

Prof. dr hab. inż. Piotr SIENKIEWICZ
Wojskowa Akademia Techniczna
Prof. emeritus

Warszawa, 2.12.2022

RECENZJA

Rozprawy doktorskiej mgr inż. Mariusza DOMAŃSKIEGO nt. „PROCES TRANSFORMACJI KSZTAŁCENIA W OBSZARZE CYBERBEZPIECZEŃSTWA W KRAKOWSKIEJ AKADEMII IM. ANDRZEJA FRYCZA MODRZEWSKIEGO”. Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Wydział Nauk o Bezpieczeństwie. Kraków 2019. Promotor: prof. dr hab. Sławomir MAZUR

1. Uwagi wstępne

Spółeczeństwo przełomu XX i XXI wieku rozwija się w klimacie niepewności i ryzyka, który postrzegany jest w różnej skali i w różnych, niemal wszelkich, sferach ludzkiej aktywności. „Wiek niepewności” ustąpił „społeczeństwu ryzyka”, o którym pisze się, że jest społeczeństwem katastrof, któremu zagraża to, że stany wyjątkowe stają się stanami normalnymi. Naczelną kategorią opisu współczesności stało się BEZPIECZEŃSTWO. Wyłonienie się na początku XXI wieku w pełni odpowiadało potrzebom społecznym, w tym edukacyjnym, ale stało się zjawiskiem istotnym dla rozwoju społeczeństw, współczesnych systemowych badań naukowych oraz wyzwań edukacyjnych. („*Nowoczesność to kultura ryzyka. Nowoczesność zmniejsza ogólną ryzykowność pewnych sfer i sposobów życia, ale jednocześnie wprowadza nowe, prawie lub całkiem nieznanie wcześniejszym epokom parametry ryzyka*”). Wiek XX zapoczątkował rewolucje cywilizacyjne, których istotą stało się

powstanie i rozwój społeczeństwa informacyjnego oraz technologii informacyjnych (cyfrowych), kształtujących jego oblicze w kategoriach CYBERPRZESTRZENI. Obecna rewolucja informacyjna jest czwartą rewolucją tego typu w historii ludzkości. Pierwszą było wynalezienie druku, drugą zapoczątkowało wynalezienie książki, trzecią zaś wynalezienie przez Gutenberga maszyny drukarskiej z ruchomymi czcionkami. Czwartą rewolucję należy wiązać się z wynalazkiem komputera i rozwojem systemów łączności (telekomunikacji) wykorzystujących energię elektryczną i potencjał elektroniki (1946). Wydarzeniem o cechach rewolucji cywilizacyjnej było wyłonienie się INTERNETU (1990) jako swoistej megasieci oraz „wchłonięcie” przez społeczeństwa technologii internetowych we wszystkich sferach aktywności społecznej. Powyższe konstatacje, określają rozległy obszar badań naukowych nad bezpieczeństwem społecznym, w wymiarze CYBERPRZESTRZENI oraz generowanych problemów CYBERBEZPIECZEŃSTWA („cybernetycznych zagrożeń”). Powyższe oczywiste uwagi zmierzają do podkreślenia znaczenia problemów wyzwań EDUKACYJNYCH związanych z potrzebami (koniecznością) społecznymi w nowych sytuacjach związanych z rewolucją informacyjną.

Zanim przejdę do konkretyzacji ocen i wniosków, pragnę, na wstępie, wyrazić uznanie dla zaprezentowanej rozprawy, którą oceniam jako wyróżniającą się wśród znanych mi w ostatnich latach dysertacji powstałych w dyscyplinie nauki o bezpieczeństwie. To duża satysfakcja dla piszącego te słowa, zwłaszcza, że objętość rozprawy, mnogość odniesień do licznych źródeł, korzystania z ogólnie dostępnej wiedzy, ale- niekiedy w nadmiarze- z wiedzy szczegółowej pochodzącej z autorskich badań empirycznych wymagały niemałego wysiłku.

2. Ocena metodologiczna

Rozprawa ma charakter analityczno - ocenowy uwzględniający zarówno aktualny stan wiedzy dotyczącej teoretycznych podstaw

cyberprzestrzeni, zagrożeń cyberbezpieczeństwa oraz sposobów przeciwdziałania cyberzagrożeniom w Polsce, ze szczególnym uwzględnieniem aspektów edukacyjnych w ramach kampanii społecznej o charakterze edukacyjno-prewencyjnym. Celem jej miało być podniesienie świadomości obywateli Rzeczypospolitej Polskiej, działających w obszarze cyberprzestrzeni. Program miał w zakresie edukacji społeczeństwa uświadamiać o zagrożeniach wynikających z użytkowania cyberprzestrzeni. Świadomość oraz wiedza społeczeństwa w efekcie realizacji programu miała pozwolić na ograniczenie ryzyka, wynikającego z pojawiających się zagrożeń w cyberświecie. Podkreślenia wymaga, fakt, iż miała mieć charakter wielowymiarowy, tak by dotrzeć do szeregu zainteresowanych grup społecznych, a w szczególności do instytucji publicznych, przedsiębiorców, organizacji społecznych, jak i użytkowników indywidualnych. Zakładała, że kampania będzie długofalowa i powszechna. Zalecano, by była skierowana głównie do dzieci, młodzieży, rodziców i nauczycieli. Wiedza o zagrożeniach, adresowana do dzieci, młodzieży i rodziców w dużej mierze miała być realizowana w placówkach oświatowych wszystkich szczebli. Analiza doświadczeń z realizacji przedsięwzięć stanowiła podstawę tworzonych programów kształcenia z zakresu cyberbezpieczeństwa, realizowanych w Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego na Wydziale Nauk o Bezpieczeństwie.

W recenzowanej pracy przyjęto: **cel eksploracyjny, opisowy i wyjaśniający**. I tak, Celem eksploracyjnym :było (...) *zaspokojenie ciekawości badacza(...)* , *zdobycie wiedzy na temat funkcjonowanie studentów w cyberprzestrzeni, zapewniające im bezpieczne użytkowanie sieci, urządzeń i aplikacji*. Celem opisowym był (...) *opis jakiejś sytuacji lub wydarzenia (...)* , *czyli przedstawienie na podstawie badań wykrytych zjawisk i faktów występujących w cyberprzestrzeni użytkowanej przez studentów*. Celem wyjaśniającym było *wskazanie, wynikające z procesu badawczego, rzeczywistych czynników wpływających na cyberbezpieczeństwo studentów wraz z próbą poznaniem ich przyczyn i uzasadnieniem pożądaných zmian*. W związku z określeniem przedmiotu i celów badań, sformułowano

następujący **problem główny**: *Czym warunkowane jest bezpieczne funkcjonowanie w cyberprzestrzeni studentów Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego?* Rozwiązanie głównego problemu badawczego, wymagało uzyskania odpowiedzi na osiem problemów szczegółowych(...). Dla tak przyjętego celu i głównego problemu badawczego sformułowano hipotezę główną. Do każdego problemu badawczego sformułowano hipotezy szczegółowe (H1.- H8.) W celu rozwiązania problemu badawczego opisano zmienną zależną oraz zmienne niezależne wraz z ich wskaźnikami. Zmienną zależną (ZZ) określono bezpieczne funkcjonowanie w cyberprzestrzeni. Do wyjaśniania zmiennej zależnej wyodrębniano zmienne niezależne(np. ZN1 - codzienne zachowania studentów w cyberprzestrzeni). Trafnie dokonano doboru celu badań oraz głównego i szczegółowych problemów badawczych i hipotezy roboczej. Na szczególne uznanie zasługuje dobór procedur i metod badawczych. Doktorant umiejętnie stosował technikę badań ankietowych, podstawowe narzędzia analizy statystycznej oraz oprogramowanie wspomagające badania(np. 30-dniowa wersja IBM SPSS Statistics). .

Doktorant wykazał bardzo dobrą znajomość wiedzy z obszaru cyberbezpieczeństwa pozwalającą na analizę zagrożeń bezpieczeństwa cyberprzestrzeni, aktywnie uczestnicząc w projektach edukacyjnych pozwalających na praktyczną weryfikację autorskich koncepcji i wnosząc istotne wartości poznawcze do dorobku zespołów projektowo-badawczych.

Rozprawa składa się z części zasadniczej(282 stron) i załącznika do rozprawy(ss 233-307). Praca dzieli się na trzy rozdziały zasadnicze , wstęp, zakończenie, bibliografię(pozycje zwarte i artykuły, liczne źródła internetowe). Między rozdziałami zachowano właściwe(?) proporcje, treść pracy zgodna jest z jej tytułem , a rozdziałów z ich nagłówkami, zaś nagłówki dają syntetyczny pogląd na rozważaną w nich treść. Wywody stanowią logicznie powiązaną całość. Strona redakcyjna i edytorska jest w pełni zadowolająca, wręcz wzorcowa(poza nielicznymi usterkami redakcyjnymi). Przedstawiono

30 rysunków i 140 tabel. Sądzę natomiast, że należało zredukować treści o charakterze „podręcznikowym” poświęcone np. pojęciom podstawowym. One zaś dominują treść, zarówno rozdziału 1, jak i rozdziału 2. Treść rozdziału 1 poświęcono w znacznej mierze analizie literatury, jest interesująca, lecz niewiele wnosi do wiedzy ogólnej z obszaru nauk o bezpieczeństwie. Uważam, że właściwe byłoby zredukowanie treści do pożądanego minimum (ponad 80 ss). Rozdział 2 poświęcono metodologii badań własnych, rozszerzonej o odwołania do ogólnej wiedzy metodologicznej badań społecznych. Ogólny proces badawczy został konsekwentnie w pełni zrealizowany. Z metodologicznego punktu widzenia rozprawa w pełni zasługuje na pozytywną ocenę. Dokonano właściwego, dla przyjętej metodologii, wyboru metod i technik badań empirycznych (np. metoda obserwacji, metoda sondażu diagnostycznego, kwestionariusz ankiety, wywiad ekspercki, itp.). Natomiast rezultaty badań własnych oraz proces ich pozyskiwania stanowią treść rozdziału 3, wyraźnie dominującego, zawierającego znaczącą wartość merytoryczną w obszarze badań społecznych na potrzeby cyberbezpieczeństwa. Analiza wyników badań bezpiecznego funkcjonowania w cyberprzestrzeni studentów Uczelni w pełni zasługuje na pozytywną ocenę.

3. Ocena merytoryczna

Wyniki badań własnych i elementy ich ewaluacji przedstawiono w ośmiu podrozdziałach rozdziału 3, a mianowicie: codzienne funkcjonowanie studentów w cyberprzestrzeni (CB), doświadczenia studentów z korzystania z CB w warunkach zagrożeń, praktyczna wiedza z wybranego obszaru CB, ocena dotychczasowej edukacji, poziom wiedzy studentów, stopień przygotowania studentów do funkcjonowania w CB, zmiany w programie kształcenia w celu przygotowania studentów do bezpiecznego korzystania z CB. Autor stwierdza, że przyjęta w rozprawie hipoteza główna została „częściowo zweryfikowana”. Stwierdzam, że zarówno z metodologicznego, jak i merytorycznego punktu widzenia

recenzowana rozprawa zasługuje na pozytywną ocenę. Ponadto posiada cechy użytecznego materiału dydaktycznego.

Podczas publicznej obrony proszę o odniesienie się do następujących kwestii:

- 1) istnieją metody i techniki analizy ryzyka zagrożeń bezpieczeństwa cyberprzestrzeni, lecz większość z nich odznacza się ograniczeniami metodologicznymi; proszę wskazać najczęściej wykazywane mankamenty w analizach porównawczych;
- 2) proszę o przedstawienie modelu statystycznego studenta Uczelni na podstawie przeprowadzonych badań własnych;
- 3) proszę o wyrażenie opinii na temat użyteczności współczesnych badań w analizie ontologii cyberbezpieczeństwa.

Stwierdzam, że praca spełnia podstawowe wymagania stawiane pracom o charakterze poznawczym w dyscyplinie nauki o bezpieczeństwie, w obszarze bezpieczeństwa cyberprzestrzeni. Zasługuje na pozytywną ocenę z merytorycznego punktu widzenia. Rozprawę oceniam jako wyróżniającą, oryginalną i innowacyjną, ukierunkowaną na wspomaganie edukacji w obszarze cyberbezpieczeństwa.

4. Uwagi końcowe i wnioski

Stwierdzam, że Doktorant:

- 1) opanował umiejętności samodzielnego rozwiązywania zagadnień naukowych, które zostały wykazane w rozprawie doktorskiej i powinny być potwierdzone podczas publicznej obrony;
- 2) opanował odpowiednio szeroką i pogłębioną ogólną wiedzę teoretyczną z dyscypliny „nauki o bezpieczeństwie”;
- 3) opanował istotne podstawy wiedzy ogólnej, niezwiązanej z zakresem specjalizacji naukowej.

Stwierdzam, że rozprawa doktorska Pana mgr inż. **Mariusza DOMAŃSKIEGO** spełnia wymagania określone ustawą z dnia 14 marca 2003 r. o stopniach i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz.U. poz. 595, ze zm.).

c

Wnoszę o dopuszczenie recenzowanej rozprawy doktorskiej do publicznej obrony.

A handwritten signature in black ink, consisting of a large, stylized initial 'S' followed by a series of smaller, connected loops and a final horizontal stroke.