

Wrocław, dnia 7 listopada 2019 r.

prof. dr hab. inż. Jerzy Świątek
Katedra Informatyki
Wydział Informatyki i Zarządzania
Politechnika Wrocławska

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA RADY WYDZIAŁU CYBERNETYKI WOJSKOWEJ AKADEMII TECHNICZNEJ
im. Jarosława Dąbrowskiego w Warszawie

(Recenzja opracowana na podstawie zlecenia Przewodniczącego Rady Wydziału Cybernetyki
WAT dra hab. inż. Kazimierza Worwy, prof. WAT, zgodnie z uchwałą Rady Wydziału
Cybernetyki WAT z dnia 24 września 2019 r.)

Temat: „Metoda odtwarzania zmian danych na dysku z systemem plików NTFS
wykorzystująca informacje zawarte w pliku systemowym \$MFT”

Autor: mgr inż. Fryderyk Stefan Darnowski

Promotor: dr hab. inż. Andrzej Chojnacki, prof. WAT

1. Cel i zakres pracy.

W ostatnich latach, w literaturze światowej, obserwujemy znaczny rozwój problematyki projektowania złożonych systemów wspomagania podejmowania decyzji, zarządzania i sterowania. Problem ten dotyczy systemów technicznych, gospodarczych i społecznych. Istotnym elementem wkomponowanym w każdy system jest podsystem informacyjny. Zadaniem podsystemu informacyjnego jest rejestracja, analiza, przekazywanie i przetwarzanie strumieni danych pochodzących z realizacji procesów zachodzących w systemie, czyli zarządzanie informacją, w celu wspomagania zadań decyzyjno-zarządczych. Podsystem zarządzania informacją jest integralnym elementem każdego systemu. Przykładowo, podsystem informacyjny jest istotnym elementem takich systemów jak: krajowe systemy wspomagające działalność administracji państwowej; systemy wspomagania zarządzania organizacjami gospodarczymi w celu maksymalizacji ich efektywności; systemy wspomagania obliczeń, projektów, analiz, klasyfikacji i in.; systemy wspomagania optymalizacji sterowań

zespołów maszyn i urządzeń technologicznych i wiele innych (służba zdrowia, obronność, transport i in.). W toku działania systemu wytwarzane są ogromne liczby dokumentów zawierających dane dotyczące monitorowanych, zarządzanych i sterowanych procesów. Większość współczesnych systemów informacyjnych jest projektowana z wykorzystaniem techniki cyfrowej. Ważnym elementem oceny systemu informacyjnego jest dokładność, użyteczność, kompletność, rzetelność oraz aktualność przekazywanych informacji. Ogólnie problematyka ta jest związana z zarządzaniem bezpieczeństwem systemu informacyjnego. Jednym z podstawowych elementów jest wiarygodność danych zawartych na nośnikach cyfrowych. Prowadzi to do zadania analizy i zabezpieczenia cyfrowych nośników danych. Z tym obszarem związana jest również „Informatyka śledcza/kryminalistyczna”, której zadaniem jest ocena wiarygodności danych znajdujących się na nośniku.

W tym obszarze należy ulokować przedstawiony, główny problem podjęty w recenzowanym opracowaniu sformułowany poprzez jasno, precyzyjnie i poprawnie postawiony problem naukowy: *„Należy wykorzystać dostępne informacje systemowe (\$MFT) i zmiany w nim zachodzące dla odzyskiwania informacji o plikach, które były zapisywane i wykasowywane w pewnym analizowanym przedziale czasu.”* Z powyższym zadaniem badawczym związany jest cel pracy, który polega na opracowaniu metody odzyskiwania informacji o zapisywanych i kasowanych plikach na dysku z systemem NTFS, w tym na charakterystykach czasowych ich nagrania i wykasowania. Rozwiązanie postawionego problemu przekłada się na następując zadania badawcze i projektowe:

- 1) analiza organizacji danych na dysku z systemem plików NTFS;
- 2) opracowanie modeli matematycznych dysku oraz akcji podejmowanych na dyskach;
- 3) przedstawienie zmian w procesie zapisów i kasowań plików na dysku jako procesu deterministycznego;
- 4) opracowanie metody odczytywania stanu dysku z przeszłości;
- 5) oszacowanie złożoności obliczeniowej zaproponowanych algorytmów;
- 6) analiza zakresu zastosowań opracowanej metody.

W świetle wcześniej przedstawionych uwag mogę stwierdzić, że podjęty temat recenzowanej rozprawy jest ważny i aktualny, a opracowane zadania mają ważny aspekt praktyczny i wnoszą istotny wkład w rozwój informatyki, a w szczególności obszarze metod modelowania i analizy cyfrowych nośników danych.

2. Przegląd treści pracy

Wyniki pracy Autor przedstawił w rozprawie doktorskiej napisanej w języku polskim, która składa się z 12. rozdziałów, spisu rysunków i tabel, wykazu załączników oraz bibliografii. Całość liczy 240 stron. Pracę uzupełnia płyta CD oraz cztery załączniki, w których opisano kolejno: najważniejsze funkcje użyte w programie, dane do symulacji z rozdziału 10., dane do symulacji z rozdziału 11. oraz zawartości załączonej płyty CD.

Rozdział pierwszy stanowi wstęp, w którym Autor wprowadza czytelnika w zakres rozprawy, lokuje jej treść na tle aktualnego rozwoju metod analizy cyfrowych nośników danych. Następnie charakteryzuje problem naukowy, którego rozwiązanie prowadzi do relacji wymienionych zadań cząstkowych. W rozdziale drugim Autor przedstawia organizację cyfrowego nośnika danych w tym system plików NTFS. Rozdział trzeci zawiera opis typowych akcji następujących w nośniku rzeczywistym. Informacje przedstawione w rozdziałach drugim i trzecim dają podstawy do precyzyjnego sformułowania i rozwiązania zadania badawczego. Oryginalne wyniki pracy rozpoczynają się od rozdziału czwartego, w którym Autor przedstawia model matematyczny nośnika danych. W szczególności formułuje założenia modelu oraz formalizuje opis obszaru danych. W tym miejscu precyzuje opis pliku \$MFT, który jest istotny dla analizy nośnika. Opisuje związek między \$MFT a obszarem danych. W rozdziale piątym, w oparciu o opracowany model, sformalizowano akcje (operacje) zapisu i kasowania plików. Z punktu widzenia analizy systemowej możemy stwierdzić, że uzyskany model przedstawia nam zależność stanu nośnika od wykonanych operacji, tj. przedstawia funkcję przejścia pomiędzy stanami. Tak przedstawiona zależność w rozdziale szóstym jest podstawą do poszukiwania tzw. odwrotnej funkcji przejścia przydatnej do konstrukcji algorytmu odzyskiwania informacji o wcześniej zapisanych plikach, co przedstawiono w rozdziale siódmym. W szczególności zaproponowano funkcje „cofnij zapis” oraz „cofnij kasowanie” dla typowych przypadków. Wprowadzone pojęcia i podejmowane akcje oraz funkcje przejścia ilustrują dobrze dobrane przykłady. Istotnym oryginalnym elementem pracy jest algorytm wyznaczania stanów początkowych (poprzednich), który opisano w rozdziale ósmym. Przedstawiono tutaj ideę algorytmu bazowego przy założeniach upraszczających w stosunku do nośnika rzeczywistego tj. przy założeniu, że stany są jednoznacznie ponumerowane niezależnie od czasu rzeczywistego. Zbadano złożoność obliczeniową algorytmu. Rozdział dziewiąty zawiera opis zmodyfikowanego algorytmu wyznaczania stanów początkowych, który uwzględnia fakt, że w czasie rzeczywistym kolejna operacja może być poprzedzona wieloma akcjami. Wymaga to zaproponowania sekwencji kolejnych „akcji do

cofnięcia”, co z kolei generuje zbiory możliwych stanów poprzednich. Rozdział 10. zawiera wyniki badań symulacyjnych na danych testowych, natomiast w rozdział 11. przedstawia wyniki testów na nośnikach rzeczywistych. W zakończeniu - rozdział 12. poświęcony jest podsumowaniu wyników pracy. Przedstawiono w nim zakres zastosowań proponowanej metody oraz wskazano na jej ograniczenia. Zaproponowano kierunki dalszych prac. Bibliografia zawiera wykaz 75 trafnie dobranych pozycji literaturowych. Większość pozycji literaturowych stanowią pozycje aktualne z ostatnich 10. lat. Informacje literaturowe jednoznacznie dotyczą tematyki rozprawy, a proponowany zbiór jest ściśle ukierunkowany na wyznaczony cel pracy. W wykazie literatury można znaleźć trzy pozycje Autora.

3. Uwagi redakcyjne

Na podstawie lektury pracy mogę stwierdzić, że podział treści jest logiczny i uporządkowany, styl oraz poziom językowy jest wysoki, a szata graficzna jest staranna i dopracowana. Sposób przekazywania treści jest bardzo dobry. Treść pracy jest wzbogacona dobrze dobranymi rysunkami oraz tabelami zawierającymi wyniki symulacji, ocen i porównań. Pracę czyta się z przyjemnością. Informacja jest dobrze wyważona. Lektura rozprawy upoważnia mnie do wyróżniającej oceny formy prezentacji wyników pracy, a czytelnik przekonany jest o wysokiej kompetencji merytorycznej Autora, który potrafi przedstawić swoje wyniki w sposób przyjazny dla czytelnika.

4. Oryginalne wyniki

Wykonanie założonego celu wiąże się z wykonaniem następujących zadań szczegółowych, które uważam za oryginalne wyniki pracy:

- W oparciu o analizę danych na nośniku z systemem NTFS opracowanie oryginalnego modelu matematycznego nośnika danych z uwzględnieniem zmiany stanu nośnika w zależności od wykonanych operacji (akcji).
- Opracowanie oryginalnego algorytmu bazowego odzyskiwania stanu nośnika w stanach poprzednich oraz jego adaptacja do warunków rzeczywistych.
- Przeprowadzanie badań testowych opracowanych algorytmów.
- Oszacowanie złożoności obliczeniowej zaproponowanych algorytmów.

5. Uwaga merytoryczna (pytanie dyskusyjne)

W trakcie analizy treści pracy nasuwa się pytanie (uwaga), o której wyjaśnienie poproszę podczas publicznej dyskusji nad przedłożoną pracą: Istotnym ograniczeniem proponowanej metody jest ahistoryczność i stacjonarność procesu przetwarzania danych na nośniku. Jaki wpływ na rozwiązanie ma wprowadzenie tego uproszczenia?

6. Ocena wiedzy doktoranta w zakresie dyscyplin naukowych związanych z tematyką rozprawy

1. Problematyka rozprawy obejmuje wiedzę z dziedziny nauk technicznych w zakresie dyscypliny informatyka, a w szczególności w zakresie zastosowania metod modelowania i analizy cyfrowych nośników danych.
2. Doktorant swobodnie posługuje się aparatem matematycznym, właściwie formułuje hipotezy badawcze i wykazuje umiejętność dokonywania trafnych wyborów i właściwego wnioskowania. Formułowane przez doktoranta wnioski są przemyślane, logiczne i spójne.
3. W stopniu biegłym opanował tematykę rozprawy w warstwie nie tylko teoretycznej, ale także praktycznej, w oparciu o dobre rozeznanie problemów związanych z metodami analizy cyfrowych nośników danych..
4. Lektura rozprawy upoważnia mnie do stwierdzenia, że doktorant swobodnie porusza się po literaturze przedmiotu, dysponuje wymaganym do prowadzenia badań naukowych zasobem wiedzy z zakresu informatyki, czyli tego obszaru nauki i techniki, którego dotyczy temat rozprawy.

7. Podsumowanie.

Na podstawie lektury recenzowanej rozprawy mogę stwierdzić, że doktorant:

- podjął ważny i aktualny problem w obszarze informatyki,
- uzyskał oryginalne wyniki w zakresie metod modelowania i analizy cyfrowych nośników danych,
- przedstawił interesujące możliwości zastosowań prezentowanych wyników, a tym samym wniósł interesujący i wkład w rozwój dyscypliny: informatyka.

W podsumowaniu mojej oceny stwierdzam, że opiniowana praca mgr inż. Fryderyka Darnowskiego nt.: „Metoda odtwarzania zmian danych na dysku z systemem plików NTFS wykorzystująca informacje zawarte w pliku systemowym \$MFT” jest kompletna i nie wymaga

żadnych zmian ani uzupełnień. Spełnia ona z nadmiarem zwyczajowe i ustawowe wymagania stawiane rozprawom doktorskim określone w „Ustawie o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki”.

Wnioskuje o przyjęcie niniejszej pracy jako rozprawy doktorskiej i wnoszę o dopuszczenie mgr inż. Fryderyka Darnowskiego do publicznej dyskusji nad przedłożoną pracą.

A handwritten signature in blue ink, appearing to read 'Jerzy Świątek', is placed on a light blue rectangular background.

prof. dr hab. inż. Jerzy Świątek