nadbryg. dr hab. inż. Paweł KĘPKA, prof. SGSP
Szkoła Główna Służby Pożarniczej

Warszawa, 06 grudnia 2018r.

RECENZJA

rozprawy doktorskiej

Pana mgr. Pawła Domańskiego

na temat: „Bezpieczeństwo aplikacji teleinformatycznych w systemach zarządzania kryzysowego na szczeblu wojewódzkim", napisanej pod kierunkiem prof. dr. hab. Krzysztofa Ficonia

Ocena wyboru i uzasadnienia problematyki rozprawy doktorskiej

Wykorzystywanie nowoczesnych technologii w bezpieczeństwie od dawna jest bezdyskusyjne i stanowi kluczowy element we właściwym zarządzaniu bezpieczeństwem, w tym zarządzaniu ryzykiem. Nieocenione jest wsparcie nowoczesnych technologii dotyczących bezpośrednio wykorzystywanego sprzętu, ale równie ważne, o ile nie ważniejsze, jest wsparcie optymalnego zarządzania poprzez systemy teleinformatyczne.

Wykorzystanie tych ostatnich niesie za sobą wiele pożytecznych rzeczy i informacji, ale stanowi także pewne niebezpieczeństwo w potencjalnych przechwyceniu danych i wykorzystaniu ich w sposób nieuprawniony. Może to być działanie nieintencjonalne, ale biorąc pod uwagę wartość tych informacji z reguły mamy do czynienia ze świadomym działaniem ukierunkowanym na osiągnięcie konkretnego celu.

Problematyka rozprawy doktorskiej Pana mgr. Pawła Domańskiego porusza problem naukowy i stanowi użyteczne działanie badawcze dotyczące bezpieczeństwa aplikacji teleinformatycznych w systemach zarządzania kryzysowego uwzględniającej aspekty funkcjonalne, organizacyjne, prawne i kompetencyjne.

Ocena rozprawy pod względem formalnym

Rozprawa doktorska Pana mgr. Pawła Domańskiego jest dziełem pełnym w rozumieniu prowadzenia badań naukowych. Zawiera całościowe sprawozdanie z przeprowadzonych badań wraz z bibliografią, wykazem rysunków, spisem tabel oraz załącznikami. Praca liczy 273 strony i zawiera wszystkie części, które ma sprawozdanie naukowe – wstęp, cztery rozdziały:

- Kierunki wykorzystania aplikacji teleinformatycznych w administracji publicznej,
- Koncepcja wykorzystania systemów teleinformatycznych do wspomagania zarządzania kryzysowego na szczeblu wojewódzkim,
- Polityka bezpieczeństwa wdrażania i użytkowania systemów teleinformatycznych w zarządzaniu kryzysowym,
- Analiza i ocena bezpieczeństwa wybranych aplikacji teleinformatycznych w zarządzaniu kryzysowym na szczeblu województwa,

oraz zakończenie, bibliografię, spis rysunków, spis tabel oraz załączniki. Rozdziały wprawdzie nie są równo podzielone co do objętości, natomiast nie ma to większego znaczenia co do merytorycznego zakresu rozprawy.

Język dysertacji nie budzi zastrzeżeń, chociaż zdarzają się błędy interpunkcyjne bez wpływu na jakość merytoryczną i poznawczą. Dysertację należy uznać za poprawną pod względem terminologicznym oraz redakcyjnym.

W recenzowanej rozprawie literatura i źródła zostały dobrane i wykorzystane prawidłowo, a zestawienie zostało podzielone na następujące bloki tematyczne: bibliografia (72. pozycje), artykuły (31 pozycji), akty prawne (26 pozycji), publikacje internetowe (44 pozycje), źródła internetowe (58 pozycji), specyfikacje i instrukcje obsługi systemów teleinformatycznych (5 pozycji), systemy teleinformatyczne i oprogramowanie komputerowe (6 pozycji) oraz pozostałe materiały z instytucji i firm (3 pozycje).

Przedmiot, cel badań i hipotezy badawcze

Autor niniejszej dysertacji wskazał, że *przedmiotem badań* jest problematyka wdrażania i użytkowania systemów teleinformatycznych w obszarze zarządzania kryzysowego uwzględniająca głównie poziom administratora systemu zajmującego się bezpieczeństwem w instytucjach publicznych.

Natomiast *cel badań* został określony jako zdiagnozowanie problemów występujących w procesie administrowania i prowadzenia nadzoru nad właściwą eksploatacją zaawansowanych systemów teleinformatycznych, a także wypracowanie propozycji rozwiązań organizacyjnych, technicznych i prawnych dla aplikacji informatycznych użytkowanych w systemie zarządzania kryzysowego. Zakres szczegółowy obejmuje kierunki wykorzystania aplikacji teleinformatycznych w administracji publicznej, koncepcję wykorzystania systemów teleinformatycznych do wspomagania zarządzania kryzysowego na szczeblu wojewódzkim, analizę obowiązujących aktów prawnych dotyczących polityk bezpieczeństwa, a także analizę i ocenę bezpieczeństwa wybranych aplikacji teleinformatycznych w zarządzaniu kryzysowym na szczeblu wojewódzkim.

Problem badawczy został określony jako: „Jak analiza oraz ocena efektywności i skuteczności działania systemów teleinformatycznych wykorzystywanych przez organy administracji publicznej wpływają na poziom bezpieczeństwa, wiarygodności i niezawodności aplikacji informatycznych wykorzystywanych w systemie zarządzania kryzysowego na szczeblu wojewódzkim?". Zaś szczegółowe problemy badawcze sformułowano w następujący sposób:

1. Czy nowe technologie informatyczne mogą wpłynąć na zwiększenie efektywności i skuteczności systemów teleinformatycznych wykorzystywanych w zarządzaniu kryzysowym na szczeblu wojewódzkim oraz jakie zagrożenia mogą nieść dla ich funkcjonowania?
2. W jakich obszarach zarządzania kryzysowego wykorzystuje się zaawansowane systemy teleinformatyczne?
3. Jakie są podstawy formalno-prawne oraz techniczno-eksploatacyjne w zakresie wdrażania, administrowania i użytkowania technologii informatycznych w zarządzaniu kryzysowym?
4. Na jakim poziomie kształtuje się ocena efektywności i skuteczności aplikacji informatycznych wykorzystywanych w obszarze zarządzania kryzysowego?

Autor niniejszej dysertacji sformułował następnie hipotezę główną i cztery hipotezy robocze.

Hipoteza główna została określona jako: „Profesjonalne użytkowanie nowoczesnych systemów teleinformatycznych w zakresie projektowania, wdrażania zabezpieczeń, eksploatacji i podejmowania działań profilaktycznych w szczególności prowadzenia regularnych szkoleń jest warunkiem koniecznym sprawnego i efektywnego zarządzania kryzysowego na szczeblu wojewódzkim".

Metodyka badań

Dysertacja jest odzwierciedleniem procesu badawczego zawierającego elementy składowe, gdzie wyróżnić należy literaturę badanego przedmiotu, problemy naukowe, postawione hipotezy, metody badawcze, badania właściwe, teorię problemu naukowego oraz pisarskie opracowanie.

Metodykę badań należy uznać za właściwą do przedstawionych celów, problemów i hipotez badawczych, gdzie wykorzystano następujące *metody badawcze*: analizę i krytykę piśmiennictwa oraz badanie dokumentów, indukcję, dedukcję, analizę, syntezę, wnioskowanie oraz uogólnienia, analizę matematyczną oraz metody sondażowe i statystyczne. W zakresie technik badawczych w dysertacji wykorzystano: obserwację, wywiady, badania dokumentów oraz ankietę.

Należy jednak podkreślić, że w dysertacji zostały wykorzystane badania ankietowe wśród użytkowników systemów teleinformatycznych wykorzystywanych w zarządzaniu kryzysowym na terenie województwa pomorskiego. Nie budzi wątpliwości wybór obszaru badań (województwo pomorskie), ale dobór grupy docelowej (str. 24) stanowiącej tylko pracowników administracji samorządowej szczebla powiatowego i gminnego. Nie ma również wskazanego podziału na grupy stanowisk w danej instytucji czy też określenia samego zatrudnienia w urzędzie lub danej służbie, straży czy inspekcji.

Struktura rozprawy

Treść rozprawy zgodna jest z jej tytułem.

Pierwszy rozdział „Kierunki wykorzystania aplikacji teleinformatycznych w administracji publicznej" to przed wszystkim naświetlenie sytuacji problemowej związanej z szerokorozumianym bezpieczeństwem teleinformatycznym, terminologią i zasadami funkcjonowania systemów teleinformatycznych, cyberprzestrzenią i cyberbezpieczeństwem oraz formalno-prawnymi zasadami funkcjonowania sieci wymiany danych. Szczegółowo zostały opisane zasady oraz aspekty funkcjonowania Internetu. Przywołano także badania o procentowym wykorzystaniu Internetu do sprawy prywatnych. Szkoda, że badając poziom powiatowy i gminny nie wskazano podobnego zestawienia dla spraw służbowych. W dysertacji został poruszony bardzo ważny aspekt związany z chmurą obliczeniową. Biorąc pod uwagę zalety tego rozwiązana, takie „zaplecze obliczeniowe" powinno być rozwijane także dla struktur zarządzania kryzysowego.

Kolejnym elementem tego rozdziału, który bezpośrednio służy osiągnięciu celu rozprawy są zasady budowy oraz kryteria oceny jakości funkcjonowania systemu teleinformatycznego zarządzania kryzysowego wraz z analizą wymagań techniczno-eksploatacyjnych, fazami przedsięwzięcia wdrożeniowego, opisem zasad funkcjonowania zespołu projektowego. Zwarzywszy na wcześniejsze badania Autora rozprawy, mówiące o sprzęcie komputerowym/obliczeniowym i coraz to nowszych jego generacjach, należy zastanowić się nad przesłankami umieszczenia aż tak konkretnych parametrów w Tabeli 1.4. – Infrastruktura technologiczna oraz wykaz licencji założeń projektowych STZK (Systemu Teleinformatycznego Zarządzania Kryzysowego). Bardzo wartościowym elementem pracy są kryteria oceny jakości funkcjonowania STZK. Kolejna część badań to analiza obszarów zagrożeń bezpieczeństwa systemów teleinformatycznych oraz metod ich zabezpieczania.

Przedstawiony schemat budowy STZK został precyzyjnie określony zarówno w aspekcie samego projektu, jaki i metody jego wdrożenia. Autor niniejszej rozprawy słusznie zauważa, że „na chwilę obecną niemożliwa jest realizacja budowy STZK bez pomocy zewnętrznych firm programistycznych". Jest to wniosek jak najbardziej prawdziwy i odzwierciedla aktualny stan zatrudnienia w strukturach zarządzania kryzysowego. Oczywiście trudno sobie wyobrazić sytuację, że wydziały zarządzania kryzysowego, służby, straże i inspekcje posiadają własne

centra programistyczne. Byłoby to wysoce nieekonomiczne rozwiązanie. Inną kwestią jest bezpieczeństwo danych i zarządzanie nimi.

Rozdział zawiera trafne wynika tej części procesu badawczego.

Rozdział drugi „Koncepcja wykorzystania systemów teleinformatycznych do wspomagania zarządzania kryzysowego na szczeblu wojewódzkim" to w głównej mierze odpowiedź na problem szczegółowy dotyczący zasad wykorzystania systemów telefonii komórkowej GSM oraz informacji przestrzennej w systemach teleinformatycznych. W rozdziale zostały przedstawione i przeanalizowane technologie informatyczne konieczne do funkcjonowania systemu zarzadzania kryzowego, takie jak: System Informacji Geograficznej (GIS), Regionalny System Ostrzegania (RSO), ISOK, system wideokonferencyjne, BlueAlert oraz bazy sił i środków.

Integralną częścią tego rozdziału jest modelowa struktura wraz z założeniami konceptualnymi STZK, która została przedstawiona w sposób konkretny i rzeczowy. Autor zaznaczył, że dane w STZK powinny być wymieniane przy użyciu sieci Internet (model klient-serwer?). Dodatkowo, rysunki 2.16, 2.17 i 2.18 wskazują na mnogość baz danych co może w przyszłości, po zaimplementowaniu systemu, generować problemy z lokalnym zarządzaniem tymi bazami, jakością danych, czasami dostępu do baz, a tym samym bezpieczeństwem, wiarygodnością i aktualnością danych.

Autor słusznie zauważył, że od samego początku powstania struktur zarządzania kryzysowego w Polsce nie powstały standardy informatyczne/teleinformatyczne, co znacznie utrudnia pracę i podejmowanie decyzji w sytuacji zagrożenia, głównie w zdarzeniach przekraczających obszar województwa. Zatem zakres merytoryczny, parametry, bazy danych, itp. mogą się w różnią na terenie Polski. Przekłada się to bezpośrednio także na wszelkie analizy, modelowania i oceny, w tym ryzyka. Jedną z nielicznych ogólnopolskich inicjatyw w zakresie ujednolicenia danych/parametrów/metodyk podjęło Rządowe Centrum Bezpieczeństwa opracowując „Procedurę opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego".

Rozdział ten jest wartościową częścią pracy, ale mimo wszystko brakuje elementów związanych z oprogramowaniem do modelowania różnych zagrożeń czy to chemicznych, powodziowych lub symulacji ewakuacji ludności z zagrożonych terenów. Dane, na podstawie których sporządza się wyżej wymienione analizy, mogą zwierać bądź zawierają informacje wrażliwe z punktu widzenia bezpieczeństwa.

Rozdział trzeci „Polityka bezpieczeństwa wdrażania i użytkowania systemów teleinformatycznych w zarządzaniu kryzysowym" to przede wszystkim analiza podstaw formalno-prawnych i wymagań techniczno-organizacyjnych w zakresie bezpieczeństwa i funkcjonowania systemów teleinformatycznych uwzględniająca procedury ochrony danych osobowych, a także sankcje i zabezpieczenie techniczne danych zgodnie z RODO. Rozdział ten stanowi bardzo ważny element dysertacji i odnosi się także do analizy zależności/współpracy zleceniodawca-wykonawca, wskazując ten element jako funkcjonalność systemu. Znamienne jest także stwierdzenie, że „brak doboru właściwej osoby pełniącej funkcję lidera, która posiada odpowiednie cechy, wiedzę, doświadczenie, a także kulturę osobistą i elokwencję może doprowadzić do frustracji, zdenerwowania, czego efektem będzie niestabilna współpraca pomiędzy obiema stronami". Analizie została także poddany zakres odpowiedzialności i rola inspektora ochrony danych w kształtowaniu polityki bezpieczeństwa informatycznego oraz przykłady naruszeń bezpieczeństwa w tych systemach.

Analiza przeprowadzona w sposób wnikliwy i całościowy.

Rozdział czwarty „Analiza i ocena bezpieczeństwa wybranych aplikacji teleinformatycznych w zarządzaniu kryzysowym na szczeblu województwa".

Rozdział ten poświęcony jest ocenie bezpieczeństwa techniczno-użytkowego systemu BlueAlert oraz jego wpływu na skuteczną komunikację pomiędzy wybranymi podmiotami/osobami. Kolejny element to analiza potencjalnych źródeł zagrożeń bezpieczeństwa systemów teleinformatycznych wraz ze wskazaniem, że czynnik ludzki jest najbardziej zawodnym ogniwem systemu. Zostały wskazane najczęstsze błędy lub niedopatrzenia skutkujące obniżeniem poziomu bezpieczeństwa lub wiarygodności.

Ważnym elementem tej części dysertacji jest przedstawianie wyników przeprowadzonych badań ankietowych w odniesieniu do skuteczności i poziomu bezpieczeństwa systemów teleinformatycznych w zarządzaniu kryzysowym.

Rozdział zakończony merytorycznymi wnioskami.

Ocena ogólna i wniosek końcowy

Rozprawa opracowana została zgodnie z tytułem. Autor uzyskał zamierzony cel jakim jest praca naukowa potwierdzająca kompetencje badawcze. Recenzowana praca prezentuje się pod względem formalnym i merytorycznym bez większych zastrzeżeń. Stanowi oryginalne i nowatorskie rozwiązanie problemu naukowego. Doktorant wykazał się podstawową wiedzą z nauk o bezpieczeństwie, a także umiejętnością samodzielnego prowadzenia prac naukowych. Recenzowana rozprawa posiada nieliczne niedociągnięcia, jednak cel badań został osiągnięty.

W związku z tym stwierdzam, że praca Pana mgr. Pawła Domańskiego spełnia wymagania określone ustawą z dnia 14 marca 2003r. *o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki* (Dz.U. Nr 65, poz. 595, ze zm.).

Wnoszę o dopuszczenie recenzowanej rozprawy doktorskiej do publicznej obrony.