prof. dr hab. Jerzy Wolanin
01-629 Warszawa
ul. Juliusza Słowackiego 52/54
Szkoła Główna Służby Pożarniczej

Warszawa 2018.09.28

**Recenzja**

rozprawy doktorskiej pt. „ Zarządzanie sytuacyjne bezpieczeństwem infrastruktury krytycznej"
mgra inż. Michała Wiśniewskiego

## 1. Formalna charakterystyka rozprawy.

Rozprawa doktorska pana mgra inż. Michała Wiśniewskiego liczy 322 stron wraz 8 załącznikami, przy czym zasadnicza jej część liczy 135 stron. Praca zawiera łącznie 141 pozycji bibliograficznych, spis rysunków i spis tabel. Ważną częścią rozprawy jest umieszczenie na końcu części zasadniczej Tezaurusa pojęć co nadało rozprawie większą przejrzystość. Każdy rozdział kończy się wnioskami, zaś zasadnicza część pracy kończy się podsumowaniem. Od strony czysto formalnej tj. przejrzystości i jasności wywodów, ilustracji ich objaśnień, sposobu przedstawiania danych, a także wyników obliczeń oraz języka w szczególności sformułowań, dotyczących problemów, z którymi autor zmierzył się praca nie budzi najmniejszych zastrzeżeń.

## 2. Merytoryczna ocena rozprawy

2.1 Ocena ogólna

Na wstępie należy zaznaczyć, że podjęta w rozprawie tematyka związana z zarządzaniem bezpieczeństwem infrastruktury krytycznej mieści się obecnie w jednym z najbardziej dynamicznie rozwijającym się obszarze badań jakim w ogóle jest bezpieczeństwo, a w szczególności bezpieczeństwo Infrastruktury Krytycznej. O ile dobrze rozpoznane są podwaliny teoretyczne i praktyczne analizy ryzyka, będącego miarą bezpieczeństwa o tyle cały obszar zarządzanie ryzykiem (bezpieczeństwem), w szczególności w Polsce, wymaga jeszcze dużo wysiłku w sferze nauki i praktyki. Cytując autora (str. 15) „...Stąd problemem badawczym jest opracowanie wspólnego systemu pojęć oraz jednolitej metodyki zarządzania bezpieczeństwem IK możliwych do zastosowania przez wszystkie podmioty odpowiedzialne za bezpieczeństwo IK..."

Rozprawa doktorska pana mgra inż. Michała Wiśniewskiego niewątpliwie stanowi wkład w tę sferę badań i to zarówno teoretyczny jak i praktyczny na poziomie piątego poziomu gotowości technologicznej. Autor „skonstruował" **integralny model bezpieczeństwa IK (IM-BIK)** oraz opracował bazującą na tym modelu **metodykę zarządzania sytuacyjnego bezpieczeństwem infrastruktury krytycznej (ZS-BIK).**Jeżeli chodzi IM-BIK to doktorant opracował jego strukturę, model sytuacji IK, modyfikując definicję sytuacji Kłykowa do potrzeb rozwiązywanego w dysertacji problemu, parametryzując elementy opisujące tę sytuację. Następnie, również w ramach IM-BIK stworzył metodę szacowania ryzyka, w szczególności wprowadzając do definicji ryzyka niezbędne rozszerzenia związane z IK i wreszcie opracował metody generowania scenariuszy, korzystając z prawa Bayes'a, dotyczącego warunkowego prawdopodobieństwa zmaterializowania się zagrożeń. Warto w tym miejscu podkreślić, że generowanie scenariuszy jest niczym innym jak szacowaniem **ryzyka warunkowego** to jest

określanie przebiegu zdarzeń niekorzystnych **pod warunkiem** zmaterializowania się zagrożenia. Jest więc to szczególny przypadek szacowania ryzyka.

Integralny model oprócz samej, według mojej oceny, bardzo dobrej jego koncepcji, uwzględniającej nie tylko „liniowe" przebiegi zdarzeń i zjawisk ale ich wzajemne oddziaływania i sprzężenia, zawiera oryginalny wkład autora w rozwiązywaniu problemów bardziej szczegółowych, o czym w dalszej części recenzji. W modelu, każdej wielkości przypisano atrybuty i ich wartości liczbowe. W celu uczynienia swoich wywodów bardziej klarownymi doktorant posłużył się licznymi przykładami obliczeniowymi, w zasadniczej części rozprawy ze zrozumiałych względów cząstkowymi. Natomiast w załącznikach można zapoznać się z kompleksowymi rozwiązaniami zaproponowanymi w rozprawie. Ściślej mówiąc z pełnymi obliczeniami wykonywanymi dla konkretnych przypadków, a dziwnie nazwanymi przez autora eksperymentami obliczeniowymi. Ostatnim elementem IM-BIK jest opracowanie metod formułowania problemu decyzyjnego. Doktorant w swojej rozprawie wydzielił obszary decyzyjne i ich elementarne decyzje, pary decyzji znajdujących się w relacji pełnej sprzeczności i wyznaczył wagi względnej istotności obszarów decyzyjnych. Kryterium podjęcia problemu decyzyjnego przez zespół analityczny stanowi prognoza według zależności (2.3d i 2.3e) zaproponowanej przez autora i dotyczy wartości określonego progu bezpieczeństwa infrastruktury krytycznej. Włączenie do IM-BIK zagadnień związanych z procesami decyzyjnymi stanowi, w świetle obecnych dyskusji naukowych, istotny wkład w naukę, dotyczącą współczesnego rozumienia analizy ryzyka

Sformułowany przez doktoranta IM-BIK pozwolił mu na opracowanie oryginalnej **metodyki zarządzania sytuacyjnego bezpieczeństwem IK**, i równocześnie na przeprowadzenie studium wykonalności tej metodyki. Metodyka „pracuje na dwóch poziomach zarządzania, mianowicie :płaskim i hierarchicznym. W ramach studium wykonalności wykonał tzw. eksperymenty obliczeniowe. Z treści rozprawy wynika, że są to po prostu obliczenia, dotyczące studium przypadku. Następnie dokonał pozytywnej i tutaj całkowicie należy zgodzić się z autorem rozprawy, oceny metodyki ZS-BIK (zarządzania sytuacyjnego bezpieczeństwem IK)

W podsumowaniu należy uznać, że wyniki uzyskane przez doktoranta w rozwiązywaniu naukowych problemów stanowią oryginalny wkład w rozwój obszaru badawczego związanego z zarządzaniem bezpieczeństwem w szczególności bezpieczeństwem IK. Według mojej oceny stworzona metodyka i metoda zarządzania noszą uniwersalny charakter jako narzędzie mogące służyć do rozwiązywania innych problemów badawczych związanych z bezpieczeństwem takich jak np. konstruowanie matryc odporności (matryc sytuacji kryzysowych).

2.2 Ocena i uwagi szczegółowe

1.W rozdziale „Wprowadzenie w problematykę badań autor formułuje ( w przypisach str. 13) definicję bezpieczeństwa IK, pisząc: "bezpieczeństwo IK-stan IK powstały w wyniku zastosowania zabezpieczeń przed zagrożeniami, w którym prognozowana dostępność funkcjonalności jest wyższa niż próg bezpieczeństwa-...". Wydaje się, że tak sformułowana definicja stanowi tautologię, gdyż definiując *bezpieczeństwo* odwołujemy się do jego charakterystyki mianowicie *progu bezpieczeństwa* (podobnie jak w definicji prawdopodobieństwa Laplace'a). Jeżeli przeanalizować całość rozprawy, to widać, że wszelkie opracowane przez doktoranta metodyki, metody, włączając w to zarządzanie, a nawet metoda generowania scenariuszy dotyczą analizy ryzyka. Zasadniczym przedmiotem badań jest więc bezpieczeństwo nierozerwalnie związane z ryzykiem. Zresztą autor nie miał innego wyjścia bo ryzyko i bezpieczeństwo stanowią integralną całość. To że autor jest tego świadomy świadczą

następujące cytaty z jego rozprawy. Str.50 cytat"... Na podstawie uzyskanego poziomu ryzyka prognozowana jest dostępność funkcjonalności IK w sytuacji wystąpienia określonego zagrożenia oraz na tej samej stronie „...jeśli tylko ryzyko związane SZN (*przyp. rec. scenariusz zdarzeń niekorzystnych)* nie pozwala na osiągnięcie progu bezpieczeństwa formułowany jest problem decyzyjny...". Str. 59 Podstawowym miernikiem dla IM-BIK jest ryzyko utraty funkcjonalności..."Str. 60 „...Podatność IK na zagrożenie zwiększa lub zmniejsza ryzyko związane z zagrożeniem..." Na marginesie ostatniego cytatu wydaje się, że podatność nigdy nie zmniejsza ryzyka związanego z jakimkolwiek zagrożeniem. Do pojęcia podatności odniosę się jeszcze w dalszej części recenzji. Tak, więc wracając do zasadniczego wątku rozważań czyli definicji bezpieczeństwa, warto się zastanowić czy nie lepiej jest zdefiniować bezpieczeństwo IK w następujący sposób: *bezpieczeństwo IK – stan powstały w wyniku zastosowania zabezpieczeń przed zagrożeniami, w którym prognozowana dostępność funkcjonalności jest wyższa niż wynika to z akceptowanej wartości ryzyka jej utraty.* Natomiast wartość akceptowanego ryzyka określa próg bezpieczeństwa. Z tej definicji bezpośrednio wynikają opracowane przez doktoranta zależności i kryteria bezpieczeństwa (2.3d) oraz (2.3e) str. 64i 65. Reasumując ryzyko jest miarą bezpieczeństwa, charakteryzującą stan otoczenia (w naszym przypadku przez otoczenie rozumie się IK). I stąd cała praca poświęcona w całości jest ryzyku i zarządzaniu nim, co jak widać jest rzeczą naturalną.

2. W przypisach na str.29 w zdaniu kończącym definicję progu bezpieczeństwa autor pisze "...i ważnych z punktu widzenia bezpieczeństwa państwa...". Moim zdaniem ta przesłanka zawarta jest w definicji IK (str. 23) i tutaj jest zbędna. Ponadto, na str. 33 autor w przypisach niepotrzebnie powtarza tę samą definicję

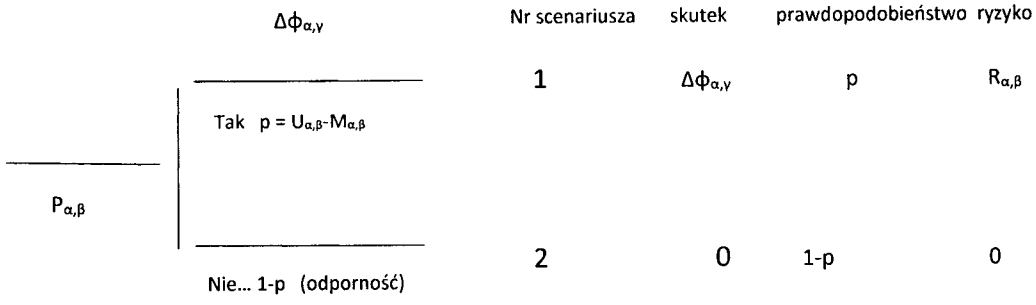
3.Na str.28 autor w sposób szczegółowy analizuje niedostatki obecnego procesu planowania cywilnego (np. brak wskazania technik i metod dedykowanych do osiągnięcia założonych celów, żeby wymienić najważniejszą z nich) i równocześnie wskazuje na rolę IM-BIK w ich likwidowaniu. Należy podkreślić, że faktycznie w chwili obecnej problemy przeanalizowane przez autora stanowią jedne z największych trudności przy wykonywaniu planów na każdym szczeblu administracji publicznej. Również należy się z nim zgodzić, że IM-BIK zaproponowany przez doktoranta te problemy rozwiązuje.

4. Jak już wspomniano na wstępie autor w celu lepszego zobrazowania swoich rozważań umieścił w pracy liczne tabele i rysunki. Do szczególnie wartościowych należą te, które podsumowują opisaną w danym rozdziale koncepcję. Do nich należy zaliczyć: tabelę pt. *Program realizacji zadań (str.20)*, rys.1.2c *Zależność etapów metodyki ZS-BIK od elementów modelu IM-BIK,* tabele od 1.4a do 1.4c.str. 40-41), rys. 2.2b (str. 54). Ilustracje te są integralną częścią koncepcji opracowanej i prezentowanej przez pana mgra inż. Wiśniewskiego w rozprawie.

5. Pewnych wyjaśnień wymaga koncepcja *podatności.* W przypisach na str. 49 autor pisze za Krupą i Ostrowską „...podatność (U) inaczej uległość jest przeciwieństwem odporności ( R ) rozumianej jako podstawowa cecha infrastruktury krytycznej ($IK_\alpha$) co wyraża się wzorem (U=1-Re) [Krupa, Ostrowska,2017, s 59-60]. A dalej na str. 60 „...Podatność jest rozumiana jako wrażliwość IK na działanie niekorzystnych czynników (zagrożeń), która wynika z cech konstrukcyjnych IK. Na tej samej stronie autor wprowadza pojęcie *stopień podatności.* Natomiast na str. 67 czytamy *„...Podatność IK na zagrożenie jest interpretowane jako prawdopodobieństwo, że zastosowane zabezpieczenia nie ochronią IK przed skutkami zagrożenia...".* W pierwszej definicji podatność definiowana jest przez odporność przy czym ta

ostatnia nie jest w rozprawie zdefiniowana. Druga definicja nic nie wnosi, gdyż zastępuje pojęcie podatności pojęciem wrażliwości przy czym autor nie definiuje tej ostatniej. Wydaje się, że najbardziej trafna jest ostatnia interpretacja podatności jako prawdopodobieństwa, ale według mnie, prawdopodobieństwa powstania określonych skutków dla danego zagrożenia bez względu czy IK posiada zabezpieczenia, czy też ich nie posiada. Jeżeli by przyjąć podaną przez autora ostatnią definicję bez poprawek to systemy IK, które nie są poddane zabezpieczeniom albo wypadają z tej definicji albo należy uznać, że nie są na nic podatne U=0, co jest sprowadzeniem ad absurdum. Tak, więc porządkując warto się zastanowić, nad następującą definicją podatności: **Podatność IK na zagrożenie jest interpretowane jako prawdopodobieństwo powstania określonych skutków (w przypadku rozprawy skutkiem jest częściowa wyrażona w % utrata funkcjonalności) w wyniku wystąpienia tego zagrożenia.** Z zaproponowanej definicji wynika, że faktycznie wartość prawdopodobieństwa wystąpienia skutków określonej wielkości jest fundamentalną charakterystyką IK zgodnie z wprowadzoną przez Krupę i Ostrowską definicją podatności i nie jest z tą definicją sprzeczna. Interpretując podatność jako prawdopodobieństwo wystąpienia określonego skutku (utraty funkcjonalności) nie ma potrzeby wprowadzać pojęcia stopnia podatności. Natomiast, wydaje się że definicję podatności określanej jako wrażliwość należy odrzucić w całości. Po pierwsze, zastąpienie słowa podatność na wrażliwość nic nie wnosi. Po drugie, wrażliwość na ogół określa się jako wielkość reakcji układu na zmiany w otoczeniu (lub np. na wielkość zmiany wartości wyników obliczeń w modelu danych wyjściowych w rezultacie zmiany danych wejściowych). Czym układ jest wrażliwszy, tym większe zmiany w układzie przy określonych zmianach w otoczeniu.

6. Fundamentalną formułą obliczeniową w IM-BIK jest wzór 2.3b (str. 60).Od razu należy zaznaczyć, że ponieważ we wzorze występuje różnica (odejmowanie) -od podatności odejmuje się wpływ zabezpieczeń- to już w tym miejscu należy dodać warunek, że dla $U_{\alpha,\beta} \leq M_{\alpha,\beta}$ różnica $U_{\alpha,\beta}-M_{\alpha,\beta} = 0$, jako warunek immanentnie przypisany do wzoru, a nie dopiero trzy strony dalej i to w przypisach. Wówczas zaproponowana metoda obliczeń pozbawiona jest tej osobliwości. Pomysł zinterpretowania skutków w klasycznym wzorze, określającym ryzyko jako zmianę funkcjonalności faktycznie stanowi nowe i zarazem oryginalne podejście do ilościowego ujęcia analizy ryzyka. Ta interpretacja nie budzi najmniejszych zastrzeżeń. . Natomiast wprowadzenie do wzoru podatności i wpływu zabezpieczeń wymaga sprawdzenia, czy w świetle istniejących metod, stanowiących kanon analizy ryzyka definicja zaproponowana przez doktoranta (wzór 2.3b) może mieć zastosowanie, to znaczy czy dalej jest to ryzyko. Warto się zastanowić nad tym, że skoro podatność jest *prawdopodobieństwem* utraty części funkcjonalności jako *skutku* wyrażonej w % (ułamku) i równocześnie poprzez zabezpieczenia




to prawdopodobieństwo można zmniejszyć (zmniejszyć podatność), to czy poprzez pomnożenie tych wielkości dalej będziemy mieli do czynienia z ryzykiem? Na rysunku

przedstawiono możliwość wyprowadzenia formuły 2.3b poprzez zastosowanie takiego klasycznego narzędzia analizy ryzyka, jakim jest drzewo zdarzeń. Metodę tę można w tym przypadku zastosować, ale tylko pod warunkiem zaproponowanej interpretacji podatności z uwzględnieniem lub nie zabezpieczeń jako prawdopodobieństwa wywołania określonego skutku $\Delta\phi$ . Wynik tej analizy pokazuje, że zmodyfikowany wzór na ryzyko wskazany przez doktoranta obejmuje: jeden z możliwych scenariuszy, określa prawdopodobieństwo i skutek zmaterializowania się zagrożenia, a więc stanowi triplet {scenariusz, p, C} Garrick'a – Kaplana, którzy w 1981 w ten klasyczny już sposób zdefiniowali ryzyko. Zależność 2.3b określa zatem wielkość rzeczywiście będącą ryzykiem. Ponieważ zależność tę można uzyskać poprzez analizę drzewa zdarzeń, niekoniecznie musiała być w rozprawie wprowadzona heurystycznie. Tak, więc osiągnięciem doktoranta nie jest sam zmodyfikowany wzór, ale po pierwsze, wprowadzenie zmiennej losowej $\Delta\phi$ tj. % utraty funkcjonalności oraz liczbowe ujęcie charakterystyki IK jaką jest podatność, a także liczbowe ujęcie wpływu zabezpieczeń zmniejszających podatność. Jeżeli mówić o zmodyfikowanym wzorze, jako twórczego wkładu doktoranta w rozwiązanie postawionego przez siebie problemu, to raczej w kontekście dostosowania do potrzeb rozwiązania problemu, wprowadzeniu wspomnianych wyżej wielkości i ich interpretacji. Niewątpliwie jest to nowe oryginalne podejście w zakresie analizy ryzyka.

7. *Warto podjąć dyskusję na temat poruszony w tym punkcie*. Na str. 61 autor podaje wzór na sumę ryzyk dla danej funkcjonalności, a pochodzących od różnych zagrożeń dla kilku rodzajów IK mających na nią wpływ. Sam wzór oczywiście nie budzi zastrzeżeń, ale jeśli się weźmie pod uwagę zależność 2.3d (str64), dotyczący prognozowanej funkcjonalności, to jego interpretacja powoduje, że pojawiają się pewne wątpliwości. Pierwszy sygnałem jest możliwość przekroczenia sumy ryzyk wartości 100%. Jeżeli tak rozumianą sumę ryzyk traktować jako % utraty funkcjonalności, jak to sugeruje autor, to jest kłopot interpretacyjny co oznacza utrata funkcjonalności ponad 100%. Z pomyślanego przez autora modelu taki wynik nie powinien mieć miejsca. Aby przedyskutować ten problem należy się cofnąć do zmodyfikowanego przez autora wzoru na ryzyko. Widać z niego, że maksymalna wartość ryzyka wynosi 1 lub 100%. Równocześnie skutki (utrata funkcjonalności) też wyrażone są w procentach, ale to są „inne" procenty niż prawdopodobieństwo wystąpienia tych skutków i według mojej opinii nie wolno ich w ten sposób sumować. Z przykładów podanych na stronie 64 widać, że każde zagrożenie ma inne prawdopodobieństwo powstania, inny skutek oraz inną podatność po uwzględnieniu wpływu zabezpieczeń. Sumując otrzymujemy wartość całkowitego ryzyka, która jak wynika z rozprawy jest niezbędna np. przy określaniu istotności obszaru decyzyjnego. Ale całkowite ryzyko nie jest prognozowaną wartością utraty funkcjonalności. To właśnie w tym miejscu widać, że przy odpowiednio dużych (bliskich jedności) wartościach wielkości występujących w zmodyfikowanym wzorze na ryzyko, suma ta może przekroczyć 100%, prowadząc do paradoksu. Problem ten można rozwiązać poprzez zdefiniowanie ryzyka utraty określonej wartości funkcjonalności jako wartości oczekiwanej. Utrata części danej funkcjonalności jest dyskretną zmienną losową z określonymi wagami dla każdego rodzaju zagrożenia. Wagi te równe są iloczynowi prawdopodobieństwa zmaterializowania się zagrożenia $P_{\alpha,\beta}$ i podatności z uwzględnieniem zabezpieczeń dla każdego zagrożenia (przykład str. 63).

$$E(\Delta\emptyset_{\alpha,\gamma}) = \sum_{\beta}^{n} R'_{\beta}$$

gdzie $R_{'\beta}$ jest ryzykiem utraty określonej wartości funkcjonalności z wagą wynikającą z normalizacji wag pochodzących od każdego zagrożenia i zmodyfikowanej podatności.

I tak w przykładzie ze str. 76 (dotyczy to również przykładów ze stron 61 oraz 63) mamy:

a. Prawdopodobieństwo utraty funkcjonalności 30% od pierwszego zagrożenia wynosi 0.5x0.7=0.35

b. Prawdopodobieństwo utraty funkcjonalności 10% od drugiego zagrożenia wynosi 0.4x0.8=0.32

c. Prawdopodobieństwo utraty funkcjonalności 15% od trzeciego zagrożenia wynosi 0.35x0.65 = 0.23

Dzieląc poszczególne prawdopodobieństwa przez ich sumę otrzymuje się wagę wkładu utraty funkcjonalności danego zagrożenia. Sumując iloczyny poszczególnych wag i przypisanych im procentów utraty funkcjonalności otrzymuje się wartość oczekiwaną utraty funkcjonalności (średnią geometryczną). Tak, więc 0.35+0.32+0.23 =0.9 stąd

$$E(\Delta\emptyset_{\propto,\gamma}) = \left(\frac{0.35}{0.90}\right)x30\% + \left(\frac{0.32}{0.90}\right)x10\% + \left(\frac{0.23}{0.90}\right)x15\% = 19.1\%$$

Wartość oczekiwana utraty funkcjonalności wynosi więc 19.1%, a nie jak podaje autor 17.113%. To właśnie tak policzone ryzyko (jako wartość oczekiwana) można zastosować do wzoru 2.3d tj. wzoru prognozującego dostępność funkcjonalności w określonym okresie. Jeśli te rozważania są poprawne, to poprawek wymagają te kolumny w tabelach, które prognozują poziom funkcjonalności np. tabela 2.5d str. 81, czy też tabela 3.4g str. 112.

Oczywiście wprowadzenie wartości oczekiwanej utraty funkcjonalności nie wpływa na konstrukcję modelu i zarządzania nim. Dotyczy tylko obliczeń, związanych z progiem bezpieczeństwa, a tym samym określenia obszarów (problemów) decyzyjnych.

3. **Uwagi szczegółowe techniczne**

Str. 127 błąd drukarski „...płaskiego problemu decyzyjnego **poległ** na...."

Str. 129 błąd drukarski „...proces panowania cywilnego..."

**Podsumowanie**

Doktorant mgr inż. Michał Wiśniewski opracował oryginalny model IM-BIK, będący jego autorskim pomysłem. Model zawiera wiele nowych opracowanych przez autora elementów rozszerzających metody analizy ryzyka. Wprowadził ilościowe mierniki zmiennej losowej jaką jest funkcjonalność, Również wprowadził i zinterpretował mierniki podatności i wpływu zabezpieczeń. To, co jest również istotne to jest uwzględnienie w modelu wzajemnych zależności między poszczególnymi rodzajami IK oraz między różnymi zagrożeniami. adoptował model sytuacji Kłykowa, ustalając kanon sytuacji IK. Zdefiniował podstawowe atrybuty zagrożeń ich zależności, podstawowe atrybuty funkcjonalności oraz atrybuty zależności IK a także atrybuty zabezpieczeń. Taki zabieg pozwolił autorowi „wyjść" na ilościową analizę ryzyka w oparciu zmodyfikowany wzór na ryzyko. Z IM-BIK nierozerwalnie związane są procesy decyzyjne, które w ujęciu autora, bazując na zaproponowanej przez niego analizie ryzyka, również mają charakter ilościowy. Model jest na tyle uniwersalny, że może być zastosowany w wielu obszarach bezpieczeństwa w szczególności bezpieczeństwa na terenie jednostek administracji publicznej (nie tylko z punktu widzenia IK) i to zarówno z płaskiego jak i hierarchicznego poziomu decyzyjnego. Integralną częścią IM-BIK jest zaproponowana przez doktoranta metodyka zarządzania sytuacyjnego bezpieczeństwem IK zilustrowana na

przykładzie studium wykonalności. Wyniki pracy pozwalają również na sformułowanie dalszych prac nad omawianą w rozprawie problematyką.

Pomimo wskazanych wyżej uwag i wątpliwości niemających fundamentalnego znaczenia dla całej koncepcji rozprawy pracę należy ocenić pozytywnie. Autor wykazał się znajomością przedmiotu badań. Potrafił twórczo rozwiązywać problemy i to zarówno natury koncepcyjnej jak i bardziej szczegółowych. Stworzył oryginalną domkniętą w sposób logiczny koncepcję, rozwijającą w sposób istotny narzędzia analizy ryzyka.

Mgr inż. Michał Wiśniewski w pełni zasługuje na uzyskanie stopnia naukowego doktora. W związku z powyższym wnioskuję o dopuszczenie doktoranta do publicznej obrony.