Szczytno, 2023.07.12.

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

RECENZJA

rozprawy doktorskiej nt.

KONCEPCJA SYSTEMU BEZPIECZEŃSTWA WYMIANY INFORMACJI W PAŃSTWOWEJ STRAŻY POŻARNEJ,

autorstwa mgr. inż. Andrzeja BARTKOWIAKA,

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

Wprowadzenie

Rozprawa doktorska dotyczy identyfikacji i poznania systemu informacyjnego istniejącego w Państwowej Straży Pożarnej (PSP) i koncentruje się także na występujących w nim niedoskonałościach - co daje asumpt do wprowadzenia istotnych zmian w jego funkcjonowaniu na bazie wniosków z badań naukowych. Mieści się ona w ramach dyscypliny nauki o bezpieczeństwie, a materiał ją tworzący stanowi zwieńczenie dotychczasowej aktywności Doktoranta w sferze nauki polskiej w przedmiotowym problemie.

Przedmiot badań zawarty w dysertacji jest aktualny, gdyż dotyczy systemu bezpieczeństwa wymiany informacji w Państwowej Straży Pożarnej. Mając tego świadomość Doktorant słusznie zdecydował się na badanie w odniesieniu do istotnego problemu dla PSP, jakim jest nie tylko szybkość ale i dokładność przepływu informacji oraz jej ochrona dla tej formacji bezpieczeństwa powszechnego w ramach bezpieczeństwa wewnętrznego państwa polskiego. Jego wieloletnie doświadczenie zawodowe związane z przepływem informacji w PSP oraz dostrzeżone niedomogi i braki w funkcjonującym systemie informacyjnym tej formacji, upoważniają go do tego, aby podjął wysiłek badawczy w celu zaproponowania usprawnień na rzecz poprawy sprawności i wyeliminowania zakłóceń w tym systemie, ponieważ to istotnie wpływa na przekaz informacji na wszystkich szczeblach funkcjonowania PSP.

Tym to kwestiom poświęcona jest dysertacja, w której do ich zbadania i wyprowadzenia z nich wniosków zastosowano naukowe metody wykorzystywane w naukach o bezpieczeństwie. Konieczność badań wynika też z postępującego rozwoju technologii

informatycznych, a ostatnio także sztucznej inteligencji, stąd wyrazy uznania, co do podjętych badań na rzecz tak ważnego przedmiotu badań zarysowanego tytułem dysertacji.

OCENA METODOLOGICZNA

Kwestie metodologiczne w dysertacji zawarto w Rozdziale 1. *PODSTAWY METODOLOGICZNE BADAŃ* - ss. 11-43, w którym wyszczególniono takie kwestie jak: 1.1. Uzasadnienie podjęcia badań (sytuacja problemowa); 1.2. Przedmiot i cel badań; 1.3. Problem (problemy) badawczy; 1.4. Hipoteza robocza; 1.5. Metody badawcze; 1.6. Proces badań.

W kwestii uzasadnienia podjęcia badań wskazano, że „wzrost zainteresowania tematyką bezpieczeństwa informacji" generuje „potrzeby dostosowywania organizacji do wymagań mających na względzie zastosowanie przepisów prawa i innych (...), których celem jest zapewnienie ochrony określonym grupom interesariuszy". Stąd – zdaniem Doktoranta - „w obszarach systemu informacyjnego może występować zjawisko niekontrolowanego przepływu informacji, należy natychmiast wdrożyć środki zaradcze w tym zakresie" - i aby to mogło stać się faktem podjęto próbę zbadania funkcjonowania systemu informacyjnego PSP, żeby uzyskać wnioski, które w oparciu o badania naukowe dawałyby podstawę do konkretnych działań dotyczący poprawy funkcjonowania tego systemu.

Przedmiotem badań w świetle sytuacji problemowej stał się – jak już wspomniano - system bezpieczeństwa wymiany informacji w Państwowej Straży Pożarnej. Zaś celem, o podwójnym charakterze – „1. Cel poznawczy: identyfikacja zagrożeń i możliwych usprawnień w systemie bezpieczeństwa informacji w Państwowej Straży Pożarnej jako organizacji publicznej. 2. Cel utylitarny: opracowanie koncepcji bezpieczeństwa systemu obiegu informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna".

Za problem badawczy przyjęto pytanie: „Jakie zmiany wprowadzić w systemie bezpieczeństwa wymiany informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna, tak aby poprawić skuteczność bezpieczeństwa obiegu informacyjnego?" Zaś jakby odpowiedzią na nie jest treść hipotezy głównej w brzmieniu: „Założono, że obecny system informacyjny w organizacji publicznej jaką jest Państwowa Straż Pożarna nie w pełni chroni informacje pozyskiwane i przetwarzane przez tą formację. Ułatwienie dostępu do danych, usprawnienie procesów przekazywania lub pobierania ich znacznych ilości w niewielkich jednostkach czasu oraz rozwój technologii przechowywania informacji mają ogromne znaczenie na funkcjonowanie tej instytucji. Natomiast odpowiednio przebiegający proces

wymiany informacji wpływa między innymi na prawidłowe wykonywanie zadań, przy założeniu, że najważniejszymi aspektami bezpieczeństwa informacji są: dostępność, poufność, niezawodność, integralność i autentyczność".

Na okoliczność weryfikacji tej hipotezy i rozwiązania głównego problemu badawczego przyjęto problemy szczegółowe badań o treści:

„1. Jak funkcjonuje system bezpieczeństwa wymiany informacji w teorii i praktyce?

2. Jak funkcjonuje system bezpieczeństwa wymiany informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna?

3. Jaka powinna być koncepcja systemu obiegu informacji w Państwowej Staży Pożarnej, aby poprawić skuteczność jego funkcjonowania?"

Jeśli się zestawi ich treść z treścią poszczególnych rozdziałów merytorycznych (które powinny odpowiadać problemom szczegółowym badań) – „rozdział 2. Podstawy zarządzania bezpieczeństwem systemu informacyjnego w instytucjach publicznych; rozdział 3. Zagrożenia bezpieczeństwa systemu informacyjnego na przykładzie Państwowej Straży Pożarnej; rozdział 3. Koncepcja bezpieczeństwa systemu informacyjnego w Państwowej Straży Pożarnej" – to można dojść do wniosku, że tylko 2/3 jest ta zgodność.

Problemom szczegółowym badań można przyporządkować hipotezy szczegółowe. I tego przykład mamy w niniejszej dysertacji, ale pomiędzy nimi powinna zaistnieć spójność logiczna typy: pytanie (jako problem szczegółowy badań) i odpowiedź (w postaci hipotezy szczegółowej). Mając tego świadomość spójrzmy, jak ta zależność funkcjonuje w niniejszej dysertacji, gdzie treść problemów szczegółowych zacytowano powyżej, a treść hipotez szczegółowych jest następująca:

„Hipoteza 1: Zakłada się, że bezpieczeństwo systemu informacji w Państwowej Straży Pożarnej regulowane jest pośrednio i bezpośrednio źródłami powszechnie obowiązującego prawa w Rzeczypospolitej Polskiej, do których należą między innymi: Konstytucja RP, ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia, akty prawa miejscowego obowiązujące na obszarze działania organów, które je ustanowiły. System bezpieczeństwa wymiany informacji to strategia działania tej formacji w zakresie zapewniania właściwej ochrony pozyskiwanych i przetwarzanych informacji. W teorii strategia ta ma zapewnić ciągłe doskonalenie podjętych działań i procedur w celu optymalizacji ryzyk związanych z naruszeniem poufności danych. Natomiast w praktyce na strategię składają się wszystkie procedury, polityki, regulaminy i instrukcje bezpieczeństwa informacji, które są wdrożone w każdej jednostce organizacyjnej. Informacja jako zasób i narzędzie stanowi podstawę

działalności analitycznej. Bez informacji i jej właściwego procedowania w systemie nie ma szans na właściwe, efektywne i szybkie wykorzystanie działalności analitycznej dla zwiększenia bezpieczeństwa państwa i obywateli, a bezpieczeństwo systemu informacyjnego świadczy o wysokim standardzie zarządzania jednostką organizacyjną.

Hipoteza 2: Zakłada się, że Państwowa Straż Pożarna jako instytucja odpowiedzialna za zapewnienie bezpieczeństwa obywatelom naszego Państwa gromadzi i przetwarza tylko niezbędna informacje w tym zakresie. Informacje te uzyskiwane są od „klientów" i instytucji, z którymi straż pożarna współpracuje. Informacje te przechowywane są w systemach informatycznych, dlatego bardzo ważne jest by prawidłowo funkcjonował system bezpieczeństwa wymiany informacji i każdy z pracowników tej instytucji powinien ją należycie chronić. Przypuszcza się natomiast, że jednym z najważniejszych potencjalnych źródeł zagrożeń dla bezpieczeństwa informacji w danej organizacji jest naruszanie przepisów chroniących te organizacje przez osoby, które posiadają dostęp do informacji. Występują zagrożenia w bezpieczeństwie sytemu informacyjnego dlatego, że dotychczasowe zabezpieczania informacji i procedury bezpieczeństwa informacyjnego nie są przez wszystkich użytkowników w należyty sposób przestrzegane. Do tego, występuje brak świadomości wśród niektórych użytkowników o skutkach łamania zasad korzystania z systemu informacyjnego i braku odpowiedzialności. Napotyka się również bariery oraz trudności powiązane bezpośrednio z wdrażaniem w życie ustawy o ochronie informacji niejawnych. Ponadto zakłada się, że jako typowe zagrożenia systemu bezpieczeństwa obiegu informacji można wyodrębnić zagrożenia wewnętrzne i zewnętrzne powstające poza organizacją, w wyniku celowego lub przypadkowego działania ze strony osób trzecich. Do tych pierwszych zaliczyć możemy: zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu błędu jak i przypadku; zagrożenie utratą lub uszkodzeniem poprzez celowe działania nieuczciwych użytkowników; zagrożenia fizyczne, w których szkoda jest spowodowana wypadkiem, awarią, lub innym nieprzewidzianym zdarzeniem losowym. Do zagrożeń zewnętrznych zaliczyć możemy: przestępstwa wykorzystujące komputer jako narzędzie; cyberterroryzm; utrata informacji związana z włamaniami komputerowymi, złośliwymi kodami i wirusami, szpiegostwem, sabotażem, czy też wandalizmem.

Hipoteza 3: Zakłada się, że należy poprawić skuteczność obiegu informacji oraz zwiększyć efektywność zabezpieczeń informacji wewnątrz organizacji publicznej jaką jest Państwowa Straż Pożarna. Aby tego dokonać należałoby ujednolicić systemy teleinformatyczne na wszystkich poziomach organizacyjnych tej formacji oraz wprowadzić

zmiany pod kątem organizacyjnym, technicznym i funkcjonalnym w zasadach użytkowania, funkcjonowania i organizacji systemu informacyjnego. Istotne jest wdrożenie i utrzymanie właściwego systemu zarządzania bezpieczeństwem informacji, który będzie umożliwiał ochronę wszystkich przetwarzanych informacji, jak również zapewniał ciągłość realizowanych procesów i zadań. Aby osiągnąć jak najwyższy stopień bezpieczeństwa informacji, należy w odpowiedni sposób przygotować zasoby organizacji, a następnie odpowiednio i odpowiedzialnie nimi zarządzać. Zakłada się, że niezbędne dla ochrony informacji w instytucji jest właściwie ułożenie i konsekwentne egzekwowanie polityki bezpieczeństwa informacji, co jest elementem decydującym o jej skuteczności, a systematyczny wielopłaszczyznowy nadzór zwiększa bezpieczeństwo informacji będących w obiegu".

Hipotezy szczegółowe mają rozbudowaną treść i wystarczającym zakresie odpowiadają na pytania zawarte w problemach szczegółowych badań.

W sferze metod badawczych mamy do czynienia z bardzo bogatą paletą teoretyczną w tym zakresie, gdzie scharakteryzowano wiele metod, które Doktorant brał pod uwagę w trakcie badań. Ponadto opisano badania empiryczne, które przeprowadzana na rzecz zbadania opinii funkcjonariuszy Państwowej Straży Pożarnej – występujących jako repondencji. Założono w nich, że „wszyscy strażacy realizują swoje zadania uczestnicząc w systemie obiegu informacji PSP". Do badań wykorzystano kwestionariusz-ankietę i sposób „doboru losowego prostego zależnego, który polega na nieograniczonym i bezpośrednim doborze potencjalnych jednostek badania do próby statystycznej". Z obliczeń wynikało, że do badań trzeba było mieć dość liczną próbę objętych badaniami, aby były one wiarygodne, stąd uzyskano „w nich łącznie 1897 poprawnie uzupełnionych kwestionariuszy ankietowych, z czego 352 dla Komend Wojewódzkich i Komendy Głównej PSP oraz 1545 dla Komend Miejskich/Powiatowych PSP. Badania zostały ukończone w styczniu 2023 roku".

Proces badań zaprezentowano w trzech jego fach: Faza I – przygotowanie badań; Faza II – prowadzenie badań; Faza III – opracowanie badań. Każdą z faz odniesiono do kroków w niej występujących, co istotnie zobrazowało proces badawczy w poszczególnych jego poczynaniach, logicznie uzasadniając wysiłek badawczy Doktoranta.

Treść metodologiczne zostały wzbogacone czteroma tabelami, czteroma rysunkami i czteroma wykresami, które istotnie pojaśniają ich rozumienie.

Część metodologiczną dysertacji uważam za właściwie opracowaną, stąd uznaję ją za wystarczającą na potrzeby prezentacji treści tej części dysertacji.

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 bezpieczeństwa wymiany informacji w Państwowej Straży Pożarnej. Zawarte w dysertacji treści mieszczą się nie tylko w aktualnych i ważnych obszarach tematycznych badań nauki polskiej, ale tworzą również solidne podstawy wiedzy na rzecz bezpieczeństwa informacyjnego w ogólności.

Dysertacja składa się z trzech rozdziałów o charakterze merytorycznym (2., 3., i 4.) oraz *Wstępu* (4 strony), *Zakończenia* (3 strony), *Bibliografii* zawartej na 10 stronach (241 pozycji), dwóch załączników (kwestionariusza wywiadu i arkusza obserwacji) oraz tabel (47), wykresów (44), a także rysunków (14), które obrazują, wzbogacają i pojaśniają rozumienie treści merytorycznej prezentowanej tekstowo. Posiada także *Streszczenie* (w językach polskim i angielskim) – 3 strony – w którym Doktorant oznajmia, że „Dysertacja składa się z wstępu i zakończenia oraz czterech zasadniczych rozdziałów merytorycznych: Rozdział 1. Podstawy metodologiczne ...". Zatem **pytanie (1.)**: czy nie jest w tym stwierdzeniu jakaś niekonsekwencja, a jeśli tak - to jaka?

W *Streszczeniu* zaprezentowano niektóre kwestie metodologiczne oraz charakterystykę rozdziałów – co do treści kwestii w nich podejmowanych.

We *Wstępie* dysertacji wskazano na rozumienie współczesnych zagrożeń rozpatrywanych w kontekście bezpieczeństwa informacyjnego będącego elementem formacji państwowej jaką jest PSP. Zaprezentowano w nim też „jednostki organizacyjne" PSP i jej zadania oraz instytucje współdziałające z tą formacją. Wskazano też na organy administracji, które w ramach Krajowego Systemu Ratowniczo-Gaśniczego wskazują zakres powinności dla struktur PSP na ich szczeblach odpowiedzialności administracyjnej - gminie, powiecie i województwie – kiedy to występuje taka konieczność, jak chociażby „w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia, środowiska i mienia zarządza ...". Kiedy to „zapewnienie bezpieczeństwa systemu informacyjnego w organizacji publicznej jest wysoce cenione, gdyż stanowi o sile jednostki we współczesnej rzeczywistości", ponieważ „racjonalność w zarządzaniu informacją zaświadcza o wysokich kompetencjach menedżerskich oraz jest synonimem podążania jednostki za nieustannym rozwojem, który wywołuje ciągłą zmienność potrzeb".

Rozdział 2. (*PODSTAWY ZARĄDZANIA BEZPIECZEŃSTWEM SYSTEMU INFORMACYJNEGO W INSTYTUCJACH PUBLICZNYCH)* – ss. 44-86 – zawiera wyniki z badań nad teorią bezpieczeństwa systemu informacyjnego w instytucjach publicznych w kontekście teoretycznym i prawnym. Wyeksponowano w nim definicję informacji, ze szczególnym wskazaniem na bezpieczeństwo informacji dla współczesnych organizacji oraz skomentowano znaczenie systemów bezpieczeństwa informacyjnego w kontekście bezpieczeństwa państwa.

Odniesiono się także do środków technicznych i strony organizacyjnej - mających wpływ na bezpieczeństwo informacji w organizacji. W kwestii prawa przedstawiono obowiązujące akty normatywne wraz z normami z nich wynikającymi. Postawiono też diagnozę systemu informacyjnego funkcjonującego w instytucjach państwowych z ujęciem zarządzania bezpieczeństwem informacyjnym w organizacji.

Rozdział zamykają *wnioski* (na 4 stratach), z których wynika m.in. i to, „że za słabe strony systemu szkolenia w Państwowej Straży Pożarnej można uznać:

- brak powiązań szkoleń ze ścieżką rozwoju zawodowego;
- brak obligatoryjności szkoleń specjalistycznych;
- brak możliwości zaspokojenia potrzeb szkoleniowych;
- niski potencjał szkoleniowy ośrodków szkolenia.

Ale największym zagrożeniem dla bezpieczeństwa systemu informacyjnego i samej informacji jest człowiek (działania człowieka mogą przybrać także formę rozmyślną, polegającą na celowych atakach na systemy). Zagrożenia najczęściej wynikają z niedbalstwa, braku wiedzy lub nieuwagi użytkowników systemów. Do negatywnych postępowań należy zaliczyć także kradzieże sprzętu i zasobów, czy też szpiegowanie lub hakowania. Biorąc pod uwagę powyższe konieczne wydaje się prowadzenie systematycznych szkoleń w organizacji tak, aby pracownicy mieli dostęp do wiedzy o istniejących zagrożeniach i możliwych postaciach ich występowania".

Wskazano też na to, że „każda informacja podczas procesu jej przekazywania ulega zniekształceniom w kanale informacyjnym. Aby zminimalizować te zniekształcenia, potrzebne jest podejmowanie wszelkich możliwych działań aby zapewnić przekazywanie informacji o treści tożsamej lub jak najbardziej zbliżonej do informacji pierwotnej. (...) Zagrożenia bezpieczeństwa informacyjnego są definiowane w różnorakich obszarach ryzyka, szczególnie wyraźnie w obszarze zagrożeń technologicznych jako następstwo rozwoju technologicznego. Jednak choć to systemy informatyczne przetwarzają dane, człowiek bogaty w wiedzę, ale

przecież niedoskonały, stwarza potencjalne zagrożenie dla bezpieczeństwa informacyjnego. (...) Człowiek jest najsłabszym ogniwem bezpieczeństwa, gdyż urządzenia techniczne, oprogramowanie to jedynie narzędzia obsługiwane przez ludzi i przede wszystkim od użytkownika będzie zależało utrzymanie informacji z dala od dostępu osób nieuprawnionych".

W rozdziale 3. (*ZAGROŻENIA BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO NA PRZYKŁADZIE PAŃSTWOWEJ STRAŻY POŻARNEJ)* – ss. 87-180 – zawarto wyniki z badań nad zagrożeniami bezpieczeństwa systemu informacyjnego na przykładzie instytucji publicznej jaką jest Państwowa Straż Pożarna oraz jej politykę bezpieczeństwa w sferze informacji, a także jej strategię, z uwypukleniem norm i standardów bezpieczeństwa systemu informacyjnego, jakie powinny obowiązywać w instytucji państwowej. Odniesiono się także do polityki prywatność, polityki bezpieczeństwa, zasad ochrony danych, przetwarzania danych osobowych, danych wrażliwych, celów w zakresie gwarancji bezpieczeństwa i ochrony informacji, warunków przetwarzania danych oraz zasad zapewniania spójnego stopnia ochrony osób fizycznych, a także polityki ochrony danych osobowych.

We *wnioskach* (5 stron) tego rozdziału stwierdzono mi.in. (co wdaje się ważne), że „zbyt duża rozpiętość i zasięg kierowania organizacją jaką jest Państwowa Straż Pożarna negatywnie wpływa na poprawne jej funkcjonowanie, co z kolei wpływa na procesy informacyjne i komunikację. Uwzględniając także stosowane rozwiązania komunikacyjne zasadnym wydaje się podjęcie działań zmierzających do usprawnienia obiegu informacji, co powinno przełożyć się na skuteczność działania w przypadku organizacji zhierarchizowanej. (...) Dynamika rozwoju systemów oraz zagrożeń powoduje konieczność wytwarzania elastycznych i podatnych na zmiany rozwiązań zabezpieczających, które pozwolą na modyfikację w krótkim czasie w przypadku zmiany środowiskowej. Zagrożenia stanowią działania ukierunkowane na składowe systemu informatycznego mogące powodować szkody. W celu zwiększenia bezpieczeństwa danych opisuje się zabezpieczenia normami i standardami bezpieczeństwa".

Ważnym wnioskiem jest stwierdzenie, że w ramach „modernizacji Systemu Wsparcia Decyzji (SWD) PSP należy dokonać zmiany architektury z rozproszonej na scentralizowaną, co usprawni procesy obsługi zdarzeń oraz umożliwi łatwiejszą integrację z zewnętrznymi systemami teleinformatycznymi, w tym w szczególności z systemem powiadamiania ratunkowego. Nowy SWD PSP powinien być także platformą współpracy z jednostkami Ochotniczych Straży Pożarnych, które powinny mieć nieodpłatny dostęp do modułu systemu. Jest to niezwykle istotna zmiana, której prawidłowe przeprowadzenie zdecydowanie poprawi

komfort pracy dyżurnego stanowiska kierowania. W chwili dysponowania jednostek ochotniczych będzie on kierował się informacjami o tym, które jednostki OSP i w jakiej sile deklarują swój udział w akcji ratowniczej. Jednocześnie system umożliwi dostęp do informacji druhom ochotnikom, którzy w chwili otrzymania zgłoszenia będą wiedzieć, do jakiego zdarzenia się udają i ilu członków ich jednostki zadeklarowało gotowość bojową".

Rozdział 4. *(KONCEPCJA BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO W PAŃSTWOWEJ STRAŻY POŻARN)* – ss.181-290 – zawiera analizę wyników z badań własnych Doktoranta oraz koncepcję rozwoju systemu informacyjnego Państwowej Straży Pożarnej w aspekcie bezpiecznej, pewnej i sprawnej komunikacji na wielu płaszczyznach, w ramach której zaproponowano: 1) strategię cyfryzacji formacji, gdzie odniesiono się do celu koncepcji rozwoju systemu wymiany informacji, 2) referencyjną architekturę cyberbezpieczeństwa w PSP, 3) wdrożenie mechanizmów w zakresie uruchamiania awaryjnych planów ewakuacji dyspozytorów i dyżurnych operacyjnych oraz sprzętu technicznego w miejsca zastępcze, 4) wdrożenie zmian prawno-formalnych.

W ramach *wniosków* z badań zawartych w rozdziale zasadnie podkreślono, że „cyfryzacja jest niezbędna dla Państwowej Straży Pożarnej, aby stać się bardziej efektywną, skuteczną i nowoczesną instytucją. Wprowadzenie cyfryzacji to także szansa na zwiększenie zaufania obywateli do PSP i poprawę jakości świadczonych usług. Dlatego PSP powinno być liderem w procesie cyfryzacji i angażować się w działania zmierzające do jej wprowadzenia. Państwowa Straż Pożarna musi być instytucją, która zdaje sobie sprawę z potrzeby cyfryzacji i modernizacji swojej działalności. W celu osiągnięcia tego celu, PSP powinno dążyć do stworzenie zespołów Citizen Developerów, które będą odpowiedzialne za tworzenie i rozwijanie aplikacji i narzędzi potrzebnych strażakom do wykonywania swoich obowiązków. Citizen Developerzy powinni współpracować z IT i powinni mieć dostęp do narzędzi typu Low-Code, No-code, które pozwolą im na szybkie i łatwe tworzenie oprogramowania dostosowanego do potrzeb strażaków"

W tym też kontekście **pytanie (2.)**: PSP liderem pośród jakich instytucji?

Rozdział ten jest największy (109 stron) spośród trzech merytorycznych i jak oznajmia Doktorant „stanowi empiryczną część pracy, obejmującą badania własne autora, które pomogły mu w opracowaniu własnej, nowatorskiej koncepcji bezpieczeństwa systemu informacyjnego w Państwowej Straży Pożarnej. Twórca nakreślił w niej kierunki zmian w funkcjonowaniu

i organizacji systemu informacyjnego na poziomach organizacyjnym, technicznym i funkcjonalnym w celu poprawy jego bezpieczeństwa".

W *ZAKOŃCZENIU* (na stronach 295 - 298) odniesiono się m.in. do celu badań przyjętego w części metodologicznej dysertacji, problemu badawczego i problemów szczegółowych badań a także hipotezy, która według Doktoranta zweryfikowała się pozytywnie – co należy uznać za słuszne. W tej części – podsumowując wysiłek badawczy – stwierdza On że „cel rozprawy został osiągnięty, a sformułowane problemy badawcze rozwiązane. Potwierdzona została również trafność przyjętych hipotez roboczych". I to też jest prawdą.

Istotnym doświadczeniem na bazie badań i wyartykułowanym w *zakończeniu* jest założenie, że „bardzo ważnymi elementami wpływającymi na skuteczność funkcjonowania instytucji Państwowej Straży Pożarnej jako organizacji zhierarchizowanej są ludzie z ich wiedzą, doświadczeniem i umiejętnościami, dopiero w dalszej kolejności struktura organizacyjna oraz system informacyjny, uwzględniając przy tym zarówno otoczenie wewnętrzne jak i zewnętrze organizacji".

Reasumując część merytoryczną należy przyjąć, że w trakcie badań skorzystano z licznych źródeł, czego ewidencję mamy w bogatej *Bibliografii* oraz przypisach dolnych – 77 pozycji. Rozprawę zawarto na 323 stronach i jest ona solidnym dziełem naukowym. Stwierdzam, iż tę część rozprawy należy ocenić jako wielce interesującą i konstruktywną w swej 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.

Konkludując należy podkreślić, że dysertacja stanowi solidną prezentacją wiedzy z obszaru zakreślonego przedmiotem badań oraz jest obszernym zbiorem wyczerpujących treści odnoszących się do systemu bezpieczeństwa wymiany informacji PSP – zarówno w obecnym stanie jak i pod względem konieczności jego usprawnienia zgodnie z warunkami bezpieczeństwa, jakie są w tym wypadku niezbędne. 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 odnoszących się do funkcjonowania PSP, a szczególnie dotyczących wymiany informacji.

Doktorant potrafi budować dzieło naukowe na bazie badań – właściwie prezentując kwestie metodologiczne oraz treści merytoryczne rozdziałów, kończąc je wnioskami 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, jaki zaprezentowano w części metodologicznej.

WNIOSEK KOŃCOWY

Oceniam rozprawę jako bardzo dobrą, gdyż Doktorant dokonał zasadnie weryfikacji hipotez, rozpracowując trudne problemy badawcze, a uzyskane wnioski istotnie wnoszą na rzecz zamieszczonej w dysertacji koncepcji systemu bezpieczeństwa wymiany informacji w Państwowej Straży Pożarnej. Dysertacja posiada elementy oryginalności, a przy jej opracowaniu użyto poprawnego języka i trafnej terminologii. Pojawiające się w dysertacji drobne potknięcia nie obniżają wartości jej treści oraz użyteczności w praktyce PSP. Pozostaje mieć nadzieję, że postawione tezy i zaproponowane rozwiązania zastosowane w procesie badawczym poddane zostaną weryfikacji przy realizacji tej koncepcji oraz kolejnych dociekaniach/rozważaniach naukowych z omawianego i badanego przez Doktoranta obszaru badań.

Doktorant wykazał się umiejętnością: analizowania naukowej literatury, projektowania badań własnych oraz ich prowadzenia, analizowania i interpretowania wyników badań, formułowania wniosków i pisania złożonych tekstów naukowych.

Stwierdzam, że przedłożona do recenzji rozprawa doktorska Pana mgr. inż. Andrzeja BARTKOWIAKA 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 *Ustawy z dnia 20 lipca 2018 r. prawo o szkolnictwie wyższym i nauce* (Dz. U. 2022 r., ze zm.).

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

.....