PRZEDSIĘBIORCZOŚĆ – EDUKACJA
ENTREPRENEURSHIP – EDUCATION
22(1) ▪ 2026
ISSN 2083-3296
DOI: 10.24917/20833296.221.2

Szymon Głownia
Uniwersytet Ekonomiczny, Kraków, Polska / Krakow University of Economics, Poland

Uwarunkowania i ryzyka wykorzystania sztucznej inteligencji w przedsiębiorstwach – opinie, obawy, postawy

Use of artificial intelligence in enterprises: opinions, concerns, attitudes

Streszczenie: Artykuł podejmuje analizę zagrożeń wynikających z wdrażania sztucznej inteligencji w przedsiębiorstwach, ze szczególnym uwzględnieniem ryzyka błędnych decyzji, dezinformacji oraz odpowiedzialności organizacyjnej i prawnej. Jego celem są identyfikacja kluczowych obszarów ryzyka związanych z wykorzystaniem systemów AI – zwłaszcza w procesach analizy dokumentów finansowych, automatyzacji kontroli oraz wspomagania decyzji biznesowych – a także wskazanie mechanizmów ograniczających ich negatywne skutki. Zastosowano podejście mieszane obejmujące przegląd literatury przedmiotu, analizę aktualnych regulacji prawnych, wyniki autorskiego badania ankietowego dotyczącego postrzegania zagrożeń i zmian na rynku pracy oraz rezultaty przeprowadzonego eksperymentu badawczego. Uzyskane wyniki wskazują, że mimo rosnącej akceptacji społecznej dla rozwoju sztucznej inteligencji użytkownicy są świadomi jej ograniczeń, takich jak halucynacje modeli, brak rozumienia kontekstu czy ryzyko nieautoryzowanego wykorzystania narzędzi AI (*shadow AI*). Wnioski z badań podkreślają konieczność zachowania równowagi między automatyzacją a nadzorem człowieka, rozwoju kompetencji użytkowników oraz wdrażania procedur kontrolnych i regulacyjnych, które warunkują bezpieczne i odpowiedzialne wykorzystanie sztucznej inteligencji w organizacjach.

Abstract: The article analyzes the risks arising from the implementation of artificial intelligence in enterprises, with particular emphasis on the risk of erroneous decisions, misinformation and organizational and legal liability. Its objective is to identify key risk areas associated with the use of AI systems especially in processes such as financial document analysis, control automation and business decision support as well as to indicate mechanisms that can mitigate their negative effects. A mixed-methods approach was applied, including a review of the relevant literature, an analysis of current legal regulations, the results of an original survey on the perception of risks and changes in the labour market, and the outcomes of a research experiment. The findings indicate that despite growing social acceptance of the development of artificial intelligence, users are aware of its limitations, such as model hallucinations, lack of contextual understanding and the risk of unauthorized use of AI tools (shadow AI). The conclusions emphasize the need to maintain a balance between automation and human oversight, to develop user competencies, and to implement control and regulatory procedures that enable the safe and responsible use of artificial intelligence in organizations.

Słowa kluczowe: AI Act; halucynacje sztucznej inteligencji; odpowiedzialność prawna; shadow AI; sztuczna inteligencja; zagrożenia AI

Keywords: AI Act; artificial intelligence; artificial intelligence hallucinations; AI risks; legal liability; shadow AI

Otrzymano: 8 luty 2026
Received: 8 February 2026
Zaakceptowano: 1 czerwca 2026
Accepted: 1 June 2026

Sugerowana cytacja/Suggested citation:

Głownia, S. (2026). Uwarunkowania i ryzyka wykorzystania sztucznej inteligencji w przedsiębiorstwach – opinie, obawy, postawy, *Przedsiębiorczość – Edukacja* [*Entrepreneurship – Education*], *22*(1), 25–40. https://doi.org/10.24917/20833296.221.2

Wstęp

Dynamiczny rozwój sztucznej inteligencji (AI) następujący w ostatnich latach istotnie zmienia sposoby funkcjonowania współczesnych organizacji. Technologie oparte na algorytmach uczenia maszynowego oraz dużych modelach językowych coraz częściej wspierają procesy decyzyjne, analityczne i administracyjne, przez co przyczyniają się do automatyzacji pracy, redukcji kosztów i zwiększenia efektywności operacyjnej. Według badań przedstawionych w 2021 r. w raporcie McKinsey 27% badanych przedsiębiorstw zadeklarowało, że co najmniej 5% zysku operacyjnego jest efektem wdrożenia AI, jednocześnie wykazało tendencje wzrostową względem wyniku poprzedniego badania, w którym takiej odpowiedzi udzieliło 22% respondentów (McKinsey, 2021; 2026, 2 czerwca). Sztuczna inteligencja znajduje zastosowanie w wielu obszarach działalności przedsiębiorstw – od obsługi klienta, przez analizę danych i zarządzanie dokumentami, aż po procesy księgowe i kontrolę finansową. Skala jej wykorzystania rośnie zarówno w dużych korporacjach, jak i w sektorze małych oraz średnich przedsiębiorstw. Według raportu SAP 82,5% przedsiębiorstw wykorzystuje co najmniej jedno rozwiązanie oparte na AI (Demkiw, 2024). Jednocześnie wraz z popularyzacją rozwiązań opartych na AI pojawiają się nowe wyzwania i zagrożenia, które nie zawsze są dostatecznie rozpoznane na etapie wdrożenia technologii. Szczególnym problemem okazuje się nadmierne zaufanie do automatycznych systemów decyzyjnych, których działanie opiera się na danych historycznych, wzorcach statystycznych oraz uproszczonej analizie semantycznej. W efekcie taki system może generować błędne klasyfikacje, nieprawidłowe rekomendacje lub fałszywe wnioski, zwłaszcza w sytuacjach wymagających interpretacji kontekstu, intencji lub znaczenia pojęć. W obecnej literaturze temat zagrożeń wynikających z wdrożenia sztucznej inteligencji nie jest jeszcze dokładnie opisany. Mimo że temat możliwości eliminacji człowieka z obsługi danych i procesów finansowych jest podejmowany w literaturze oraz w licznych internetowych artykułach, to przyjmuje on często formę pesymistycznej wizji fali bezrobocia technologicznego (AI zabierze nam pracę? Ci, którzy z nią pracowali, boją się tego najbardziej, 2024; 2026, 2 czerwca). Obszarem wymagającym dalszych badań są postawa obecnych i przyszłych pracowników wobec zmian, technologii, nowych procesów oraz ich pogląd na nie. Temat zagrożeń wynikających z wdrożenia sztucznej inteligencji do przedsiębiorstw nie został również poddany szerszym analizom (Kalus, 2025; 2026, 2 czerwca). Eksperci z różnych branż zauważają szczególnie

potencjalne zagrożenia związane z bezpieczeństwem oraz wyciekami danych (Duszczyk, 2024; 2026, 14 czerwca). Fakt, że coraz więcej firm wprowadza rozwiązania oparte na AI do swoich systemów, stwarza przestrzeń do kolejnych analiz i ryzyko potencjalnych zagrożeń wynikających z tych działań.

Celem niniejszego artykułu jest analiza zagrożeń związanych z wykorzystaniem sztucznej inteligencji w przedsiębiorstwach, ze szczególnym uwzględnieniem błędów wynikających z automatycznej analizy dokumentów finansowych, detekcji słów kluczowych oraz sposobów uniknięcia tych zagrożeń. Głównym pytaniem badawczym pracy jest: jakie zagrożenia wynikają z wykorzystywania sztucznej inteligencji w przedsiębiorstwach oraz jak minimalizować ich negatywne skutki. W artykule zaprezentowano zarówno przegląd literatury przedmiotu, wyniki własnych badań ankietowych, jak i analizę aktualnych regulacji prawnych, w tym unijnego AI Act. Podjęta tematyka ma na celu ukazanie, że skuteczne i bezpieczne wdrażanie sztucznej inteligencji wymaga nie tylko zaawansowanych technologii, lecz także odpowiednich procedur, kompetencji użytkowników oraz nadzoru człowieka.

Artykuł rozpoczyna się wprowadzeniem, w którym przedstawiono kontekst wykorzystania sztucznej inteligencji w przedsiębiorstwach, cel pracy oraz główne pytanie badawcze. Następnie zaprezentowano przegląd literatury koncentrujący się na zastosowaniach AI oraz zagrożeniach identyfikowanych w literaturze. Kolejna część jest poświęcona metodologii badań własnych i obejmuje opis zastosowanych metod i charakterystykę próby badawczej. W dalszej części omówiono rolę sztucznej inteligencji w transformacji procesów biznesowych oraz przeanalizowano kluczowe ryzyka związane z jej wdrażaniem. Artykuł kończy się podsumowaniem, w którym sformułowano najważniejsze wnioski oraz wskazano kierunki dalszych badań.

Przegląd literatury

Literatura dotycząca sztucznej inteligencji wskazuje, że systemy AI coraz szerzej są wykorzystywane do wspierania zadań biznesowych, edukacyjnych i administracyjnych. Zalewski (2020) definiuje AI jako system zdolny do uczenia się i działania w sposób częściowo autonomiczny, co pozwala zastępować człowieka w zadaniach powtarzalnych. Badania potwierdzają, że społeczeństwo coraz częściej korzysta z narzędzi opartych na sztucznej inteligencji. Badania przeprowadzone m.in. przez zespół naukowców z University of Melbourne we współpracy z firmą KPMG objęły próbę ponad 48 tys. respondentów z 47 krajów, w tym 1082 osoby z Polski. W każdym z analizowanych krajów dane zbierano z wykorzystaniem reprezentatywnych paneli badawczych. Respondenci byli zapraszani do udziału w ankiecie internetowej, a proces gromadzenia danych realizowano od listopada 2024 r. do połowy stycznia 2025 r. Według badania niemal 70% badanych Polaków regularnie korzysta ze sztucznej inteligencji; 9% respondentów obawia się cyberzagrożeń związanych z tą technologią, a 44% osobiście doświadczyło ich skutków. Z dezinformacją wygenerowaną przez AI zetknęło się 54% badanych, a 48% zwróciło uwagę na negatywne skutki automatyzacji (KPMG, 2025; 2025, 31 grudnia).

Sztuczna inteligencja to system, który pozwala na wykonywanie zadań wymagających uczenia się i uwzględniania nowych okoliczności w toku rozwiązywania danego problemu. System ten może w różnym stopniu, w zależności od konfiguracji, działać autonomicznie oraz wchodzić w interakcję z otoczeniem (Zalewski, 2020). Rodzajów urządzeń i programów wykorzystujących AI można znaleźć wiele i z pewnością będą powstawały nowe, jednak

w literaturze wyodrębnia się trzy podstawowe rodzaje substratów zwanych „agentami", przez które AI działa. Są to:

- robot (w sensie nośnika), który często jest zaopatrzony w sensory fizyczne i akumulatory;
- system ekspertowy, któremu człowiek dostarcza informacji, po czym ten wykonuje zadanie;
- software, który działa w środowisku czysto obliczeniowym (Maciąg, Maciąg, 2017).

W przedsiębiorstwach rozwiązania oparte na tych trzech rodzajach agentów wprowadza się przede wszystkim w celu automatyzacji procesów, redukcji kosztów, zwiększenia szybkości działania oraz poprawy jakości decyzji. Roboty fizyczne wykonują zadania operacyjne i magazynowe, systemy ekspertowe wspierają pracowników w analizie danych i podejmowaniu decyzji, z kolei software'owe narzędzia AI integruje się z istniejącymi systemami informatycznymi firmy, aby obsługiwały dokumenty, komunikację, workflow oraz procesy biurowe. AI umożliwia eliminację ograniczeń tradycyjnej automatyzacji, zmniejsza zapotrzebowanie na pracę ludzką w powtarzalnych zadaniach i zwiększa efektywność operacyjną. W miarę jak AI staje się integralną częścią każdego procesu i zadania, coraz ważniejsze jest dysponowanie umiejętnościami, które pozwalają na efektywne wykorzystanie tych technologii w codziennej pracy (Wieteska, 2024; 2025, 30 września).

Proces wdrażania narzędzi opartych na sztucznej inteligencji najczęściej przebiega według jednego z trzech modeli: realizacji całkowicie przez firmę zewnętrzną (32%), wdrożenia przez wewnętrzny zespół we współpracy z dostawcami zewnętrznymi (29%) lub realizacji wyłącznie przy użyciu zasobów własnych (26%) (Olak, 2023; 2025, 2 czerwca). Tak równomierne rozłożenie wskazuje, że przedsiębiorstwa nadal eksperymentują z różnymi podejściami, starając się dopasować rozwiązania do swoich potrzeb i możliwości. Badania sugerują również, że wraz z rosnącym doświadczeniem firmy coraz częściej decydują się na korzystanie z usług zewnętrznych ekspertów dysponujących bardziej rozbudowaną wiedzą i praktyką w zakresie AI. Wdrożenie systemów sztucznej inteligencji w procesach biznesowych, mimo licznych korzyści organizacyjnych i ekonomicznych, wiąże się z występowaniem istotnych zagrożeń, które mogą wpływać na jakość decyzji, bezpieczeństwo danych oraz odpowiedzialność prawną organizacji. Analiza literatury oraz praktyki biznesowej pozwala wyróżnić kilka kluczowych kategorii ryzyka, które korespondują z najczęściej spotykanymi obszarami zastosowań AI w przedsiębiorstwach.

Pierwszym istotnym zagrożeniem są ograniczenia analizy danych oraz ryzyko błędnych decyzji podejmowanych przez systemy AI. Algorytmy, mimo zdolności do przetwarzania dużych wolumenów danych, działają, opierając się na danych historycznych i zdefiniowanych wzorcach, co ogranicza ich zdolność do interpretacji kontekstu oraz wychwytywania niestandardowych sytuacji (Muller, Massaron, 2021). W efekcie system AI może generować błędne klasyfikacje, fałszywe alarmy lub nieuzasadnione rekomendacje, co zostało potwierdzone m.in. w obszarze automatyzacji procesów księgowych oraz kontroli dokumentów (Damioli, Van Roy, Vertesy, 2021).

Odrębnym, lecz powiązanym problemem są halucynacje systemów generatywnej sztucznej inteligencji, polegające na generowaniu informacji nieprawdziwych, niezweryfikowanych lub całkowicie zmyślonych. Badania wskazują, że skala tego problemu jest istotna także w profesjonalnych rozwiązaniach komercyjnych (*Firmy coraz częściej odwracają się od AI. W cenie znów człowiek, ale może być za późno*, 2025; 2026, 2 czerwca).

Drugą kategorią zagrożeń jest problem odpowiedzialności prawnej i organizacyjnej za decyzje podejmowane z wykorzystaniem AI. W środowisku, w którym decyzje

są częściowo lub całkowicie zautomatyzowane, pojawia się trudność w jednoznacznym przypisaniu odpowiedzialności za skutki błędów algorytmicznych. Kwestia odpowiedzialności za błędy popełniane przez systemy sztucznej inteligencji stanowi obecnie jedno z najtrudniejszych zagadnień prawnych. W praktyce odpowiadają za nie różne podmioty, w zależności od źródła błędu oraz etapu, na którym on powstał. Odpowiedzialność ta może spoczywać na użytkowniku instytucjonalnym, dostawcy technologii lub integratorze systemu, co rodzi liczne wyzwania interpretacyjne i prawne (Peeler, 2023; 2026, 2 czerwca; Skowrońska, 2024; Szczudło, 2025; 2026, 2 czerwca). Po pierwsze, to użytkownik instytucjonalny, najczęściej przedsiębiorstwo, ponosi odpowiedzialność wobec klientów lub kontrahentów za skutki decyzji podjętych z wykorzystaniem AI, nawet jeśli błąd wynikał bezpośrednio z działania algorytmu. Organizacja jest zobowiązana do właściwego wdrożenia systemu, nadzoru nad jego działaniem oraz zapewnienia, że sztuczna inteligencja jest wykorzystywana zgodnie z jej przeznaczeniem. Po drugie, odpowiedzialność może ponosić dostawca technologii, jeśli okaże się, że błąd wynikał z wady samego systemu, jego konstrukcji lub niewłaściwego działania, za które odpowiada producent. Po trzecie, odpowiedzialność może ponosić integrator, czyli firma wdrażająca i konfigurująca system, jeżeli nieprawidłowości powstały na etapie instalacji, dostosowania lub integracji AI z istniejącą infrastrukturą przedsiębiorstwa. Wreszcie, po czwarte, prawo dopuszcza możliwość uznania błędu za nieprzewidywalny, a więc powstały mimo zachowania należytej staranności przez wszystkie zaangażowane strony. W takim przypadku żadna ze stron nie ponosi odpowiedzialności, jednak wykazanie nieprzewidywalności błędu wymaga udokumentowania, że system działał zgodnie z obowiązującymi standardami oraz że przeprowadzono odpowiednie testy i nadzór (Szczudło, 2025; 2026, 2 czerwca).

Trzecim istotnym zagrożeniem jest zjawisko *shadow AI*, rozumiane jako nieautoryzowane wykorzystywanie narzędzi sztucznej inteligencji przez pracowników, bez wiedzy i kontroli organizacji, np. gdy pracownicy samodzielnie korzystają z takich narzędzi jak ChatGPT, Copilot, Gemini czy Midjourney, aby szybciej wykonać zadanie, napisać raport czy przygotować prezentację, bez informowania o tym swoich przełożonych lub działu IT (Wiązowska, 2025; 2026, 2 czerwca). Praktyka ta zwiększa ryzyko wycieków danych, naruszeń bezpieczeństwa informacji oraz niezgodności z regulacjami dotyczącymi ochrony danych osobowych (Wiązowska, 2025; 2026, 2 czerwca). *Shadow AI* stanowi szczególne zagrożenie w organizacjach, które nie mają jasno określonych zasad korzystania z narzędzi AI ani odpowiednich szkoleń dla pracowników. W tym kontekście konieczne jest opracowanie odpowiednich regulaminów oraz dobrych praktyk przez firmy. W takich dokumentach powinny zostać zawarte ogólne zasady korzystania z narzędzi AI w codziennej pracy, rodzaj narzędzi, z jakich można korzystać, oraz warunki, kiedy i w jakim celu dopuszcza się korzystanie z nich. Szczególne zagrożenia pojawia się, gdy do systemu są wgrywane poufne dane firmy, informacje o danych osobowych lub wręcz całe pliki danych. Kluczowe jest przeprowadzanie szkoleń z pracy z AI oraz kursów z cyberbezpieczeństwa. Dobrym rozwiązaniem będzie również udostępnienie pracownikom bezpiecznych programów sztucznej inteligencji. Przykładem takiego programu może być Microsoft 365 Copilot. Jest on korzystny dla firm przede wszystkim dlatego, że zwiększa bezpieczeństwo danych firmowych, a jednocześnie usprawnia pracę zespołów i automatyzuje powtarzalne zadania. Działa też jako kontrolowany i nadzorowany punkt dostępu do informacji, dzięki czemu ogranicza ryzyko wycieków, błędnych uprawnień czy przekazywania danych poza firmę, ponieważ wszystkie operacje wykonywane są w ramach systemów i baz przedsiębiorstwa,

a nie w niesprawdzonych kanałach komunikacji. Copilot pozwala również na monitorowanie interakcji pracowników z zasobami, egzekwowanie polityk bezpieczeństwa oraz ograniczenie przypadkowego ujawnienia informacji poufnych, a jednocześnie przyspiesza pracę, generuje dokumenty oparte na wewnętrznych standardach i pomaga utrzymać wysoką jakość obiegu informacji bez zwiększania ryzyka naruszeń czy nieautoryzowanych dostępów (Microsoft, 2025, 3 grudnia). Rozwiązanie takie wdrożyła między innymi spółka Żabka. W ramach partnerstwa Żabka Polska jako pierwsza firma w Polsce zapewniła 2,5 tys. swoich pracowników inteligentnego asystenta – Copilota dla Microsoft 365. Copilot, zaszyty w takich narzędziach jak Outlook, Excel, Word, PowerPoint i Teams, pomaga im szybciej wykonywać powtarzalne i nierzadko żmudne czynności oraz uwalnia ich czas na bardziej kreatywne działania i rozwój kompetencji cyfrowych. Asystent m.in. podsumowuje spotkania, pomaga w przygotowaniu treści maila, projektuje prezentację czy też wspiera pracowników w efektywnym planowaniu tygodnia (Żabka, 2024, 2026, 2 czerwca).

Czwartą, ostatnią kategorią zagrożeń są ryzyka regulacyjne i społeczne związane z naruszaniem praw podstawowych, brakiem transparentności działania systemów oraz niewystarczającą kontrolą nad ich wykorzystaniem. Ważnym aspektem związanym z zagrożeniami związanymi z wdrożeniem sztucznej inteligencji jest również odbiór tych systemów oraz zmian, jakie za sobą niosą, przez przyszłych i obecnych pracowników finansowych. Częściową odpowiedzią na wskazane wyzwania jest unijny Akt o sztucznej inteligencji – AI Act, oparty na podejściu do ryzyka oraz nakładający obowiązki w zakresie nadzoru, dokumentacji i kompetencji użytkowników (*Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689*). Rozporządzenie, obowiązujące od 2 lutego 2025 r., stanowi pierwszą na świecie tak kompleksową i spójną regulację porządkującą zasady funkcjonowania oraz kontroli systemów AI w Unii Europejskiej, ukierunkowaną na ochronę przed nadużyciami i negatywnymi skutkami automatyzacji. Od lutego 2025 r. stosowane są jego początkowe rozdziały, a od 2 czerwca 2025 r. sukcesywnie wdrażane są kolejne części, co wiąże się ze stopniowym zaostrzaniem wymagań wobec twórców i użytkowników tych systemów.

Równocześnie w Polsce Ministerstwo Cyfryzacji prowadzi prace nad ustawą o systemach sztucznej inteligencji, która ma dostosować krajowe procedury nadzorcze do unijnych regulacji (Prorok, 2025; 2026, 2 czerwca). W AI Act wprowadza się podejście oparte na ryzyku, klasyfikujące systemy AI do czterech kategorii: ryzyka nieakceptowalnego, wysokiego, ograniczonego i minimalnego. Systemy o nieakceptowalnym ryzyku są całkowicie zakazane. Ta grupa obejmuje m.in. manipulację behawioralną, systemy social scoringu obywateli, predykcyjne profilowanie czy identyfikację biometryczną w czasie rzeczywistym w przestrzeni publicznej. W kontekście badań nad błędami AI ma to istotne znaczenie, ponieważ część praktyk szczególnie narażonych na zniekształcenia danych, halucynacje modeli czy stronniczość algorytmiczną została całkowicie wyłączona z legalnego użycia. Najbardziej rozbudowane regulacje dotyczą systemów wysokiego ryzyka, które mogą w znaczący sposób wpływać na prawa jednostek, bezpieczeństwo lub decyzje o istotnych skutkach społecznych. Dla takich systemów AI Act narzuca obowiązek prowadzenia szczegółowej dokumentacji, zapewnienia wysokiej jakości danych treningowych, ciągłego monitorowania działania, nadzoru człowieka oraz wykrywania i raportowania błędów. Ma to na celu ograniczenie ryzyka błędnych decyzji systemów, takich jak nieprawidłowe klasyfikacje, nieadekwatne oceny czy automatyczne decyzje oparte na wadliwych danych. W praktyce oznacza to, że organizacje wdrażające systemy AI muszą wprowadzać procedury kontrolne i przestrzegać standardów jakości.

Dla systemów o ograniczonym ryzyku, takich jak generatywna AI wykorzystywana w komunikacji, edukacji czy obsłudze klienta, AI Act wprowadza obowiązki transparentności. Użytkownik musi być jasno poinformowany, że ma do czynienia z treściami generowanymi przez AI. Istotnym elementem regulacji jest również wymóg podnoszenia kompetencji użytkowników systemów AI, czyli tzw. *AI-literacy*. Podkreśla się, że błędy systemów często wynikają z niewłaściwego sposobu ich wykorzystania, nieprecyzyjnych zapytań, błędnej interpretacji wyników lub nadmiernego zaufania do automatycznych rekomendacji. AI Act wskazuje, że organizacje korzystające z AI mają obowiązek zapewnić użytkownikom odpowiednie szkolenia i zasady nadzoru nad systemami. Tym samym podkreśla się współodpowiedzialność człowieka i technologii w procesie podejmowania decyzji. Stopniowe wprowadzanie AI Act ma duże znaczenie dla badań nad błędami i bezpieczeństwem systemów sztucznej inteligencji. Rozporządzenie nie tylko porządkuje obszar prawny, lecz także wyznacza ramy, w których powinny odbywać się projektowanie, testowanie i wdrażanie AI. Wprowadzenie jednolitych, obowiązkowych standardów dla całej Unii Europejskiej sprawia, że zarówno błędy techniczne, jak i organizacyjne stają się przedmiotem regulacji, nadzoru oraz odpowiedzialności prawnej.

Regulacje te nie eliminują zagrożeń całkowicie, lecz wyznaczają ramy odpowiedzialnego i bezpiecznego stosowania AI w organizacjach. Obszarem wymagającym pogłębionej analizy pozostają sposób, w jaki przedsiębiorstwa faktycznie reagują na błędne decyzje podejmowane przez systemy automatyczne, a także przebieg procesów identyfikacji, wyjaśniania i korygowania tych błędów.

Metodologia

W pracy zastosowano podejście mieszane, łączące metody jakościowe i ilościowe, co pozwoliło na wieloaspektową analizę zagrożeń związanych z wykorzystaniem sztucznej inteligencji w przedsiębiorstwach. Zastosowanie podejścia mieszanego w badaniu wynika ze złożonego charakteru analizowanego zjawiska, które obejmuje zarówno mierzalne aspekty wykorzystania sztucznej inteligencji w organizacjach, jak i subiektywne postawy, doświadczenia oraz percepcję zagrożeń przez użytkowników. Metody ilościowe umożliwiły określenie skali zjawiska, częstości występowania określonych opinii oraz identyfikację dominujących tendencji w badanej próbie. Z kolei metody jakościowe pozwoliły na pogłębioną interpretację uzyskanych wyników, wyjaśnienie ich kontekstu oraz lepsze zrozumienie mechanizmów leżących u podstaw obserwowanych zależności. Zastosowane podejście miało charakter komplementarny i sekwencyjny. Analiza ilościowa stanowiła w nim punkt wyjścia dla interpretacji jakościowej. Dodatkowo wykorzystano elementy triangulacji poprzez zestawienie wyników badań ankietowych z analizą literatury przedmiotu oraz przykładami praktyki biznesowej, co przyczyniło się do zwiększenia wiarygodności i spójności formułowanych wniosków.

Podstawę badań stanowiła analiza literatury przedmiotu obejmująca publikacje naukowe, raporty branżowe, publikacje w czasopismach branżowych oraz akty prawne dotyczące zastosowań AI, jej ograniczeń i odpowiedzialności za decyzje algorytmiczne. Zostały one wybrane na podstawie określonych słów kluczowych związanych ze sztuczną inteligencją, z automatyzacją procesów oraz zagrożeniami wynikającymi z jej stosowania. Choć przegląd miał charakter narracyjny, a nie systematyczny, to wykorzystane źródła umożliwiły konceptualizację kluczowych zagrożeń związanych z wdrożeniem AI, w tym problemów

związanych z bezpieczeństwem danych, odpowiedzialnością prawną, błędami systemów oraz dezinformacją. Takie podejście pozwoliło zbudować spójną ramę analityczną, która stanowi punkt odniesienia dla dalszych analiz empirycznych.

Dodatkowo przeprowadzono badanie ankietowe metodą sondażu diagnostycznego z wykorzystaniem autorskiego kwestionariusza internetowego. Badanie zostało przeprowadzone za pomocą formularza Google. W ankiecie wzięło udział 116 osób. Wśród badanych było 39 mężczyzn, 75 kobiet i 2 osoby nieidentyfikujące się z żadną z płci. Przedmiotem badania były postawy, zachowania oraz stosunek wobec różnych narzędzi sztucznej inteligencji. Podmiotem badawczym były osoby dorosłe, zamieszkujące zarówno obszary wiejskie, jak i miejskie. Narzędzie badawcze stanowiła autorska ankieta internetowa. Ankieta została poddana walidacji merytorycznej przez dwóch ekspertów z branży sztucznej inteligencji, a pilotaż nie wykazał problemów ze zrozumieniem pytań. Dobór próby badawczej był celowy, prowadzony metodą doboru nielosowego, kryterialnego. Cel doboru polegał na objęciu mieszkańców wsi i miast o zróżnicowanej strukturze demograficznej (wiek, wykształcenie, status zawodowy), aby uzyskać reprezentatywność strukturalną kluczowych grup docelowych zainteresowanych sztuczną inteligencją (tabela 1). Dane uzyskano w formie ankiety online, która była dystrybuowana za pośrednictwem grup tematycznych w mediach społecznościowych (Facebook, fora internetowe).

Tabela 1. Rozkład respondentów ze względu na wiek i wykształcenie

Wykształcenie	Przedział wiekowy respondentów						Suma
	65+ lat	18–25 lat	26–33 lat	34–41 lat	42–49 lat	50–57 lat	
Jeszcze studiuję	-	72	2	-	-	-	74
Nie podjąłem / Nie podjęłam studiów	-	9	1	2	2	4	18
Mam ukończone studia	1	5	5	3	7	3	24
Suma końcowa	1	86	8	5	9	7	116

Źródło: opracowanie własne.

Respondenci zostali poinformowani o anonimowości badania i dobrowolności udziału, a wypełnienie ankiety było równoznaczne z wyrażeniem zgody na udział. Ankieta ilościowa pozwoliła na określenie skali i częstości występowania postaw oraz doświadczeń respondentów na podstawie odpowiedzi na pytania dotyczące poziomu korzystania z AI i postrzeganych zagrożeń.

W ramach procedury badawczej zrealizowano także test eksperymentalny polegający na kontrolowanym wykorzystaniu ogólnodostępnych narzędzi AI do analizy treści wybranych 20 faktur kosztowych za usługi zakwaterowania. Narzędziom przekazano jednolicie sformułowany prompt ukierunkowany na identyfikację zdefiniowanego zestawu słów kluczowych mogących sugerować występowanie wydatków o charakterze prywatnym. Otrzymane wskazania systemów AI porównano następnie z rzeczywistą kwalifikacją pozycji kosztowych dokonaną przez człowieka, co umożliwiło ocenę skali błędów interpretacyjnych wynikających z analizy opartej wyłącznie na kryteriach leksykalnych, bez uwzględnienia kontekstu dokumentu.

Podsumowując – przeprowadzona analiza dostarczyła pogłębionych informacji na temat mechanizmów ryzyka oraz kontekstu obserwowanych zjawisk, wspierając interpretację

wyników ilościowych i formułowanie wniosków. Powiązanie zastosowanych metod z postawionymi pytaniami badawczymi umożliwiło spójne i uzasadnione wnioskowanie oraz ograniczyło ryzyko niejednoznaczności interpretacyjnych. W analizie uwzględniono również charakter próby badawczej oraz potencjalne błędy systemów AI, co pozwoliło na świadome ograniczenie nadmiernego uogólniania wniosków i precyzyjniejsze określenie granic interpretacji uzyskanych wyników.

Wyniki badań ankietowych

Wdrażanie sztucznej inteligencji w przedsiębiorstwach jest związane przede wszystkim ze zmianami i z wyzwaniami dla pracowników. Wielu obecnych pracowników musi nauczyć się bowiem współdziałania w nowym środowisku, w przypadku przyszłych pracowników lub poszukujących nowej pracy oznacza to często konieczność uzyskania nowych kompetencji, które czasem można zdobyć jedynie w praktyce. Wyniki autorskiego badania ankietowego ukazują, że obecni i przyszli pracownicy dostrzegają zmiany, które się dokonują w przedsiębiorstwach, oraz podejście pracodawców do przyszłych i obecnych pracowników (tabela 2).

Tabela 2. Czy uważa Pan/Pani, że technologia zmieniła podejście pracodawców i zapotrzebowanie na pracowników?[1]

Możliwe odpowiedzi	Liczba odpowiedzi respondentów			Suma
	niestudiujących	jeszcze studiujących	absolwentów studiów	
Tak, wiele zawodów stało się przestarzałych, a powstały nowe, wymagające kompetencji technologicznych	6	32	7	45
Tak, technologia sprawiła, że pracodawcy szukają osób z umiejętnościami cyfrowymi i technologicznymi	8	31	10	49
Tak, zwłaszcza w kontekście pracy zdalnej i cyfrowej współpracy	5	26	8	39
Tak, widoczna jest rosnąca potrzeba elastyczności i adaptacji do nowych narzędzi	3	25	9	37
Tak, ale zmiany są stopniowe i wciąż istnieje zapotrzebowanie na tradycyjne zawody	4	28	7	39
Częściowo, technologia wpłynęła na podejście pracodawców – obecnie większą wagę przywiązuje się do automatyzacji procesów i efektywności pracy	4	18	2	24

1 W pytaniu była możliwość wyboru maksymalnie trzech odpowiedzi.

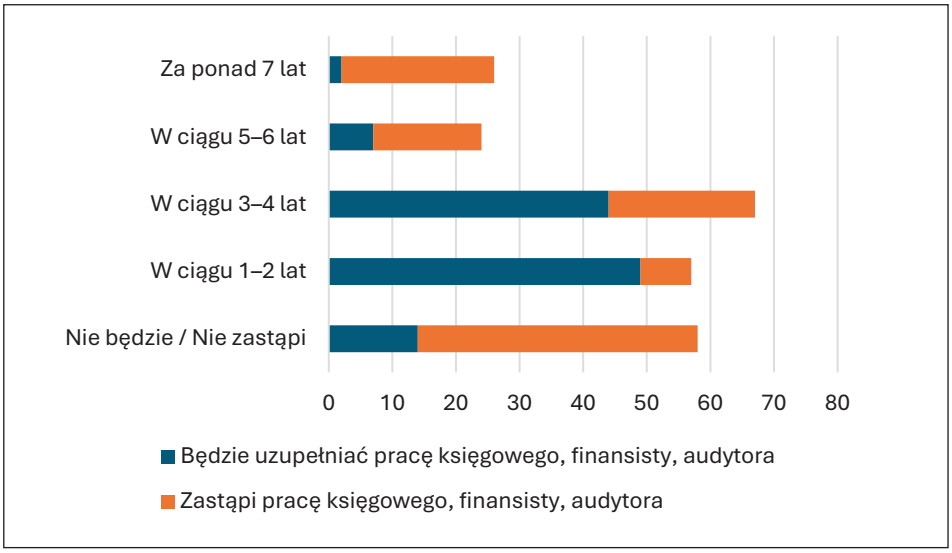
Nie do końca, technologia zmieniła narzędzia pracy, ale podstawowe umiejętności i cechy pracownika są nadal cenione	2	5	1	8
Nie, nadal dominuje tradycyjne podejście do pracy i zatrudnienia	1	0	0	1

Źródło: opracowanie własne.

Analiza wyników ankiety wskazuje, że większość respondentów dostrzega wyraźny wpływ technologii, w tym sztucznej inteligencji, na transformację rynku pracy, co w kontekście artykułu należy interpretować również jako potencjalne zagrożenie dla pracowników i organizacji. Najwięcej wskazań uzyskały odpowiedzi podkreślające, że wiele zawodów stało się przestarzałych, a jednocześnie pojawiły się nowe, wymagające kompetencji technologicznych (45 głosów), oraz że pracodawcy coraz częściej poszukują osób z umiejętnościami cyfrowymi i technologicznymi (49 głosów). Te wyniki wskazują, że wdrożenie AI w procesy biznesowe może prowadzić do przemian w strukturze zatrudnienia, w której tradycyjne role są stopniowo eliminowane lub przekształcane, a brak odpowiednich kwalifikacji staje się czynnikiem ryzyka wykluczenia zawodowego. Respondenci zauważają również rosnącą potrzebę elastyczności i adaptacji do nowych narzędzi oraz pracy zdalnej i cyfrowej współpracy (37–39 głosów). Wskazuje to, że nawet jeśli dana osoba nie traci pracy bezpośrednio z powodu automatyzacji, to wciąż musi się dostosowywać do zmieniającego się środowiska pracy, co może wywoływać presję psychiczną, wymuszać szybkie nabywanie nowych kompetencji i zwiększać ryzyko błędów w sytuacjach wymagających współpracy człowiek–AI. Pojawia się również ryzyko niedopasowania pracowników. Potrzeby pracodawców zmieniają się bowiem bardzo dynamicznie, a pracownicy potrzebują jednak czasu na poznanie nowej, ciągle zmieniającej się technologii. Część respondentów dostrzega tylko częściowy wpływ technologii, np. w zakresie automatyzacji procesów, zdalnej rekrutacji czy zwiększonej efektywności pracy (16–24 odpowiedzi). Wyniki te sugerują, że transformacja zachodzi nierównomiernie, co może prowadzić do zróżnicowanych doświadczeń pracowników – część będzie korzystać z ułatwień wynikających z AI, podczas gdy inni mogą napotkać bariery w adaptacji lub zostać pominięci w procesie automatyzacji. Niewielka liczba odpowiedzi wskazujących, że technologia nie zmieniła istotnie pracy (1–8 odpowiedzi), potwierdza, że tradycyjne zawody nadal istnieją, jednak w miarę dalszego rozwoju AI mogą stopniowo tracić znaczenie, co tworzy potencjalne zagrożenie dla stabilności zawodowej i rynku pracy w dłuższej perspektywie. Respondenci dostrzegają również, że sztuczna inteligencja będzie w coraz większym stopniu wspierać pracę osób na stanowiskach finansistów, audytorów i księgowych, a z czasem nastąpi również częściowe przejście z uzupełniania pracowników do ich eliminowania (rycina 1).

Najwięcej osób zadeklarowało, że w ciągu najbliższych lat (1–2) AI będzie wspierać specjalistów, co wskazuje na przekonanie, że w nadchodzącym czasie jej rola ograniczy się do automatyzacji rutynowych zadań przy jednoczesnym zachowaniu roli człowieka w podejmowaniu decyzji. W dłuższym horyzoncie czasowym, szczególnie w przedziale 3–4 lat oraz powyżej 7 lat, zauważalnie wzrasta liczba osób, które dopuszczają możliwość zastąpienia pracowników przez sztuczną inteligencję. Aż 24 osoby wskazały, że za ponad 7 lat może dojść do pełnej automatyzacji tych zawodów. Interpretując te wyniki, można stwierdzić, że respondenci są świadomi nadchodzących zmian technologicznych, jednak

Rycina 1. Rozkład odpowiedzi na pytanie: Kiedy sztuczna inteligencja zastąpi/będzie uzupełniać pracę finansisty, audytora i księgowego?



Źródło: opracowanie własne.

w zdecydowanej większości zakładają, że rola sztucznej inteligencji będzie polegała raczej na wspieraniu niż zastępowaniu pracy człowieka. Obawy dotyczące pełnej automatyzacji pojawiają się głównie w długoterminowej perspektywie, co sugeruje, że cyfrowa transformacja jest postrzegana jako proces ewolucyjny, a nie rewolucyjny. Wśród respondentów 39% uważało, że rozwój sztucznej inteligencji powinien być kontynuowany, jednak aż 70% wszystkich badanych uważa, że powinny wejść w życie szczegółowe przepisy regulujące zastosowanie sztucznej inteligencji w Polsce. Jedynie mały odsetek badanych (<5%) uważa, że dalszy rozwój sztucznej inteligencji powinien być wstrzymany i że powinno się mu wręcz przeciwdziałać.

Wyniki badania ukazują, że respondenci w większości są pozytywnie nastawieni do sztucznej inteligencji, jednak dostrzegają konieczność wprowadzenia jasnych przepisów regulujących korzystanie ze sztucznej inteligencji. Analizując wyniki badania ankietowego, można stwierdzić, że ankietowani są bardzo świadomi zagrożeń wynikających ze sztucznej inteligencji i z jej potencjalnego nadużywania.

Wyniki testu eksperymentalnego

W kontekście automatyzacji procesów księgowych i kontrolnych coraz częściej wykorzystuje się systemy sztucznej inteligencji do analizy dokumentów finansowych, takich jak faktury kosztowe. Istotnym ograniczeniem tego podejścia jest jednak brak zdolności systemu do jednoznacznej oceny, czy wykryte informacje odnoszą się do rzeczywistego kosztu ujętego na fakturze, czy jedynie do wyrazu występującego w nazwie usługi, nazwie obiektu lub w opisie o charakterze marketingowym. W rezultacie może dochodzić do błędnych klasyfikacji dokumentów oraz formułowania nieuzasadnionych wniosków dotyczących ich zgodności z polityką firmy.

Sztuczna inteligencja działa na podstawie danych historycznych i dopasowania. Przykładowo na ich podstawie firma definiuje słowa kluczowe, które AI ma wykrywać. Podstawowym problemem w tym wypadku jest to, że program wykrywa słowa kluczowe niezależnie od miejsca ich występowania w dokumencie. Występowanie słowa określonego jako słowo kluczowe w nazwie firmy, adresie lub opisie niezwiązanym z realnym kosztem jest dla systemu bez znaczenia. Człowiek podejmuje często decyzję na podstawie intuicji, dopuszczając różne możliwości. Rezygnacja z korzystania ze słów kluczowych lub ograniczenie ich wykrywania tylko do pozycji kosztowych (zwanych również częścią szczegółową faktury) nie rozwiązują problemów, zwłaszcza w przypadkach, gdy w tej części faktury pojawia się skrótowy opis kosztu, a jego rozwiniecie znajduje się w innej części dokumentu, np. gdy faktura zawiera pozycję: „Pakiet Biznesowy*", a realny opis znajduje się w legendzie dokumentu.

Eksperyment przeprowadzony na potrzeby niniejszego badania polegał na wykorzystaniu ogólnodostępnych narzędzi sztucznej inteligencji do analizy treści wybranych 20 faktur za usługi zakwaterowania. Systemom AI przekazano treść dokumentów wraz z poleceniem identyfikacji słów kluczowych, które mogłyby sugerować występowanie kosztów dodatkowych, niezwiązanych bezpośrednio z usługą noclegową. W szczególności oczekiwano wykrywania określeń wskazujących na wydatki o potencjalnie prywatnym charakterze, takich jak opłaty za bar, minibar, saunę, masaż, usługi spa oraz inne świadczenia towarzyszące pobytowi.

Uzyskane wyniki ujawniły szereg istotnych ograniczeń takiego podejścia. Modele AI, opierając się przede wszystkim na analizie leksykalnej i wyszukiwaniu słów kluczowych, nie zawsze prawidłowo interpretowały kontekst zapisów na fakturach. W konsekwencji dochodziło do błędnej kwalifikacji niektórych pozycji kosztowych jako wydatków prywatnych, mimo że w rzeczywistości stanowiły one element standardowej usługi hotelowej lub były prawidłowo uzasadnione służbowo.

Rezultaty eksperymentu wskazują, że zastosowanie narzędzi AI w analizie dokumentów księgowych wymagających interpretacji kontekstowej może prowadzić do dezinformacji oraz nieprawidłowych decyzji kontrolnych, jeśli proces ten nie jest wsparty dodatkową weryfikacją ekspercką. Co istotne, problem ten nie ogranicza się wyłącznie do narzędzi ogólnodostępnych. Doświadczenia z praktyki biznesowej pokazują, że również profesjonalne systemy AI wykorzystywane w finansach, księgowości i audycie wykazują podatność na generowanie błędnych wniosków w sytuacjach, w których konieczna jest interpretacja znaczenia, a nie jedynie identyfikacja występowania określonych fraz. Zgodnie z danymi publikowanymi przez Upwork modele sztucznej inteligencji generują fałszywe lub nieuzasadnione informacje średnio od 10 do 12% przypadków (*Firmy coraz częściej odwracają się od AI. W cenie znów człowiek, ale może być za późno*, 2025; 2026, 2 czerwca). Wyniki te podkreślają konieczność krytycznej oceny zastosowań AI w procesach decyzyjnych oraz potrzebę uwzględnienia mechanizmów kontroli i nadzoru ludzkiego. Wprowadzenie audytorów odpowiedzialnych za weryfikację losowo wybranych przypadków rozstrzygniętych przez system AI, a także za ocenę sygnałów ostrzegawczych generowanych przez te systemy stanowi istotny mechanizm kontrolny. Rolą audytorów byłoby rozstrzyganie, czy problem wskazany przez system ma charakter rzeczywisty, czy też wynika z błędnej interpretacji treści dokumentu. Takie podejście może znacząco ograniczyć ryzyko podejmowania decyzji opartych na halucynacjach modeli AI, a jednocześnie zwiększyć wiarygodność i zaufanie do automatycznych systemów wspierających procesy kontrolne i księgowe. Dodatkowo

stały nadzór człowieka pozwala na bieżące doskonalenie algorytmów poprzez identyfikację powtarzalnych błędów i luk w danych treningowych. W efekcie współpraca człowieka z AI może przyjąć formę modelu hybrydowego, w którym technologia wspiera odpowiedzialność decyzyjną, lecz jej nie zastępuje.

W przypadku dużych modeli językowych, takich jak ChatGPT czy Gemini, badacze oraz użytkownicy zauważyli, że mogą one podawać błędne informacje, mylące, niepotwierdzone lub zmyślone. Zjawisko to jest nazywane przez badaczy halucynacjami sztucznej inteligencji (Roose, 2023; 2026, 2 czerwca). Należy jednak zauważyć, że źródłem halucynacji chatbotów może być również nieprecyzyjne formułowanie promptów przez użytkowników. Błędne sformułowanie polecenia, niedostateczne doprecyzowanie problemu lub niejednoznaczności językowe mogą prowadzić do generowania odpowiedzi odbiegających od rzeczywistego kontekstu analizy (2025, 29 listopada). W konsekwencji jakość uzyskanych wyników jest w istotnym stopniu uzależniona nie tylko od możliwości samego narzędzia AI, lecz także od kompetencji użytkownika w zakresie właściwego konstruowania zapytań. Dobry prompt to jasne i konkretne polecenie zawierające pełen kontekst, cel oraz oczekiwania: należy wyraźnie określić, czego się chce (np. napisania streszczenia, wyjaśnienia czegoś, przeredagowania tekstu), wskazać odbiorcę, styl i format, doprecyzować ograniczenia, takie jak długość, język, czy przykłady (Kacprzak, 2024).

Podsumowując, należy stwierdzić, że współpraca człowieka z AI może skutkować zwiększoną innowacyjnością organizacyjną. Dzięki możliwościom analizy ogromnych zbiorów danych AI dostarcza precyzyjnych i aktualnych informacji, co przekłada się na lepsze decyzje strategiczne oraz operacyjne. W ten sposób firmy mogą uzyskać przewagę konkurencyjną (Giacomo Damioli, Van Roy, Vertesy, 2021). Jednak wyjście poza liczby jest dla tych systemów problemem. Interpretacja danych wiąże się z koniecznością spojrzenia poza nie. Sztuczna inteligencja nigdy nie zrozumie, że dane mogą wskazywać na coś innego, niż pozornie może się wydawać. Człowiek potrafi stwierdzić, że dane są nieprawdziwe lub sfałszowane, mimo że nie ma bezpośrednich dowodów o tym świadczących. Dla sztucznej inteligencji dostarczone dane zawsze będą wiarygodne (Mueller, Massaron 2021).

Podsumowanie

Przeprowadzona analiza literatury, przykładów praktycznych oraz wyników badań empirycznych potwierdza, że sztuczna inteligencja stanowi jedno z kluczowych narzędzi transformacji cyfrowej przedsiębiorstw. Jednocześnie wyniki badań wskazują, że systemy AI nie są pozbawione istotnych ograniczeń. W określonych warunkach mogą one generować błędne wnioski, sprzyjać dezinformacji oraz zwiększać ryzyko organizacyjne, zwłaszcza w sytuacjach wymagających interpretacji kontekstowej i oceny znaczenia informacji.

Szczególnie problematyczne okazują się rozwiązania oparte na analizie słów kluczowych oraz danych historycznych, które nie uwzględniają pełnego kontekstu dokumentów ani intencji użytkowników. Przykład analizy faktur kosztowych pokazuje, że automatyczna detekcja określonych terminów może prowadzić do fałszywych alarmów i nieuzasadnionego odrzucania dokumentów, nawet w przypadku profesjonalnych systemów komercyjnych. Zjawisko halucynacji sztucznej inteligencji, potwierdzone zarówno w literaturze przedmiotu, jak i w obserwacjach z praktyki biznesowej, dodatkowo podkreśla, że konieczne jest ostrożne i krytyczne podejście do wyników generowanych przez algorytmy.

Istotnym wnioskiem płynącym z przeprowadzonych badań jest potrzeba zachowania równowagi między automatyzacją a nadzorem człowieka. Wdrażanie mechanizmów kontroli, takich jak losowa weryfikacja decyzji AI, audyty systemów czy jasno określone procedury odpowiedzialności, może znacząco ograniczyć ryzyko błędów. Równie istotne jest inwestowanie w kompetencje użytkowników, w tym umiejętność precyzyjnego formułowania zapytań oraz krytycznej interpretacji uzyskiwanych wyników. Wprowadzenie regulacji prawnych, takich jak AI Act, jest ważnym krokiem w kierunku zwiększenia bezpieczeństwa i transparentności wykorzystania sztucznej inteligencji. Regulacje te nie eliminują jednak wszystkich zagrożeń, lecz wyznaczają ramy odpowiedzialnego projektowania i stosowania systemów AI. Ostateczna skuteczność tych rozwiązań zależy od świadomości organizacji, jakości wdrożeń oraz kultury odpowiedzialnego korzystania z technologii.

Należy jednocześnie wskazać na ograniczenia przeprowadzonego badania, które mogą wpływać na interpretację uzyskanych wyników. Zastosowany dobór próby miał charakter nielosowy i celowy, co ogranicza możliwość pełnego uogólniania rezultatów na populację osób dorosłych lub wszystkich użytkowników sztucznej inteligencji w przedsiębiorstwach. Struktura próby charakteryzowała się nadreprezentacją osób młodych oraz studiujących, co mogło oddziaływać na sposób postrzegania zagrożeń związanych z AI, zwłaszcza w kontekście doświadczenia zawodowego i praktycznego kontaktu z rozwiązaniami stosowanymi w biznesie. Kolejnym ograniczeniem było wykorzystanie ankiety internetowej opartej na deklaracjach respondentów, co wiąże się z ryzykiem subiektywizmu, błędu samooceny oraz tendencji do udzielania odpowiedzi zgodnych z oczekiwaniami społecznymi. Badanie miało ponadto charakter przekrojowy, co uniemożliwia analizę zmian postaw i percepcji zagrożeń w czasie. Świadome uwzględnienie tych ograniczeń pozwala na ostrożniejszą i bardziej adekwatną interpretację wyników oraz wyznacza kierunki dalszych badań, które mogłyby obejmować większe i bardziej zróżnicowane próby, zastosowanie odmiennych metod badawczych oraz pogłębione analizy jakościowe.

Dalsze badania w tym obszarze powinny koncentrować się na praktycznych mechanizmach ograniczania błędów systemów AI oraz na sposobach ich bezpiecznej integracji z procesami decyzyjnymi, w których kluczową rolę nadal odgrywa człowiek. W szczególności zasadne są identyfikowanie i testowanie rozwiązań organizacyjnych oraz proceduralnych, takich jak wielopoziomowa weryfikacja wyników generowanych przez AI, mechanizmy *human-in-the-loop*, losowe audyty decyzji systemów czy standardy odpowiedzialności za decyzje wspierane algorytmicznie. Istotnym kierunkiem badań jest również analiza wpływu jakości promptów, kompetencji cyfrowych użytkowników oraz kontekstu organizacyjnego na trafność i wiarygodność wyników generowanych przez modele AI. Pozwoli to lepiej zrozumieć, w jakim stopniu błędy przypisywane technologii wynikają z ograniczeń samych modeli, a w jakim z niewłaściwego sposobu ich wykorzystania. Warto także rozwijać badania nad projektowaniem procedur współpracy człowieka z systemem AI w środowisku pracy, obejmujące m.in. podział odpowiedzialności, transparentność działania algorytmów, interpretowalność wyników oraz budowanie zaufania do technologii. Uzupełnieniem tych analiz powinny być studia przypadków przedsiębiorstw, w których AI została wdrożona w obszarach finansów, kontroli, księgowości i audytu, co pozwoli na wypracowanie dobrych praktyk możliwych do zastosowania w szerszym kontekście organizacyjnym.

Literatura
References

AI zabierze nam pracę? Ci, którzy z nią pracowali, boją się tego bardziej. (2024; 2026, 2 czerwca). Pozyskano z: https://businessinsider.com.pl/praca/ai-zabierze-nam-prace-ci-ktorzy-z-nia-pracowali-boja-sie-tego-bardziej/6wkvzmd.

Damioli, G., Van Roy, V., Vertesy, D. (2021). The impact of artificial intelligence on labor productivity. *Eurasian Business Review*, *11*, 1–25.

Demkiw, M. (2024). Sztuczna inteligencja to narzędzie do osiągania celów biznesowych, a nie cel sam w sobie. W: *Biznes napędzany cyfrowo – czy przez ludzi? AI, ESG i fundusze unijne z perspektywy polskich menadżerów*. Warszawa: SAP, 8–16.

Duszczyk, M. (2024; 2026, 14 czerwca). *Nadchodzą ciężkie czasy w sieci. Eksperci wieszczą potężne zagrożenia*. Pozyskano z: https://pro.rp.pl/raporty-ekonomiczne/art41624791-nadchodza-ciezkie-czasy-w-sieci-eksperci-wieszcza-potezne-zagrozenia.

Kalus, K. (2025; 2026, 2 czerwca). *Alarmujący przykład z Niemiec. „Człowiek może stać się zbędny"*. Pozyskano z: https://www.money.pl/gospodarka/niemiecka-firma-juz-na-to-wpadla-ekspert-czlowiek-moze-stac-sie-zbedny-7202552656710240a.html.

Kacprzak, A. (2024). *Prompt engineering i ChatGPT. Poradnik skutecznej komunikacji ze sztuczną inteligencją*. Gliwice: Helion.

KPMG. (2025; 2025, 31 grudnia). *Sztuczna inteligencja w Polsce – krajobraz pełen paradoksów*. Pozyskano z: https://assets.kpmg.com/content/dam/kpmgsites/pl/pdf/2025/07/pl-Raport-KPMG-w-Polsce-KPMG-AI-Trust-2025-web.pdf.

Maciąg, M., Maciąg, K. (2017). *Trendy i rozwiązania technologiczne – odpowiedź na potrzeby współczesnego społeczeństwa*, t. 2. Lublin: Wydawnictwo Naukowe Tygiel.

McKinsey. (2021; 2026, 2 czerwca). *Global survey: The state of AI in 2021*. Pozyskano z: https://www.mckinsey.com/capabilities/quantumblack/our-insights/global-survey-the-state-of-ai-in-2021.

Microsoft. (2025, 3 grudnia). *Microsoft 365 Copilot*. Pozyskano z: https://www.microsoft.com/pl-pl/microsoft-365-copilot.

Mueller, J.P., Massaron, L. (2021). *Sztuczna inteligencja dla bystrzaków*. Gliwice: Helion.

Olak, R. (2023; 2025, 2 czerwca). *Badanie EY: implementacja narzędzi sztucznej inteligencji w polskich firmach nabiera tempa*. Pozyskano z: https://www.ey.com/pl_pl/newsroom/2023/11/ey-jak-polskie-firmy-wdrazaja-ai.

OpenAI. (2025, 29 listopada). Warunki użytkowania (aktualizacja: 11 grudnia 2024). Pozyskano z: https://openai.com/pl-PL/policies/row-terms-of-use/.

Peeler, R. (2023, 2026, 2 czerwca). *The hidden costs of implementing AI in enterprise*. Pozyskano z: https://www.forbes.com/councils/forbestechcouncil/2023/08/31/the-hidden-costs-of-implementing-ai-in-enterprise/.

Prorok, B. (2025; 2026, 2 czerwca). *Sztuczna inteligencja w polskim porządku prawnym*. Pozyskano z: https://www.parp.gov.pl/component/content/article/88768:sztuczna-inteligencja-w-polskim-porzadku-prawnym-jakie-rozwiazania-przewiduje-krajowa-ustawa.

Roose, K. (2023; 2026, 2 czerwca). *Why a conversation with Bing's chatbot left me deeply unsettled*. Pozyskano z: https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG) (Dz.Urz. UE z 12.07.2024 r. L 2024/1689).

Firmy coraz częściej odwracają się od AI. W cenie znów człowiek, ale może być za późno. (2025; 2026, 2 czerwca). Pozyskano z: https://cyfrowa.rp.pl/globalne-interesy/art43002871-firmy-coraz-czesciej-odwracaja-sie-od-ai-w-cenie-znow-czlowiek-ale-moze-byc-za-pozno.

Skowrońska, J. (2024). *Prawnokarne aspekty technologii wykorzystującej sztuczną inteligencję ze szczególnym uwzględnieniem kwalifikacji prawnej, przypisania sprawstwa i odpowiedzialności twórcy*. Łódź: Uniwersytet Łódzki, Wydział Prawa i Administracji.

Szczudło, A. (2025; 2026, 2 czerwca). *Jak bezpiecznie wdrożyć AI w biznesie – poradnik od prawnika*. Pozyskano z: https://creativa.legal/jak-bezpiecznie-wdrozyc-ai-w-biznesie/.

Wiązowska, K. (2025; 2026, 2 czerwca). *AI „pod biurkiem" może kosztować miliony. Nowe zagrożenie dla biznesu*. Pozyskano z: https://www.bankier.pl/wiadomosc/Sztuczna-inteligencja-za-plecami-szefa-Shadow-AI-rosnie-w-sile-i-zagraza-klientom-9045436.html.

Wieteska, M. (2024; 2025, 30 września). *Era sztucznej inteligencji. Kompetencje i umiejętności przyszłości – jak zmieni się rynek i edukacja w obliczu rewolucji AI?* Pozyskano z: https://sklep.infor.pl/artykul-era-sztucznej-inteligencji-kompetencje-i-umiejetnosci-przyszlosci-jak-zmieni-sie-rynek-i-edukacja-w-obliczu-rewolucji-ai.

Zalewski, T. (2020). Definicja sztucznej inteligencji. W: L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*. Warszawa: C.H Beck, 1–14.

Żabka. (2024, 2026, 2 czerwca). *Żabka podpisała strategiczne partnerstwo z Microsoft w obszarze AI*. Pozyskano z: https://cdn.zabka.pl/wp-content/uploads/2024/07/11155453/Komunikat_Zabka-podpisala-strategiczne-partnerstwo-z-Microsoft-w-obszarze-AI_11-07-2024.pdf.

Szymon Głownia, lic., student kierunku przedsiębiorczość i innowacje w gospodarce oraz absolwent studiów licencjackich na kierunku doradztwo inwestycyjno-gospodarcze na Uniwersytecie Ekonomicznym w Krakowie. Jego główne zainteresowania naukowo-badawcze koncentrują się wokół innowacji, finansów oraz nowych technologii. Stypendysta programu „Złote Indeksy NBP" przeznaczonego dla najlepszych studentów kierunków ekonomicznych w Polsce. Aktywny członek Koła Naukowego Przedsiębiorczości i Innowacji w Gospodarce działającego przy Uniwersytecie Ekonomicznym w Krakowie.

Szymon Głownia, a student of *Entrepreneurship and Innovation in the Economy* and a graduate with a Bachelor's degree in *Investment and Economic Advisory* from the Krakow University of Economics. His main academic and research interests focus on innovation, finance and new technologies. He is a recipient of a "Golden Indexes of the National Bank of Poland" scholarship, awarded to the top students in economics-related fields in Poland. He is also an active member of the Student Research Group on Entrepreneurship and Innovation in the Economy at the Krakow University of Economics.

ORCID: https://orcid.org/0009-0004-8129-7842

Adres/Address:

Uniwersytet Ekonomiczny w Krakowie
Katedra Przedsiębiorczości i Innowacji
ul. Rakowicka 27
31-510 Kraków

e-mail: 225126@student.uek.krakow.pl