Prof. dr hab. inż. Dominik Sankowski
Instytut Informatyki Stosowanej
Politechnika Łódzka

Łódź, 4 października 2021r.

RECENZJA ROZPRAWY DOKTORSKIEJ PRZYGOTOWANA DLA RADY WYDZIAŁU CYBERNETYKI WOJSKOWEJ AKADEMII TECHNICZNEJ

Tytuł rozprawy:
„Mechanizmy bezpieczeństwa cyfrowych platform integracyjnych wspomagających realizację zadań publicznych"

Autor rozprawy: **mgr inż. Jarosław Wilk**

Rozprawa została przygotowana pod merytoryczną opieką **dr hab. inż. Bolesława Szafrańskiego prof. WAT**, któremu Rada Wydziału Cybernetyki Wojskowej Akademii Technicznej powierzyła obowiązki Promotora.

Decyzją Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej z dnia 13.07.2021r. zostały mi powierzone obowiązki recenzenta.

Dobór tematu i zakres pracy

Rozprawa składa się z 7 rozdziałów, bibliografii, spisu rysunków i tabel oraz z dwóch załączników. Pierwszy z rozdziałów stanowi wprowadzenie, a siódmy zawiera wnioski końcowe.

Rozdział 1 i 2 stanowią stan wiedzy dotyczący platform cyfrowych, obszaru ich zastosowań, matematycznych i architektonicznych modeli informatycznych z naciskiem na bezpieczeństwo obsługi zadań publicznych. Do stanu wiedzy należy zaliczyć także załączniki 1 i 2 ściśle związane z zasadniczą treścią rozprawy. Przykładowo, wybór diagramów UML na potrzeby opracowania ram architektonicznych przedstawionych w rozdz. 5 rozprawy, został poprzedzony analizą zgodnie z zasadami dobrze znanymi w literaturze, a opisanymi w załączniku nr 2.

W ramach stanu wiedzy Autor rozprawy przedstawił proces technologiczny przetwarzania informacji dotyczących zadań publicznych. Uwzględnione zostały istotne aspekty usług elektronicznych takie jak systematyka zadań publicznych oraz relacje, jakie zachodzą między podmiotami uczestniczącymi w procesach świadczenia usług, czyli osobami fizycznymi (z ang. C-Citizen lub Customer), przedsiębiorcami (z ang. B-Business) i podmiotami publicznymi (z ang. A-Administration): B2B (Business to Business) -B2C (Business to Citizen) C2C (Citizen to Citizen) - C2B (Citizen to Business) A2B / B2A (Administration to Business / Business to Administration) A2C / C2A (Administration to Citizen / Citizen to Administration).

Podrozdział 2.3.2 „Zagadnienie bezpieczeństwa informacyjnego obsługi zadań publicznych w środowisku platform elektronicznych" zawiera istotne informacje związane z celem pracy. Dokonano analizy zalet i wad wielostronnych ram interoperacyjności. W tabeli 2.1 przedstawiono wnioski analizy poszczególnych modeli bezpieczeństwa przy uwzględnieniu pięciu kryteriów oceny. Jako najbardziej adekwatny do przedstawionego problemu, autor wybrał model bezpieczeństwa dla rozproszonych scentralizowanych baz danych wykorzystujący własności krat do integracji sterowania dostępem i przepływem danych. Zawiera on m. in. definicje operacji składania uprawnień, badania niesprzeczności krat dziedzinowych i ideę wyznaczania „superkraty", jako sposobu odzwierciedlenia zintegrowanej polityki bezpieczeństwa dla takich baz danych. (Model Szafrańskiego – pozycja 15 z ww. tabeli).

W **rozdziale 3** Autor, opierając się na własnych bogatych doświadczeniach zawodowych związanych z branżą IT, wykazał iż w firmach informatycznych nie ma standardowej metody zastosowania analizy systemowej w połączeniu z modelowaniem matematycznym. Sformułowany został przez Autora problem badawczy w formie tezy, do której recenzent niniejszej rozprawy ustosunkował się krytycznie w dalszej części opinii (vide merytoryczna ocena rozprawy).

W końcowej części tego rozdziału Autor w sposób niejasny formułuje cel rozprawy: „stworzenie ram architektonicznych przy zastosowaniu diagramów UML uwzględniając aspekt modelowania matematycznego doprowadzając do zaprojektowania i wytworzenia wiarygodnych mechanizmów bezpieczeństwa, opartych na modelach matematycznych o jednoznacznie zdefiniowanych własnościach".

W **rozdziale 4** Autor przedstawił:

- model matematyczny obsługi zadań publicznych,
- model bezpieczeństwa procesów obsługi realizowanych w środowisku platform dziedzinowych i trans-dziedzinowych.

Ponadto Doktorant podał warunki, dla których celowym jest wykorzystanie teorii krat do procesowego ujęcia reguł bezpieczeństwa obsługi zadań publicznych w środowisku platform elektronicznych. Wskazał także zalety stosowania modelowania matematycznego.

Doktorant w **rozdziale 5.** przedstawia autorskie opracowanie ram architektonicznych zarządczych i funkcjonalnych, opartych na wcześniej przygotowanym modelu matematycznym. Ramy te pozwalają na utworzenie mechanizmów bezpieczeństwa cyfrowej platformy wsparcia realizacji zadań publicznych. Zostały one zaprojektowane zgodnie z regułami architektury korporacyjnej z wykorzystaniem modelowania obiektowego (diagramy UML).

W **rozdziale 6.** Doktorant wykorzystując diagramy pakietów i komponentów opracował architekturę trans-dziedzinowej platformy integracyjnej z uwypukleniem kratowego mechanizmu bezpieczeństwa.

W **rozdziale 7.** Autor rozprawy dokonał podsumowania osiągniętych wyników oraz zasygnalizował dalsze kierunki badań.

Załączniki 1 i 2 ściśle związane są z zasadniczą treścią rozprawy. W dokumentach tych przygotowano zestawienie znanych modeli bezpieczeństwa baz danych ich analizę oraz przegląd elementów języka modelowania UML, zatem stan wiedzy w znaczącej części przeniesiony został do załączników. Również Model Szafrańskiego, na którym oparte jest nowatorskie rozwiązanie autorskie, jest przedstawiony poza treścią główną rozprawy.

Merytoryczna ocena rozprawy

Rozprawa **mgr. inż. Jarosława Wilka** jest opracowaniem nowej metodyki kształtowania mechanizmów bezpieczeństwa Centralnej Platformy Integracyjnej (CPIN) opartej na modelach procesowych oraz matematycznych. Dotyczy ona w szczególności zastosowania teorii krat do rozwiązania problemu bezpieczeństwa wykonywania usług publicznych za pomocą platform komputerowych.

Prowadząc projekty badawcze i naukowe Autor umiejętnie wykorzystał bogate doświadczenia zawodowe z tematyki związanej ściśle z rozprawą doktorską.

Głównym celem badawczym niniejszej rozprawy było opracowanie niezawodnych mechanizmów bezpieczeństwa w zakresie zapewniania poufności procesu obsługi zadań publicznych.

Autor w pierwszym rozdziale rozprawy przedstawia zagadnienia związane z procesami technologicznymi przetwarzania informacji. Doktorant następnie wykonuje analizę dostępnych i znanych modeli bezpieczeństwa baz danych. Niestety, nie wykonuje pogłębionej analizy stanu wiedzy dotyczącej tematu: **„Mechanizmy bezpieczeństwa cyfrowych platform integracyjnych wspomagających realizację zadań publicznych"**. Choć w literaturze podaje się wiele mechanizmów zabezpieczających serwisy usług komputerowych, tu nie jest przytoczona ani jedna pozycja. Przykładowo A. Singhal, T. Winograd, K. Scarfone, Guide to Secure Web Services Recommendations of the National Institute of Standards and Technology, Gaithersburg, August 2007:

https://www.govinfo.gov/content/pkg/GOVPUB-C13-3026b188380c98f88e763eb79b1c2af1/pdf/GOVPUB-C13-3026b188380c98f88e763eb79b1c2af1.pdf

Na podstawie wykonanego porównania piętnastu modeli bezpieczeństwa baz danych (rozdz. 2.3.2), został wybrany jeden (model Szafrańskiego opracowany w 1987 roku.).

Jako kryterium wyboru Autor rozprawy spośród pięciu przedstawionych na str. 23 przyjął:

a) kryterium określenia i weryfikacji wspólnych (wypadkowych) reguł ochrony poufności dla mechanizmów/systemów działających w środowisku rozproszonym,

b) kryterium integracji modeli ochrony poufności w ramach jednolitego, wspólnego, nadrzędnego modelu ochrony poufności wyrażającego wspólną dla danego systemu rozproszonego politykę bezpieczeństwa.

Model Szafrańskiego zorientowany jest na obiekty baz danych i wymagał zmian w celu zastosowania go do obiektów będących usługami elektronicznymi. Głównym

osiągnięciem rozprawy jest więc adaptacja ww. modelu na potrzeby rozproszonych systemów udostępniania usług publicznych, co stanowi novum i niezaprzeczalną wartość naukową.

Postawiona przez Doktoranta teza rozprawy brzmi :

„Wykorzystanie modelowania matematycznego, zasad architektury korporacyjnej oraz modelowania obiektowego umożliwia opracowanie metody projektowania, której zastosowanie w procesie projektowania zapewni wytworzenie mechanizmów bezpieczeństwa o formalnie i jednoznacznie potwierdzonych własnościach. Wykorzystanie w procesach obsługi zadań publicznych elektronicznych usług i platform dziedzinowych i trans-dziedzinowych mechanizmów zaprojektowanych zgodnie z opracowaną metodą, przyczyni się do automatyzacji i zwiększenia bezpieczeństwa elektronicznej obsługi zadań publicznych. Stanie się tak pod warunkiem, że wymagania bezpieczeństwa wyrażone najpierw w języku zależności matematycznych zostaną poprawnie odzwierciedlone w języku modelowania obiektowego (ramach architektonicznych) i tym samym uwzględnione w prowadzonych pracach projektowych."

Mój komentarz: Uważam, że ze względu na klarowność i lepsze zrozumienie zawartości merytorycznej zasadnym byłoby podzielenie tezy na dwie części:

Teza 1:

Wykorzystanie modelowania matematycznego, zasad architektury korporacyjnej oraz modelowania obiektowego umożliwia opracowanie metody projektowania, której zastosowanie w procesie projektowania zapewni wytworzenie mechanizmów bezpieczeństwa o formalnie i jednoznacznie potwierdzonych własnościach.

Teza 2:

Wykorzystanie w procesach obsługi zadań publicznych elektronicznych usług i platform dziedzinowych i trans-dziedzinowych mechanizmów zaprojektowanych zgodnie z opracowaną metodą, przyczyni się do automatyzacji i zwiększenia bezpieczeństwa elektronicznej obsługi zadań publicznych. Stanie się tak pod warunkiem, że wymagania bezpieczeństwa wyrażone najpierw w języku zależności matematycznych zostaną poprawnie odzwierciedlone w języku modelowania obiektowego (ramach architektonicznych) i tym samym uwzględnione w prowadzonych pracach projektowych.

Doktorant z sukcesem wykorzystał dobrze udowodnione własności wybranej teorii matematycznej (w tym przypadku teorii krat) do opracowania ram architektonicznych, których wykorzystanie zapewni integrację efektów modelowania matematycznego

i obiektowego w procesie projektowania mechanizmów bezpieczeństwa. Umożliwiło to współdziałanie oraz właściwe zrozumienie poruszanych zagadnień zarówno przez specjalistów z dziedziny matematyki jak i informatyki, w celu dalszej rozbudowy opracowanej koncepcji.

Spójne wykorzystanie modeli kratowych (w tym szczególnie operatorów krat) oraz odpowiednio dobranych diagramów UML pozwoliło oddać zarówno statyczne, jak i dynamiczne aspekty funkcjonowania mechanizmów bezpieczeństwa.

Autor rozprawy opracował ramy architektoniczne w postaci diagramów UML uwzględniających efekty modelowania matematycznego, dzięki którym zapewniono wytworzenie wiarygodnych mechanizmów bezpieczeństwa, opartych na modelach matematycznych.

Uwagi krytyczne

1. Brakuje spisu skrótów i terminów anglojęzycznych stosowanych w rozprawie. Pierwszym wystąpieniom akronimów nie towarzyszy opis (np. UML).
2. Wykonana analiza stanu wiedzy jest niewystarczająca. Choć w literaturze podaje się wiele mechanizmów zabezpieczających serwisy usług komputerowych, tu nie jest przytoczony ani jeden. Dodatkowo, brak jest wyjaśnienia podstawowych informacji (haseł) powiązanych z dziedziną cyfryzacji procesów dostarczania usług:
    - BPM – Business Process Management. Grupa narzędzi należących do BPM stanowi podstawę formalizowania procesów przetwarzania informacji, a szczególnie informacji typu zadanie publiczne.

      (https://www.gov.pl/web/popcwsparcie/zarzadzanie-procesami-biznesowymi-bpm)
    - Brak informacji na temat RODO.

      (https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pl.htm)
    - Opis kwestii bezpieczeństwa cyfrowych platform integracyjnych został w rozprawie przedstawiony marginalnie.
    - Brak odniesienia do SOA – Service Oriented Archtecture.

http://www.redbooks.ibm.com/redbooks/pdfs/sg247310.pdf

3. Istotne fragmenty stanu wiedzy, pozwalające lepiej zrozumieć treść rozprawy, zostały przeniesione do załączników. Znaczna część kluczowych informacji pozostała poza treścią główną rozprawy.

4. Doktorant stwierdza na stronie 27 (rozdz.3.1): „Moje doświadczenia… jednoznacznie wskazują na brak metodycznego, standardowego wykorzystania w projektowaniu systemów (rozwiązań) informatycznych wyników analizy systemowej i modelowania matematycznego. Ww. brak wyraża się przede wszystkim w tym, że nawet najbardziej zaawansowane metodyki zarządzania procesami projektowania systemów informatycznych nie zawierają skutecznych mechanizmów absorpcji efektów uzyskanych dzięki budowie i badaniu modeli matematycznych. Nie ma bowiem uznanego języka komunikacji między dziedziną modelowania matematycznego i wynikającego z tzw. dobrych praktyk dziedziną zaawansowanych metodyk zarządzania projektami informatycznymi." Nie można się zgodzić z tak kategorycznym stwierdzeniem Autora, gdyż w literaturze istnieje szereg rozwiązań, metodyk do których Doktorant się w ogóle nie odniósł. Na przykład TOGAF (ang. The Open Group Architecture Framework) – szkielet dla architektury korporacyjnej, który zapewnia kompleksowe podejście do projektowania, planowania, implementacji oraz zarządzania informacyjną architekturą organizacji. The Open Group, korporacja w skład której wchodzą takie firmy jak: IBM, Sun, HP, Hitachi i Fujitsu, podkreśla znaczenie metodyki wytwarzania architektury korporacyjnej, jako podstawowej zalety ram architektonicznych TOGAF.

5. Strona 30 (Rozdz. 3.2). Język nie jest językiem naukowym: „W kolejnym kroku należało połączyć dwa światy: świat modelowania matematycznego (reprezentowanego przez modele kratowe) ze światem realnego projektowania informatycznego (reprezentowanego przez diagramy UML)." Autor zapewne miał na myśli syntezę dziedzin modelowania matematycznego i technik projektowania informatycznego.

6. Spis treści rozdziałów z załączników nie jest uwzględniony w głównym spisie treści rozprawy.

7. Nawet bibliografia poszczególnych załączników podana jest osobno, co w pewien sposób utrudnia czytanie opracowania. Pomimo wskazanych istotnych uwag, podkreślić należy, iż samo opracowanie pod kątem merytorycznym, zostało przygotowane rzetelnie.

8. Zasadność stosowania serwerów amerykańskich (Azure Integration Services) do prowadzenia usług publicznych w Polsce może być wątpliwa w kontekście ochrony informacji. Wrażliwe dane pozostają w niebezpieczeństwie bez względu na zastosowane rzeczone algorytmy weryfikacji dostępu.

9. Odczuwalny jest brak wstępnej systematyki aspektów technologicznych. Czy jako aspekt technologiczny Autor widzi dziedzinę realizacji zadania publicznego, czy wpływa ona na stosowane procesy i narzędzia wytwórcze? Czy technologiczny aspekt relacji interesariuszy ma znaczenie w kontekście bezpieczeństwa? Jakie są relacje pomiędzy aspektami technologicznymi, w jaki sposób mogą wpływać na siebie w kontekście bezpieczeństwa systemów wielodomenowych?

10. Brak odwołania do normy WCAG przy odniesieniu do zasady „braku wykluczenia". WCAG (ang. Web Content Accessibility Guidelines) jest to zbiór wytycznych dotyczących dostępności treści internetowych.

11. Autor przedstawiając modele relacji modułów systemu wielodomenowego posiłkuje się dwoma topologiami: topologia pełnego połączenia i topologia gwiazdy (nomenklatura systemów rozproszonych). Raczej bezzasadne jest tworzenie nowych określeń typu: „modelu wielostronnych ram interoperacyjności", zwroty takie mocno zaciemniają przekaz. Wiadomym jest, iż opracowanie dotyczy aspektów bezpieczeństwa. W opracowaniu brakuje natomiast istotnych informacji nt. wad takich jak: wąskie gardło (ang. bottleneck) czy utrata niezawodności.

    Komentarz: Autor nie przytacza żadnych technologii, narzędzi czy wszechstronnie dostępnych rozwiązań architektonicznych czy implementacyjnych. Brak krytycznej analizy dostępnych rozwiązań choćby z tematyki BPM, SAO, mikroserwisów (kontenerów), serwisów REST, policy management etc.

12. Pracę wzbogaciłaby aplikacja utworzona przy zastosowaniu opracowanych autorskich rozwiązań. W rozprawie istnieje teoretyczny opis opracowania, natomiast brak jest opisu realizacji (implementacji). Wygląda jakby projekt nie został wdrożony do celów testowych.

Uwagi szczegółowe

Liczne błędy typograficzne oraz nieliczne interpunkcyjne i stylistyczne wprowadzają utrudnienie w poprawnym odbiorze pracy naukowej. Dodatkowo, język jakim posługuje się Autor choć celnie obfituje w liczne abstrakcje i uogólnienia, w niektórych miejscach

przybiera formę nadmiarową. Zamiast objaśniać wywołuje u odbiorcy szereg zasadnych pytań pozostawiając je jednocześnie bez odpowiedzi.

W pracy znajdują się nieliczne błędy interpunkcyjne i edycyjne:

- str. 15 – Nieczytelne zdanie: „czyli zadania, dla obsługi, których konieczne jest",
- str. 15 – „Usługi proste są zawsze usługami dziedzinowymi." – kropka zamiast przecinka przy wyliczeniu,
- liczne błędy typograficzne; przykład na stronie 17,
- str. 23 – akapit z małej litery: „potrzebę syntetycznego ujęcia",
- str. 23 – skrajnie nieczytelny zwrot: „Uwzględniając wcześniej założoną jednoznacznego określenia reguł ochrony poufności gwarantujących dopuszczenie do realizacji wyłącznie bezpiecznych dostępów lub przepływów danych wywoływanych przez usługi elektroniczne",
- str. 26 – Nieczytelne zdanie: " Wykazano także zasadność wykorzystania w procesie modelowania dorobku teorii krat także w celu wykazania formalnej zdefiniowania i następnie badania poprawności respektowania tych reguł.",
- (Rys. 4.1; str. 35) diagram nie jest wykonany zgodnie z zasadami tworzenia schematów blokowych. Brak bloków rozpoczynających i kończących algorytm,
- str. 36 – powielenie treści ze wstępu rozprawy (cała strona),
- str. 51 – Nieczytelne zdanie: „Rozszerzony opis procedury składania krat można został przedstawiony w…".

Podsumowanie

Przytoczone powyżej uwagi krytyczne nie umniejszają wartości naukowej ocenianej pracy. Uważam, że praca **zawiera** wartościowy i oryginalny dorobek naukowy Doktoranta posiadającego bogate doświadczenia wyniesione zarówno z realizacji zadań badawczo-rozwojowych, jak i projektowo-wdrożeniowych wykonywanych w okresie studiów doktoranckich na Wydziale Cybernetyki WAT, a także w polskich i zagranicznych firmach informatyczno-eksperckich (SoftwareONE Comparex Poland w Warszawie Siemens Corporate Research w Princeton, NJ, USA i Research & Development Laboratories w L'Aquila, Włochy).

W rozprawie Doktorant przedstawił:

- wyniki analizy, definicje i klasyfikację pojęć związanych z obsługą zadań publicznych w środowisku platform elektronicznych,
- modele matematyczne procesów obsługi zadań publicznych w środowisku platform elektronicznych, ze szczególnym uwzględnieniem ochrony poufności, jako podstawowej cechy bezpieczeństwa.
- ramy architektoniczne (funkcjonalne i zarządcze) opracowane z wykorzystaniem dorobku architektury korporacyjnej oraz modelowania obiektowego
- propozycje dotyczące praktycznych (technologicznych i implementacyjnych) aspektów wykorzystania uzyskanych wyników.

Zakres i poziom uzyskanych wyników badawczych odpowiada ustawowym i zwyczajowym wymaganiom stawianym rozprawom na stopień doktora nauk technicznych. Uwzględniając wyżej wymienione dokonania Doktoranta, a także koncepcje rozwojowe dalszych prac (kierunki dalszych prac zostały sformułowane w zakończeniu podsumowania), wnioskuję do Wysokiej Rady Dyscypliny Naukowej Informatyki Technicznej i Telekomunikacji Wydziału Cybernetyki Wojskowej Akademii Technicznej o **przyjęcie** rozprawy i dopuszczenie Autora **mgr inż. Jarosława Wilka** do jej publicznej obrony.