

RECENZJA

rozprawy doktorskiej Pana mgr. inż. Krzysztofa WOSIŃSKIEGO

na temat:

Znaczenie wywiadu opartego na otwartych źródłach (OSINT) w zapewnieniu bezpieczeństwa systemów teleinformatycznych i bezpieczeństwa osobowego,

opracowanej pod kierownictwem naukowym dr. hab. inż. Piotra DELI

Ocena wstępna rozprawy

Podstawą sporządzenia niniejszej recenzji jest Uchwała Rady Naukowej Dyscypliny Nauk o Bezpieczeństwie Akademii Kaliskiej nr 3/NOB/2023 z dnia 26.01.2023 r. Przedstawiona do recenzji rozprawa doktorska to praca pisemna, która prezentuje ogólną wiedzę teoretyczną autora w *dziedzinie nauk społecznych, w dyscyplinie nauki o bezpieczeństwie* oraz sposób samodzielnego prowadzenia przez niego pracy naukowej. Przedmiotem rozprawy są: oryginalne rozwiązanie problemu naukowego oraz przedstawione w pracy wyniki badań naukowych autora w sferze społecznej. Praca napisana jest w języku polskim, a do pracy dołączone zostało streszczenie w języku polskim i w języku angielskim.

Zasadnicza część pracy składa się ze wstępu, pięciu rozdziałów, w tym rozdziału zawierającego założenia badawcze (rozdział 1) oraz zakończenia i bibliografii. Do pracy dołączono spisy tabel i rysunków oraz wykaz skrótów. Załącznikiem do pracy są: arkusz wywiadu z pytaniami dla ekspertów oraz wyniki przeprowadzonego przez autora wywiadu eksperckiego. Całość przedstawionej do recenzji pracy zawiera się na 181 stronach, a każdy rozdział merytoryczny pracy zakończony jest wnioskami własnymi autora.

Tytuł rozprawy i tematyka przedstawionej do recenzji pracy oraz przyjęte w niej założenia metodologiczne wskazują na naukowe dociekania autora, których celem jest odpowiedź na zawarty w pracy główny cel badawczy oraz uzyskanie odpowiedzi na wskazane problemy badawcze (główny i szczegółowe) w ujęciu diagnostycznych oraz w ujęciu prognostycznym. Autor wykazał zatem potrzebę zbadania podjętej w dysertacji problematyki, osądzając swoje poznawcze działania w dotychczasowym stanie teorii i praktyki, wynikającej także z własnych doświadczeń życiowych oraz zawodowych.

Ocena charakteru rozprawy

1. Ocena założeń badawczych pracy

W recenzowanej dysertacji autor właściwie przedstawił uzasadnienie podjęcia badań, wskazał jak ważna jest z punktu widzenia bezpieczeństwa teleinformatycznego i osobowego podjęta tematyka badawcza i wskazał jako przedmiot badań: *zabezpieczenia systemów teleinformatycznych, podłączonych do Internetu oraz procedury bezpieczeństwa osobowego w zakresie ochrony informacji o aktualnym położeniu i statusie osób, a także w odniesieniu do informacji technologicznych z nimi związanych (str.16)*. Podjęta tematyka jest także analizowana w pracy przez autora z punktu widzenia własnych doświadczeń zawodowych jako trenera cyberbezpieczeństwa.

Jako główny cel poznawczy badań autor wskazał na *identyfikację i ustalenie możliwości uzyskania szczegółowych informacji, wynikających z przeprowadzanego wywiadu otwartoźródłowego, w odniesieniu do systemów teleinformatycznych oraz indywidualnych osób, a także zidentyfikowanie zagrożeń wynikających z tego typu działań oraz metod skutecznej obrony przed przedmiotowym rozpoznaniem*. Celem pragmatycznym dla autora było *opracowanie koncepcji i weryfikacja dostępnego zbioru informacji zawierających szczegóły techniczne, osobowe oraz geolokalizacyjne, dotyczące systemów teleinformatycznych oraz osób, a także określenie możliwości wprowadzenia zabezpieczeń przed działaniem zidentyfikowanych technik (str.17)*. Główny problem badawczy (str.17) autor postawił w postaci pytania: *w jakim zakresie dostępne narzędzia, służące do gromadzenia informacji w ramach wywiadu otwartoźródłowego oraz techniki ich analizy wpływają na bezpieczeństwo systemów teleinformatycznych oraz bezpieczeństwo osobowe, a także jakie są możliwości obrony przed zidentyfikowanymi technikami?*

Do tak przedstawionego problemu głównego autor wskazał na problemy szczegółowe (str.17) zawarte w 4 pytaniach: *Jakie narzędzia i techniki wywiadu otwartoźródłowego są dostępne dla użytkowników Internetu? W jaki sposób należy poddawać analizie zebrane informacje, aby uniknąć ich błędnej interpretacji? Jakie zagrożenia płyną z powszechnej możliwości stosowania wywiadu otwartoźródłowego oraz nieprawidłowej analizy danych pozyskanych w ramach przedmiotowych działań w Internecie? Jakie są możliwości zabezpieczenia infrastruktury teleinformatycznej oraz zapewnienia bezpieczeństwa osobowego przed działaniami wynikającymi z prowadzonego wywiadu otwartoźródłowego?*

Próbie odpowiedzi na pytanie zawarte w problemie głównym autor sformułował w postaci hipotezy roboczej, zakładając iż w związku z coraz szerszym wachlarzem narzędzi i usług, dostarczających szeroki zakres danych w Internecie oraz poprzez coraz powszechniejszy dostęp do Internetu i znajomości sposobów na wyszukiwanie w nim treści, a także ze względu na fakt, że praktycznie wszystkie aspekty życia osobistego i zawodowego mają swoje odzwierciedlenie w systemach operujących w chmurze, istnieje zwiększające się zagrożenie zarówno dla bezpieczeństwa systemów teleinformatycznych, które te dane przetwarzają, jak i bezpieczeństwa osobowego, które jest bezpośrednio związane z kwestią poufności i integralności przetwarzanych danych. Możliwości i umiejętności użytkowników Internetu dają im sposobność na sprawdzenie jakie dane mogą zdobyć bez narażania się na bezpośrednio niebezpieczeństwo związane z infiltracją źródeł danych. Podobnie odniósł się w swoich przypuszczeniach i sądach do wskazanych wcześniej problemów szczegółowych, przedstawiając w pracy 4 szczegółowe hipotezy robocze, zapisane na str.18-20.

Cel główny, główny problem badawczy i główna hipoteza robocza są poprawnie sformułowane i właściwie ze sobą skorelowane, podobnie prawidłowo zostały sformułowane problemy szczegółowe i hipotezy odnoszące się do tych problemów. Autor nie wskazał w założeniach badawczych celów szczegółowych do głównego celu badawczego a takie wskazanie pozwoliłoby właściwie prześledzić wywód naukowy autora przedstawiony w ramach założeń badawczych w odniesieniu do problemów i hipotez szczegółowych. Nie mniej jednak założenia badawcze tej części dysertacji są prawidłowe.

2. Ocena piśmiennictwa

Oceniam, iż w pracy wykorzystano wystarczającą ilość źródeł. Na bibliografię składa się 25 pozycji zwartych, 10 dokumentów oraz 3 słowniki a także ponad 45 źródeł internetowych (źródła takie wskazane są dodatkowo w załączniku do pracy tj. w analizie odpowiedzi z wywiadu eksperckiego. W przedstawionym w bibliografii wykazie znaleźć można także prace promotora recenzowanej dysertacji oraz materiał autora. Pewną trudność w dokładnej analizie tej części może budzić fakt, że autor nie zdecydował się na ponumerowanie wykazu bibliograficznego.

Na podstawie wykazu przedstawionych źródeł można stwierdzić, że autor wnikliwie dokonał wyboru dostępnych materiałów zwartych i źródeł internetowych i właściwie dobrał literaturę przedmiotu, stwarzając tym samym warunki do jej krytycznej analizy na potrzeby recenzowanej dysertacji.

3. Ocena metod, technik i narzędzi badawczych

Autor wskazał w dysertacji na wykorzystanie jakościowych metod badawczych, jednak przedstawił ten element założeń metodologicznych bardzo ogólnie, posiłkując się jedynie cytataми z literatury dotyczącej metodologii badań. Wskazał jedynie na technikę wywiadu jako wiodącą w swoich badaniach empirycznych. Podobnie w części dotyczącej metod teoretycznych, autor wskazał na krytyczną analizę literatury oraz przedstawił te źródła, które były wykorzystane w poszczególnych etapach jego badań. Ta część dysertacji powinna zostać przedstawiona bardziej szczegółowo. Warto również zauważyć, że pomimo wskazania w ramach metod jakościowych, metody obserwacji, nie została ona wykorzystana w badaniach autora.

Mimo wskazanych uwag, autorowi udało się rozwiązać główny problem badawczy, a także potwierdzić założenia głównej hipotezy roboczej oraz przyjętych hipotez szczegółowych. Oceniając zastosowane metody badawcze można stwierdzić ich właściwe, aczkolwiek ograniczone zastosowanie. Pomimo wskazanych uwag, ocena tej części dysertacji jest pozytywna.

4. Ocena wyników badań

Autor właściwie dokonał krytycznej analizy literatury i wskazanych źródeł, prawidłowo wyciągając wnioski końcowe, dostosowane do każdego z rozdziałów teoretycznych dysertacji. Zastosował wystarczające metody, techniki i narzędzie badawcze, wykorzystane do potwierdzenia hipotez wstępnych i osiągnięcia celu badań. Narzędzie badawcze w postaci arkusza wywiadu i pytań tam zawartych zostało przygotowane prawidłowo a wyniki przeprowadzonego wywiadu pozwoliły autorowi odpowiedzieć na pytania problemowe i przygotować wnioski końcowe pracy.

Autor zrealizował dzięki takiej metodyce badawczej cel pracy związany z weryfikacją dostępnego zbioru informacji zawierających szczegóły techniczne, osobowe oraz geolokalizacyjne, dotyczące systemów teleinformatycznych oraz osób, a także prawidłowo określił możliwości wprowadzenia zabezpieczeń przed działaniem zidentyfikowanych przez siebie technik. Jednak drugim z celów pragmatycznych badań było opracowanie koncepcji w w/w wskazanym w pracy środowisku. Takiej koncepcji w pracy nie odnaleziono, nie została też taka koncepcja dołączona do pracy jako jej załącznik.

W pracy brakuje też charakterystyki próby badawczej tj. charakterystyki ekspertów wybranych do badań. Autor nie wskazał takich ekspertów, nie dokonał ich charakterystyki

a jedynie przedstawił anonimowo ich odpowiedzi na przygotowane wcześniej pytania i wskazał na źródła internetowe, które zostały wykorzystane w tej części sprawozdania.

W sprawozdaniu z badań teoretycznych autor przygotował i posługuje się rysunkami i tabelami, które wzmacniają wnioskowanie autora przedstawione w poszczególnych rozdziałach pracy. Są one bardzo estetycznie wykonane i zawierają niezbędne dane pozwalające śledzić proces badawczy autora.

Mimo wskazanych uwag, procedura badawcza zastosowana w pracy jest prawidłowa i jej zastosowanie doprowadziło autora do rozwiązania zidentyfikowanego problemu naukowego. Wnioskowanie autora na podstawie wyników badań empirycznych także jest prawidłowe i krytyczne, co podnosi wartość przedstawionych w pracy wyników i daje możliwość ich zastosowania ich w praktyce. Przedstawione wyniki badań oceniam jako oryginalne, stanowiące wartość naukową i wartość praktyczną dla kolejnych tego typu badań.

5. Ocena rozwiązania problemu badawczego

Po analizie treści rozprawy doktorskiej w części dotyczącej sformułowania głównego problemu badawczego oraz problemów szczegółowych, można stwierdzić, że autor zaproponował samodzielne rozwiązanie, którego podstawę stanowiły kompetentnie przeprowadzone badania naukowe, zarówno teoretyczne jak i empiryczne. Oryginalne rozwiązanie problemu badawczego przez autora obejmuje m.in. weryfikację dostępnego zbioru informacji zawierających szczegóły techniczne, osobowe oraz geolokalizacyjne, dotyczące systemów teleinformatycznych oraz osób, a także prawidłowe określenie możliwości wprowadzenia zabezpieczeń przed działaniem zidentyfikowanych przez siebie technik.

W ramach pierwszego rozdziału merytorycznego autor skupił się na umiejscowieniu OSINT-u w środowisku różnorodnych rodzajów rozpoznania, gdzie współistnieje on m.in. z takimi rodzajami jak: HUMINT, SIGINT, IMINT oraz MASINT (rozdział 2). Autor wskazał także na czynniki ludzkie, mogące mieć wpływ na proces prowadzenia wywiadu otwartoźródłowego. Przedstawił także metody minimalizowania wpływu tego typu czynników na wyniki prowadzonego rozpoznania i zdrowie samych analityków (rozdział 3). Zidentyfikował także metody wykorzystania wywiadu otwartoźródłowego w zakresie bezpieczeństwa systemów teleinformatycznych oraz bezpieczeństwa osobowego i biznesowego. Dodatkowo wskazał zabezpieczenia, które należy wziąć pod uwagę w zakresie bezpieczeństwa osobowego (rozdział 4). Autor przedstawił także możliwe do wprowadzenia zalecenia bezpieczeństwa w zakresie przeciwdziałania wywiadowi

otwartoźródłowemu, co stanowi zestawienie metod i technik ochrony, zarówno infrastruktury firmowej lub organizacyjnej, jak i osobowej. Wskazał też dwa obszary, w których wykorzystywany jest OSINT – w zakresie rozpoznania podmiotu będącego celem, oraz samoweryfikacji zabezpieczeń, poprzez stworzenie programu testów zakresu możliwego pozyskania informacji przy wykorzystaniu technik OSINT-owych oraz zaproponował wprowadzenie odpowiednich zabezpieczeń przeciwko potencjalnym atakom z ich wykorzystaniem. Wskazał w pracy także normy, zestawienia i techniki, które mogą stanowić bazę do wprowadzania metod zabezpieczeń.

Dodatkowo autor określił zasady, które muszą zostać zachowane, aby zminimalizować ryzyko działań w Internecie, wraz ze wskazaniem ich rozróżnienia dla obszaru bezpieczeństwa biznesowego i osobistego. W dysertacji przedstawione zostały także podstawy i metody rozszerzenia wskazanych zasad zabezpieczeń na otoczenie kluczowych osób w organizacjach, ze względu na ich dostęp do cennych informacji decyzyjnych, które mogą stanowić obiekt zainteresowania osób lub organizacji atakujących (rozdział 5).

Zawarte w rozdziałach merytorycznych analizy i przedstawione wnioski pozwoliły autorowi rozwiązać szczegółowe problemy badawcze, co w konkluzji miało wpływ na rozwiązanie głównego problemu badawczego. Ten aspekt rozprawy oceniam pozytywnie.

6. Ocena formalna rozprawy

Recenzowana dysertacja została przedstawiona w postaci sprawozdania z badań jako zwarte opracowanie naukowe na 181 stronach. Układ pracy przedstawiony został w spisie treści. W pracy umieszczono jej streszczenia w języku polskim i angielskim. Problematyka pracy została zawarta w rozdziale metodologicznym i 4 kolejnych rozdziałach merytorycznych. W pracy wyszczególniono bibliografię oraz przedstawiono spisy tabel i rysunków a także wykaz zastosowanych w pracy skrótów. Do pracy dołączono załącznik w postaci arkusza wywiadu (10 pytań do ekspertów) i wyników tych badań. Struktura recenzowanej rozprawy doktorskiej jest prawidłowa i przemyślana. Struktura rozprawy jest czytelna, a przeprowadzone wywody stanowią logicznie powiązaną i uporządkowaną całość. Każdy z czterech zawartych w rozprawie rozdziałów merytorycznych zakończony został syntetycznymi wnioskami własnymi autora, ułatwiającymi śledzenie i analizę treści wywodu naukowego prowadzonego przez doktoranta. W pracy doktorant zachował właściwą proporcję pomiędzy rozdziałami.

W ramach pierwszego rozdziału merytorycznego autor skupił się na umiejscowieniu OSINT-u w środowisku różnorodnych rodzajów rozpoznania, gdzie współlistnieje on m.in. z takimi rodzajami jak: HUMINT, SIGINT, IMINT oraz MASINT. Określił ramy, w jakich musi mieścić się rozpoznanie, aby było uznawane za OSINT w rozumieniu nomenklatury NATO-wskiej oraz amerykańskich dyrektyw wywiadowczych. Wskazał także odrębny obszar rozpoznania, którego bazą są media społecznościowe – SOCMINT. W drugim rozdziale merytorycznym autor skupił się na procesie analizowania informacji, pozyskanych z zasobów internetowych jako fundamentu wywiadu, szczególnie w aspekcie tworzenia wiedzy wywiadowczej na podstawie zebranych informacji oraz wpływu psychologicznych cech ludzkich na poprawne prowadzenie tego typu procesu. W ramach trzeciego rozdziału merytorycznego wskazane zostały przez autora zidentyfikowane metody wykorzystania wywiadu otwartoźródłowego w zakresie bezpieczeństwa systemów teleinformatycznych oraz bezpieczeństwa osobowego i biznesowego. Czwarty rozdział merytoryczny, w którym autor przedstawił możliwe do wprowadzenia zalecenia bezpieczeństwa w zakresie przeciwdziałania wywiadowi otwartoźródłowemu, stanowi zestawienie metod i technik ochrony, zarówno infrastruktury firmowej lub organizacyjnej, jak i osobowej.

Opracowane przez autora i zestawione w opisanych wyżej rozdziałach merytorycznych rezultaty badań naukowych zakończone zostały uzasadnionymi wnioskami, stanowiącymi uogólnione odpowiedzi na wygenerowane wcześniej i przedstawione w rozdziale metodologicznym problemy naukowe, będące konstatacją całości dysertacji.

W dysertacji autor przedstawił zatem logicznie uporządkowany i interesujący materiał naukowy o charakterze poznawczym, będący spójnym i sensownym opracowaniem przedmiotu badań i ich wyników.

Strona formalna rozprawy nie budzi większych zastrzeżeń. Tytuł rozprawy jest w pełni zgodny z jej treścią i przedmiotem prowadzonych badań. Praca przygotowana jest w swojej formie bardzo estetycznie i mimo drobnych uwag i niedociągnięć językowych czy edycyjnych, przygotowana jest na wysokim poziomie edytorskim. Cytowania, przypisy i odsyłacze wykorzystane są prawidłowo. Język dysertacji jest właściwy dla rozpraw doktorskich a opracowanie tekstu sprawozdania poprawne. Ocena formalna rozprawy jest pozytywna.

7. Uwagi recenzenta i pytania na obronę

Uwagi i niedociągnięcia wskazane w recenzji dotyczą m.in. braku wyraźnego określenia/przedstawienia koncepcji dotyczącej weryfikacji dostępnego zbioru informacji zawierających szczegóły techniczne, osobowe oraz geolokalizacyjne a także możliwości wprowadzenia zabezpieczeń przed działaniem zidentyfikowanych przez autora technik, co zostało zawarte przez autora w celu pragmatycznym badań.

W pracy brakuje też charakterystyki próby badawczej tj. charakterystyki ekspertów wybranych do badań. Autor nie wskazał takich ekspertów, nie dokonał ich charakterystyki a jedynie przedstawił anonimowo ich odpowiedzi na przygotowane wcześniej pytania. Pomimo opisu jakościowych metod badawczych przyjętych w założeniach badawczych autor nie wykorzystał w badaniach obserwacji jako metody możliwej do zastosowania w przyjętej procedurze badawczej, zwłaszcza, że w metodzie tej możliwe było wykorzystanie doświadczenia zawodowego autora dysertacji oraz jego środowiska pracy.

Wskazanie uwag i niedociągnięć oraz wątpliwości w przedstawionej recenzji powinno być podstawą do dyskusji naukowej w ramach publicznej obrony rozprawy doktorskiej. Wskazanie powyższych uwag i niedociągnięć nie ma wpływu na pozytywną ocenę poszczególnych części pracy przedstawionych w recenzji, ale wymaga ich wyjaśnienia i odniesienia się do nich przez doktoranta w ramach odpowiedzi na poniższe pytania:

1. Proszę o odniesienie się do faktu braku dokładnego wskazania/przedstawienia koncepcji zawartej w treści określającej cel pragmatyczny badań?
2. Proszę o odniesienie się do faktu anonimizacji ekspertów, którzy brali udział w badaniach empirycznych i braku charakterystyki tej próby badawczej?
3. Proszę o odniesienie się do braku wykorzystania obserwacji jako możliwej do zastosowania jakościowej metody badawczej?
4. Proszę o wyjaśnienie z punktu widzenia przedmiotu badań pojęć: *bezpieczeństwo informacyjne i bezpieczeństwo informacji?*

Wnioski końcowe

Rozprawę doktorską Pana mgr. inż. Krzysztofa WOSIŃSKIEGO na temat *Znaczenie wywiadu opartego na otwartych źródłach (OSINT) w zapewnieniu bezpieczeństwa systemów teleinformatycznych i bezpieczeństwa osobowego* oceniam jako wartościowe i oryginalne rozwiązanie problemu naukowego w *dziedzinie nauk społecznych, w dyscyplinie nauki o bezpieczeństwie*. Wyniki badań przedstawione w pracy wskazują na wiedzę metodologiczną autora oraz jego umiejętności rozwiązywania

problemów naukowych. Autor rozprawy wykazał się także wiedzą w obszarze prowadzonych badań i umiejętnościami posługiwania się metodami, technikami i narzędziami badawczymi wykorzystywanymi w prowadzonych badaniach naukowych. Autor prawidłowo dostrzega problem naukowy określony w rozprawie, prawidłowo uzasadnia jego istnienie i właściwie go rozwiązuje.

Biorąc pod uwagę powyższe uznaję, że rozprawa doktorska Pana mgr. inż. Krzysztofa WOSIŃSKIEGO odpowiada wymogom artykułu 187 ustawy z dnia 20 lipca 2018 r. roku *Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2022 r. poz. 574, 583, 655, 682, 807, 1010, 1079, 1117, 1459, 2185, 2306, z 2023 r. poz. 212) i przedstawiam Radzie Naukowej Dyscypliny Nauk o Bezpieczeństwie Akademii Kaliskiej wniosek o przyjęcie recenzowanej rozprawy doktorskiej i dopuszczenie jej autora do publicznej obrony.



