Szczytno, 2025.10.08.

Prof. dr hab. inż. Ryszard JAKUBCZAK
Wydział Bezpieczeństwa i Nauk Prawnych
Akademia Policji w Szczytnie

RECENZJA

rozprawy doktorskiej nt.

TRANSAKCJE NIEUPRAWNIONE W SYSTEMIE BEZPIECZEŃSTWA BANKOWEGO,

autorstwa mgr Kamila Przyłuskiego,

napisanej pod kierunkiem prof. dr hab. inż. Jarosława WOŁEJSZO

Wprowadzenie

Rozprawa doktorska poświęcona została funkcjonowaniu banków komercyjnych z uwzględnieniem transformacji technologicznych i rosnącego zagrożenia występującego wskutek nieuprawnionych transakcji w systemach bankowych. Wyniki badań zaprezentowane w niej dotyczą ważnego obszaru gospodarki cyfrowej, w którym usługi finansowe mają znamiona dynamicznych zmian, gdzie bezpieczeństwo operacji elektronicznych stanowi krytyczny element w zaufaniu do instytucji finansowych, ponieważ rola banków komercyjnych w obiegu pieniądza w gospodarce jest newralgiczna. Stąd działalność tych instytucji finansowych istotnie wpływa na różne aspekty funkcjonowania gospodarki narodowej. Zaś banki nie tylko uczestniczą w procesach kreowania pieniądza, czy też alokacji kapitału, lecz również zapewnianiu płynności finansowych przedsiębiorstw, co i gospodarstw domowych oraz obsługi płatności w gospodarce narodowej. Drożność finansowa w transakcyjnych instytucji bankowych ma istotny wpływ na szybkość obiegu pieniądza w gospodarce narodowej, co i na parytet jego wartości siły nabywczej. Zatem system bankowy jest fundamentem funkcjonowania gospodarki, a on sam podlega dynamicznym przeobrażeniom związanym z rozwojem technologii cyfrowych.

Ze względu na rozwój Elektronicznych Kanałów Dostępu do usług bankowych, jak chciałby bankowość elektroniczna i mobilna, następuje przy tym identyfikacja zjawiska występowania transakcji nieuprawnionych, czyli działań bez wiedzy i zgody właściciela rachunku bankowego, swoistej formy nadużyć finansowych – co ma wymiar zarówno ekonomiczny, jak i prawny oraz społeczny i technologiczny.

Stąd transakcje nieuprawnione stanowią poważne zagrożenie dla integralności systemu bankowego oraz bezpieczeństwa środków i tożsamości klientów banków. A także mogą godzić

w zaufanie do instytucji finansowych. Zatem tym kwestiom poświęcona jest w szczególności niniejsza rozprawa doktorska, gdyż prezentuje istotne a zarazem interesujące zagadnienia z powyższego zakresu tematycznego w oparciu nie tylko o źródła polskie, ale i międzynarodowe – koncertując wysiłek badawczy przede wszystkim na aspektach kryptologicznych i technologicznych oraz zarządzaniu ryzykiem operacyjnym i informacyjnym, a także modelach zachowań użytkowników w kontekście cyber-oszustw.

Podjęty problem jest ważny i aktualny, gdyż dotyczy w równym stopniu bezpieczeństwa banków, co i obywatel. A tym samym wymaga oceny i doskonalenia, nie tylko w kwestiach związanych z bezpieczeństwem polskiego sektora bankowego - ale przede wszystkim prawnych, na co zasadnie zwrócono uwagę w dysertacji.

Struktura dysertacji zawiera wstęp, cztery rozdziały (w tym jeden metodologiczny i trzy merytoryczne), bibliografię, spisy tabel i wykresów oraz załącznik.

OCENA METODOLOGICZNA

W **pierwszym rozdziale** *Metodologiczne podstawy badań* (ss. 5-25), zawarto problemy i hipotezy badawcze. Omówiono metody techniki i narzędzia badawcze. Została określona także próba badawcza. Odniesiono się do *Sytuacji problemowej,* w której zawarto, iż „Procesy udoskonalania systemów bezpieczeństwa banków komercyjnych tworzą podstawy dla ich funkcjonowania. Wynika to z istoty banku jako instytucji powstałej na bazie założenia określającego bank jako osobę prawną utworzoną zgodnie z przepisami ustaw oraz powołaną między innymi do świadczenia usługi zaufania oraz wydawania środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania. Z uwagi na swoją istotę bank funkcjonuje według ściśle określonych procedur, które go definiują. Każdy bank musi wedle założeń posiadać swój własny statut i spisaną *Politykę bezpieczeństwa* organizacji, która powinna szczegółowo wymieniać katalog i sposób przeprowadzenia określonych czynności bankowych w zakresie bezpieczeństwa. W praktyce *polityka bezpieczeństwa* i *księga procedur* stanowią podstawę funkcjonowania każdej instytucji finansowej. Permanentnym elementem falsyfikującym poprawność ich działania są transakcje nieuprawnione (ang. fraud), które de facto determinują konieczność modyfikacji reguł dotyczących obszarów bezpieczeństwa".

Zatem w tej części opracowania naukowego przyjęto, że „wybór tematu dysertacji został podyktowany potrzebą diagnozy i wskazania trendów występowania transakcji nieuprawnionych na polskim rynku bankowym. Tematyka, mimo swojego ogromnego potencjału, nie doczekała się kompleksowego opracowania. Niniejsza praca ma na celu

wyeksponowanie obszarów systemów bezpieczeństwa bankowego, które w najwyższym stopniu obarczone są ryzykiem fraudów. Co zdaniem Autora może stano wić przyczynek do modyfikacji i rozwoju procedur bezpieczeństwa.

Przedmiotem badań dysertacji jest: funkcjonowanie systemu bezpieczeństwa banków komercyjnych. Zakresem przestrzennym dla przedmiotu badań jest polski rynek bankowy ze szczególnym uwzględnieniem banków komercyjnych. Zakres czasowy obejmuje okres od 2020 roku do końca 2023 roku (raport roczny KNF).

Powyższa sytuacja problemowa była podstawą do sformułowania **celu** dysertacji, jakim jest: „wskazanie zagrożeń dla systemu bankowego w zakresie transakcji nieuprawnionych oraz propozycja rozwiązań zwiększających poziom bezpieczeństwa transakcyjnego. Wieloaspektowość tak nakreślonego celu głównego implikuje konieczność jego po głębienia w postaci celów szczegółowych, które są pomocne w jego osiągnięciu:

1. Przedstawienie funkcjonowania systemu bezpieczeństwa banków komercyjnych.

2. Zaprezentowanie, w jaki sposób transakcje nieuprawnione wpłynęły na kształtowanie procedur bezpieczeństwa bankowego

3. Wskazanie usprawnień systemu bezpieczeństwa banków komercyjnych w przeciwdziałaniu transakcjom nieuprawnionych".

W niniejszej dysertacji - stosownie do przyjętego celu badań oraz zdefiniowanego przedmiotu badań, główny **problem badawczy** wyrażony został w postaci pytania o treści: Jakie zmiany należy wprowadzić w systemie bezpieczeństwa banków komercyjnych, aby nie dopuścić do występowania transakcji nieuprawnionych?

Na rzecz rozwiązania tego problemu przyjęto następujące problemy szczegółowe:

1. Jak funkcjonuje system bezpieczeństwa banków komercyjnych?

2. W jaki sposób transakcje nieuprawnione wpłynęły na kształtowanie procedur bezpieczeństwa bankowego?

3. Jakie powinny być usprawnienia w zakresie bezpieczeństwa banków komercyjnych w przeciwdziałaniu transakcjom nieuprawnionych?

Problemom tym poświecono poszczególne rozdziały merytoryczne dysertacji.

Do przyjętego celu i głównego problemu badawczego sformułowano **hipotezę główną** w brzmieniu: „Przypuszcza się, że aby nie dopuścić do zaistnienia transakcji nieuprawnionych należy wprowadzić zmiany w bezpieczeństwie banków komercyjnych w zakresie modyfikacji procedur oraz systemów. Zakłada się, że zmiany powinny dotyczyć przekształcenia procedury silnego uwierzytelniania i udoskonalenie systemów identyfikacji akceptanta. W związku z tym

istnieje potrzeba prognozowania trendów występowania transakcji nieuprawnionych w celu poprawy bankowych praktyk bezpieczeństwa".

W jej kontekście sformułowano trzy hipotezy szczegółowe o treści:

1. Przypuszcza się, że system bezpieczeństwa banków komercyjnych funkcjonuje wadliwie. Do defektów systemu wpływających na możliwość zaistnienia transakcji nieuprawnionych zaliczyć należy: brak praktycznej możliwości wprowadzenia procedury silnego uwierzytelnienia w kanałach zdalnych, brak formalnych procedur determinujących funkcjonowanie agregacji rachunków według Account Information Service (AIS), luki w zabezpieczeniach przy Payment Initiation Service (PIS) oraz nieścisłości dotyczące identyfikacji transakcji co do zasad księgowania.

2. Zakłada się, że transakcje nieuprawnione w znaczący sposób wpłynęły na kształtowanie procedur bezpieczeństwa bankowego, a w szczególności na rozwój zabezpieczeń bankowości elektronicznej, do których zaliczają się: obowiązek oceny ryzyka w obszarze Anti Money Laundering (AML), analizowania profili klientów i transakcji wedle zasady risk based approach a także prawna konieczność informowania Generalnego Inspektora Informacji Finansowej o możliwości wystąpienia transakcji podejrzanych.

3. Należy sądzić, że usprawnienia w zakresie bezpieczeństwa banków komercyjnych w przeciwdziałaniu transakcjom nieuprawnionym powinny skupiać się na prawidłowej identyfikacji akceptanta transakcji. W tym celu konieczne jest zastąpienie tokenów numerycznych nośnikami biometrycznymi pod rygorem wycofania możliwości przeprowadzenia operacji płatniczej, wprowadzenie zasad analityki behawioralnej oraz profilowania klienta. Ponadto istotna jest synchronizacja księgowania transakcji wychodzących i przychodzących w ramach jednolitego systemu płatniczego opartego o systemy typu Real-Time Gross Settlement (RTGS) zamiast tradycyjnych opartych o sesje oraz możliwości preautoryzacji płatniczych dla wszystkich operacji zdalnych.

Metodologicznie dysertacja jest logiczna i właściwie prezentuje treści, które są istotne dla procedury badawczej w odniesieniu do przedmiotu badań.

Na zakończenie tej części metodologicznej słusznie zaprezentowano szereg metod i technik wykorzystywanych w dysertacji, stąd podczas obrony proszę zaprezentować tabelarycznie, które metody odniesiono do poszczególnych rozdziałów i jaki przyniosło to rezultaty badawcze.

Podsumowują tę część dysertacji należy podkreślić, że kwestie metodologiczne zaprezentowane w niej zaświadczają o dużej znajomości i rzetelności Doktoranta w rozumieniu

i stosowaniu metod naukowych dla podjętych przez niego badań. Tym samym uznaję, tę część dysertacji za właściwą oraz wystarczającą na potrzeby niniejszego opracowania.

OCENA MERYTORYCZNA

Mając na względzie ocenę merytoryczną dysertacji należy podkreślić, że zawarte w niej treści mają dużą wartość użyteczną - bo m.in. poznawczą, edukacyjną i szkoleniową. To zaś przekłada się na odpowiednie zakresy wiedzy odnoszącej się do funkcjonowania systemu bankowego w kontekście jego bezpieczeństwa.

Część merytoryczna opracowania naukowego, gdzie zawarto wyniki z pracy badawczej, obejmuje rozdziały od drugiego do czwartego oraz zakończenie i bibliografię, a także spisy rysunków, tabel i wykresów oraz kwestionariusz ankiety.

W **drugim** rozdziale *System bezpieczeństwa bankowego w bankach komercyjnych* (ss. 26-50) zostały omówione istotne - z punktu widzenia tematu rozprawy - zagadnienia prawne, infrastrukturalne, proceduralne oraz trendy związane z automatyzacją i robotyzacją systemów wykrywania nadużyć systemowych. Rozważania podjęte przez Autora dotyczą także strukturalnych modeli bezpieczeństwa opartych o czynniki biometryczne i behawioralne.

Na uwagę zasługuje umiejętność analizy kwestii podniesionych w tej części dysertacji i ich prezentacja w kontekście podsumowania, które kończy rozdział, gdzie przyjęto, że „A zatem, (na marginesie) nielegalne działania nie opłacałyby się, gdyby rzeczywisty zysk byłby mniejszy niż mógłby być w wyniku mniej ryzykownych, uczciwych działań" (...)

1. W ten sposób Gary Becker podsumował swój matematyczny wywód dotyczący racjonalności wyborów stosowanych przez przestępców popełniających zbrodnie. Ten wybitny ekonomista zakładał, że zaostrzenie regulacji prawnych w połączeniu z wprowadzeniem zaawansowanych technologicznie systemów teleinformatycznych udaremni próby popełniania nadużyć w sektorze bankowym. Wniosek sformułowany przez Beckera byłby słuszny, gdyby w celu udaremnienia każdego potencjalnego przestępstwa wystarczyłoby stworzyć odpowiedni model oparty na założeniu, że każdy przestępca kieruje się zdroworozsądkową kalkulacją potencjalnego zysku i straty wiążącą się z podejmowanym przez niego działaniem

2. Należy podkreślić, że nie wszystkie działania potencjalnych sprawców mają charakter stricte racjonalny, część z nich może kierować się motywami nieracjonalnymi - nie dających się jednocześnie wyjaśnić najbardziej skomplikowanym modelem matematycznym. W zrozumieniu motywacji działania przestępców może być pomocna wywodząca się z

pogranicza kognitywistyki i nauk społecznych ekonomia behawioralna. Jej czołowy przedstawiciel Richard Thaler zauważył, że (...) „jak na ironię, właśnie dzięki formalnym modelom opartym na niewłaściwym rozumieniu ludzkich zachowań ekonomia cieszy się opinią najpotężniejszej ze wszystkich nauk społecznych"(...). W opinii Autora na bazie założeń ekonomii behawioralnej wykształcone mogą zostać wykorzystywane w bezpieczeństwie bankowym metody, które mają szansę istotnie wpłynąć na poprawę stanu bezpieczeństwa bankowego. Przed systemem bezpieczeństwa bankowego stoją rozmaite wyzwania. Wykazane wyżej trendy wskazują na konieczność sprawnej implementacji rozwiązań prawnych, informatycznych oraz strukturalnych modeli bezpieczeństwa opartych o czynniki biometryczne i behawioralne. Stan bezpieczeństwa banków komercyjnych zależny jest od obecnie stosowanego tempa wprowadzanych rozwiązań. Praktyka wskazuje na to, że proces legislacyjny w za kresie prawa bankowego powinien zostać usprawniony, ponieważ w obecnym stanie ciężar odpowiedzialności za ewentualne nadużycia i zagrożenia bezpieczeństwa spoczywa wyłącznie na bankach komercyjnych. Kłóci się to ze strategią przyjętą przez Komitet Bezpieczeństwa Finansowego przy Generalnym Inspektorze Informacji Finansowej, zakładającą włączenie banków komercyjnych w obszar bezpieczeństwa narodowego. Z uwagi na rację biznesową banki komercyjne same wprowadzają innowacyjne rozwiązania dotyczące zakresu bezpieczeństwa.

Zatem w tej części wyników z badań, proszę o podanie własnych sugestii na rzec rozwiązania problemu, który tu podniesiono.

Trzeci rozdział (ss. 58-67) *Transakcje nieuprawnione w polskich bankach komercyjnych* zawiera definicje, systematykę i podział transakcji nieuprawnionych w Polsce. Rozważania Autora uwypuklają złożoność zagadnień związanych z występowaniem transakcji nieuprawnionych, te mogą znaleźć się pośród wszystkich rodzajów rozliczeń finansowych, co jest zaprezentowane w opisywanym rozdziale.

Na zakończenie jego treści przyjęto, iż „Płynące z powyższych rozważań wnioski uwypuklać mogą jedynie złożoność zagadnień związanych z występowaniem transakcji nieuprawnionych. Transakcje nieuprawnione mogą znaleźć się pośród wszystkich rodzajów rozliczeń finansowych jak i tych, które do tyczyć będą jedynie transferu danych. Wydaje się również, że obecny system prawny nie jest przygotowany na nowe rodzaje zagrożeń. Przeciwdziałanie transakcjom nieuprawnionym rozpoczyna się od ich szybkiego wykrywania a wyniki raportów publikowanych przez Narodowy Bank Polski ewidentnie wykazują relatywnie wysoką skuteczność banków komercyjnych w tym zakresie, co szczególnie dobrze widać na tle innych uczestników rynku finansowego. Występowanie transakcji

nieuprawnionych jest zjawiskiem powszechnym na rynku bankowym. Z uwagi na rozwój systemów transakcyjnych istnieje zagrożenie związane ze zwiększaniem się skali tego zjawiska. Nie sposób nie docenić, jednak inicjatyw Narodowego Banku Polskiego w zakresie ochrony instrumentów rozliczeniowych. Zaangażowanie ze strony władz Banku Centralnego pozwala na określenie rzeczywistej skali występowania nadużyć. Zastanawiająca jest w tym wypadku zauważalna dysproporcja pomiędzy danymi dotyczącymi notowania nadużyć transakcyjnych spływających z banków komercyjnych i agentów płatniczych. Co świadczyć może o lepszym przygotowaniu banków komercyjnych do przeciwdziałania przestępstwom. Zagrożeniem dla wprowadzania nowych koncepcji ochrony systemów płatniczych są niekorzystne z punktu widzenia instytucji finansowych przepisy. Otwartym pozostaje pytanie czy obowiązująca wykładnia dotycząca *Ustawy o usługach płatniczych* nie zniechęca banków komercyjnych do rozwoju systemów płatniczych i niezwykle ważnej edukacji klientów w zakresie dobrych praktyk transakcyjnych wykonywanych przez klientów banków? Rozsądnym wydawać się zatem może stanowisko Związku Banków Polskich nawołujące do reinterpretacji obowiązków płatnika.

Proszę zatem w trakcie obrony w tym kontekście zaprezentować niektóre z tych „reinterpretacji" obowiązki i odnieść się do ich zasadności.

W **czwartym rozdziale** (ss. 68-166) - *Usprawnienia systemu przeciwdziałania transakcjom nieuprawnionym* - celem przeprowadzonych badań było rozwiązanie szczegółowego problemu badawczego zawartego w pytaniu: Jakie powinny być usprawnienia systemu bezpieczeństwa banków komercyjnych w przeciwdziałaniu transakcjom nieuprawnionym? Autor dysertacji prezentuje wyniki badań empirycznych, w których zastosowano metodę sondażu diagnostycznego. Rezultaty przedstawiono w formie graficznej. Ponadto sformułowano wnioski wynikające z odpowiedzi respondentów biorących udział w badaniu. W rozdziale zaproponowano również zastosowanie *Cyberbehawioralnego Modelowania Profili Klientów* jako zalecenia Autora mające pomóc w przeciwdziałaniu transakcjom nieuprawnionym, poprzez zwiększenie zdolności do predykcji zdarzeń przez systemy antyfraudowe. Jest to najważniejszy rozdział spośród innych, gdyż prezentuje ogrom wyników z badań umiejętnie zaprezentowanych w oparciu o liczne zobrazowania i stosowne opisy do tego.

Stąd podczas obrony na bazie sporządzonej tabeli proszę omówić negatywy i pozytywy tego procesu, jakie w trakcie jego funkcjonowania mogą wystąpić. A i wskazać na zalecenia „autorskie" jakie mogą wynikać z przeprowadzonych badań, co do kwestii bezpieczeństwa klientów i samych banków.

Proszę także uzasadnić pogłębioną opinią własną zasadność doboru respondentów – dlaczego tacy i tylu?

W **Zakończeniu** uwypuklono zasadnie to, że „podsumowując badania teoretyczne i empiryczne należy zauważyć, że modele bezpieczeństwa systemów bankowych oparte o czynniki biometryczne i behawioralne stanowią element strukturalnego podejścia do ochrony transakcji. Obecny poziom bezpieczeństwa systemów bankowych jest w znacznej mierze uzależniony od tempa wdrażania rozwiązań technologicznych, w mniejszym zaś stopniu od procesów legislacyjnych W obecnym stanie prawnym odpowiedzialność za zagrożenia i nadużycia spoczywa na bankach komercyjnym, co wydaje się sprzeczne z kierunkiem wyznaczonym przez Komitet Bezpieczeństwa Finansowego przy Generalnym Inspektorze Informacji Finansowej, który zakłada szersze włączenie banków komercyjnych w system bezpieczeństwa narodowego. Dbałość o obszary wymagające poprawy bezpieczeństwa przez banki komercyjne wpływa także na ich reputacje, a ta ma znaczenie także na ich wyniki finansowe. Skuteczne przeciwdziałanie nieuprawnionym transakcjom rozpoczyna się od ich szybkiej identyfikacji. Samo występowanie transakcji nieuprawnionych jest niestety zjawiskiem powszechnym na rynku bankowym. Zauważają to władze Narodowego Banku Polskiego, podejmując działania w zakresie ochrony instrumentów rozliczeniowych. Procesy oparte głównie o gromadzenie danych z rynku bankowego wydają się jednak niewystarczające. Nowe koncepcje ochrony systemów płatniczych mogą spotkać się z niezrozumieniem – *Ustawa o usługach płatniczych* nie zachęca wystarczająco władz instytucji finansowych do rozwoju nowych systemów płatniczych i edukacji klientów w zakresie dobrych praktyk. Oznacza to, że zasadnym byłoby wykorzystywanie dostępnych technologii przy jednoczesnej maksymalizacji wyników monitoringu antyfraudowego. Autor za rozsądne uznaje stanowisko Związku Banków Polskich, by część odpowiedzialności prawnej za zaistnienie transakcji nieuprawnionej scedować na płatnika. Takie rozwiązanie dałoby narzędzia prawne do wprowadzenia Cyberbehawioralnego Modelowania Profili Klientów, który mógłby funkcjonować tylko za zgodą klientów banków".

Nadmieniono tu także, że przyjęte hipotezy zweryfikowały się pozytywnie – co jest stanem faktycznym. I przyjęto także zasadnie, iż „Przedstawione w niniejszej rozprawie wnioski wskazują na potrzebę dalszych badań nad integracją systemów biometrycznych i behawioralnych w ramach strukturalnych modeli bezpieczeństwa transakcyjnego a zaproponowana propozycja *Cyberbehawioralnego Modelowania Profili Klientów* stanowi w istocie pierwszą fazę tworzenia nowego systemu bezpieczeństwa transakcyjnego banków

komercyjnych w obliczu zmieniającego się środowiska zagrożeń i rosnącej roli pieniądza elektronicznego w globalnej gospodarce".

Pracę badawczą wzbogaca **93** wykresy, **32** tabele, **3** rysunki oraz **123** pozycji bibliograficznych, a także **liczne** przypisy dolne, które to pojaśniają zasadnicze kwestie podjęte w trakcie badań, a tym samym podnoszą wartość naukową dysertacji i czytelność podejmowanych kwestii.

Dysertacja w części merytorycznej stanowi dowód na to, że w trakcie badań skorzystano z licznych źródeł, czego ewidencję mamy w bogatej *Bibliografii* oraz przypisach dolnych. Rozprawę zawarto na **188** stronach i jest ona solidnym dziełem naukowym. Stwierdzam, iż tę część rozprawy należy ocenić jako wielce interesującą i konstruktywną w swojej generalnej wymowie. Prowadzone analizy są przekonujące i poprawne logicznie. Pozytywnie oceniając część merytoryczną rozprawy warto podkreślić, że jest ona dobrze ułożona treściowo i napisana poprawnie, a poszczególne tezy są przekonująco uzasadnione – co promuje ją do **wyróżnienia**, o co wnoszę, mimo moich „refleksji".

Konkludując, należy podkreślić, że dysertacja stanowi solidną prezentację wiedzy z obszaru zakreślonego przedmiotem badań oraz jest obszernym zbiorem wyczerpujących treści odnoszących się do kwestii ogólnie pojmowanego bezpieczeństwa w sferze bankowości, która jest istotnym obszarem prawidłowo funkcjonującego państwa demokratycznego w obecnym stanie, jak i pod względem konieczności usprawnienia tego współdziałania organizacyjno-prawnego. Treści zamieszczone i przeanalizowane z wykorzystaniem metod naukowych pretendują Doktoranta do uznania Go za dojrzałego naukowca, który posiada umiejętności badawcze (z wykorzystaniem metod właściwych dla nauk o bezpieczeństwie), doświadczenie zawodowe i panowanie nad obszernym zasobem wiedzy fachowej w wielu kwestiach dotyczących funkcjonowania obszarów bezpieczeństwa.

Doktorant potrafi budować dzieło naukowe na bazie badań – właściwie prezentując kwestie metodologiczne oraz treści merytoryczne rozdziałów, kończąc je wnioskami (w tym wypadku podsumowaniami) z badań zawartych w tych rozdziałach. Ta umiejętność pozwoliła mu przedłożyć do oceny (recenzji) utwór naukowy (jako rezultat w formie rozprawy doktorskiej) o charakterze zwartym, nowatorskim i wyczerpującym główne założenia badawcze, jakie zaprezentowano w części metodologicznej. Obszerne wnioski w części merytorycznej są jego ogromnym atutem w trakcie prezentacji efektów z badań.

WNIOSEK KOŃCOWY

Oceniam rozprawę jako bardzo dobrą, gdyż Doktorant dokonał zasadnie weryfikacji hipotez, rozpracowując trudne problemy badawcze, a uzyskane wnioski istotnie wnoszą na rzecz nauk o bezpieczeństwie. Dysertacja posiada elementy oryginalności, a przy jej opracowaniu użyto poprawnego języka i trafnej terminologii. Pojawiające się w dysertacji drobne potknięcia językowe nie obniżają wartości jej treści oraz użyteczności w praktyce. Pozostaje mieć nadzieję, że postawione tezy i zaproponowane rozwiązania zastosowane w procesie badawczym poddane zostaną weryfikacji przy realizacji sugestii naukowych Doktoranta (które zaproponowano) oraz kolejnych dociekaniach/rozważaniach naukowych z omawianego i badanego przez Doktoranta przedmiotu badań.

Stwierdzam, że przedłożona do recenzji rozprawa doktorska Pana Kamila PRZYŁUSKIEGO jest dojrzałym merytorycznie dziełem promocyjnym, dobrze udokumentowanym poznawczo i logicznie skonstruowanym w dowodowym wykładaniu myśli naukowej. W kontekście kwalifikacji promocyjnych jednoznacznie unaocznia umiejętności autorskie predestynujące Go do samodzielności naukowej. Posiada wyraziste znamiona poznawcze i metodologiczne. Tym samym odpowiada wymaganiom obowiązującej *Ustawy*, określającej wymogi w tym względzie.

Na tej podstawie wnoszę o dopuszczenie Doktoranta do publicznej obrony recenzowanej rozprawy i innych procedur z tym związanych.

.....Ryszard Jakubczak.....