Dr hab. inż. Jerzy Tchórzewski, prof. nzw. UPH
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Ścisłych, Instytut Informatyki
Pracownia Sztucznej Inteligencji, 08-110 Siedlce, ul. 3-Maja 54
Adres do korespondencji: 08-110 Siedlce, ul. Starowiejska 47a

Warszawa, 08.01.2018 r.

Dotyczy: Umowa nr 0009/11/W5/2017 na opracowanie recenzji

Recenzja rozprawy doktorskiej dla Rady Wydziału Elektrycznego Politechniki Wrocławskiej

Tytuł rozprawy: **Bezpieczeństwo cyfrowe inteligentnych dystrybucyjnych sieci elektroenergetycznych**

Autor rozprawy: **Mgr inż. Robert Czechowski**

Promotor: **Prof. dr hab. inż. Eugeniusz Rosołowski, prof. zw.**

Promotor pomocniczy: **dr inż. Piotr Pierz**

Miejsce i data wydania rozprawy: **Katedra Energoelektryki Wydziału Elektrycznego Politechniki Wrocławskiej, Wrocław, 21 listopada 2017 r.**

1. Autor rozprawy w sposób jasny i wyczerpujący sformułował ogólny cel rozprawy jako:

„udowodnienie, że główną rolą wdrożenia systemu detekcji ataku docelowo jest informowanie o tym administratora systemu w celu podjęcia przez niego działań mających na celu minimalizacje negatywnych skutków powstałych w wyniku przeprowadzenia udanego ataku",

oraz tezę rozprawy:

„uwzględnienie nowoczesnych metod bezpieczeństwa cybernetycznego w procesie projektowania i eksploatacji układów teleinformatyki i automatyki elektroenergetycznej, ograniczy skutki zamierzonych i przypadkowych ataków na obiekty elektroenergetyczne i przyczyni się do zwiększenia bezpieczeństwa pracy systemu elektroenergetycznego".

Realizacja ww. tezy rozprawy w celu osiągnięcia konkluzji, tj. jest w celu ograniczenia skutków ataków na obiekty elektroenergetyczne i wpływu na zwiększenie bezpieczeństwa pracy systemu elektroenergetycznego jest udowadniania w oparciu m.in. o cztery zasadnicze przesłanki (potraktowane także w pewnym sensie jako tezy pierwotne), to jest:

1) rozwój inteligentnych sieci elektroenergetycznych dzięki coraz to większej integracji z systemami ICT przyczynia się do sprawniejszego nimi zarządzania, ale zwiększa jednocześnie ich podatność na ataki,

2) wdrożenie i stosowanie polityki bezpieczeństwa jest najważniejszym elementem w planowaniu strategii bezpieczeństwa dedykowanej systemom elektroenergetycznym,

3) stosowanie indywidualnych i nieszablonowych rozwiązań bezpieczeństwa opartych na technice cyfrowej (certyfikowanych i opartych na otwartych protokołach), zapewnia najwyższy możliwy do osiągniecia poziom bezpieczeństwa systemu.

4) stosowanie zbyt skomplikowanych mechanizmów zabezpieczeń z czasem powoduje, że osoby sprawujące nad nimi nadzór same zaczynają je w pewien sposób omijać, co często prowadzi do powstawania luk w polityce bezpieczeństwa, a zatem cyberbezpieczeństwo i stopień jego implementacji stanowią pewnego rodzaju kompromis pomiędzy budżetem, skomplikowaną obsługą oraz wydajnością.

Na bazie ww. czterech przesłanek (tez podstawowych) Doktorant sformułował szczegółowy cel pracy, którym jest:

„opracowanie i przedstawienie rozwiązań oraz zasad podejmowania możliwych (automatycznych) działań w sieciach inteligentnych w odpowiedzi na cyberataki i zakłócenia zewnętrzne w celu złagodzenia ich skutków",

oraz cel uzupełniający, którym jest:

„jednoczesne przedstawienie zbioru zasad w komunikacji cyfrowej wszystkich komponentów i podmiotów uczestniczących w sterowaniu i zarządzaniu siecią elektroenergetyczną".

Ww. wymiarze rozprawę doktorską można traktować jako analizę i dobór koncepcji oraz wytycznych sformułowanych w celu fizycznego zapewnienia bezpieczeństwa cyfrowego operatorów inteligentnych sieci elektroenergetycznych z zakresu Smart Grid i Smart Metering, a zatem ma ona charakter aplikacyjny poprzedzony m.in. opracowaniem:

- koncepcji polityki bezpieczeństwa inteligentnych sieci elektroenergetycznych, konstrukcji sieci inteligentnych z punktu widzenia logicznej struktury jako architektury Smart Grid,
- pięciu modeli sieci o różnym stopniu skomplikowania i różnym obszarze funkcjonowania inteligentnych sieci elektroenergetycznych, wraz z opisem stanowisk laboratoryjnych, procedur testowych, badań symulacyjnych, itp.,

- poziomu szacowana ryzyka i oceny zagrożeń oraz aktualnych technik bezpieczeństwa Smart Grid, itp.

2. Doktorant wykazał się wystarczającą wiedzą z zakresu bezpieczeństwa cyfrowego inteligentnych sieci elektroenergetycznych, gdyż w trakcie realizacji rozprawy opublikował 32 prac ogółem[1], których był autorem lub współautorem, z tego:

- 20 publikacji naukowych (artykuły naukowe punktowane na liście filadelfijskiej Web of Science (lista A) - 4, artykuły punktowane na liście filadelfijskiej ministerialnej (lista B) - 5 oraz referaty naukowe recenzowane – 11),
- 11 sprawozdań z prac naukowych,
- jedną pracę na zasadzie preprintu.

Na uwagę zasługuje też fakt, iż w toku realizacji rozprawy Doktorant zgromadził i wykorzystał dane liczbowe (zanonimizowane) pozyskane od jednego z dystrybutorów energii elektrycznej w Polsce oraz wykorzystał 125 prac zamieszczonych w wykazie literatury przedmiotu, które zostały w sposób wystarczający omówione w rozprawie, z tego 88 książek, artykułów i recenzowanych referatów naukowych, 11 ustaw, rozporządzeń, zarządzeń, itp., 6 raportów oraz 20 publikacji zamieszczonych na stronach internetowych.

W zasadzie opracowana rozprawa nosi charakter samodzielnej monografii naukowej, napisanej w sposób profesjonalny, uzupełnionej o rozwiązania o charakterze aplikacyjnym, stąd już na wstępie pragnę zauważyć, że zasługuje na wyróżnienie.

Rozprawa została napisane na 239 stronach formatu A4 o strukturze 9 zasadniczych części, na które składają się podziękowania i streszczenia w języku polskim oraz w języku angielskim, wstęp, sześć zasadniczych rozdziałów zatytułowanych:

Rozdz. 1. Polityka Bezpieczeństwa Inteligentnych Sieci Elektroenergetycznych,

Rozdz. 2. Logiczna architektura Smart Grid,

Rozdz. 3. Badania i symulacje,

Rozdz. 4. Analiza ryzyka i ocena zagrożeń,

Rozdz. 5. Techniczne rozwiązania cyfrowej ochrony ISE

Rozdz. 6. Wnioski i uwagi końcowe,

[1] Wykazanych w bazie DONA (Centrum Wiedzy i Informacji Naukowo-Technicznej Politechniki Wrocławskiej) – dostęp w dniu 08.01.2018 r.

a także bibliografia, wykaz rysunków w liczbie 122 oraz zamieszczony na 15 stronach wykaz skrótów i oznaczeń wykorzystanych w rozprawie.

Omawiając Politykę Bezpieczeństwa Inteligentnej Sieci Elektroenergetycznej (ISE) Doktorant wykazał m.in., że wprowadzenie nowoczesnego standardu zarządzania sieciami ma wpływ na zmiany dotychczasowych wzorców konsumpcji energii, oraz sprawia, że wzrasta świadomość odbiorców w zakresie poszukiwania możliwości bardziej efektywnego wykorzystania energii elektrycznej tak przez podmioty indywidualne, w tym przez konsumentów i gospodarstwa domowe, jak też przez podmioty zbiorowe, w tym instytucje publiczne.

Wskazał też, że pomimo wielu obaw związanych z modernizacją sieci elektroenergetycznej, lepsze i bardziej ukierunkowane nimi zarządzanie poprzez zastosowanie teleinformatycznych środków ochrony informacji i bezpieczeństwa systemów bazodanowych może przyczynić się do zwiększenia jej bezpieczeństwa i efektywności, a to bezpośrednio przekłada się na potanienie m.in. eksploatacji i potanienie energii elektrycznej u końcowego odbiorcy.

Doktorant zauważył też m.in., że ważną zaletą ISE jest możliwość przystosowania jej do istniejącego systemu elektroenergetycznego w celu zwiększenia efektywności zarządzania poprzez scalenie: rozproszonej generacji, instalacji odnawialnych źródeł energii, systemów magazynowania energii oraz w rezultacie zwiększenie efektywności i sprawności całego systemu elektroenergetycznego.

Autor wyczerpująco omówił w rozprawie wyniki analizy stanu literatury przedmiotu, jasno określił stan wiedzy w zakresie badanej tematyki, to jest m.in. w zakresie rozwoju technologii teleinformatycznych w różnych systemach elektroenergetycznych, w tym wskazał rolę podejścia typu Smart Grid i Smart Matering, jak też ich rolę w zakresie zapewnienia bezpieczeństwa odbiorców energii elektrycznej.

Autor bardzo dokładnie opisał źródła zagrożeń, wyspecyfikował najczęściej spotykane problemy związane z projektowaniem architektury sieci inteligentnych i jej zarządzaniem oraz opisał główne motywy ataków na sieć inteligentną.

Pan mgr inż. Robert Czechowski wskazał m.in., że ataki na system elektroenergetyczny oraz na sieć elektroenergetyczną mogą przybierać różne formy, czas działania, czas przygotowania do ataku, miejsce powstania, czy zaangażowane do tego celu środki oraz zauważył, że przekształcenie obecnej struktury sieci elektroenergetycznej w sieć inteligentną

wymusza wprowadzenie szeregu nowych rozwiązań ochrony wzorowanych na już stosowanych rozwiązaniach, dotyczących typowych problemów współczesnych urządzeń informatyki takich jak hacking, kradzież danych, a nawet cyberterroryzm (atak na wszelaką informację cyfrową, sygnały sterujące procesami teleinformatycznymi, urządzenia i media transmisji danych odpowiedzialnych za poprawne działanie dystrybucji energii i zarządzania systemem elektroenergetycznym, itp.), które zostały już w sposób właściwy sformułowane w polskim kodeksie karnym.

Cyberbezpieczeństwo stało się ważne z racji zwracania coraz to większej uwagi nie tylko na niezawodność funkcjonowania systemu elektroenergetycznego, ale również na stosowanie w systemie rozwiązań teleinformatycznych w celu poprawy skuteczności i efektywności działania systemu oraz zwiększenia poziomu bezpieczeństwa jego działania.

Autor dokonał przeglądu literatury przedmiotu w zakresie cyberterroryzmu na świecie zwracając m.in. uwagę na fakt gwałtownego wzrostu liczby cyberataków z roku na rok wskazując, że w 2010 r. odnotowano ich zaledwie 50, a już w 2015 ich liczba wzrosła aż do 138, przy czym średni czas wykrycia ataku wynosi aż 170 dni, czas usunięcia skutków aż 45 dni, a koszt usunięcia jest nadal bardzo wysoki i średnio wynosi 1.6 mln USD. Zwrócił też uwagę na możliwość wywołania cyberatakiem blackout-u i awarii sieci szkieletowej, co jest nowych zjawiskiem w funkcjonowaniu systemu elektroenergetycznego.

Doktorant w sposób właściwy zwrócił uwagę na stan literatury przedmiotu w zakresie opisu wyników analizy cyberataków stosowanych na systemy i sieci elektroenergetyczne, wskazując też na inne przyczyny backout-ów niż cyberataki, np. spowodowane awariami sieci w wyniku wystąpienia kilku zdarzeń losowych, awarii sieciowych, wyłączeniem elektrowni, wystąpieniem ekstremalnych warunków atmosferycznych, a także zwykłymi błędami ludzi obsługujących urządzenia.

Jednakże pewnym niedociągnięciem rozprawy jest zbyt skromne zaprezentowanie wyników analizy literatury przedmiotu w zakresie rozwiązań z obszaru elastycznych i zrobotyzowanych systemów automatyki, które obok teleinformatyki i automatyki zabezpieczeniowej mają bezpośredni wpływ na fakt uznawania, że sieć lub system elektroenergetyczny staje się typu Smart Grid lub Smart Power System, co generalnie nie umniejsza wartości rozprawy, której ocena jest wysoka, ale ww. uzupełnienie mogłoby stanowić właściwą równowagę pomiędzy wkładem rozwiązań hardware-owych w rozwiązaniach software-owych wyczerpująco wykazanych w rozprawie.

3. Pan mgr inż. Robert Czechowski rozwiązał sformułowane zagadnienie, tezy udowodnił, cele osiągnął. Wykazał m.in., że nowa infrastruktura inteligentnych sieci elektroenergetycznych, zbudowana według nowej koncepcji, przyniesie operatorom sieci dystrybucyjnej nie tylko nowe dane pomiarowe, czy też statystyczne, z których dany dostawca będzie mógł korzystać w celu poprawy jakości usług lub zwiększenia zysków, ale zapewni też spełnienie nowych wyzwań związanych z bezpieczeństwem jej funkcjonowania, w tym w zakresie przeciwdziałania zagrożeniom w przypadku ingerencji cyberprzestępców, gdyż technologie Smart Grid wprowadzają do sieci elektroenergetycznej wiele nowych komponentów bardzo ważnych dla interoperacyjności i niezawodności jej funkcjonowania.

Do oryginalnych rozwiązań rozprawy można zaliczyć m.in.: zbadanie pięciu różnych modeli symulacyjnych, których analiza może pozwolić na zrozumienie i poznanie niekorzystnych zjawisk występujących w sieciach elektroenergetycznych, w szczególności mających duży wpływ na skuteczność transmisji jak i bezpieczeństwo wymiany informacji, to jest stanowisk laboratoryjnych, procedur testowania, różnych wariantów symulacji oraz wyników badania, to jest następujących modeli:

- trzech modeli rzeczywistej sieci inteligentnego opomiarowania:
  - modelu 1 - modelu BPL do obserwacji utraty i nawiązywania połączenia przez liczniki energii elektrycznej wyposażonych w moduły komunikacyjne (badanie zachowania się na zmianę warunków panujących w sieci typu wyłączanie i załączanie źródeł światła, silników i falowników, itp.) w celu m.in. sklasyfikowania rodzajów zakłóceń),
  - modelu 2 - modelu Smart Matering PLC do dynamicznej zmiany topologii sieci z uwzględnieniem urządzeń stanowiących o ich hierarchii w sieci,
  - modelu 3 – modelu Smart Matering PLC odzwierciedlającego wpływ zakłóceń na komunikację cyfrową, w tym także na autokonfigurację urządzeń, połączenia automatyczne w celu dynamicznej zmiany połączeń transmisyjnych w ślad za dynamiczną zmianą topologii sieci),

  wraz z uwzględnieniem testów stabilności i statystyk zdarzeń logicznych,

- modelu 4, to jest modelu teoretycznego infrastruktury teleinformatycznej ICT (opartego o dane rzeczywiste), odzwierciedlającego wspieranie procesów kontrolno-sterujących oraz wymagania i agregację danych, zaprojektowanego z wykorzystaniem oprogramowania

CySeMoL4, mającego na celu umożliwienie przeprowadzenia analizy potencjalnych zagrożeń, które mogą wynikać z ataków cybernetycznych ukierunkowanych na infrastrukturę elektroenergetyczną i informatyczną systemów sterowania i systemów pomiarowych,

– modelu 5, to jest modelu referencyjnego sieci dystrybucyjnej typu ATP - EMTP5, umożliwiającego pomiar wskazanych przez użytkownika przebiegów chwilowych prądów, napięć, mocy i energii elektrycznej oraz wybranych parametrów mechanicznych w celu szybkiej i automatycznej rekonfiguracji sieci przy jednoczesnym odizolowaniu części uszkodzonych.

Na podstawie analizy ww. pięciu modeli Autor wykazał, że możliwa okazała się ocena bezpieczeństwa i ocena ryzyka zagrożeń oraz ich skutki dla poszczególnych rodzajów badanych zakłóceń i celowych ataków. Autor wykazał ponadto, że modele pozwalają również na przeprowadzenie analizy dla bardzo dużej liczby wariantów scenariuszy awarii systemu oraz wielu analiz działań zmierzających do samoczynnego i automatycznego przywrócenia funkcjonowania sieci elektroenergetycznej nie objętej awarią. Wykazał też, że poddane analizie modele umożliwiają pozyskanie materiału badawczego w celu dokładniejszej i wielokryterialnej analizy ataków zgodnie z przyjętymi scenariuszami.

Doktorant przeprowadził ponadto wyczerpujące badania w zakresie szacowania ryzyka, w tym w zakresie analizy i oceny prawdopodobnego wystąpienia zagrożeń na przykładach różnych scenariuszy ataku, np. na pojedynczy obiekt składowy, na cały systemu jak i na związane ze zmianą nastawień układy automatyki pomiarowej i automatyki zabezpieczeniowej, w tym związane z przesterowaniem wartości progowych, które mogą doprowadzić do zapaści systemu elektroenergetycznego i w efekcie doprowadzić do wielkoobszarowych awarii systemowych (tzw. blackout-ów).

Autor pokazał ponadto wyniki badania ataków m.in. na sieć szkieletową, na teleinformatyczne centrum operatora, a także na sieci niskiego napięcia, w której stosowane są inteligentne liczniki energii elektrycznej, koncentratory, urządzenia aktywne sieci teleinformatycznej oraz media transmisji danych. W tym duchu p. mgr inż. Robert Czechowski przedstawił też wyniki badań wynikające z analizy aktualnych zagadnień i problemów spotykanych przy projektowaniu inteligentnych sieci elektroenergetycznych.

W rozprawie przedstawiono rozwiązania i metody mogące pomóc w zwiększeniu bezpieczeństwa zmodernizowanych istniejących sieci oraz projektowanych nowych sieci elektroenergetycznych wykorzystujących układy automatyki cyfrowej i rozwiązania

teleinformatyczne, opartych na technologiach IT oraz ICT. W tym zakresie Autor pokazał algorytmy detekcji anomalii, nadużyć oraz włamań wraz z regułami filtracji ruchu sieciowego oraz omówił zasady komunikacji i autoryzacji użytkowników i urządzeń w każdym obszarze systemu elektroenergetycznego. Zaprezentował ponadto dedykowane rozwiązania dostępne na rynku, które są w stanie nie tylko wykryć, ale także skutecznie odeprzeć ataki. Generalnie rzecz ujmując Doktorant przekonywująco przedstawił uzyskane wyniki badań i właściwie je umiejscowił na tle przeglądu literatury przedmiotu, zwłaszcza światowej.

Pewnym mankamentem rozprawy jest brak podania źródeł w opisach niektórych rysunków, a także podanie zbyt skromnych oznaczeń do niektórych rysunków jak np. do rysunków o numerach od 1.3 do 1.7, od 2.1 do 2,5, od 3.1 do 3.4, itp. Niedociągnięciem rozprawy jest też w pewnym sensie niepotrzebne rozbudowanie jej części teoretycznej w sposób opisowy, a nie ściśle sformalizowany, kosztem ograniczenia części praktycznej rozprawy, co niepotrzebnie pomniejsza jej komercyjny charakter.

Jednakże w prezentowanym zakresie recenzowana praca zawiera wyniki badań uzyskane na wysokim poziomie badań empirycznych, które umiejętnie zostały uzupełnione o wyniki analizy teoretycznej. Istnieje możliwość kontynuacji badań m.in. w zakresie modeli oraz w zakresie ich dostosowania do analizy różnych sytuacji pracy systemu elektroenergetycznego, zwłaszcza w zakresie poszukiwania ogólnego modelu systemu elektroenergetycznego dla warunków rozwojowych.

W zakresie strony redakcyjnej praca zawiera pewne błędy natury stylistycznej i gramatycznej, jak też tzw. przejęzyczenia, literówki i urwane zdania, które generalnie rzecz ujmując nie są zbyt liczne i nie mają większego wpływu na jej czytelność, stąd ich nie przytaczam.

4. W podsumowaniu wyraźnie stwierdzam, że przedłożona mi do recenzji rozprawa doktorska p. mgr inż. Roberta Czechowskiego **stanowi oryginalne podejście** do rozwiązania aktualnego i bardzo istotnego dla praktyki w elektroenergetyce problemu naukowego w zakresie bezpieczeństwa cyfrowego inteligentnych dystrybucyjnych sieci elektroenergetycznych.

Uważam, że rozprawa wnosi **istotny wkład do rozwoju problematyki z zakresu systemów typu Smart Grid oraz Smart Matering, a także** wykazuje **odpowiednią ogólną wiedzę teoretyczną Doktoranta w dyscyplinie naukowej elektrotechnika oraz umiejętność samodzielnego prowadzenia pracy naukowej.** Z pełnym przekonaniem stwierdzam, że rozprawa opracowana przez mgr inż. Roberta Czechowicza **spełnia**

wymagania stawiane rozprawom doktorskim przez ustawę z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki[2] z wyraźnym nadmiarem, stąd **oceniam ją bardzo wysoko i wnioskuję o dopuszczenie jej do publicznej obrony**, a nawet skłaniam się do opinii, że **zasługuje na wyróżnienie**, co uzależniam jednakże od przedyskutowania następujących dwóch kwestii:

Kwestia 1.

W akapicie 1 p. 3.1 na str. 126 rozprawy Doktorant podsumował ww. pięć rożnych modeli symulacyjnych konstatując, że ich analiza może pozwolić na zrozumienie i poznanie niekorzystnych zjawisk występujących w sieciach elektroenergetycznych, a w szczególności tych, które mają duży wpływ na skuteczność transmisji i bezpieczeństwo wymiany informacji.

Ze względu na to, że Autor zauważył (str. 20, akapit 1 od góry) skuteczność jest kluczowym wymogiem bezpieczeństwa cyfrowej komunikacji, którą przyjął jako procentowy udział liczby wszystkich zarejestrowanych połączeń danego urządzenia do liczby zdarzeń uznanych za zaistnienie skutecznej transmisji w zależności od przyjętego kryterium (str. 78, akapit 1, ostatnie zdanie), a więc stopień osiągnięcia celu mierzony w [%], czyli miernik, w którym nie bierze się pod uwagę nakładu, a tylko efekt, a z kolei w odwołaniu nr 12 (u dołu strony) wyjaśnił, że kryterium ujęte przy obliczeniu Skuteczności I nie zawiera zdarzeń typu odłączenie, a kryterium ujęte przy obliczeniu Skuteczności II nie zawiera zdarzeń logicznych typu: odłączenie i rejestrowanie, co wskazuje na przyjęcie bardziej szczegółowej definicji skuteczności niż definicja ogólna, której nie odnajduję w rozprawie, stąd proszę o wyjaśnienie **w jaki sposób Doktorant zastosował definicję ogólną dla ww. szczególnych rozwiązań oraz proszę o przedyskutowanie w jaki sposób definicja skuteczności przyjęta w pracy została wykorzystana do wyznaczenia wpływu parametrów urządzeń występujących w sieci, w tym w szczególności liczników końcowych (terminals) oraz liczników pośredniczących (switches1) na jakość oraz poziom skuteczności transmisji danych, a także jaki był wpływ innych czynników, w tym w szczególności zakłóceń na skuteczność transmisji danych na przykładzie modelu 4**?

Ponadto proszę o przedyskutowanie ww. zakresie w jaki sposób należałoby zdefiniować efektywność transmisji danych wykorzystując zdefiniowane w pracy pojęcie skuteczności i jaka byłaby wówczas efektywność sieci wyposażonej w urządzenia Smart Grid i Smart Matering w stosunku do sieci niewyposażonej w urządzenia inteligentne?

[2] Dz. U. z 2003 r., Nr 65, poz. 595, ze zm., Dz. U. z 2017 r. poz. 1789, t.j.

Kwestia 2.

Pan mgr inż. Robert Czechowski na str. 12, akapit ostatni, podaje m.in., że temat pracy jest powiązany z zadaniami realizowanego międzynarodowego grantu badawczego dotyczącego bezpieczeństwa cyfrowego inteligentnych sieci niskiego napięcia, którego Autor rozprawy jest jednym z głównych wykonawców, nie podając żadnych szczegółów, w tym przynajmniej tematu i głównych wykonawców oraz założonych i zrealizowanych efektów, rezultatów i produktów, itp. w ramach grantu, co zupełnie niepotrzebnie obniża wartość rozprawy. Proszę zatem o wyjaśnienie, co to za grant i w jakim zakresie temat rozprawy doktorskiej jest powiązany z zadaniami ww. grantu, a więc z konkretnymi rozwiązaniami praktycznymi mającymi wartość komercyjną?

Proszę także o przedyskutowanie oryginalnych osiągnięć Doktoranta zamieszczonych w rozprawie doktorskiej, to jest wykonanych jako własne, wykonanych jako współautorskie z wkładem ponad 50% oraz wykonanych z wkładem poniżej 50%, zwłaszcza w części praktycznej rozprawy, a więc w zakresie przeprowadzonego projektowania, analizy i badania każdego z ww. pięciu modeli, w tym ich wykorzystania dla różnych przypadków szczegółowych symulacji i badań?

Ponadto bardzo proszę o szerszą dyskusję w jaki sposób Doktorant udowodnił, że główną rolą wdrożenia systemu detekcji ataku docelowo jest informowanie o tym administratora systemu w celu podjęcia przez niego działań mających na celu minimalizację negatywnych skutków powstałych w wyniku przeprowadzenia udanego ataku, z podaniem założeń i uzyskanych wyników badań.

Jerzy Tchórzewski