Akyildirim, Erdinc, Corbet, Shaen, Efthymiou, Marios, Sensoy, Ahmet (2024), HACKED: Understanding the stock market response to cyberattacks, Finance Research Letters, Vol. 68, Part B, 105965.

Ali, Syed Ehsan, Appolloni, Andrea, Cavallaro, Fausto, D'Adamo, Idiano (2021), The Long-Run Impact of Information Security Breach Announcements on Investors' Behavior and Firms' Financial Performance: Evidence from the US Healthcare Industry, Sustainability, Vol. 13, No. 3, 1066.

Amani, Farzaneh, Magnan, Michel, Moldovan, Rucsandra (2025), Cybersecurity Risks and Incidents Disclosure: A Literature Review, Accounting Perspectives, Vol. 24, No. 3, pp. 605–667.

Anderson, Ross (2020), Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., John Wiley & Sons, Indianapolis.

Arcuri, Maria Cristina, Brogi, Marina, Gandolfi, Giuseppe (2018), The Effect of Cyber-Attacks on Stock Returns, Corporate Ownership & Control, Vol. 15, No. 2, pp. 70–83.

Campbell, Katherine, Gordon, Lawrence A., Loeb, Martin P., Zhou, Lei (2003), The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, Journal of Computer Security, Vol. 11, No. 3, pp. 431–448.

Cavusoglu, Huseyin, Mishra, Birendra K., Raghunathan, Srinivasan (2004), The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, International Journal of Electronic Commerce, Vol. 9, No. 1, pp. 69–104.

Gordon, Lawrence A., Loeb, Martin P., Zhou, Lei (2011), The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?, Journal of Computer Security, Vol. 19, No. 1, pp. 33–56.

Huygen, Lennart, Beulen, Erik (2025), Cyber shocks: The financial impact of cyber events, Social Sciences & Humanities Open, Vol. 12, 101770.

Muktadir-Al-Mukit, D., Ali, M.H. (2025), The Dynamics of Stock Market Responses Following the Cyber-Attacks News: Evidence from Event Study. Inf Syst Front (2025). https://doi.org/10.1007/s10796-025-10639-6