Zielona Góra, 02 lutego 2022

dr hab. inż. Justyna Patalas-Maliszewska, prof. UZ
Instytut Inżynierii Mechanicznej
Uniwersytet Zielonogórski
E-mail: J.Patalas-Maliszewska@iim.uz.zgora.pl

Recenzja

rozprawy doktorskiej Pani mgr inż. Estery Pietras
pt.: „Zarządzanie bezpieczeństwem informacji w przedsiębiorstwach branży motoryzacyjnej".

Promotor: dr hab. inż. Marcin Knapiński, prof. PCz.

Recenzję wykonano na zlecenie Przewodniczącej Rady Dyscypliny Naukowej: Nauki o Zarządzaniu i Jakości, Wydział Zarządzania, Politechnika Częstochowska, na podstawie pisma R-WZ-BODN-510-5/2021.

1. Ogólny opis recenzowanej rozprawy doktorskiej

Przedstawiona do recenzji rozprawa doktorska pt.: „Zarządzanie bezpieczeństwem informacji w przedsiębiorstwach branży motoryzacyjnej" obejmuje 285 stron, składa się ze wstępu, sześciu głównych rozdziałów i podsumowania.

W rozdziale pierwszym dokonano analizy literatury przedmiotu w obszarze bezpieczeństwa i ochrony informacji w przedsiębiorstwach, a następnie w rozdziale drugim zaprezentowano systemy zarządzania bezpieczeństwem informacji. Kolejny rozdział to cel i zakres podjętych badań, rozdział czwarty przedstawia wyniki przeprowadzonych prac badawczych. W rozdziale piątym opisano badania eksperymentalne, a w rozdziale szóstym dokonano oceny poziomu bezpieczeństwa informacji w wybranym przedsiębiorstwie. Rozprawa zawiera ponadto streszczenie w języku angielskim oraz spis literatury (122 pozycji), 75 rysunków, 31 tabel oraz dodatkowe materiały w postaci kwestionariusza ankiety badawczej, arkusza obserwacji, kwestionariusza wywiadu, polityki bezpieczeństwa informacji oraz procedury zgodnej ze schematem postępowania systemowego. Układ pracy oraz sposób omówienia poszczególnych obszarów badawczych jest prawidłowy.

W pracy autorka podjęła się rozwiązania ważnego tematu badawczego związanego z zagadnieniem zarządzania bezpieczeństwem informacji w przedsiębiorstwach. Temat jest szczególnie aktualny w kontekście dynamicznego rozwoju technologii informacyjnych, których zastosowanie umożliwia zarówno przechowywanie dużej ilości danych i informacji w postaci cyfrowej, jak również ich przesyłanie w cyberprzestrzeni. Technologie informacyjno-komunikacyjne wspierają realizowanie procesów w przedsiębiorstwach, m.in. prowadzenie działań produkcyjnych, dostarczanie danych, informacji oraz transfer wiedzy między pracownikami. Zdefiniowany problem badawczy w postaci poszukiwania metodyki zarządzania bezpieczeństwem informacji pokazuje aktualność podejmowanej

tematyki w kontekście konieczności wdrażania technicznych i organizacyjnych środków zabezpieczeń w przedsiębiorstwach stosujących technologie informacyjno-komunikacyjne.

2. Ocena formalna poszczególnych części recenzowanej rozprawy doktorskiej oraz uwagi ogólne

We wstępie pracy nakreślono ważność ochrony danych i informacji oraz potrzebę prowadzenia działań zmniejszających ryzyko naruszenia bezpieczeństwa danych i informacji dostępnych w przedsiębiorstwach w cyberprzestrzeni. Następnie przedstawiono zakres pracy i treści poszczególnych rozdziałów. W tej części pracy niedosyt budzi brak zdefiniowania potrzeby prowadzenia badań w obszarze zarzadzania bezpieczeństwem informacji w przedsiębiorstwach branży motoryzacyjnej. Ponadto, wprowadzenie spisu skrótów na początku pracy i wyjaśnienie ich w pracy niewątpliwie ułatwiłoby zrozumienie ich stosowania (na przykład: ZBI, BI).

Rozdział pierwszy szczegółowo charakteryzuje obszar bezpieczeństwa i ochrony informacji w przedsiębiorstwie. Opisano bezpieczeństwo informacji (dalej skrót: BI) w podziale na bezpieczeństwo fizyczne, osobowo-organizacyjne, prawne oraz teleinformatyczne, jak również pojęcie informacji i elementy BI. W dalszej części pracy dokonano identyfikacji zagrożeń bezpieczeństwa informacji oraz opisano w postaci odrębnych podrozdziałów zagrożenia socjotechniczne, teleinformatyczne oraz prawne w kontekście BI. Powstaje pytanie, dlaczego nie dokonano opisu tych zagrożeń BI w kontekście uprzednio wprowadzonego podziału na rysunku nr 1. Taki brak narracji, jak również brak opisu zastosowanych skrótów utrudnia czytelność tej części pracy.

W rozdziale drugim podjęto badania dotyczące systemów zarządzania bezpieczeństwem informacji w kontekście zmniejszania ryzyka utraty informacji. Rozważania rozpoczęto od omówienia systemu zarządzania bezpieczeństwem informacji (dalej skrót: SZBI), tj. w szczególności przedstawiono zadania (rozdział 2.2), a następnie rolę elementów tego systemu (rozdział 2.3). Następnie opisano aspekt zarządzania ryzykiem oraz przedstawiono znane w literaturze przedmiotu metody szacowania ryzyka. Wyjaśnienia wymaga zaproponowana formuła (wzór 1), którą opisano ryzyko. W dalszej części zaprezentowano podejście, w którym wdrożenie SZBI w przedsiębiorstwie oparte jest na modelu Plan-Do-Check-Act. Czy można wskazać inne metodologie, które z sukcesem są stosowane w takich wdrożeniach? W części dotyczącej praktycznej przykładów systemów bezpieczeństwa informacji oczekiwano dyskusji o korzyściach i problemach w procesie wdrożenia systemów w przedsiębiorstwach produkcyjnych, w szczególności branży motoryzacyjnej.

W rozdziale trzecim sformułowano główny cel pracy jako zidentyfikowanie czynników zagrażających BI w organizacjach oraz opracowanie systemu, którego zastosowanie umożliwi zarządom przedsiębiorstw dynamiczne reagowanie na pojawiające się zagrożenia. Problem badawczy poszukiwania metodyki zarządzania bezpieczeństwem informacji dedykowanej dla danej klasy przedsiębiorstw przedstawiono za pomocą pięciu pytań badawczych. W rozdziale 3.2 sformułowano hipotezę badawczą, która nie budzi zastrzeżeń. Jednakże w dalszej części pracy (str. 112) podano po raz drugi cel pracy, odmienny niż ten na str. 111. W kolejnych dwóch podrozdziałach scharakteryzowano obiekty badawcze oraz metody i narzędzia badawcze. W mojej ocenie brakuje w tej części zdefiniowania etapów podejmowanych prac badawczych czy też diagramu pokazującego poszczególne kroki podjęte do rozwiązania problemu badawczego. Nie jest też zrozumiałe, na jakiej podstawie dokonano wyboru dziewięciu przedsiębiorstw branży motoryzacyjnej. Wprawdzie opisano, iż „ (...) są to liderzy wśród

dostawców na rynku motoryzacyjnym w Europie (...)", ale w moje ocenie ustalenie i przyjęcie określonej klasy przedsiębiorstw jako obiektu badawczego pozwoliłoby na lepsze zrozumienie doboru próby badawczej. Podrozdział 3.5 jest dobrym wprowadzeniem do części badawczej.

Rozdział czwarty rozpoczyna drugą części pracy, w której przedstawiono wyniki badań własnych. Wyniki badań empirycznych zostały przedstawione w sposób właściwy i staranny oraz pozwoliły na dokonanie oceny poziomu bezpieczeństwa informacji w badanych przedsiębiorstwach. Pozytywnie oceniam zbudowane diagramy przyczynowo skutkowe, które wskazują na zagrożenia utraty bezpieczeństwa informacji w przedsiębiorstwie w perspektywie personelu, na skutek zarządzania czy w perspektywie systemów komputerowych, systemów bezpieczeństwa, metod i tzw. osób trzecich.

W rozdziale piątym przeprowadzono eksperyment badawczy mające na celu sprawdzenie stosowania przez pracowników procedur zawartych w Polityce Bezpieczeństwa Informacji. Przygotowano założenia i plan przebiegu eksperymentu, a następnie stwierdzono, że konieczne jest zbudowanie katalogu występujących zagrożeń. W mojej ocenie, na podstawie zbudowanych diagramów zagrożenia utraty bezpieczeństwa informacji w przedsiębiorstwie (rysunek 67, rysunek 68, rysunek 69) można zdefiniować listę takich zagrożeń, co zostało przedstawione w rozdziale szóstym, w tabeli 13. Dlatego uważam, że rozdział 5 powinien zostać przesunięty do części końcowej rozprawy jako pokazujący możliwość implementacji metodyki zarządzania bezpieczeństwem informacji (rysunek 71).

Rozdział szósty przedstawia zbudowaną listę zagrożeń dla bezpieczeństwa informacji w przedsiębiorstwie (tabela 13). Następnie zaproponowano nową metodykę zarządzania bezpieczeństwem informacji (rysunek 71) oraz rozwiązania w celu zabezpieczenia się przedsiębiorstwa przed zidentyfikowanymi zagrożeniami (tabela 30). Zdecydowanie pozytywnie oceniam ten rozdział, w którym pokazano istotne osiągnięcie będące wynikiem przeprowadzonych badań.

W podsumowaniu przedstawiono wnioski poznawcze oraz utylitarne. Dodatkowe materiały zawarto w końcowej części pracy, jednak nie oznaczono ich jako odrębnych załączników. Spis pozycji literatury uważam za prawidłowy i wystarczający.

3. Ocena merytoryczna pracy

Zagadnienie naukowe i ocena oryginalności rozwiązania problemu naukowego

Podejmowany problem obejmuje poszukiwanie i zidentyfikowanie zagrożeń utraty informacji w przedsiębiorstwie oraz zbudowanie metodyki zarządzania bezpieczeństwem informacji. Autorka pracy w sposób opisowy i poprawny przedstawiła cele pracy i podejmowany problem naukowy, jednakże pewien niedostatek odczuwa się w postaci braku graficznej prezentacji poodejmowanego problemu badawczego. Za oryginalne osiągnięcia w pracy, które wnoszą wkład w rozwój dyscypliny: „nauki o zarządzaniu i jakości" uznaję:

- Wyznaczenie zagrożeń bezpieczeństwa informacji na podstawie analizy wyników badań w przedsiębiorstwach produkcyjnych branży motoryzacyjnej w podziale na kategorie: metoda, maszyna i technologia, personel, osoby trzecie oraz zarządzanie.
- Zbudowanie katalogu zagrożeń bezpieczeństwa informacji na podstawie analizy wyników badań.

- Zdefiniowanie elementów zabezpieczeń informacji stosowanych w przedsiębiorstwach.
- Zbudowanie metodyki zarządzania bezpieczeństwem informacji dla przedsiębiorstw produkcyjnych.
- Zaprojektowanie systemu przepływu pracy i zabezpieczenia informacji.
- Wykazanie utylitarności wyników badań.

Aktualność tematyki i ocena wyników badań

W mojej ocenie podjęty temat badawczy jest bardzo aktualny, w szczególności w kontekście powszechnego zastosowania narzędzi wspomagających informacyjnie pracę przedsiębiorstw i konieczności ochrony informacji w cyberprzestrzeni. Autorka zastosowała właściwe metody badawcze (ankietowanie, obserwacja nieuczestnicząca, wywiad swobodny, test odporności na ataki ujawnienia informacji). Ponadto przedstawione rozwiązanie jest odpowiedzą na potrzeby menadżerów przedsiębiorstw w kontekście wdrożenia spójnych działań na rzecz bezpieczeństwa informacji. Uwagi szczegółowe do pracy przedstawiłam poniżej.

Krytyczna analiza treści rozprawy i uwagi szczegółowe

Analizowana rozprawa powinna zawierać bardzie doprecyzowaną metodykę prowadzonych prac badawczych ze wskazaniem:

- Uzasadnienia wyboru grupy badawczej w postaci dziewięciu przedsiębiorstw produkcyjnych branży motoryzacyjnej.
- Wyjaśnienia przyjętych i zastosowanych formuł do obliczenia poziomu ryzyka.
- Wyjaśnienia zasadności i założeń dla przeprowadzonej analizy doświadczalnej.

Ponadto autorka deklaruje opracowanie systemu bezpieczeństwa informacji, który będzie wyposażony w funkcje autoadaptacji, którego zastosowanie umożliwi dynamiczne reagowanie na pojawienie się zagrożeń. Wprawdzie zaprojektowano system przepływu pracy i zabezpieczenia informacji, jednakże w treści pracy nie znajduje się opisu deklarowanych funkcji systemu.

Uwagi szczegółowe:

1. We wstępie pracy podano informacje dotyczące kosztów ataków internetowych dla przedsiębiorstw. Do jakiej klasy przedsiębiorstw odnoszą się te dane? Ponadto nie dokonano opisu metod badawczych zastosowanych w pracy (ankietowanie, obserwacja nieuczestnicząca, wywiad swobodny, test odporności na ataki ujawnienia informacji) oraz nie wyjaśniono wyboru grupy badawczej w procesie badawczym.

2. W rozdziale 1 w przyjętej definicji bezpieczeństwa informacji wprowadzano pojęcie: „zapis w pamięci ludzkiej". Oczekuje się wyjaśnienia tego sformułowania. Jakie można wskazać przykłady informacji w przedsiębiorstwach, w szczególności branży motoryzacyjnej?

3. Wprowadzenie w pracy spisu skrótów niewątpliwie ułatwiłoby czytelność zawartych treści. Ponadto oczekuje się uporządkowania i wyjaśnienia stosowanych pojęć: informacja, bezpieczeństwo informacji, ochrona informacji, ryzyko utraty informacji, zagrożenie bezpieczeństwa informacji, zarządzanie bezpieczeństwem informacji, system zarządzania

bezpieczeństwem informacji, zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem informacji. Taki glosariusz znacznie ułatwiłby odbiór poszczególnych treści zawartych w pracy.

4. Wyjaśnienia wymaga przyjęta klasyfikacja systemu zarządzania bezpieczeństwem informacji zgodnie z modelem PDCA (rozdział 2). Ponadto należy wyjaśnić przyjętą formułę do wyznaczenia poziomu ryzyka (wzór nr 1, rozdział 2). W podsumowaniu rozdziału nr 2 brakuje krytycznej dyskusji dotyczącej stosowanych systemów zarządzania bezpieczeństwem informacji w przedsiębiorstwach, w szczególności branży motoryzacyjnej.

5. Nadmiarowo zdefiniowano cel pracy w kontekście: „opracowania systemu, który wyposażony będzie w funkcje autoadaptacji". Dlaczego przyjęto metody badawcze takie jak: ankietowanie, obserwacja nieuczestnicząca, wywiad swobodny, test odporności na ataki ujawnienia informacji?

6. Należy przedstawić uzasadnienie wybory grupy badawczej w postaci dziewięciu przedsiębiorstw branży motoryzacyjnej.

7. Rozdziały 4-6. Rozdziały ten stanowią oryginalny wkład autorki w obszarze badań dotyczących bezpieczeństwa informacji w przedsiębiorstwach.
   - Na jakiej podstawie dokonano doboru elementów metody 5M jako gałęzi w diagramie Ishikawy w postaci: Personel, Zarządzanie, Systemy Komputerowe, Systemy Bezpieczeństwa, Osoby trzecie (rozdział 4).
   - Dlaczego przeprowadzono eksperyment badawczy dotyczący stanu wiedzy pracowników wybranego przedsiębiorstwa odnośnie bezpieczeństwa informacji (rozdział 5)? W jaki sposób wnioski z tego badania przyczyniły się do zbudowania katalogu zagrożeń bezpieczeństwa informacji na podstawie analizy wyników badań czy metodyki zarządzania bezpieczeństwem informacji dla przedsiębiorstw produkcyjnych?
   - Zastosowany wzór nr 3 do oceny ryzyka wymaga wyjaśnienia w kontekście wzoru nr 1.
   - Brakuje oznaczenia (numeracji) etapów postępowania w kontekście zbudowanej metodyki zarządzania bezpieczeństwem informacji (rysunek 71). Na jakiej podstawie ustalono trzy obszary nowych zabezpieczeń? Jak należy rozumieć zabezpieczenia fizyczne i techniczne?
   - Oczekuje się dyskusji nad możliwościami wykorzystania proponowanego rozwiązania w postaci systemu przepływu i zabezpieczenia i informacji (rozdział 6.3) w perspektywie możliwości integracji wdrożenia proponowanego systemu ze strategią przedsiębiorstwa.

4. Uwagi redakcyjne

W pracy zauważono błędy stylistyczno-redakcyjne i niezręczności językowe. Występują również powtórzenia i nieścisłości oznaczeń.

str. 5	Niezręczność językowa: „ideą pracy jest przedstawienie znaczenia wpływu (...)".
str. 10	Brak tytułu tabeli, niezręczność językowa: „do działań w sferze bezpieczeństwa (...) można zaliczyć, następujące: [12]".
str. 11-12	Niezręczności językowe: „(...) staramy się chronić (...)"; „Często słyszymy określenie (...)".
str. 18	Brak odniesienia w treści do rysunku nr 2.

str. 25	Brak odniesienia w treści do tabeli nr 2.
str. 26	Brak tytułu tabeli.
str. 34	Brak tytułu tabeli.
str. 35	Niezręczności językowe: „Rozróżniamy dwie metody (...)"; „(...) nie jesteśmy świadomi (...)".
str. 42	Brak odwołania w treści do tabeli nr 9.
str. 46	Brak odwołania w treści do rysunku nr 6.
str. 54	Brak odwołania w treści do rysunków nr 7 i nr 8.
str. 57	Brak odwołania w treści do rysunku nr 9.
str. 62	Brak odniesienia w treści do rysunku nr 10. Ponadto podpis został umieszczony nad rysunkiem (w pracy przyjęto, że podpisy rysunków umieszczane są pod rysunkami).
str. 67	Brak odwołania w treści do rysunku nr 12.
str. 71	Brak odwołania w treści do rysunku nr 13. Błąd: „wg", który pojawia się również w dalszej części pracy.
str. 74-75	Brak odwołania w treści do rysunków nr 14 i nr 15.
str. 78	Rysunek nr 16 jest nieczytelny. Brak odwołania w treści do rysunków nr 16 i nr 17.
str. 80-81	Brak odwołania w treści do rysunków nr 18 i nr 19.
str. 85	Brak odwołania w treści do rysunku nr 21.
str. 90-91	Brak odwołania w treści do rysunków nr 22 i nr 23.
str. 96	Brak odwołania w treści do rysunku nr 25.
str. 100-101	Brak odwołania w treści do rysunków nr 27 i nr 28.
str. 123	Niezręczności językowe: „(...) istniejący stan zagrożeń, który wskazał (...)"; „(...) wskazuje na wdrożenie systemu zabezpieczeń (...)".
str. 157	Niezręczności językowe: „(...) Podsumowując spostrzeżenia można powiedzieć (...)"; „Wiąże się to nieodłącznie z wdrażaniem coraz to nowych (...)".
str. 167	Brak odwołania w treści do rysunków nr 67, nr 68 i nr 69.
str. 183-189	Brak odwołania w treści do tabeli nr 13, tabeli nr 14 oraz tabeli nr 15.
str. 206	Niezręczność językowa: „W systemie zaaplikowano sposoby postępowania (...)".
str. 209	Podano odwołanie do załącznika nr 4, a w dodatkowe materiały nie zostały oznaczone jako odrębne załączniki.

5. Wnioski końcowe

Merytorycznie dysertację oceniam pozytywnie. Zbudowany katalog zagrożeń bezpieczeństwa informacji oraz metodyka zarządzania bezpieczeństwem informacji dla przedsiębiorstw produkcyjnych stanowi poprawne rozwiązanie formalne postawionego problemu. Ponadto autorka przedstawiła możliwości zastosowania proponowanego podejścia w praktyce gospodarczej.

Stwierdzam, że autorka rozprawy mgr inż. Estera Pietras przedstawiła osiągnięcie będące wynikiem przeprowadzonych badań, które wnoszą wkład w rozwój dyscypliny: nauki o zarządzaniu i jakości. W mojej opinii Autorka wykazała się dobrą znajomością obszaru bezpieczeństwa informacji w przedsiębiorstwach. Ponadto udowodniła, że potrafi prowadzić samodzielnie odpowiedzialne badania naukowe.

Przedstawiona rozprawa doktorska Pani mgr inż. Estery Pietras spełnia warunki Ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz. 1668, z późn. zm.). Stawiam wniosek o uznanie pracy jako spełniającej ustawowe wymagania dla rozprawy doktorskiej w zakresie nauk w dyscyplinie „nauki o zarządzaniu i jakości" oraz wnioskuję o dopuszczenie pani mgr inż. Estery Pietras do publicznej obrony pracy.