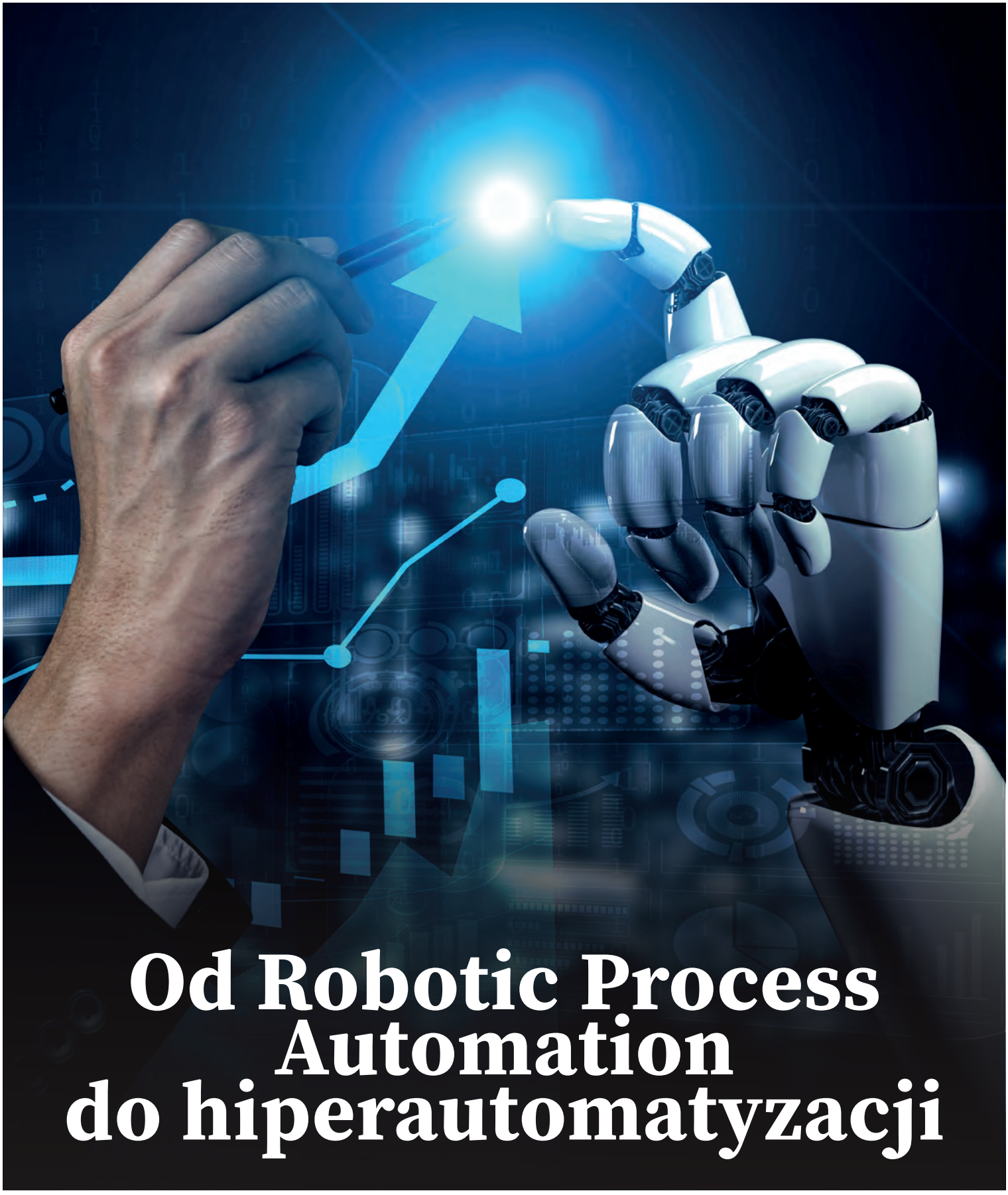
Partner strategiczny raportu

COMARCH

Partnerzy raportu

cloudware FORTINET PIVOTAL



Od Robotic Process Automation do hiperautomatyzacji

KONFERENCJE/SZKOLENIA

Podsumowanie 2020

online

18
Konferencji
2020

31
Szkoleń
2020

6821
Uczestników
2020

82% POWRACAJĄCYCH FIRM PARTNERSKICH

94% POZYTYWNYCH REKOMENDACJI UCZESTNIKÓW

200+ PARTNERÓW KONFERENCJI I SZKOLEŃ

www.aleBank.pl/konferencje

Centrum Prawa Bankowego i Informacji
www.cpb.pl

Związek Banków Polskich

Od Robotic Process Automation do hiperautomatyzacji

WARSZAWA, 2021

OD ROBOTIC PROCESS AUTOMATION DO HIPERAUTOMATYZACJI

Raport przygotowany przez
Związek Banków Polskich
oraz Centrum Prawa Bankowego i Informacji

ZWIĄZEK BANKÓW POLSKICH

Centrum Prawa Bankowego i Informacji
www.cpb.pl

Warszawa, wrzesień 2021
Wydawnictwo Centrum Prawa Bankowego i Informacji

Hiperautomatyzacja to nie futurologia

Wciąż trwa pandemia. W międzyczasie astronauci amatorzy odbyli pierwszą cywilną misję na orbitę okołoziemską. W centrum handlowym na warszawskich Młocinach robot przygotowuje kawę. Badania przeprowadzone przez Facebooka wykazały, że aplikacja Instagram jest szkodliwa dla milionów młodych użytkowników. Bankowe chatboty opowiadają dowcipy. W *„Bombie megabitowej"* Stanisław Lem napisał *„Każda bez wyjątku nowa technologia ma awers korzyści i zarazem rewers nowych, nieznanych dotychczas bied"*. Czy ponad dwadzieścia lat od publikacji tych słów nie są one bardziej aktualne niż kiedykolwiek?

Fot. ZBP

Joanna Barbrich
ZWIĄZEK BANKÓW POLSKICH

Dla nikogo z nas nie jest żadnym odkryciem fakt, że razem możemy więcej, dalej, szybciej. Ten model organizacji pracy albo inaczej procesu, bo tak brzmi to bardziej biznesowo, pozostaje powszechnie stosowany w otaczającym nas świecie. Ostatnie lata przyniosły bardzo dynamiczny rozwój robotyzacji. To, co jeszcze niedawno pozostawało w obszarze zainteresowania futurologów, staje się faktem każdego dnia. Przestawało i przestaje też dziwić nas zwykłych użytkowników. Choć na początku tego procesu podchodziliśmy do niego z pewną taką nieufnością, to z każdym dniem było coraz łatwiej. Robot budował dla nas samochody, płytki procesorowe, montował telefony, zaczął obsługiwać nas w banku czy urzędzie – stał się zwykłym elementem naszej codzienności.

Ale człowiek chciał pójść nieco dalej, wiedząc, że razem możemy więcej i więcej. Programował, asystował, wyznaczał nowe zadania, które maszyny cierpliwie wykonywały. W każdym obszarze, gdy praca stawała się żmudna, nudna, powtarzalna, zaczynał zastępować nas robot. Po pewnym czasie odkryliśmy, że w prostych procesach możemy łączyć pracę chatbotów, voicebotów, platform oraz narzędzi niskokodowych i bezkodowych. Ale brakowało czegoś jeszcze – brakowało inteligencji, abstrakcyjnego myślenia. Gdy człowiek wzbogacił pracę robotów o sztuczną inteligencję z elementami uczenia maszynowego, stworzył hiperautomatyzację – nowe, wspaniałe narzędzie, które dziś i w niedalekiej przyszłości posłuży nam do cyfrowej transformacji świata biznesu.

Jak więc zhiperautomatyzować bank? Odpowiedź na to pytanie znajdą Państwo w niniejszym raporcie. Pozwoli on nie tylko zrozumieć sens samego zagadnienia, ale także uniknąć możliwych błędów. Chociaż nie obiecujemy, że hiperautomatyzacja będzie remedium na wszystkie bolączki, z którymi mierzy się sektor bankowy, to wierzymy, że podrzucona moneta upadnie awersem do góry.

Dziękuję prof. **Andrzejowi Sobczakowi** i dr. **Tomaszowi Kulisiewiczowi**, że zgodzili się na przyjęcie zaproszenia do współpracy, a Państwu życzę pożytecznej lektury.

Robot to brzmi dumnie

Upowszechnienie robotów w gospodarce pozwala zredukować koszty prowadzenia biznesu nawet o 80%. To nie ustalenie z najnowszych raportów globalnych firm doradczych, tylko fragment powieści fantastycznonaukowej **Karela Čapka** „R.U.R", która ukazała się dokładnie sto lat temu. Genialny czeski prozaik, który w swym dziele wykreował znane dziś na całym świecie słowo *„robot"*, okazał się prawdziwym wizjonerem: oszczędności, generowane dzięki automatyzacji kolejnych dziedzin gospodarki co najmniej dorównują literackiej wizji sprzed stulecia, a nierzadko wręcz znacząco ją przewyższają.

Fot. W. Łączyński

Karol Mórawski
REDAKTOR PROWADZĄCY
„MIESIĘCZNIK FINANSOWY BANK"

Dziś udział robotów w wypracowywaniu globalnego PKB jest istotny i cały czas się zwiększa, a bez udziału cyfrowych asystentów trudno sobie wyobrazić funkcjonowanie jakże wielu sektorów gospodarki, w tym oczywiście branży finansowej. W dużej mierze odpowiada za to nasze, ludzkie lenistwo, które bywa tak jednym z siedmiu grzechów głównych, jak i siłą napędową wszelakich innowacji. Ułatwienia dla milionów konsumentów, jakie pojawiły się wraz z rewolucją cyfrową, przyczyniły się nie tylko do gruntownej zmiany kanałów dystrybucji usług bankowych, ubezpieczeniowych bądź inwestycyjnych, ale nade wszystko wykreowały całkiem nową mentalność klientów, której istotę najlepiej oddaje hasło *one click*. To zaś skłania banki nie tylko do udostępniania kolejnych, coraz bardziej zaawansowanych produktów i usług online, ale też do tworzenia coraz bardziej intuicyjnych interfejsów, których użytkownik może liczyć na wszechstronne wsparcie ze strony wszędobylskich botów.

Ich znaczenie rośnie nawet w kanałach tradycyjnych, do niedawna uważanych za ostoję dla *„czynnika ludzkiego"* – obecnie, kontaktując się z bankowym call center, nie mamy pewności, czy faktycznie rozmawiamy z człowiekiem, czy też miły doradca po drugiej stronie istnieje wyłącznie jako zaawansowany algorytm, zapisany na bankowym serwerze lub coraz częściej w chmurze obliczeniowej.

Automaty nie tylko czynią usługi bankowe łatwiej dostępnymi i prostszymi, ale zwiększają też wydatnie ich bezpieczeństwo. To dzięki sztucznej inteligencji, uczeniu maszynowemu i zaawansowanym rozwiązaniom z zakresu biometrii behawioralnej traci znaczenie odwieczny konflikt pomiędzy wygodą a bezpieczeństwem użytkowania, a świat, w którym dokonujące się bez naszego zaangażowania mikropłatności nie stanowią otwartej furtki dla cyberoszustów, materializuje się na naszych oczach. Robotyzacja i AI są też jedynym sposobem, by we współczesnym świecie uczynić zadość rosnącym wymogom regulacyjnym. Samo wszak monitorowanie tysięcy procesów dokonujących się w cyberprzestrzeni stanowi zadanie ponad siły choćby i najwyśmienitszych audytorów, a co dopiero mówić o implementacji nowych przepisów prawa i zaleceń nadzoru finansowego...

Za sprawą innowacyjnych rozwiązań proces robotyzacji gospodarki wchodzi w kolejną fazę, zwaną hiperautomatyzacją. Jej podstawą jest zastępowanie człowieka w realizacji działań biznesowych tam, gdzie tylko to możliwe przez rozwiązania IT, począwszy od czatbotów, a skończywszy na skomplikowanej obsłudze procesów back office. Pojęcie hiperautomatyzacji, choć pojawiło się zaledwie dwa lata temu, zdążyło już awansować do rangi jednego z głównych trendów we współczesnej gospodarce, obejmując praktycznie wszelkie obszary bankowej działalności, tak w zakresie front, jak i back office.

Wbrew pesymistycznym wizjom, roztaczanym niekiedy w mediach społecznościowych, sam proces hiperautomatyzacji nie jest nakierowany na redukcję załogi, wręcz przeciwnie, w wielu przypadkach osoby, wykonujące dotąd żmudne i powtarzalne czynności, zyskują niepowtarzalną szansę rozwoju kariery, wykonując zadania wymagające kreatywności, inteligencji i empatii. W tym kontekście wizja Karela Čapka, który w kolejnych rozdziałach swej powieści opisał narastający bunt maszyn, aż do przejęcia przez nie władzy nad światem, z pewnością nam nie grozi, całkiem realnym wyzwaniem są natomiast konsekwencje niewłaściwie przeprowadzonego procesu robotyzacji – nie tyle wyparcie ludzi przez ich cyfrowych następców, ile nieskuteczne funkcjonowanie całego biznesu. To zaś jest prosta droga do postępowania restrukturyzacyjnego, o ile nie upadłości likwidacyjnej, po której, jak to mawiał swego czasu pewien ekscentryczny kandydat na prezydenta RP, *„nie będzie niczego"* – ani ludzi, ani robotów...

Jakie zagrożenia pojawiają się na drodze hiperautomatyzacji instytucji finansowych? Czego powinniśmy wystrzegać się, by proces ten był oparty na silnych podstawach i zapewnił długofalowy rozwój organizacji, a nie jedynie spektakularny efekt marketingowy? Jakie kryteria natury etycznej należy uwzględniać w toku automatyzacji, jak i planując cały proces, by cyfrowe procedury back office nie stały się okazją do obchodzenia prawa, a czatboty nie uprawiały missellingu? Odpowiedzi na te, i wiele innych pytań znajdą Państwo w niniejszym opracowaniu. •

Spis treści

O autorach

Fot. Arch. prywatne

Dr Tomasz Kulisiewicz
– analityk rynku komunikacji elektronicznej, wykładowca. Ekspert Ośrodka Studiów nad Cyfrowym Państwem, autor i współautor publikacji i raportów analitycznych na temat gospodarczych i społecznych aspektów technologii informacyjnych ze szczególnym uwzględnieniem usług e-administracji. Sekretarz Sektorowej Rady ds. Kompetencji – Informatyka przy Polskim Towarzystwie Informatycznym.

Fot. Arch. prywatne

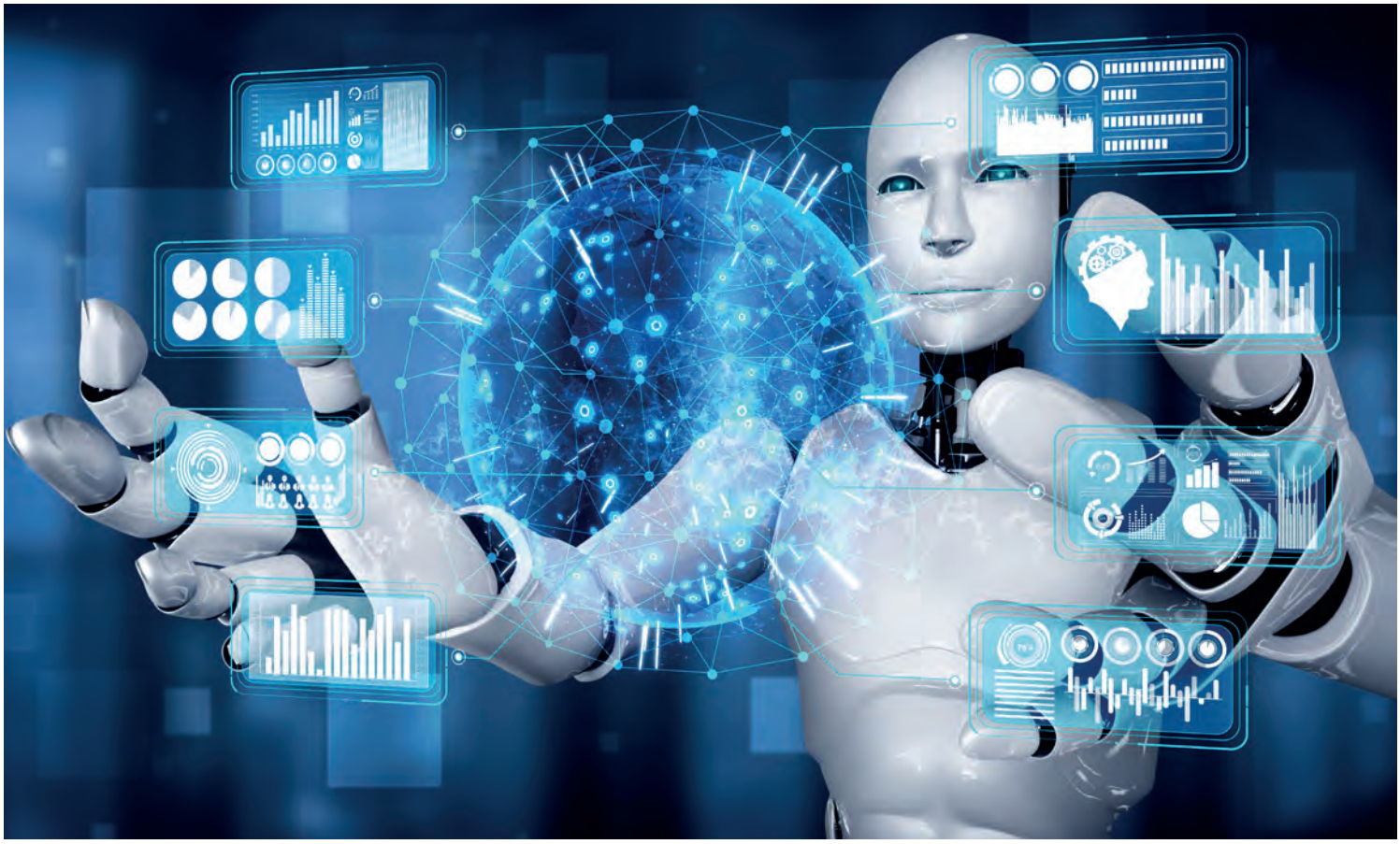
Prof. dr hab. Andrzej Sobczak
– kierownik Zakładu Zarządzania Informatyką w Szkole Głównej Handlowej w Warszawie. Twórca Liderzy.AI – polskiej społeczności skupionej wokół problematyki hiperautomatyzacji. Redaktor serwisu Robonomika.pl. Od kilku lat zajmuje się zarządzaniem strategicznym IT, ładem danych (Data Governance) i architekturą korporacyjną (Enterprise Architecture). Obecnie swoje zainteresowania koncentruje wokół hiperautomatyzacji – zaawansowanej automatyzacji, w tym robotyzacji procesów biznesowych.
Uczestniczył w projektach doradczych i prowadził szkolenia m.in. dla: BNP Paribas Banku Polska, Getin Noble Bank, ING Banku Śląskiego, Banku Gospodarstwa Krajowego, Nationale Nederlanden, PZU, Europejskiego Funduszu Leasingowego. Prace na rzecz popularyzacji robotyzacji procesów biznesowych zostały docenione przez otoczenie zewnętrzne. W 2019 r. od Związku Banków Polskich otrzymał Nagrodę im. prof. R. Kaszubskiego, zaś w 2020 r. nagrodę 12. Forum Gospodarczego TIME w kategorii ambasador ICT w obszarze nauki i edukacji.

1. Wstęp

Niniejsze opracowanie ma na celu przedstawienie kluczowych idei związanych z wdrażaniem rozwiązań hiperautomatyzacji w sektorze bankowym. Na początku definiujemy, czym jest, a czym nie jest hiperautomatyzacja, przedstawiając także krótko „antywzorce" działań, które w zamierzeniach mają pomóc wdrażać hiperautomatyzację, ale w praktyce generują duże problemy, a czasami wręcz podważają sens podejmowanych inicjatyw. W kolejnym punkcie opracowania prezentujemy główne składowe oraz metody hiperautomatyzacji, a także obszary, w których jest ona stosowana w bankach. W punkcie tym proponujemy też prostą klasyfikację poziomów zaawansowania wdrażania hiperautomatyzacji. Punkt piąty zawiera przykłady wdrożeń rozwiązań hiperautomatyzacji w działających w Polsce instytucjach finansowych. Punkt szósty poświęcony jest zapowiadanym regulacjom oraz podnoszonym coraz częściej aspektom etycznym implementacji hiperautomatyzacji w sektorze bankowym. Opracowanie kończy punkt prezentujący aktualne trendy hiperautomatyzacji w bankowości oraz potencjalne kierunki jej rozwoju i wpływu na przyszłość banków jako kluczowych instytucji sektora finansowego.

W pracy omawiamy także wyniki autorskich badań nad wybranymi aspektami wdrażania hiperautomatyzacji w krajowym sektorze finansowym. Jednak z uwagi na to, że badania te nie były prowadzone oddzielnie dla banków i oddzielnie dla innych organizacji sektora finansowego (np. firmy ubezpieczeniowe), w niektórych częściach materiału odwołujemy się do nich łącznie.

2. Czym jest, a czym nie jest hiperautomatyzacja



2.1. Definicja – czym jest hiperautomatyzacja

Lata 2018–2019 to na świecie okres boomu na robotyzację procesów biznesowych – realizowaną przede wszystkim z wykorzystaniem narzędzi RPA (*Robotic Process Automation*), w mniejszym stopniu – narzędzi RDA (*Robotic Desktop Automation*).

Termin „hiperautomatyzacja" pojawił się po raz pierwszy w październiku 2019 r. – od razu na czele listy „Top 10 Strategicznych trendów technologicznych na rok 2020" firmy doradczej Gartner, jako koncepcja wpisująca się w rozwój robotyzacji procesów. Podchwyciły go inne znane firmy analityczne i dostawcy technologiczni, używając też określeń „cyfrowa automatyzacja procesów" czy „inteligentna automatyzacja procesów". W tym ujęciu narzędzia RPA/RDA są zarówno prekursorem, jak i składową hiperautomatyzacji.

Ogólnie przez hiperautomatyzację rozumiane jest wykorzystywanie połączonych ze sobą zaawansowanych narzędzi informatycznych – takich jak rozwiązania do robotyzacji procesów biznesowych (RPA/RDA), chatbotów /voicebotów, platform oraz narzędzi niskokodowych i bezkodowych (*Low-Code/No-Code*) – wzbogaconych wszędzie tam, gdzie jest to zasadne – o elementy sztucznej inteligencji (w tym w szczególności uczenia maszynowego) zastosowane do zautomatyzowanego wykonywania zadań realizowanych wcześniej przez człowieka. Hiperautomatyzacja postrzegana jest jako istotne narzędzie cyfrowej transformacji instytucji publicznych oraz organizacji komercyjnych.

Na podstawie doświadczeń z wdrożeń projektów hiperautomatyzacyjnych można stwierdzić, że hiperautomatyzacja umożliwia uwolnienie pracowników od czynności uciążliwie monotonnych i pracochłonnych, pozwalając się im skoncentrować na działaniach o wyższej złożoności i wartości, co może się przełożyć na obniżenie kosztów działania, redukcję stopy błędów oraz podwyższenie wydajności całej organizacji (firmy), a także na podnoszenie poziomu produktów i usług dostarczanych klientom/użytkownikom (podwyższanie satysfakcji klientów). Podwyższanie poziomu satysfakcji klientów ma oczywiście przełożenie na rentowność banków, m.in. poprzez zwiększanie lojalności klientów i obniżenie współczynnika odejść (*churn*). Natomiast postrzeganie banków jako instytucji zaufania publicznego i podwyższanie poziomu zaufania społecznego pozytywnie wpływa na sprawność ich działania.

Należy podkreślić, że poziom automatyzacji działań możliwy do osiągnięcia dzięki hiperautomatyzacji jest dużo wyższy niż poziom automatyzacji osiągany przy oddzielnym użyciu poszczególnych narzędzi – w szczególności tylko z robotyzacji procesów biznesowych realizowanej za pomocą narzędzi RPA/RDA. Powoduje to, że wdrożenie hiperautomatyzacji może być także wykorzystywane do doskonalenia lub zmiany składowych modelu biznesowego organizacji – w tym również banku – np. poprzez wprowadzenie kategorii produktów lub stworzenie usług dla nowego segmentu klientów, które przy tradycyjnych metodach automatyzacji byłyby nieopłacalne lub bardzo trudne do wdrożenia, zajmując przy tym wiele czasu.

W dodatku wiele elementów składowych hiperautomatyzacji realizowanych jest nie przez działy IT (jak to ma miejsce w przypadku „twardej automatyzacji"), ale przez działy biznesowe, albo przez dedykowane CoE (*Center*

ANTYWZORCE HIPERAUTOMATYZACJI

Odkrywanie koła na nowo – nieuwzględnianie faktu, że rozwiązania z zakresu hiperautomatyzacji (w szczególności roboty programowe, chatboty, voiceboty) należy traktować jak oprogramowanie, począwszy od etapu analizy potrzeb przez ich budowę oraz utrzymywanie. Prowadzi to do straty czasu i energii na ponowne odkrywania znanych od lat i stosowanych z powodzeniem metodyk, technik i dobrych praktyk zarządzania budową i utrzymaniem oprogramowania;

Słomiany zapał – wynikający z braku ciągłego i rzeczywistego wsparcia procesu hiperautomatyzacji przez zarząd banku (procesu często dłuższego i bardziej złożonego, niż się to pierwotnie wydawało). Skutkiem może być porzucenie przedsięwzięcia przy wystąpieniu pierwszych trudności lub istotne ograniczenie jego zakresu, co powoduje utratę korzyści z łączenia różnych narzędzi automatyzacji;

Zosia-Samosia – działy biznesowe zaczynają stosować narzędzia hiperautomatyzacji (np. do budowy robotów lub wdrażania chatbotów) bez konsultacji z działami IT, co zwykle skutkuje problemami ze skalowalnością i utrzymywaniem rozwiązań, zarządzaniem zmianą oraz bezpieczeństwem; innym podtypem tego antywzorca jest jak najpóźniejsze informowanie działu IT o realizowanych działaniach. Niestety odbija się to na jakości wdrożenia, a i później relacje z działem IT bywają trudne;

Tanio zaczniemy, a potem się zobaczy – koncentracja wyłącznie na jak najszybszym budowaniu jak najtańszych rozwiązań. Najczęstszym skutkiem negatywnym jest niedoszacowanie kosztów utrzymania takich rozwiązań;

Chęci ponad potrzeby – przeszacowanie potencjału (obszarów) do wdrażania poszczególnych kategorii narzędzi hiperautomatyzacji; np. w trakcie przedsięwzięcia okazuje się, że znacznej części procesów nie opłaca się robotyzować z wykorzystaniem narzędzi klasy RPA, a te, które by się opłacało, zostały już wcześniej zautomatyzowane innymi środkami. Innym przykładem może być przeszacowanie potencjału wykorzystania narzędzi do eksploracji procesów (*process mining*) – okazuje się, że stopień złożoności i wielkość procesów nie znajduje uzasadnienia dla zastosowania takich narzędzi;

Tylko roboty – pod wpływem pierwszych, stosunkowo szybkich i spektakularnych efektów kierownictwo chce stosować roboty we wszelkich możliwych miejscach, bez rozważenia innych podejść do automatyzacji procesów (co jest immanentną częścią wrażania hiperautomatyzacji). Skutkiem są zwykle problemy techniczne i efektywnościowe wynikające z wdrożenia robotyzacji w miejscach, w których nigdy nie powinno się używać takich rozwiązań;

Hiperautomatyzacja = technologia – traktowanie budowy rozwiązań hiperautomatyzacji jako projektu stricte technicznego, a nie organizacyjnego i czasami wręcz kulturowego, co skutkuje problemami z obsługą sytuacji nadzwyczajnych, problemami komunikacyjnymi oraz problemami z priorytetyzacją działań;

Ciemność widzę – brak jakiejkolwiek dokumentacji tworzonych rozwiązań hiperautomatyzacji (zarówno robotów, jak i aplikacji budowanych z wykorzystaniem mechanizmów Low-Code/No-Code), bo założono, że wystarczy sam kod rozwiązania. Skutkiem są problemy z przekazaniem rozwiązań do utrzymania oraz z ich zmianami i utrzymaniem (zwłaszcza, jeśli zmieni się zespół, który je tworzył);

Zapomniany skarb – wdrażający automatyzację koncentrują się na działaniach, nie zwracając uwagi na dane, a w szczególności na jakość tych, które są przetwarzane w ramach podjętych działań. Powoduje to błędy w działaniu narzędzi, a także niepełne wykorzystanie potencjału procesów, które można by automatyzować – dotyczy to zwłaszcza automatyzacji kognitywnej, która musi mieć dostęp do wysokiej jakości danych;

Automatyzacja bałaganu – automatyzacja procesu, który nie był do tego przygotowany (nie został wcześniej wystandaryzowany ani zoptymalizowany). Z tego powodu rozwiązanie zastosowane w danym procesie jest mniej wydajne, a w dodatku niepotrzebnie złożone i trudne do ewentualnej modyfikacji;

Do odważnych świat należy – wprowadzanie zmian w oprogramowaniu automatyzacyjnym w środowisku produkcyjnym, bez wcześniejszego przetestowania w dedykowanym środowisku testowym. Skutkiem może być zakłócenie ciągłości realizacji procesów biznesowych oraz konieczność pracochłonnego i kosztownego „odkręcania" błędów popełnionych przez niedokładnie przetestowane rozwiązania;

Automatyzacja = samoobsługa – ignorowanie organizacyjnych aspektów utrzymania oprogramowania automatyzacyjnego, co powoduje przede wszystkim brak szybkiej reakcji w przypadku nieoczekiwanych przerw w działaniu zautomatyzowanych procesów, trudno jest także osiągnąć przyjęte wskaźniki wydajności (KPI – *Key Performance Indicators*);

Wiara w inteligencję rozwiązań – oczekiwanie, że tworzone rozwiązania okażą się ponadprzeciętnie inteligentne i można pomijać okresowe weryfikacje wyników ich pracy. Może to powodować duże straty wynikające z późno zauważonego nieprawidłowego działania zastosowanych rozwiązań automatyzacyjnych;

Na husarza – brak standardów tworzenia rozwiązań hiperautomatyzacji, w szczególności kodu oprogramowania. Powoduje to problemy ze zmianami i utrzymaniem, zwłaszcza gdy zmieni się zespół, który je tworzył. Zespoły developerów zajmujące się różnymi elementami automatyzacji nie mogą się wzajemnie zastępować;

Ruchy Browna – rozpoczęcie przedsięwzięcia bez przemyślanej strategii i wizji docelowej, zamiast niej hiperautomatyzacja prowadzona jest w postaci chaotycznych, przypadkowych i niepowiązanych ze sobą działań, wynikających z próby realizacji kolejnych zamówień spływających z działów biznesowych. Skutkiem są zwykle problemy ze skalowalnością, z priorytetyzacją obszarów wybieranych do hiperautomatyzacji, a także wysokie koszty utrzymania rozwiązań stworzonych bez przemyślanego, całościowego podejścia;

Archipelagi automatyzacji – realizacja oderwanych od siebie (organizacyjnie i technologicznie) inicjatyw automatyzacyjnych (BPMS, RPA, RDA, chatbotów, voicebotów...), co powoduje trudności ze zbudowaniem całościowego i efektywnego podejścia do robotyzacji, a dodatkowo wiąże się z dublowanie się inicjatyw i prac. Należy podkreślić, że takie „wyspowe" działania są sprzeczne z istotą hiperautomatyzacji, polegającej na zastosowaniu powiązanych ze sobą zaawansowanych technologii cyfrowych.

of Excellence) – ulokowane często w działach operacji biznesowych lub w strukturze macierzowej – pomiędzy działami IT i biznesowymi.

2.2. Czym nie jest hiperautomatyzacja

Hiperautomatyzacja nie jest metodą czy środkiem do pozbywania się ludzi z wdrażających ją instytucji i firm. Nie jest też kamieniem filozoficznym, dzięki któremu rozwiązane zostaną wszelkie problemy niedoboru pracowników o odpowiednich kompetencjach, zwłaszcza specjalistycznych i społecznych. Hiperautomatyzacja nie jest też metodą radykalnej i szybkiej obniżki kosztów działania, ani równie radykalnego i szybkiego zwiększenia przychodów wdrażających ją banków. Wynika to m.in. z faktu, że świadome wdrożenie hiperautomatyzacji (lub co najmniej jej kilku składowych) jest dużo bardziej złożone od samej robotyzacji procesów.

W zasobach polskiej społeczności hiperautomatyzacji (dostępnych pod adresem https://www.liderzy.ai/) tworzony jest katalog antywzorców hiperautomatyzacji. Pierwotnie został on opracowany na poziomie ogólnym – dla wszystkich organizacji komercyjnych – ale jego główne spostrzeżenia i zalecenia mogą pomóc uniknąć ewentualnych błędów w projektach hiperautomatyzacji realizowanych w bankach; błędów, które mogłyby wynikać z nieprawidłowego definiowania hiperautomatyzacji w projekcie lub nierealistycznych oczekiwań dotyczących efektów.

3. Dlaczego banki wdrażają hiperautomatyzację i czego od niej oczekują

Mimo szerokiego zakresu regulacji sektora finansowego rynek finansowy jest rynkiem o bardzo wysokim stopniu konkurencyjności. Wymusza to od działających na nim graczy osiąganie coraz wyższej wydajności i sprawności obsługi przy jednoczesnej ścisłej kontroli kosztów. Stopień konkurencyjności rynku bankowego wyraźnie wzrósł od końca lat 90. XX w., kiedy obok tradycyjnych banków, nierzadko mających za sobą stulecia tradycji, w których narzędzia informatyczne służyły początkowo tylko do obsługi procesów wewnętrznych oraz wsparcia transakcji, pojawiły się na nim banki „internetowe". One to cały model biznesowy zbudowały na stosowaniu rozwiązań informatycznych do obsługi klientów w trybie samoobsługowym, wykorzystujący do tego najpierw serwisy webowe, a wraz z upowszechnieniem się smartfonów – aplikacje mobilne. Oczywiście banki tradycyjne musiały zareagować na to wyzwanie i udostępnić klientom takie rozwiązania. W Polsce dynamiczny rozwój bankowości internetowej rozpoczął się w 2001 r. wraz z pojawieniem się dwóch banków „całkowicie internetowych" – mBanku i Inteligo[1].

Wyzwaniom konkurencyjności w sektorze towarzyszy w ostatnich dekadach silny wzrost złożoności coraz silniej egzekwowanych regulacji. Zarówno pod względem stopnia konkurencyjności, jak i zakresu regulacji bankowość przypomina rynek operatorów komunikacji elektronicznej, zwłaszcza w mocno regulowanym obszarze dostępu do sieci.

Rosnąca złożoność wewnętrznych procesów, a także konieczność poszerzania portfolio usług i podwyższania ich jakości i niezawodności, zwłaszcza dla klientów korporacyjnych, wymaga coraz wyższego poziomu kompetencji pracowników banków, w tym dotyczących tworzenia, konfigurowania, utrzymywania i rozwijania rozwiązań informatycznych. Jest to duże wyzwanie wobec deficytu specjalistów IT w Polsce, Europie i na całym świecie.

W ciągu kilku minionych lat na rynku usług finansowych pojawiły się specyficzne przedsiębiorstwa – fintechy. Są to firmy, które początkowo oferowały tylko niektóre usługi finansowe, np. płatności błyskawiczne, płatności w określonych obszarach (np. bilety, opłaty parkingowe) lub usługi crowdfundingowe, realizując je na bazie specjalizowanych rozwiązań informatycznych, w zasadzie zupełnie zautomatyzowanych. Firmy te są przeważnie niewielkie (niskie koszty nielicznego personelu), a wobec szybko rosnącej dostępności i jakości usług chmurowych nie muszą nawet mieć rozbudowanej infrastruktury sprzętowej i systemowej. Ich pozycja w odniesieniu do banków jest przykładem zjawiska „coopetition" – w określonych obszarach fintechy konkurują z bankami, a jednocześnie muszą korzystać z ich usług i coraz częściej z nimi współpracują[2]. Niektóre z fintechów rozszerzyły ostatnio zakres oferowanych usług tak bardzo, że zdecydowały się bezpośrednio konkurować z bankami „tradycyjnymi" i w tym celu uzyskały licencje bankowe.

Można więc twierdzić, że sektor bankowy zaczął stosować rozwiązania automatyzacji i robotyzacji procesów (a następnie łączyć je w całościowych projektach hiperautomatyzacji) z jednej strony po to, by uporać się z problema-

1 W listopadzie 1998 r. uruchomiony został internetowy dostęp do kont w łódzkim Powszechnym Banku Gospodarczym, ale po przejęciu PBG przez Bank Pekao SA rozwój tego rozwiązania uległ spowolnieniu. Równolegle z mBankiem i Inteligo serwis internetowy uruchomił też Volkswagen Bank Polska, który był niemal całkowicie „bankiem internetowym", mając w kraju tylko jeden oddział fizyczny.

2 Istotnym elementem takiej współpracy są interfejsy otwartej bankowości udostępniane przez banki do współpracy z dostawcami usług finansowych, np. Standard PolishAPI, opracowany pod auspicjami Związku Banków Polskich (https://polishapi.org).

mi złożoności, jakości i szybkości obsługi oraz zgodności z regulacjami (*compliance*), a z drugiej – by utrzymać poziom swojej konkurencyjności rynkowej w warunkach rosnącej presji ze strony fintechów[3].

Oczekiwane korzyści z wdrożenia rozwiązań hiperautomatyzacji w bankowości są zbliżone do takich oczekiwań w innych organizacjach, jednak w stosunku do firm i instytucji „generycznych" sektor bankowy jest silnie regulowany zarówno przez regulatorów instytucjonalnych (państwowe nadzory bankowe/finansowe), jak i przez wypracowane wewnętrznie reguły compliance. Rezultatem są (a przynajmniej – powinny być) precyzyjne definicje procesów biznesowych, które ułatwiają wdrażanie automatyzacji i robotyzacji, a także osiąganie planowanych korzyści.

W warunkach bardzo nowoczesnego polskiego sektora bankowego trochę mniejsze znaczenie ma korzyść wymieniana np. w opracowaniach dotyczących bankowości USA – możliwości otwarcia konta nawet w ciągu kilku minut zamiast kilku czy kilkunastu dni. Korzyść ta została już w zasadzie „skonsumowana" przez wiodące banki działające w Polsce. Trochę dłużej trwają jeszcze nadal procedury zamykania konta osobistego, ale i w tym obszarze wykorzystywane są w coraz większym zakresie rozwiązania automatyzacji i robotyzacji.

Można w tym miejscu przytoczyć powiedzenie **Johana Torgeby'ego**, prezesa zarządu szwedzkiego banku SEB (Skandinaviska Enskilda Banken), który w jednym z wywiadów udzielonych w 2018 r. stwierdził, iż w sektorze finansowym: „whatever can be automated will be automated". Oznacza to głęboką zmianę w sposobach działania instytucji finansowych – zarówno po stronie back office, jak i front office[4]. Wydaje się, że słowa te stają się coraz bardziej prorocze – chociażby w kontekście banku, którego oddział zawitał właśnie do Polski – czyli Aion Banku.

3 Według opublikowanej w czerwcu 2021 r. kolejnej edycji „Mapy polskiego fintechu 2021" w bieżącym roku działały w kraju 273 fintechy i projekty fintechowe, a oprócz nich tego typu usługi oferowało w Polsce 39 fintechów zagranicznych (https://www.cashless.pl/10141-mapa-polskiego-fintechu-2021-raport).

4 https://robonomika.pl/zapraszam-na-moje-wystapienie-podczas-konferencji-sztuczna-inteligencja-i-robotyzacja-w-sektorze

OCZEKIWANE KORZYŚCI Z HIPERAUTOMATYZACJI

- Redukcja kosztów – szacowana nawet na 40–80% w porównaniu do kosztów pracy ludzkiej na robotyzowanych stanowiskach (pamiętając jednak o zastrzeżeniach wspomnianych w p. 2.2);
- Krótki czas i łatwość wdrożenia rozwiązań – ocenia się, że dobrze przygotowane wdrożenie automatyzacji poszczególnych procesów powinno się zakończyć w czasie 8 do 12 tygodni. Dodatkową korzyścią może być takie opracowanie rozwiązania (np. robota programowego), które umożliwia jego szybką parametryzację w celu zastosowania w innym procesie. Oczywiście zależne jest to od obszarów i procesów, w których wdrażane są rozwiązania;
- Praca „cyfrowych pracowników" w trybie 24/7, bez problemów z koniecznością dostosowywania harmonogramów zmianowości czy wolnych dni do możliwości pracowników – choć należy pamiętać, że nie jest to tryb 24/7/365, bo jednak wymagane są przerwy technologiczne dające czas na wprowadzanie poprawek, modernizację oprogramowania itp.;
- Wyższa prędkość i wydajność wykonywania rutynowych zadań przez cyfrowych pracowników w porównaniu z prędkością i wydajnością ludzi;
- Niższa stopa błędów – zwłaszcza tych, które w przypadku ludzi wynikają ze zmęczenia lub nieuwagi przy wykonywaniu działań żmudnych i wielokrotnie powtarzanych;
- Skalowalność rozwiązań – pod warunkiem, że zostały prawidłowo zaprojektowane i wykonane;
- Uzyskiwanie w trakcie realizacji zrobotyzowanych procesów informacji przydatnych do ich optymalizacji;
- Możliwość zautomatyzowanej kontroli w czasie rzeczywistym przestrzegania zarówno wymagań regulacyjnych, jak i wewnętrznych reguł compliance w banku oraz automatycznego zbierania danych wymaganych przez nadzór finansowy oraz przez własne reguły;
- Podniesienie poziomu nie tylko satysfakcji klientów (*Customer Experience*), ale także pracowników (*Employee Experience*) – dzięki uwalnianiu ich od działań pracochłonnych, monotonnych, o niskiej wartości dodanej.

4. Elementy i narzędzia hiperautomatyzacji, jej metody i obszary zastosowań

Choć pojęcia hiperautomatyzacji i „klasycznej automatyzacji" wydają się niemal tożsame, to jednak należy wprowadzić rozróżnienie. Klasyczna automatyzacja realizowana jest za pomocą m.in.:

- aplikacji dziedzinowych (obsługujących większość procesów biznesowych),
- szyn integracyjnych (duże banki często posiadają dwie szyny),
- „ciężkich" platform i systemów do zarządzania procesami (BPMS – *Business Process Management Systems*).

Projekty z obszaru „klasycznej automatyzacji" (realizowanej w bankach praktycznie „od zawsze") prowadzone są przez działy IT, mają duże budżety, a czas ich realizacji wynosi wiele miesięcy, a nawet lat.

Natomiast w ślad za definicją przytoczoną w punkcie 2, należy podkreślić, że elementami i narzędziami hiperautomatyzacji polegającej na wykorzystywaniu połączonych ze sobą zaawansowanych technologii cyfrowych są przede wszystkim narzędzia robotyzacji procesów, które w sposób kompleksowy łączone są innymi rozwiązaniami automatyzacji procesów biznesowych.

4.1. Elementy i narzędzia hiperautomatyzacji

W przypadku hiperautomatyzacji wyróżniamy następujące rozwiązania:

- narzędzia do zrobotyzowanej automatyzacji procesów (RPA – *Robotic Process Automation*),
- narzędzia do zrobotyzowanej automatyzacji stanowiska pracy (RDA – *Robotic Desktop Automation*),
- narzędzia do kognitywnej/inteligentnej automatyzacji procesów (CPA/IPA – *Cognitive/Intelligent Process Automation*),
- chatboty/voiceboty,
- platformy/narzędzia niskokodowe i bezkodowe (*Low-Code/No-Code*),
- narzędzia do zarządzania interfejsami programowymi (*API Management*),
- narzędzia do eksploracji procesów (*process mining*) i eksploracji działań i zachowań użytkowników (*task mining*).

Narzędzia RPA/RDA/CPA-IPA oraz chatboty/voiceboty pozwalają na tworzenie „cyfrowych pracowników" (często określanych też mianem „cyfrowej siły roboczej"). Celem ich zastosowania jest automatyzacja działań wykonywanych do tej pory przez człowieka-operatora.

W zależności od stopnia zaawansowania cyfrowych pracowników można ich podzielić na (patrz tabela 1):

- roboty budowane z wykorzystaniem narzędzi RPA,
- roboty budowane z wykorzystaniem narzędzi RDA,
- roboty budowane z wykorzystaniem narzędzi C-RPA/I-RPA.

Z punktu widzenia trybu pracy roboty programowe dzielimy na:

- roboty nadzorowane (pracujące w trybie nadzorowanym, nazywane *software assistant*) – bezpośrednio współpracujące z człowiekiem-operatorem na jego stanowisku pracy. Roboty takie uruchamiane są i zatrzymywane przez operatora, obsługują proste czynności wykonywane dotąd przez niego – może on nadzorować pracę kilku takich robotów, pełniąc rolę koordynatora (orkiestratora) ich pracy,
- roboty nienadzorowane (pracujące w trybie nienadzorowanym, z dużym zakresem autonomii działania, nazywane *standalone robot*) – obsługujące realizację wielu działań składowych danego procesu biznesowego, często pełniące rolę integratora pomiędzy różnymi systemami, zwłaszcza systemami zastanymi (*legacy*). Uruchamiane są i działają na bazie wcześniej zdefiniowanych reguł biznesowych, pracownik pełni jedynie rolę nadzorcy i interweniuje w sytuacjach nadzwyczajnych. Zazwyczaj pracują na wydzielonym komputerze czy serwerze wirtualnym.

Chatboty i voiceboty pozwalają na komunikację z klientami lub pracownikami banku z wykorzystaniem języka naturalnego lub w sposób dobrze naśladujący język naturalny.

Chatboty to programy automatyzujące komunikację tekstową w języku naturalnym, wykorzystujące w tym celu interfejs tekstowy – własny albo interfejsy tekstowe popularnych komunikatorów. Mogą też działać jako chatboty webowe, niezależne od komunikatorów i podpięte do stron WWW. W nowszych generacjach chatbotów tekst wejściowy jest analizowany semantycznie przy użyciu metod AI, następnie wybierana lub tworzona jest odpowiedź wysyłana do interfejsu tekstowego.

Tabela 1. Klasyfikacja narzędzi do robotyzacji procesów i obszary ich zastosowań

Klasa narzędzia do robotyzacji	Procesy automatyzowane	Obszar zastosowań w banku	Zasady działania
RPA – Robotic Process Automation	procesy o charakterze powtarzalnym, masowym, których realizacja jest czasochłonna, czynności często związane z systemami legacy	procesy o charakterze wspierającym i operacyjnym, przeważnie niemające bezpośredniego styku z klientami	zwykle działają na dedykowanych maszynach (fizycznych lub wirtualnych) i są stosunkowo skomplikowane w budowie
RDA – Robotic Desktop Automation	automatyzują zwykle nie całe procesy, lecz ich działania składowe, stosowane zwykle tam, gdzie pozyskiwane są dane z różnych (cyfrowych) źródeł, a operator większość czasu poświęcał na przesyłanie danych pomiędzy aplikacjami, ich weryfikację, wizualizację itp.	procesy realizowane na styku firmy z jej otoczeniem (np. klientami) lub procesy wspierające	współpracują z chatbotami/voicebotami
C-RPA/I-RPA – Cognitive/Intelligent Process Automation	procesy o charakterze złożonym, których realizacja jest czasochłonna, stosowane tam, gdzie możliwie szybko trzeba przetworzyć bardzo dużą ilość danych ustrukturalizowanych, a zwłaszcza nieustrukturalizowanych, i podjąć na tej podstawie decyzję	wszystkie rodzaje procesów realizowanych w banku ze szczególnym uwzględnieniem procesów strategicznych	wykorzystują zaawansowane metody i techniki AI i ML

Voiceboty to programy automatyzujące komunikację głosową w języku naturalnym, wykorzystujące w tym celu mechanizmy rozpoznawania i „rozumienia" wypowiedzi głosowej (mechanizmy NLU – *Natural Language Understanding*). Przetwarzają one komunikat głosowy na tekst, który poddawany jest analizie semantycznej z użyciem metod AI. Po wyborze/sformułowaniu odpowiedzi przez silnik bota uruchamiany jest mechanizm przetwarzania tekstu odpowiedzi na głos (*text-to-speech*).

Platformy i narzędzia niskokodowe lub bezkodowe (*Low-Code/No-Code*) to oprogramowanie redukujące konieczność tworzenia kodu programu (ręcznego kodowania) przez użytkowników budujących aplikacje. Umożliwiają one tworzenie aplikacji biznesowych bez znajomości języków programowania. Użytkownicy tych narzędzi tworzą rozwiązania, posługując się wizualnymi kreatorami oraz korzystając z predefiniowanych komponentów.

Istotą hiperautomatyzacji jest stosowanie współpracujących ze sobą różnorodnych mechanizmów automatyzujących, bardzo ważne jest zatem prawidłowe przekazywanie sobie nawzajem danych (wyników pracy) przez poszczególne rozwiązania. Często jest to realizowane przez wykorzystanie interfejsów programowych (API – *Application Programming Interface*), sformalizowanych opisów reguł komunikacji między programami. Ponieważ w systemach stosowanych w organizacjach – w szczególności w bankach – może być wiele różnych API tworzonych przez różnych dostawców oprogramowania, konieczne jest stosowanie narzędzi i systemów zarządzania API (*API Management*). Umożliwiają one nie tylko zarządzanie stosowanymi API i ich zabezpieczanie, ale także optymalizację stosowanych API dzięki zbieraniu danych dotyczących efektywności wymiany danych oraz tworzenie nowych API.

Stosowane w bankach narzędzia do analiz procesów biznesowych (*process mining*) służą do budowy modeli procesów, ich weryfikacji i rozbudowy na podstawie danych pochodzących z dzienników zdarzeń (logów) dostępnych w systemach informatycznych i odzwierciedlających rzeczywisty (niehipotetyczny) przebieg procesów biznesowych. W analizie tej wykorzystywane są też np. dane ze ścieżek wewnętrznej komunikacji pracowników. Dzięki analizie procesów można prowadzić:

- oceny efektywności realizacji procesów biznesowych,
- optymalizację procesów,
- weryfikację, czy procesy są realizowane zgodnie z wytycznymi/standardami/regulacjami –badania stopnia zgodności (*compliance*) realizacji procesów.

W analizie procesów wykorzystywane są zaawansowane mechanizmy eksploracji danych z wykorzystaniem metod AI.

Narzędzia do analizy działań użytkowników (*task mining*) pozwalają na obserwację i analizę sposobów działania użytkowników korzystających z systemów. Analiza działań i zachowań użytkowników (stosowana w narzędziach *task mining*) wykorzystuje m.in. mechanizmy rozpoznawania wzorców oraz przetwarzania języka naturalnego.

Można powiedzieć, że celem analizy procesów jest obserwacja całego procesu, realizowanego na wielu serwerach i stacjach roboczych. Natomiast w analizie działań (*task mining*) obserwowane są działania wykonywane przez użytkownika na pojedynczej stacji roboczej.

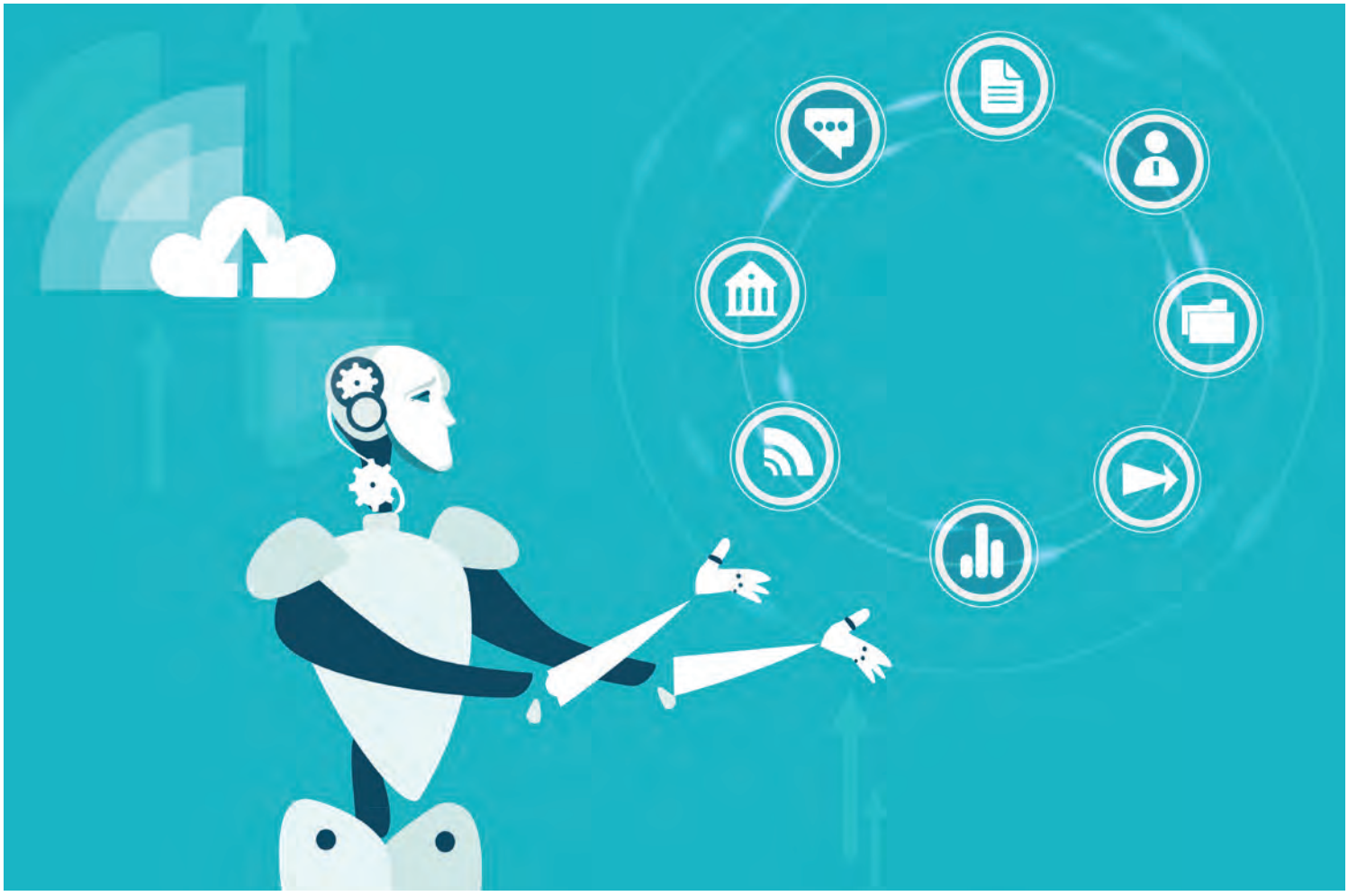
Narzędzia do analiz procesów biznesowych oraz działań użytkowników nie służą wprost do automatyzacji procesów, ale pozwalają zidentyfikować potencjał do tych prac – miejsca, w których automatyzacja ma sens.

4.2. Obszary podlegające hiperautomatyzacji w bankach

Podobnie jak w innych sektorach gospodarki, hiperautomatyzacja pojawia się w sektorze finansowym, w tym w bankach, właściwie we wszystkich obszarach ich działalności – zarówno w warstwie back office, jak i w kontaktach z klientami (front office). Jeśli trzeba byłoby określić obszar wdrożeń charakterystyczny dla banków, to jest nim back office, w szczególności podstawowe operacje biznesowe.

> ***Stosowane w bankach narzędzia do analiz procesów biznesowych (process mining) służą do budowy modeli procesów, ich weryfikacji i rozbudowy na podstawie danych pochodzących z dzienników zdarzeń (logów) dostępnych w systemach informatycznych i odzwierciedlających rzeczywisty (niehipotetyczny) przebieg procesów biznesowych.***

Regulacje nadzoru bankowego – krajowe i międzynarodowe – są coraz ściślejsze, wymagają od banków gromadzenia danych wymaganych przez regulatorów oraz wykazywania zgodności z regulacjami. Działania związane z compliance (zewnętrznym i wewnętrznym) stają się coraz bardziej złożone i pracochłonne,



coraz więcej czynności związanych z regulacjami trzeba wykonywać w czasie rzeczywistym lub niemal rzeczywistym. Dlatego coraz większą wagę w sektorze bankowym – zwłaszcza w miarę rozwoju kognitywnych technologii RPA – zyskuje tworzenie i wdrażanie rozwiązań automatyzujących działania wymagane przez regulacje, m.in. dotyczące bezpieczeństwa obrotu finansowego oraz wykrywania i zapobiegania fraudom oraz praniu pieniędzy. Pojawiły się już firmy nazywane RegTech, oferujące zautomatyzowane rozwiązania wspomagające zarówno regulatorów sektora finansowego, jak i podmioty podlegające regulacjom. Obszarem zastosowań oferowanych przez RegTech narzędzi RPA jest np. generowanie raportów z audytów.

Banki widzą w automatyzacji/robotyzacji działań wymaganych przez regulacje nie tylko możliwość oszczędności czasu i pracochłonności kontroli zgodności z wymaganiami, ale także zwiększenie pewności, że zgodność ta jest rzeczywiście uzyskiwana w zakresie satysfakcjonującym regulatorów. Z kolei regulatorzy – obok zmniejszenia pracochłonności audytów regulacyjnych – oczekują od automatyzacji/robotyzacji zwiększenia precyzji działań kontrolnych oraz pozyskiwania całościowego obrazu zgodności z regulacjami, a także uzyskania możliwości szybszego reagowania na ewentualne niezgodności czy zagrożenia stabilności sektora.

W bankowości dla masowych klientów indywidualnych i mikrofirm – nie wymagających (i raczej nie oczekujących) zindywidualizowanego podejścia i osobistych doradców – obszarem, w którym wcześnie rozpoczęto robotyzację była obsługa pytań i zgłoszeń klientów. Ponieważ większość pytań i zgłoszeń konsumentów i mikrofirm dotyczy zagadnień powtarzających się i typowych, zatem stosunkowo łatwo jest opracowywać i wdrażać zarówno boty (chatboty, voiceboty, videoboty) na „pierwszej linii kontaktu" z klientami, jak i roboty programowe do obsługi typowych przypadków zgłaszanych na infoliniach czy czatach. Banki w tych wdrożeniach w obszarach obsługi typowych zdarzeń w bankowości podążyły drogą wytyczoną przez operatorów telekomunikacyjnych. Warto także zauważyć, że – zwłaszcza w przypadku dużych banków – chatboty wykorzystywane są przez wewnętrzne działy (takie jak HR czy IT) do zwiększenia efektywności obsługi własnych pracowników czy współpracowników (np. sieci partnerskiej).

Specyficznymi przypadkami wdrożeń hiperautomatyzacji jest wdrażanie jej rozwiązań w organizacjach globalnych. Kilka czoło-

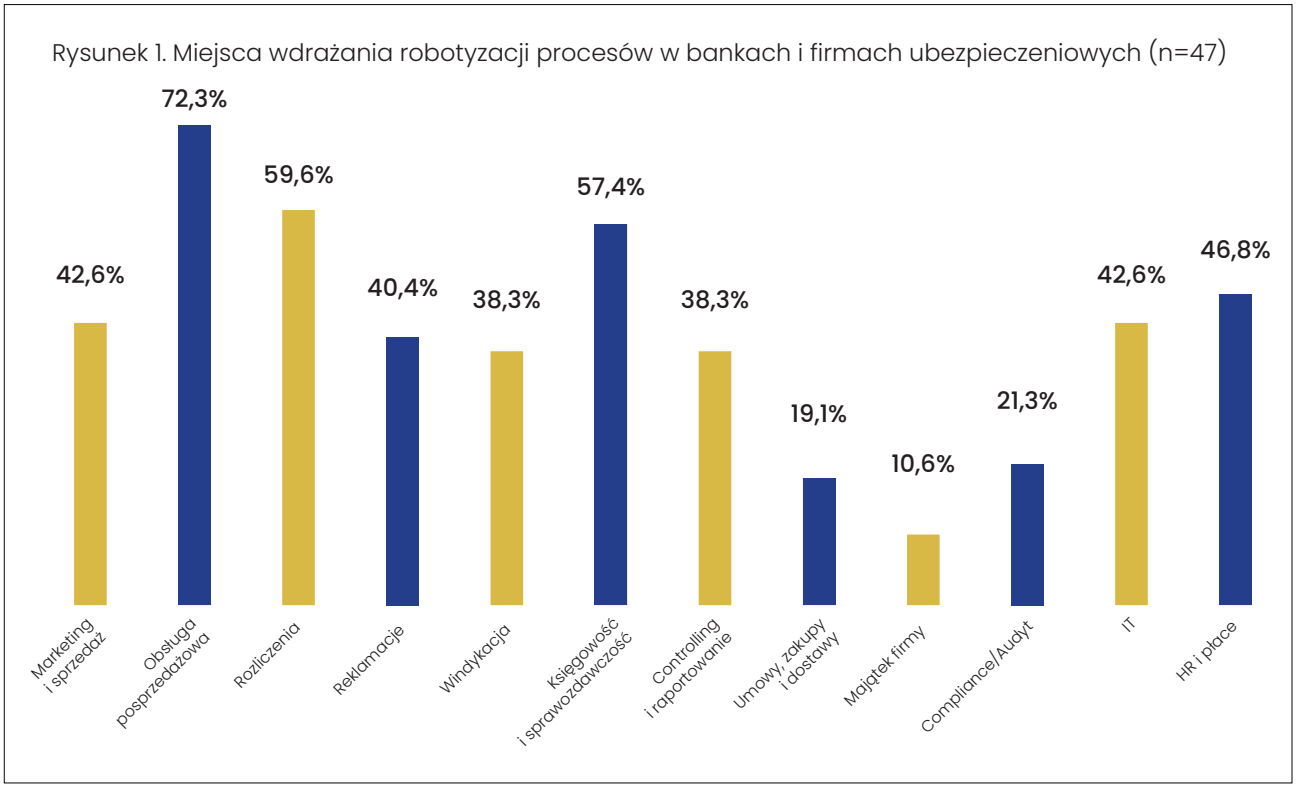
wych banków działających w Polsce należy do wielkich, globalnych korporacji bankowych. Jak wskazują doświadczenia, wdrożenia w globalnych korporacjach mają swoją specyfikę i różnią się od wdrożeń w bankach lokalnych. We wdrożeniach globalnych pojawiają się problemy wynikające ze skali działania (liczne zespoły, liczne poziomy i ciała zatwierdzające decyzje). Skala organizacji (banków) globalnych wymaga też uwzględnienia nie tylko złożoności i różnorodności procesów i aktywności, ale także różnorodności modeli kosztowych w różnych jednostkach i pionach (co wynikać może z silosowości jednostek i pionów), różnorodności modeli, warunków i obszarów obowiązywania licencji na oprogramowanie oraz wersji narzędzi (i ogólnie: oprogramowania) w skali organizacji globalnej. Czynnikiem pozytywnym wdrożeń w bankach globalnych jest to, iż w wielkich strukturach jest więcej „nisko zwisających kiści" – obszarów o niskiej efektywności działania, w których jeszcze nie zaimplementowano rozwiązań automatyzacji/robotyzacji, a w których można szybko osiągnąć duże i spektakularne korzyści.

W przypadkach przejęć banków czy włączania ich do struktur globalnych oraz wynikających z takich zdarzeń konieczności migracji danych między systemami (np. między systemami stosowanymi w banku włączanym do grupy czy przejmowanym a systemami nowej grupy czy banku) rozwiązania zautomatyzowane stosowane są do przeprowadzania i kontroli dość złożonych czynności, jakimi są migracje danych między bazami i systemami.

Na razie dość rzadko analizowanym obszarem zagadnień wdrożeniowych jest przygotowanie koncepcji czy planu określającego, czy bank jest w stanie zrezygnować ze stosowania niektórych rozwiązań automatyzacji/robotyzacji. Choć prognozowany jest stały rozwój automatyzacji/robotyzacji/hiperautomatyzacji w bankach i nikt nie zakłada odwrotu od takich rozwiązań, to jednak mogą zdarzyć się sytuacje, w których rezygnacja z określonych robotów, chatbotów czy innych elementów może się okazać konieczna. Sytuacjami, w którym może być konieczne posiadanie „planu B" może być np. zmiana regulacji wykluczająca automatyzację konkretnych działań czy obszarów, przejęcie banku przez inny bank, który stosuje rozwiązania całkowicie odmienne i nie dające się pogodzić z dotychczas stosowanymi itp.

Dla zarządzania bankiem bardzo ważne są zagadnienia oceny ryzyka (np. ryzyka strat w działalności kredytowej) i ogólnie: tworzenia modeli wspomagających zarządzanie oraz oceny

Rysunek 1. Miejsca wdrażania robotyzacji procesów w bankach i firmach ubezpieczeniowych (n=47)



rezultatów obliczeń prowadzonych z ich wykorzystaniem. W tym obszarze pojawiają się coraz nowsze rozwiązania będące przykładami hiperautomatyzacji – kompleksowych zastosowań oprogramowania korzystające z zaawansowanych metod sztucznej inteligencji – począwszy od tworzenia modeli bazujących np. na sieciach neuronowych przez uczenie maszynowe wykorzystywane w trenowaniu opracowywanych modeli po zaawansowane techniki wizualizacji rezultatów obliczeń.

Obszarem zastosowań automatyzacji są także rozwiązania z obszaru tzw. otwartej bankowości, bazujące m.in. na dostępie do wdrożonych standardów komunikacji np. Standard PolishAPI[5] i obsługujące współpracę banków z innymi podmiotami finansowymi, w tym z fintechami.

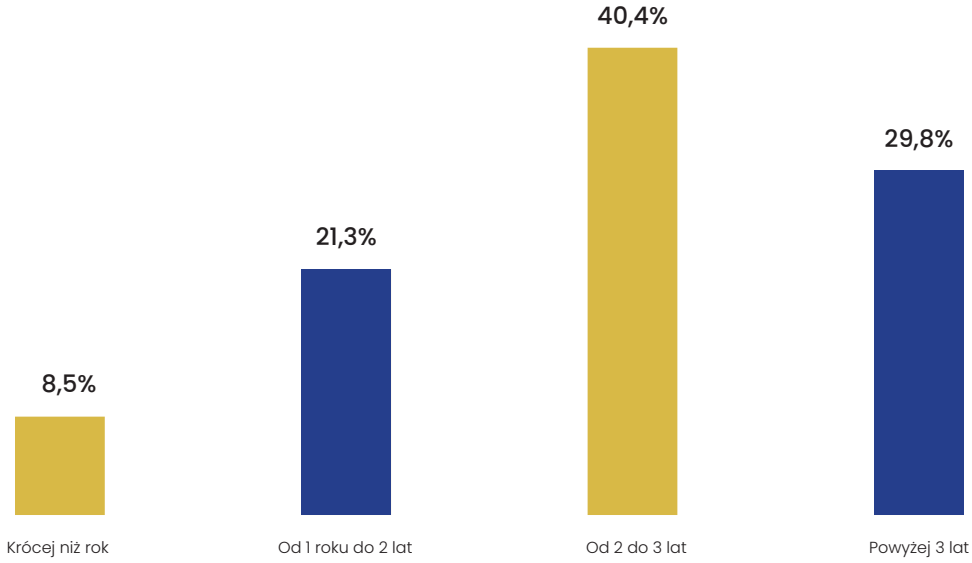
W drugim kwartale 2020 r. serwis Robonomika.pl przeprowadził rozbudowane badanie ankietowe dotyczące hiperautomatyzacji, w szczególności robotyzacji procesów biznesowych. Badanie miało charakter jakościowy, na ankiety odpowiedzieli zajmujący się tymi zagadnieniami menedżerowie z niemal 240 firm działających w Polsce, w tym 47 banków i firm ubezpieczeniowych. Respondenci z banków i firm ubezpieczeniowych jako główne obszary wdrożeń podali obsługę posprzedażową (ponad 72% odpowiedzi), rozliczenia (niemal 60%) i księgowość oraz sprawozdawczość (ponad 57%). Rozkład udzielonych odpowiedzi przedstawiono na rysunku (patrz wykres 1.)

Automatyzacja w obszarze marketingu i sprzedaży w badaniu zajmowała jeszcze pozycję „w środku stawki" (niecałe 43% odpowiedzi respondentów), ale wraz z rozwojem voicebotów/chatbotów korzystających z coraz lepiej działających rozwiązań przetwarzania języka naturalnego, a także ze wsparcia urządzeniami („inteligentne" bankomaty/wpłatomaty, a właściwie obsługowe kioski wielofunkcyjne) można zauważyć rozszerzanie się zakresu zastosowań w tym obszarze. Przejawem tej tendencji jest szybki przyrost liczby „oddziałów bezgotówkowych" banków, w jakie przekształcane są dotychczasowe placówki. W połowie 2021 r. liczba oddziałów, w których nie ma już obsługi kasowej przekroczyła pół tysiąca[6]. ING Bank Śląski na 272 placówki ogółem miał

5 https://polishapi.org – zob. przypis 2.

6 https://prnews.pl/raport-prnews-pl-liczba-bankowych-placowek-bezgotowkowych-ii-kw-2021-460544

Wykres 2. Od kiedy wdrażana jest robotyzacja procesów biznesowych w badanych bankach i firmach ubezpieczeniowych



już 179 takich oddziałów bezgotówkowych, w których klientów wspierają doradcy, zaś obsługa transakcji gotówkowych została przeniesiona do zainstalowanych w tych miejscach bankomatów/wpłatomatów. W pierwszej trójce pod względem liczby oddziałów bezgotówkowych były też BNP Paribas Bank Polska (131 oddziałów) oraz Bank Millennium (82 oddziały). Banki zapowiadają, że wobec rosnącej roli kanałów cyfrowych wspieranych rozwiązaniami automatyzacji większość ich oddziałów w najbliższej przyszłości będą stanowiły właśnie te bezgotówkowe. Wprowadzanie takiego modelu obsługi klientów jest oczywiście uzależnione od automatyzacji wpierającego je zaplecza transakcyjnego, jednocześnie przyspiesza tempo i zwiększa zakres hiperautomatyzacji banków.

4.3. Poziomy zaawansowania hiperautomatyzacji

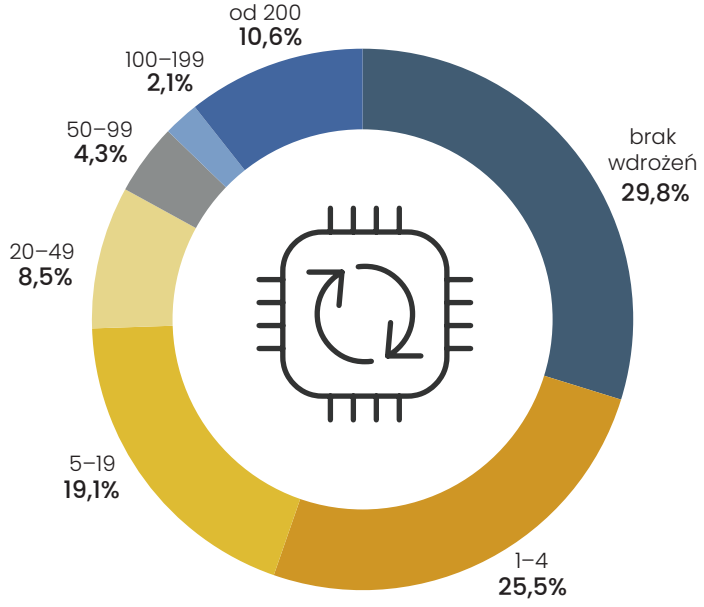
Ogólne metody oceny zaawansowania robotyzacji i hiperautomatyzacji przedsiębiorstwa (organizacji komercyjnej) można zastosować do przedsiębiorstw finansowych – a w szczególności do banków. Stopień automatyzacji i robotyzacji banku można określić **wskaźnikiem inteligencji robotycznej (RQ)**, oceniając poziom zaawansowania procesów hiperautomatyzacji na sześciostopniowej skali dojrzałości:

Poziom 0 – „Ignorancja” – w banku nie podjęto jeszcze żadnych działań związanych z automatyzacją; często na zerowym poziomie dojrzałości zarząd banku nie ma nawet świadomości, że konkurencja wdraża już rozwiązania z obszaru automatyzacji i nie widzi potrzeby zmiany przyjętego modelu pracy; niemal nic o automatyzacji nie wiedzą pracownicy. Można zaryzykować stwierdzenie, że w warunkach polskich tak niski poziom nigdy nie występował, gdyż polskie banki są bardzo otwarte na innowacje.

Poziom 1 – „Lokalni bohaterowie” – w pojedynczych komórkach rodzi się świadomość konieczności automatyzacji; przy użyciu prostych środków zaczyna się automatyzacja pojedynczych, rutynowych i łatwo zdefiniowanych działań, ale inicjatywy te nie są skoordynowane w skali całej organizacji, zaś pracownicy raczej przyglądają się z zaciekawieniem, nie widząc zagrożenia, ale raczej szanse na odciążenie od monotonnych prac. Ten poziom dojrzałości praktycznie wszystkie polskie banki mają już dawno za sobą.

Poziom 2 – „Wyłania się porządek” – automatyzacja obejmuje coraz więcej komórek organizacyjnych banku; następują próby koordynacji

Wykres 3. Liczba robotów nadzorowanych działających w badanych bankach/firmach ubezpieczeniowych



tych przedsięwzięć; powoływane są dedykowane zespoły/projekty; automatyzowane są działania coraz bardziej złożone, ale ciągle o charakterze deterministycznym (algorytmizowalnym); część pracowników włącza się w te działania, postrzegając je jako szansę na rozwój zawodowy; pojawiają się wśród pracowników obawy, ale są minimalizowane przez odpowiednią komunikację.

Poziom 3 „Skoordynowana automatyzacja – hiperautomatyzacja" – prace związane z automatyzacją są usystematyzowane i mają charakter ciągły, realizując istotę hiperautomatyzacji; zdecydowana większość komórek (tam gdzie jest to uzasadnione biznesowo) wdrożyła lub wdraża automatyzację; działają dedykowane jednostki i role związane z tymi działaniami, wprowadzane są profesjonalne (i wystandaryzowane) narzędzia do automatyzacji stosowane zarówno do działań prostych, jak i złożonych, często bazujących na skomplikowanej logice; pracownicy widzą przed sobą jedną z trzech ścieżek: a) przechodzą do realizacji działań bardziej kreatywnych (tam, gdzie są potrzebne heurystyki); b) intensywnie pracują w obszarze utrzymania i rozwoju automatyzacji; c) opuszczają bank.

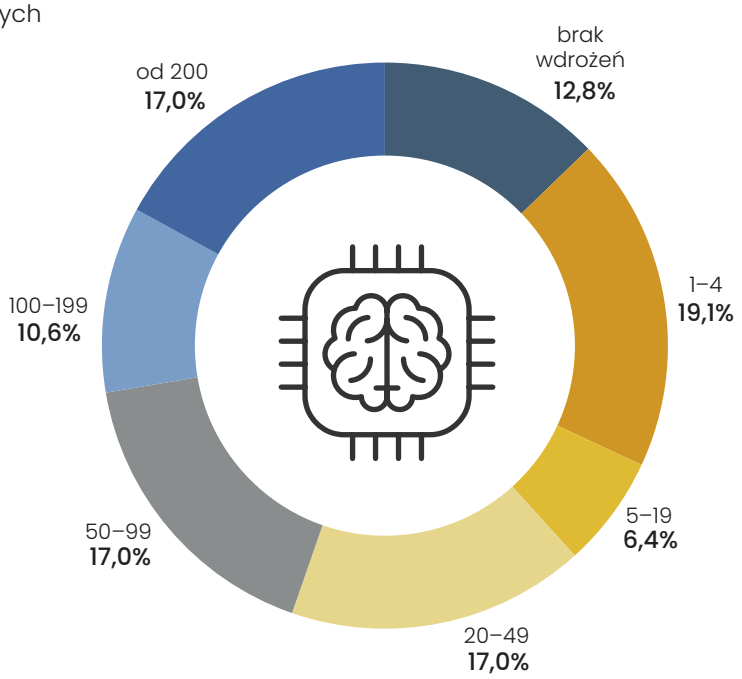
Poziom 4 „Częściowa autonomia" – w ramach hiperautomatyzacji wprowadzane są mechanizmy automatyzacji kognitywnej, pozwalające na kompleksową obsługę procesów niemożliwych do objęcia klasycznymi metodami automatyzacji; w banku rośnie rola nowych kompetencji, związanych z łączeniem automatyzacji i robotyzacji z elementami sztucznej inteligencji; część pracowników włącza się w ten obszar rozwoju, więcej pracowników niż na poziomie 3 jest przesuwane do coraz bardziej złożonych działań, część odchodzi.

Poziom 5 „Szeroka autonomia" – dzięki głębokiemu połączeniu automatyzacji procesów i sztucznej inteligencji bank w wielu obszarach działa praktycznie autonomicznie, bez udziału człowieka, choć personel zachowuje funkcje nadzorcze i podejmuje decyzje strategiczne; struktura i liczba zatrudnionych może być mocno ograniczona w stosunku do punktu wyjściowego (np. poziomu 1); stopień hiperautomatyzacji banku jest ograniczony w zasadzie tylko regulacjami prawnymi – a bank w sposobie działania upodabnia się do fintechu.

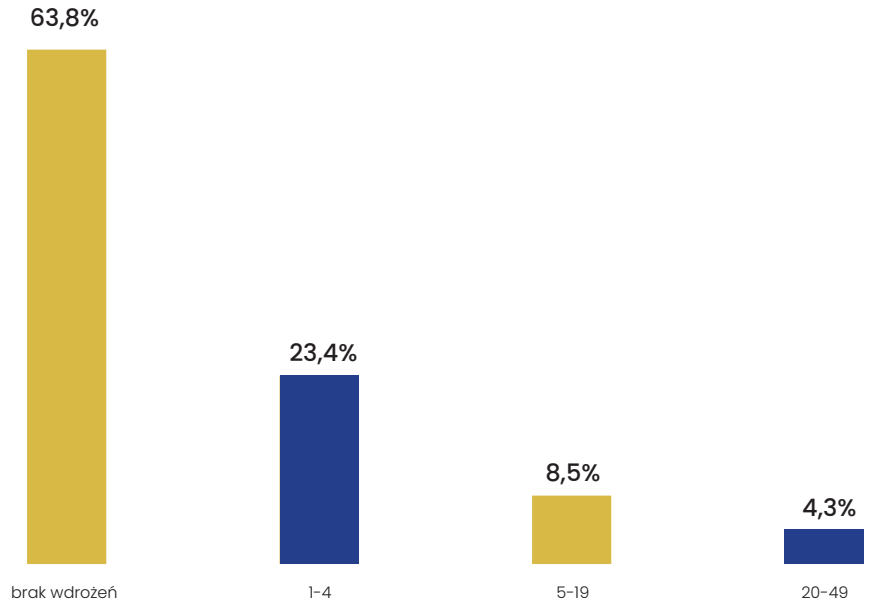
Dane z badania przedstawione na wykresie 2 pokazują, że automatyzacja procesów w bankach i firmach ubezpieczeniowych jest już prowadzona co najmniej od dwóch lat. Odpowiedziała tak zdecydowana większość respondentów (łącznie od dwóch do trzech lat i powyżej trzech lat stanowiło niemal 70% odpowiedzi).

Na stopień zaawansowania automatyzacji wskazują też liczby wdrożonych robotów, zwłaszcza nienadzorowanych – tylko w nie-

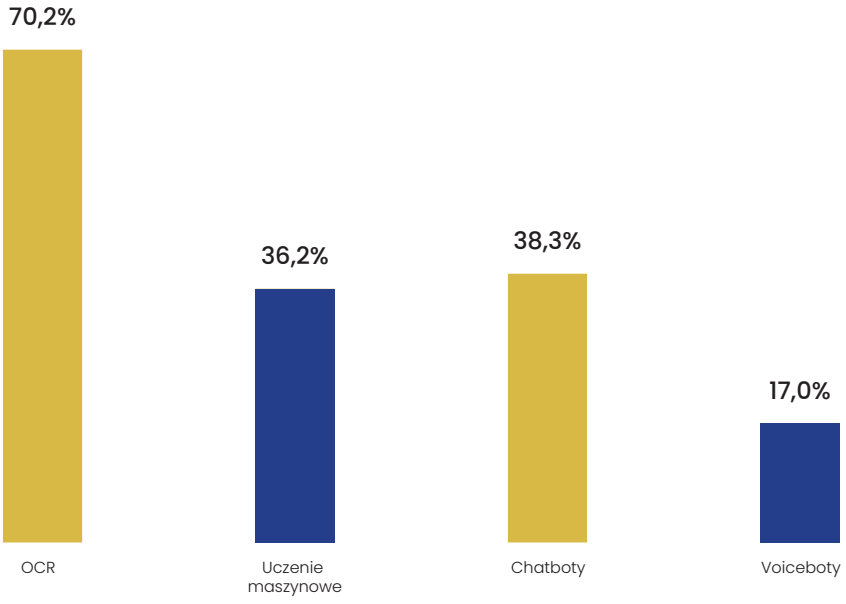
Wykres 4. Liczba robotów nienadzorowanych działających w badanych bankach/firmach ubezpieczeniowych



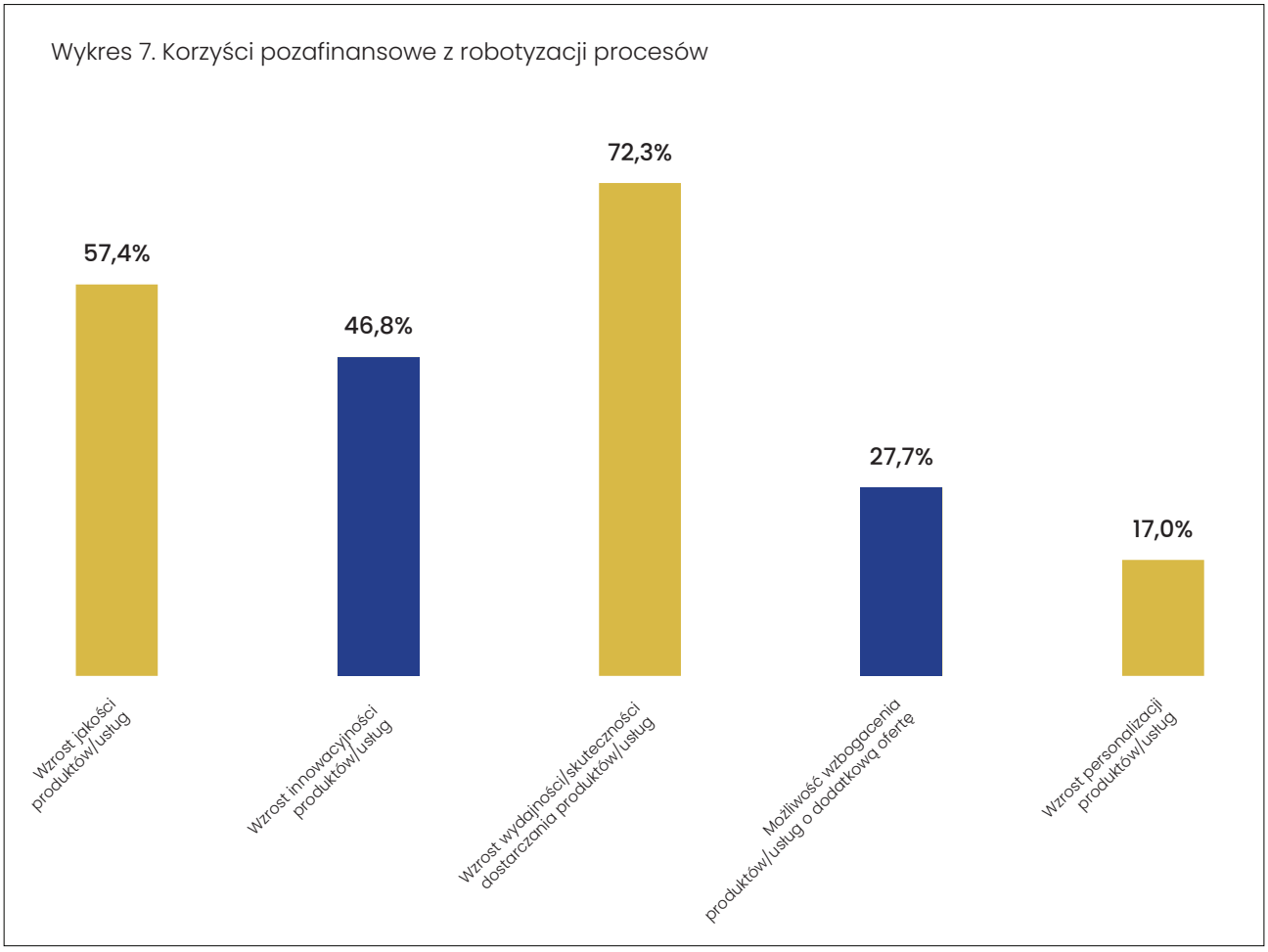
Wykres 5. Liczba robotów inteligentnych w badanych bankach/firmach ubezpieczeniowych



Wykres 6. Rozwiązania z hiperautomatyzacji stosowane w badanych bankach/firmach ubezpieczeniowych (oprócz robotów programowych)



Wykres 7. Korzyści pozafinansowe z robotyzacji procesów



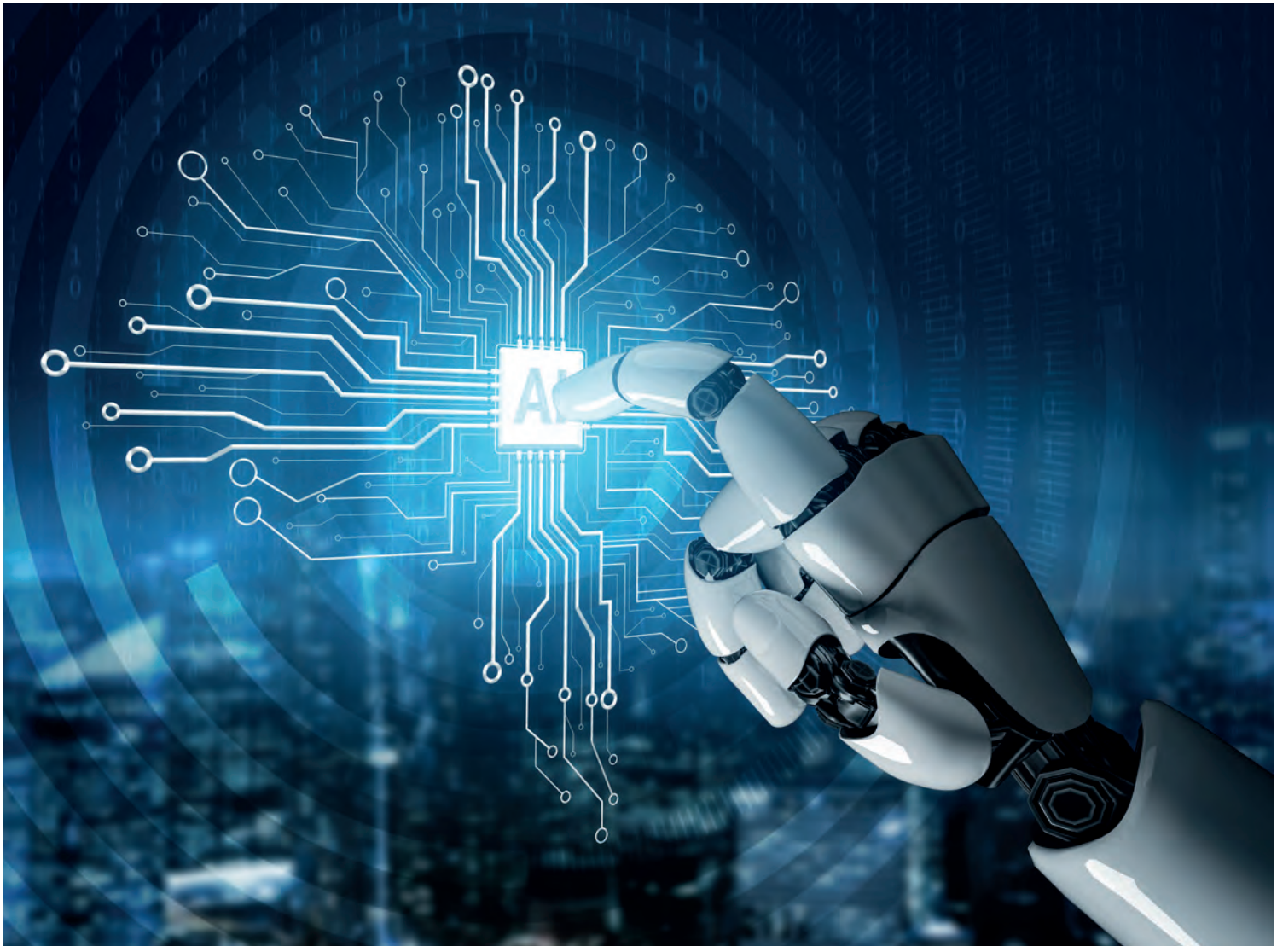
całych 13% badanych banków i firm ich nie ma. Niemal 11% respondentów wskazało, że w ich banku/firmie działa 200 i więcej robotów nadzorowanych (patrz wykres 3), jeszcze wyższy (17%) był udział odpowiedzi wskazujących na 200 lub więcej robotów nienadzorowanych (patrz wykres 4).

Niewielki był w czasie badania udział banków/firm ubezpieczeniowych, w których działały roboty inteligentne (w badaniu rozróżniono kategorię robotów nienadzorowanych od robotów inteligentnych) – niemal 64% ankietowanych informowało o braku takich robotów w ich firmie, większość podawała liczbę kilku–kilkunastu działających robotów inteligentnych, tylko ok. 4% ankietowanych poinformowało, że jest ich więcej niż 20 (patrz wykres 5).

Poza robotami programowymi najczęściej stosowanym narzędziami hiperautomatyzacji są urządzenia i oprogramowanie OCR (patrz wykres 6) – do rozpoznawania treści dokumentów dostarczanych w postaci graficznej, np. papierowych (ponad 70% odpowiedzi) oraz narzędzia do komunikacji z klientami, przede wszystkim chatboty (ponad 38%), w mniejszym zakresie voiceboty (17%). Choćby tylko z konieczności trenowania chatbotówi i voicebotów wynika stosunkowo duża popularność metod uczenia maszynowego (ponad 36% odpowiedzi).

Niemal 60% respondentów pytanych o aspekty finansowe efektów wdrożeń podało, że robotyzacja przyczyniła się do obniżenia kosztów działania, natomiast tylko 17% odpowiedzi wskazywało na podwyższenie marży. Korzyści pozafinansowe przedstawia wykres 7. Najwięcej ankietowanych (ponad 72%) wskazało na wzrost wydajności i skuteczności dostarczania usług, ponad 57% podkreślało wzrost jakości, niemal 47% – przyrost innowacyjności. Na razie dość umiarkowany okazał się wzrost stopnia personalizacji produktów i usług banku/firmy – tę korzyść podało tylko 17% respondentów.

5. Przykłady wdrożeń hiperautomatyzacji



Doświadczenie to wiedza i umiejętności uzyskane przez zaangażowanie w realizację określonych prac. Często „płacimy drogo za własne doświadczenia, ponieważ nie wykorzystujemy cudzych". Dlatego autorzy w ramach inicjatywy Liderzy.AI gromadzą i przekazują – w formie sprawdzonych receptur – esencję doświadczeń osób zajmujących się szeroko rozumianą hiperautomatyzacją w polskich firmach. Poniżej zaprezentowaliśmy wybrane doświadczenia liderów sektora finansowego.

ING Bank Śląski

Zaawansowane rozwiązania automatyzacji i robotyzacji biznesu w ING Banku Śląskim[7] obejmują zarówno obsługę kontaktów z klientami (front office), jak i wewnętrzne procesy biznesowe (back office). Dzięki wzajemnemu powiązaniu tworzonych rozwiązań i ich wdrożeń możemy mówić o działaniach o charakterze hiperautomatyzacji. Przykładem z obszaru front office jest

7 https://robonomika.pl/wykorzystanie-robotow-w-ing-bank-slaski-stan-obecny-i-perspektywy-na-przyszlosc

udostępniony w I kwartale 2018 r. chatbot „Mój Asystent" – system konwersacyjny porozumiewający się z klientami w języku naturalnym (polskim i angielskim). Obsługuje on pytania klientów korzystających z bankowości internetowej Moje ING, dostępny jest przez przeglądarkę oraz w bankowości mobilnej banku. Wdrożenie „Mojego Asystenta" poprzedzone zostało opracowaniem chatbota dla pracowników banku, co dostarczyło cennych doświadczeń związanych z obsługą w języku naturalnym.

Warto podkreślić, że prace nad wdrożeniami rozwiązań klasy RPA rozpoczęto w ING Banku Śląskim ponad 10 lat temu, traktując je jako narzędzia optymalizacji procesów bankowych. Obecnie w Pionie Operacji działa już ponad 1500 robotów, z których pomocy korzysta ok. 500 użytkowników, zaś liczba uruchomień robotów w ciągu roku sięga 600 tys. Roboty wykorzystywane są m.in. do parametryzacji i opisu w skrypcie procesu księgowania zmian wynikających z podpisania z klientem aneksu do umowy kredytowej. Dzięki temu wprowadzanie tych zmian w zasadzie nie wymaga angażowania pracownika banku. W Pionie Operacji roboty wykorzystywane są także do analizy wyciągów, segregowania zeskanowanej dokumentacji oraz analizy danych pobranych z kartotek klientów i ksiąg wieczystych. Poza Pionem Operacji rozwiązania RPA wdrażane są m.in. w Pionie Finansów, Ryzyka i w Contact Center ING Banku Śląskiego. Dla usprawnienia prac nad hiperautomatyzacją zorganizowano CoE (*Center of Excellence* – Centrum Doskonałości) robotyzacji procesów. Działający w jego ramach eksperci tworzą rozwiązania wdrażane nie tylko w Polsce, ale również w całej grupie ING, m.in. w Belgii, Francji, Holandii, Rumunii i Szwajcarii. Natomiast w ramach platformy „End User Computing" bank rozwija autorską platformę RPA o nazwie RoboPlatform (jest ona również sprzedawana jako produkt firmom zewnętrznym). Umożliwia ona pracownikom nie będącym specjalistami IT tworzenie robotów oraz szybką implementację rozwiązań robotyzacyjnych o różnym stopniu złożoności – także dzięki temu, że w banku prowadzone są regularne szkolenia z zakresu RPA dla pracowników. Platformę charakteryzuje duża elastyczność, umożliwiając szybkie wdrażanie robotów stosunkowo niskim kosztem.

BNP Paribas Bank Polska[8]

Program wdrażania rozwiązań RPA trwa od maja 2017 r. W I kwartale 2018 r. w banku działały już roboty zastępujące cztery pełne etaty pracownicze w 22 procesach, w I kwartale 2019 r. zrobotyzowanych było już 46 procesów, a w III kwartale 2020 r. w siedmiu obszarach działalności banku 93 procesy. Zaczęto też wycofywanie robotów „przestarzałych". Rekordowo szybka obsługa (procesu przekazania akt z aktualizacją spraw do zewnętrznej firmy prawniczej) trwa 0,07 sekundy, najdłuższy proces polegający na rekoncyliacji raportów dotyczących sald na rachunkach zajmuje 31 minut. Najbardziej złożony jest proces obsługi przypadku zgonu klienta, wymagający zamknięcia wszystkich relacji – współpracuje z ośmioma aplikacjami banku i składa się z 83 podstron procesu. W listopadzie 2020 r. najstarszy z wdrożonych robotów działał już w banku ponad 1300 dni. Największa liczba spraw obsługiwanych dziennie przez jednego robota wynosiła ok. 1600. Czas realizacji dyspozycji obsługiwanych we współpracy ludzi i robotów udało się skrócić od 30 do 70%. W przypadku niektórych wniosków kredytowych roboty umożliwiły księgowanie środków kredytowych na koncie kredytobiorcy w dniu decyzji o przyznaniu kredytu. Prace te wykonywało poprzednio ok. 40 pracowników. Najszybciej – w ciągu zaledwie trzech dni – udało się wdrożyć robota obsługującego zmianę terminu spłaty pożyczki (wakacje kredytowe). W obszarze operacji rozwijane są obecnie roboty kognitywne korzystające z metod sztucznej inteligencji. Po zastosowaniu kognitywnej robotyzacji w automatycznej obsłudze korespondencji – od digitalizacji korespondencji wchodzącej i sprawdzaniu poprawności obróbki OCR przez klasyfikację dokumentów, ekstrakcję treści potrzebnych do rejestracji pisma po rejestrację pisma w systemie kancelaryjnym i przekazanie do obsługi przez pracowników merytorycznych

> ***Obszarem zastosowań automatyzacji są także rozwiązania z obszaru tzw. otwartej bankowości, bazujące m.in. na dostępie do wdrożonych standardów komunikacji np. Standard PolishAPI i obsługujące współpracę banków z innymi podmiotami finansowymi, w tym z fintechami.***

8 Na podstawie wystąpienia Arkadiusza Lubiny i Michała Kosonia (BNP Pribas) w drugiej edycji konferencji Hiperautomatyzacja w listopadzie 2020 r.

– główne kierunki planowanych zastosowań AI to optymalizacja transportów gotówki, obsługa reklamacji przychodzących z systemu SWIFT, obsługa polis ubezpieczeniowych, automatyczna weryfikacja dokumentacji wymaganej do kredytów hipotecznych oraz wsparcie procesów KYC (*Know Your Customer* – procedura należytej staranności w identyfikacji klientów i zbieraniu wymaganych informacji o klientach). Rozwój i zarządzanie technologią oraz całą „farmą" robotów są prowadzone w jednostce nazwanej „Robotic Center of Excellence".

Alior Bank[9]

Robotyzacja i automatyzacja były kluczowymi założeniami strategii Alior Banku na lata 2017–2020, określonej nazwą „Cyfrowego buntownika". Działania te miały pomóc w osiągnięciu współczynnika efektywności kosztowej C/I (*Cost-to-Income* – koszty do dochodów) rzędu 39%. Zakładano, że do 2020 r. projekty związane z automatyzacją i robotyką dostarczą 20–30% oszczędności kosztów, a także zapewnią poprawę zadowolenia klientów. W czerwcu 2017 r. w banku utworzono Centrum Kompetencji RPA, pierwsze roboty wdrożono w sierpniu 2018 r., zaś produkcyjnie, w głównych procesach biznesowych – w lipcu 2019 r.

W ramach realizacji strategii Alior Bank opracował, wdrożył i rozwija Dronna – wirtualnego doradcę korzystającego z zaawansowanych metod sztucznej inteligencji, biometrii oraz analizy mowy. Dronn może prowadzić z klientami swobodną rozmowę, reagując na odpowiedzi i zadając odpowiednie pytania. Przetworzone informacje z rozmowy dostarczane są do środowiska do obliczeń statystycznych. Środowisko to działając w czasie rzeczywistym pozwala systemowi Dronn wybierać dalszy przebieg rozmowy na podstawie danych pozyskanych od klienta. System wykorzystywany jest m.in. w procesie miękkiej windykacji, a także w badaniach marketingowych, procesach segmentacji klientów i kontaktach z wybranymi klientami np. w celu zebrania ich oświadczeń o rezydencji podatkowej.

DOBRE PRAKTYKI DOTYCZĄCE WDROŻEŃ HIPERAUTOMATYZACJI – PERSPEKTYWA TECHNOLOGICZNA

- dążenie do tworzenia komponentów niewielkich i nadających się do wielokrotnego używania w różnych częściach rozwiązania (zasada re-use),
- unikanie tworzenia komponentów do realizacji funkcji wykonywanych w danym systemie przez dotychczas działające rozwiązania (arkusze kalkulacyjne, struktury SQL lub REST),
- umożliwienie odrębnego tworzenia i testowania oddzielnych części systemu (co umożliwia ich tworzenie i testowania w zespołach działających według metodyk zwinnych),
- rozdzielanie komponentów realizujących logikę procesów biznesowych od komponentów realizujących współpracę z innymi aplikacjami.
- tworzenie standardów obsługi sytuacji wyjątkowych,
- dokładne dokumentowanie (opisywanie) obsługi sytuacji wyjątkowych, staranne prowadzenie statystyk takich sytuacji,
- dość szczegółowe komentowanie kodu i parametrów ułatwiające rozumienie struktur logicznych i działania tworzonych rozwiązań, opisywanie w komentarzach warunków i rezultatów punktów decyzyjnych, stosowanie ramek i kolorów do grupowania elementów powiązanych.

Na podstawie wystąpienia Krzysztofa Karaszewskiego (HSBC) w pierwszej edycji konferencji Hiperautomatyzacja w czerwcu 2020 r.

Po czterech latach wdrażania robotyzacji zweryfikowano pod kątem robotyzacji, optymalizacji oraz użycia OCR ponad 1140 procesów, zespół RPA wdrożył 125 automatyzacji, uruchomiono 57 robotów/maszyn wirtualnych. Zespół robotyzacji w pionie Operacji liczył w listopadzie 2020 r. 15 pracowników. Bardzo duży nacisk położono na tworzenie reużywalnych grup funkcjonalności oraz budowę modułów obsługujących mikroprocesy. W repozytorium mikroprocesów (wewnętrznym marketplace) zgromadzono 58 modułów/mikroprocesów.

Kolejnym programem realizowanym w latach 2020–2022 jest „Więcej niż Bank". Hasłem jest „demokratyzacja robotyzacji", polegająca na włączaniu pracowników, którzy chcą wprowadzać usprawnienia w swojej codziennej pracy w swoich obszarach działania. W ramach Akademii Robotyzacji w 2020 r. zorganizowano trzy edycje zaawansowanych szkoleń dla 25 takich pracowników. Rozwój narzędzia (m.in. stosowanie kolejnych metod uczenia maszynowego, głównie w celu zwiększania zdolności rozumienia

9 Na podstawie wystąpienia Marcina Małka i Krystiana Kozłowskiego (Alior Bank) w drugiej edycji konferencji Hiperautomatyzacja w listopadzie 2020 r.

KLUCZOWE PROBLEMY WDRAŻANIA HIPERAUTOMATYZACJI

- źle zaprojektowany proces po jego automatyzacji jest nadal procesem źle zaprojektowanym (i nieefektywnym),
- automatyzacja procesu nieoptymalnego (nieefektywnego) może jeszcze pogorszyć jego efektywność z powodu „przesztywnienia" realizacji procesu biznesowego, poniesienia nakładów na konieczną infrastrukturę oraz konieczności ponoszenia kosztów jej utrzymania,
- automatyzacja procesu zaprojektowanego do interakcji z człowiekiem może spowodować problemy z wydajności oraz spowodować pojawienie się błędów w systemach zależnych, które nie były widoczne, gdy system działał z prędkością pracującego z nim człowieka.

Na podstawie wystąpienia Tomasza Ćwika (BNP Paribas Bank Polska) w pierwszej edycji konferencji Hiperautomatyzacja w czerwcu 2020 r.

GŁÓWNE WYZWANIA ZWIĄZANE Z WDRAŻANIEM HIPERAUTOMATYZACJI

Ludzie

- niska świadomość możliwości i zastosowań AI,
- niska skłonność do akceptacji błędu maszyny (w porównaniu do akceptacji błędów człowieka),
- oczekiwanie szybkich sukcesów do zaawansowanej technologii;

Organizacja

- trudność zgromadzenia rozsianych po całej organizacji osób potrzebnych do grupy wdrażającej,
- problemy z priorytetyzacją działań w dużej organizacji (na innowacje przyjdzie czas później);

Technologia

- brak danych do walidacji wyników modeli, w szczególności dla zastosowań OCR, konieczne zbudowanie oddzielnego postprocessingu albo ręcznego przygotowywania danych,
- zapewnienie bezpiecznego środowiska developerskiego do przetwarzania dużych ilości danych produkcyjnych (w tym danych wrażliwych),
- integracja środowiska modelowego z używanymi systemami IT.

Na podstawie wystąpienia Kamila Gajdasa i Grzegorza Roguskiego (ING Bank Śląski) w pierwszej edycji konferencji Hiperautomatyzacja w czerwcu 2020 r.

języka naturalnego) realizowany jest w ramach wdrażania systemu IBM Watson.

Credit Agricole Bank Polska[10]

W rozpoczętym w połowie 2017 r. programie wdrażań RPA w banku – który do października 2020 r. z poziomu „Proof-of-Concept" doszedł do poziomu „Business as usual" z 50 aktywnymi robotami programowymi – nacisk położono na skalowalność rozwiązań w całej organizacji banku, szukając obszarów, w których wprowadzane zmiany prowadzą do zwiększania potencjału robotyzacji oraz do zwiększania tempa wdrożeń narzędzi RPA. Zwracano też uwagę na szerokość i kompletność oferty narzędzi RPA oraz ich wzajemną kompatybilność, w tym możliwości rejestracji procesów oraz ich analizy metodami process mining, a także współpracę z istniejącymi i tworzonymi interfejsami (API) systemów stosowanych w banku, zaś przy wyborze obszarów do robotyzacji – robotyzacja wspólnych procesów. Stworzone Centrum Kompetencji RPA zaczęło też działać dla innych jednostek grupy kapitałowej Credit Agricole, współpracując z nimi na poziomie infrastruktury, tworzenia robotów, uruchamiania kolejnych pilotaży i PoC oraz wymiany doświadczeń.

mBank[11]

Robotyzację procesów w mBanku rozpoczęto w 2017 r., projekty opracowywania i wdrożenia robotów prowadziło mCO – Centrum Operacji banku. W kolejnych działaniach mBank powierzył, w trybie outsourcingu, dalsze prace w firmie zewnętrznej, ale będącej startupem założonym ze wsparciem mAkceleratora, własnego funduszu Venture Capital mBanku. W toku kolejnych prac duży nacisk położono na odpowiednie „zagospodarowanie" pracowników, których stanowiska zostały zautomatyzowane. Części z nich zaproponowano reskilling, w którego rezultacie przeszli oni do tworzonego zespołu Pasterzy Ro-

10 Na podstawie wystąpienia Radosława Repczyńskiego (CABP) w drugiej edycji konferencji Hiperautomatyzacja w listopadzie 2020 r.

11 Na podstawie wystąpień Olgi Kacprzak (mBank) w pierwszej edycji konferencji Hiperautomatyzacja (czerwiec 2020 r.) oraz Radosława Pałcza (mBank) w drugiej edycji konferencji Hiperautomatyzacja (listopad 2020 r.)

botów w założonej firmie. W 2019 r. w zespole tym pracowało już 30 osób.

W kolejnych fazach robotyzacji mBank skoncentrował się na zaawansowanej analizie procesów. Jednym z rezultatów analizy było stwierdzenie, że trzy pełne etaty można zaoszczędzić dzięki stosunkowo prostej automatyzacji pobierania danych z systemów, innym – że 60% wniosków niepotrzebnie obciąża systemy informatyczne banku. Wnioski z analizy procesów prowadziły do uruchomienia projektu OPI (*Operational Process Improvement*) w ramach Wydziału Analiz i Optymalizacji Procesów. Jednym z planowanych wskaźników było osiągnięcie 10-proc. oszczędności etatów dzięki zakładanemu zmniejszeniu pracochłonności. Dodatkowo sformułowano cel redukcji kosztów zewnętrznych, obniżenia poziomu ryzyka operacyjnego oraz poprawienie jakości usług postrzeganej przez klientów oraz jakości danych, bardzo istotnej dla działania operacyjnego. W tym celu powołano dedykowany zespół OPI Hunters – łowców optymalizacji – wyposażając go w zaawansowane narzędzia RPA, dostęp do platformy Low-Code, a także specjalny system do zbierania, weryfikowania oraz kolejkowania zgłoszeń OPI i przekazywania ich do realizacji i oceny wyników. W 2019 r. zgłoszenia OPI (ponad 300 pomysłów) przyszły łącznie od 150 osób. Dotyczyły one ponad 20 aplikacji i systemów. Dzięki wdrożeniu 190 zgłoszeń OPI uzyskano założony wskaźnik 10-proc. oszczędności etatów.

Bank Pekao[12]

Automatyzacja z wykorzystaniem systemów BPM rozpoczęła się w Banku Pekao jeszcze w 2012 r., natomiast pierwsze wdrożenia narzędzi RPA – w 2018 r. W listopadzie 2020 r. bank doszedł do poziomu ponad 80 zrobotyzowanych procesów, 13 systemów obsługiwanych przez 27 „cyfrowych pracowników", realizujących dziennie ok. 10 tys. zadań. Robotyzowane są procesy w Centrum Operacji, w bankowości detalicznej, bankowości dla sektora MŚP, w private bankingu oraz w rachunkowości banku. Widomym efektem robotyzacji jest skrócenie czasu obsługi dyspozycji o ok. 50%. W zorganizowanym w Banku Pekao Centrum Kompetencji Automatyzacji i Robotyzacji ponad 50 osób w pięciu zespołach rozwijało aplikacje w przyrostowym postępowaniu scrum.

Dobrym przykładem korzyści z wdrożonych RPA jest obsługa reklamacji – procesu trudnego i pracochłonnego w realizacji „ręcznej". Korzystając z modelu zbudowanego z wykorzystaniem sieci neuronowej stworzono narzędzie optymalizacji procesu i robotyzacji jego obsługi. W rezultacie osiągnięto 90% dokładności w określaniu typu reklamacji i 76% dokładności w określeniu produktu lub usługi, których dotyczyła reklamacja. Bardzo cenne okazały się doświadczenia z budowy i wdrażania tego zaawansowanego rozwiązania. Początkowe uczenie sieci neuronowej trwało pięć dni, ale po wymianie silnika bazowego czas ten skrócił się do pięciu godzin. Do trenowania sieci wykorzystano ponad 140 tys. przykładów reklamacji, do walidacji stworzonego rozwiązania ok. 19 tys.

Ciekawym przypadkiem zastosowania innowacyjnych rozwiązań była recenzja aplikacji PeoPay. Skorzystano z rozwiązań nie tylko rozpoznających głos klienta, ale także prowadzących analizę sentymentu i klasyfikujących odpowiedzi. Użyto w tym celu wielu różnych technologii, w tym uczenia maszynowego i rozwiązań klasy Business Intelligence, aplikację tworzono z wykorzystaniem narzędzi Low-Code. Uzyskano 80% trafności w określeniu sentymentu osoby oceniającej PeoPay i od 63 do 83% trafności w klasyfikacji czego dotyczyła ocena (logowania, wydajności, współpracy z innymi rozwiązaniami itp.). Sprawdziło się też zastosowanie platformy Low-Code (bardzo krótki czas budowy aplikacji), kilka godzin trwało też jej trenowanie.

12 Na podstawie wystąpienia Jana M. Kowalskiego (Bank Pekao) w drugiej edycji konferencji Hiperautomatyzacja w listopadzie 2020 r.

6. Aspekty regulacyjne i etyczne hiperautomatyzacji

Na razie niewiele jest jeszcze regulacji odnoszących się bezpośrednio do automatyzacji w sektorze bankowym. Można jednak oczekiwać, że regulacje takie będą musiały się pojawić w miarę wzrostu skali wdrożeń hiperautomatyzacji w bankowości. Podobnie jak w innych sektorach gospodarki, coraz więcej uwagi będzie się poświęcać aspektom etycznym hiperautomatyzacji z uwagi na jej potencjalne oddziaływania społeczne.

6.1. Obecne i potencjalne regulacje hiperautomatyzacji bankowości

Regulacje, które można odnieść do tej problematyki dotyczą ochrony danych osobowych oraz kwestii odpowiedzialności banków i dostawców rozwiązań, a także zgodności implementowanych rozwiązań z ogólnymi regulacjami sektora finansowego.

REGULACJE DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH (RODO)

Zgodnie z ust. 1 art. 22 ogólnego rozporządzenia o ochronie danych (RODO)[13] zatytułowanego „Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie": „1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa." Wynikające stąd regulacje wyłączeń od tak sformułowanej reguły oraz postanowienia dotyczące prawa do informacji o podstawach decyzji podejmowanych w przetwarzaniu zautomatyzowanym zostały wprowadzone ustawą z 21 lutego 2019 r. m.in. do Prawa bankowego[14].

OCENA PRAWNA MOŻLIWOŚCI WDROŻENIA

Choć jak wspomniano powyżej, z wyjątkiem aspektów związanych z RODO niewiele jest jeszcze regulacji sektora bankowego odnoszących się bezpośrednio do automatyzacji/robotyzacji, to jednak przed wdrażaniem rozwiązań hiperautomatyzacji należy przeprowadzić prawną ocenę ich możliwości. Niezależnie od tego, czy wdrożenie ma być realizowane przez firmę zewnętrzną, czy własne działy banku, istotne jest przeprowadzenie analizy uwzględniającej następujące aspekty:

- zakres i rodzaj danych przetwarzanych automatycznie, zapewnienie ochrony danych (dane osobowe, tajemnica bankowa itp.);
- odpowiednie zabezpieczenia prawne dotyczące odpowiedzialności w przypadkach nieutrzymania ciągłości działań lub innych błędów zrobotyzowanych rozwiązań;
- zgodność zrobotyzowanych działań z regulacjami krajowymi i międzynarodowymi;
- zakres odpowiedzialności zewnętrznych dostawców rozwiązań oraz zgodność ich rozwiązań z regulacjami sektora bankowego/finansowego
- prawidłowe ustalenia kontraktowe dotyczące licencji oprogramowania stosowanego w rozwiązaniach RPA (np. jak zwyczajowe postanowienia licencyjne dotyczące liczby użytkowników mają się do „cyfrowych pracowników").

Wraz z rozwojem sektora RegTech i stosowania rozwiązań automatyzacji/robotyzacji w dziedzinie zgodności z regulacjami można oczekiwać pojawiania się dwóch podobszarów regulacji bezpośrednio dotyczących zagadnień hiperautomatyzacji:

- regulacji dotyczących reguł i obszarów stosowania rozwiązań hiperautomatyzacji w bankach i instytucjach finansowych,
- regulacji dotyczących samych regulatorów – metod automatyzacji i robotyzacji prowadzenia audytów regulacyjnych, pozyskiwania oraz analizy danych pobieranych od banków, wspierania narzędziami RPA formułowania ocen i wydawania decyzji regulatorów.

Dość oczywistym kierunkiem rozwoju zastosowań narzędzi RPA w tym drugim podobszarze będzie pobieranie przez regulatorów wymaganych danych online i reagowanie w trybie niemal rzeczywistym – co będzie wymagało odpowiednich zmian legislacyjnych dotyczących podstaw działania organów nadzoru finansowego.

---

13 https://uodo.gov.pl/pl/404/224

14 Do art. 105a Prawa bankowego został wprowadzony ust. 1a: „Banki (....) mogą podejmować decyzje, opierając się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, danych osobowych – również stanowiących tajemnicę bankową – pod warunkiem zapewnienia osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz do wyrażenia własnego stanowiska".

6.2. Aspekty etyczne hiperautomatyzacji w bankach

Aspekty etyczne hiperautomatyzacji można podzielić na dwa obszary: dotyczący pracowników banków oraz ich klientów.

ASPEKTY DOTYCZĄCE PRACOWNIKÓW

Są one w zasadzie wspólne dla wszystkich organizacji (komercyjnych i niekomercyjnych), w których wprowadzane są narzędzia automatyzacji, robotyzacji i hiperautomatyzacji – w tym także banków. Wynikają one przede wszystkim z obaw pracowników o to, że „roboty odbiorą im pracę".

Choć na razie obawy o stosowanie zaawansowanych metod analiz behawioralnych z wykorzystaniem sztucznej inteligencji dotyczą głównie klientów banków, to jednak w miarę upowszechniania się rozwiązań AI wspierających procesy rekrutacji pracowników oraz oceny ich wydajności i przydatności w firmie (np. przy podejmowaniu decyzji dotyczących redukcji personelu) pojawiają się obawy pracowników o to, że dotyczące ich decyzje pracownicze podejmowane będą w sposób zrobotyzowany. Tym większa jest waga budowania algorytmów oraz trenowania oprogramowania wspomagającego procesy HR na danych dobranych w sposób niedyskryminujący z uwagi na pochodzenie etniczne, kolor skóry, wyznanie, płeć, wiek i status ocenianych osób.

ASPEKTY DOTYCZĄCE KLIENTÓW BANKÓW

To przede wszystkim obszar decyzji podejmowanych w sposób operacyjny w zrobotyzowanych procesach, np. oceny zdolności kredytowej klienta, warunków prowadzenia jego kont (oprocentowanie, limity autoryzacyjne), wielkości przyznawanych kredytów oraz kryteriów przyznawania lub odrzucania wniosków kredytowych. Wobec stałego rozbudowywania i rozszerzania mechanizmów bezpieczeństwa (m.in. ochrona przed nieautoryzowanymi transakcjami, procedury antyfraudowe, pranie brudnych pieniędzy, działalność antyterrorystyczna) w coraz szerszym zakresie wspomaganych narzędziami hiperautomatyzacji należy uwzględniać potencjalne skutki zarówno zbyt słabego działania tych narzędzi (przepuszczanie transakcji nieautoryzowanych lub niedozwolonych), jak i zbyt silnego (blokowanie transakcji legalnych i prawidłowych), np. w wyniku nieprawidłowych danych stosowanych w trenowaniu robotów programowych.

W dalszej perspektywie pojawiają się obawy wynikające z coraz szerszego stosowania nie tylko narzędzi cyfrowego marketingu usług bankowych, ale także zaawansowanych metod sztucznej inteligencji w analizach behawioralnych klientów.

KONTEKST ETYCZNY WDRAŻANIA HIPERAUTOMATYZACJI

Wraz z coraz szerszym wprowadzaniem narzędzi hiperautomatyzacji pojawiają się już propozycje kodeksów lub ram etycznych, które określałyby przede wszystkim reguły działania robotów. Jeden z dostawców narzędzi RPA (firma NICE) zaproponował etyczne ramy robotyzacji procesów biznesowych (ang. *Robo-Ethical Framework*). Choć formalnie dotyczyły one tylko robotyzacji, to jednak można je odnieść także do kompleksowych wdrożeń składających się na hiperautomatyzację banków. Składają się one z pięciu punktów:

1. Automatyzacja musi być projektowana pod kątem pozytywnego oddziaływania na otoczenie. Skoro hiperautomatyzacja może wywołać radykalne zmiany na rynku pracy, to automatyzację należy prowadzić w taki sposób, by miała ona pozytywne oddziaływanie na kwestie społeczne, ekonomiczne i środowiskowe.
2. Automatyzacja musi być projektowana w taki sposób, aby ignorować specyficzne tożsamości grupowe w celu minimalizacji ryzyka stronniczego podejmowania decyzji przez automaty (nie powinny one uwzględniać cech osobniczych: pochodzenia etnicznego, koloru skóry, wyznania, płci, wieku i statusu osób, których dotyczą ich działania).
3. Automaty muszą być projektowane w taki sposób, aby zminimalizować ryzyko wyrządzenia indywidualnej krzywdy. Projektanci automatyzacji powinni określić, jakie decyzje do podejmowania można powierzać automatom, zaś algorytmy i procesy, na podstawie których działają automaty, muszą być przejrzyste i stworzone w taki sposób, aby umożliwiały wyjaśnianie i uzasadnienie podejmowanych przez nie decyzji. Ludzie muszą być w stanie przeprowadzić audyt procesów i decyzji podejmowanych przez automaty, a jeśli okaże się, że robot może zaszkodzić człowiekowi, człowiek musi móc interweniować, by naprawić taką sytuację i zapobiec jej występowaniu w przyszłości.
4. Automaty muszą być przeszkolone i funkcjonować, wykorzystując znane, zweryfikowane i zaufane źródła danych. Dane wykorzystywane do szkolenia algorytmów powinny pozwalać na odwołanie się do ich oryginalnego źródła.
5. Automaty muszą być zaprojektowane z zachowaniem określonych mechanizmów zarządzania i nadzoru. Ludzie powinni być informowani o możliwościach i ograniczeniach rozwiązań automatyzacji. Platforma wykorzystywana do automatyzacji procesów powinna być zaprojektowana tak, aby chronić przed nadużyciem władzy i nielegalnym dostępem poprzez ograniczanie, proaktywne monitorowanie i uwierzytelnianie każdego dostępu do niej. Platforma musi umożliwiać monitorowanie każdej podjętej na niej akcji.

Pierwszy z powyższych punktów odnosi się do wspomnianych wyżej aspektów dotyczących pracowników obawiających się zwolnienia z pracy. Jeśli rozwiązania zautomatyzowane miałyby być stosowane także do oceny pracowników, to do tych aspektów odnosi się także częściowo punkt drugi, mówiący o konieczności ignorowania cech osobniczych. Punkty trzeci, czwarty i piąty proponowanych ram odnoszą się do aspektów dotyczących przede wszystkim klientów banków.

7. Co dalej – perspektywy bliższe i dalsze, nowe wyzwania

Głównym i bardzo silnym trendem w hiperautomatyzacji jest rozwijanie rozwiązań korzystających z metod sztucznej inteligencji, w szczególności z uczenia maszynowego. Banki oczekują, że dzięki dołączeniu mechanizmów sztucznej inteligencji pojawi się możliwość kompleksowej automatyzacji coraz bardziej złożonych procesów.

7.1. Aktualne trendy hiperautomatyzacji w bankach

W zdecydowanej większości złożonych procesów biznesowych występują zarówno dane ustrukturyzowane, jak i nieustrukturyzowane.

> *W zdecydowanej większości złożonych procesów biznesowych występują zarówno dane ustrukturyzowane, jak i nieustrukturyzowane. Przetwarzanie danych nieustrukturyzowanych wymagało dotąd przeważnie ingerencji człowieka, który potrafił (czasem niemal intuicyjnie) rozpoznawać złożone zależności między nimi.*

Przetwarzanie danych nieustrukturyzowanych wymagało dotąd przeważnie ingerencji człowieka, który potrafił (czasem niemal intuicyjnie) rozpoznawać złożone zależności między nimi. Jednak podejście takie jest praktycznie niemożliwe do realizacji w przypadku danych masowych oraz szybko zmieniających się, a w dodatku obciążone sporym ryzykiem popełnienia błędów (nietrafnych ocen danych). Rozwiązania takich problemów oczekuje się od dalszego rozwoju narzędzia do kognitywnej/inteligentnej automatyzacji procesów.

Uczenie maszynowe zdecydowanie przyspieszyło też rozwój narzędzi komunikacji systemów z ludźmi przy użyciu języka naturalnego, w tym także narzędzi inteligentnych potrafiących rozumieć na podstawie ich kontekstu, a nawet intonacji, komunikaty niekoniecznie precyzyjnie sformułowane przez człowieka. Intensywnie rozwijane są też metody syntezy mowy, nawet w językach trudnych fonetycznie (np. takich, w których istotną rolę w zdaniu odgrywa tonalność: chiński, wietnamski). W rozwoju komunikacji w języku polskim (podobnie w innych językach nietonalnych) coraz istotniejsze jest nadanie mowie „maszynowej" jak najwięcej cech ludzkich, a więc wzbogacanie jej intonacją odpowiednią do kontekstu komunikatu.

Wraz z pojawieniem się w bankach „cyfrowych pracowników" coraz więcej uwagi poświęca się współpracy ludzi z robotami programowymi. Wyposażenie pracowników we wspierające ich roboty – wykonujące dla nich różne działania: zbieranie i przygotowywanie informacji ułatwiających podejmowanie decyzji – zasadniczo zwiększa wydajność pracowników, dlatego tak istotne jest nie tylko opracowywanie robotów, ale także uczenie pracowników, jak z nich korzystać w sposób najbardziej efektywny, zwłaszcza w sytuacjach i procesach nazywanych „Human-in-the-Loop". Są to przede wszystkim sytuacje wyjątkowe, nie obsługiwane w całości przez roboty i wymagające skutecznej interwencji człowieka potrafiącego skutecznie korzystać z ich pomocy.

Warto podkreślić, że według analityków Forrestera do końca 2021 r. 30% developerów będzie się posługiwać narzędziami i platformami Low-Code, zaś analitycy Gartnera prognozują, że w 2024 r. ok. 65% aplikacji stosowanych w gospodarce tworzonych będzie przy użyciu takich platform i narzędzi.

7.2. W kierunku zautomatyzowanego banku

Analitycy Deloitte w opracowaniu „2021 banking regulatory outlook"[15] zwracają uwagę na wpływ zmian trybu pracy instytucji finansowych w warunkach COVID-19. Sytuacja w wielu przypadkach ukazała w świetle dziennym niską sprawność i ukryte problemy systemów zastanych (*legacy*), wymuszając na bankach i firmach ubezpieczeniowych przyspieszenie cyfrowej transformacji, której nieodłącznym elementem są narzędzia RPA i ogólnie – rozwiązania hiperautomatyzacji. Zmiany odbywają się w sytuacji stałego naci-

15 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-2021-Regulatory_Outlook_Banking_FINAL.pdf

sku konkurencyjnego ze strony fintechów, dla których COVID-19 okazał się okolicznością bardzo korzystną, istotnie powiększając ich pole działania i tworzenia nowych rozwiązań.

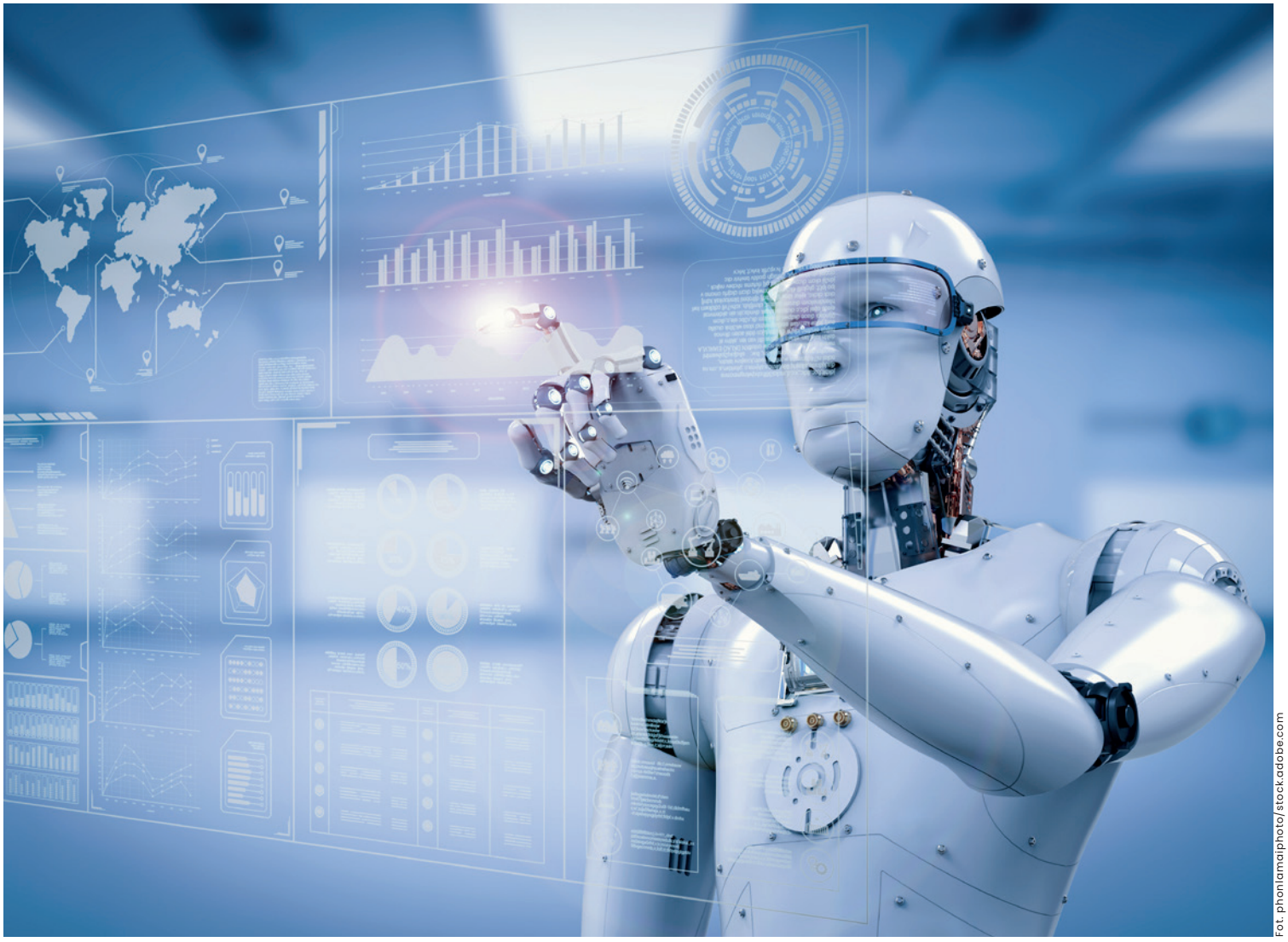
W sektorze finansowych coraz wyraźniejsza jest też obecność światowych gigantów technologicznych nazywanych BigTech, do których spośród firm amerykańskich zaliczane są Amazon, Apple, Faceboook, Google/Alphabet i Microsoft, a których konkurentem – także nastawionym na ekspansję na rynku usług finansowych – są wielkie chińskie firmy technologiczne – Baidu, Alibaba, Tencent i Xiaomi.

Wspomniane firmy technologiczne wraz z operatorami telekomunikacyjnymi oraz fintechami przyczyniły się w ostatnich latach do szybkiego rozwoju bankowości mobilnej. Operatorzy telekomunikacyjni (zwłaszcza telefonii mobilnej) zrezygnowali z prób angażowania się w działalność bankową, koncentrując się na zapewnianiu jak najszybszej, najpewniejszej i bezpiecznej łączności klientom usług finansowych oferowanych przez instytucje finansowe i fintechy. Warto przy tym zauważyć, że rozwój nowoczesnej bankowości mobilnej i innych usług płatności, ubezpieczeń itp., oferowanych w trybie mobilnym przyczynia się do kształtowania w świadomości klientów – zwłaszcza indywidualnych konsumentów i mikrofirm – obrazu „banku wirtualnego", z którym właściwie nie ma żadnego kontaktu poza tym realizowanym poprzez środki komunikacji elektronicznej. Taka „wirtualizacja" banku prowadzi do zmiany modelu działania całego sektora, który z punktu widzenia jego klientów przekształca się w usługę BaaS (*Banking-as-a-Service*). Realizować usługę BaaS może zarówno bank tradycyjny (nazywany już „zasiedziałym", a więc takim samym określeniem, jakie stosowano do operatorów telekomunikacyjnych wywodzących się z dawnych „operatorów narodowych"), jak i bank zautomatyzowany w tak dużym zakresie, w jakim tylko będzie to dozwolone przez regulacje sektora. Równie dobrze może to być konsorcjum firm – banków, fintechów czy firm technologicznych. W dodatku umożliwiane przez fintechy płatności peer-to-peer, bezpośrednio między klientami, powodują, że w ich oczach znika potrzeba istnienia banku – co dla sektora bankowego jest na pewno dużym wyzwaniem.

Obszarem, w którym hiperautomatyzacja bankowości odegrać może bardzo istotną rolę, a jednocześnie zachodzące w nim zjawiska będą akceleratorem wdrażania hiperautomatyzacji, jest zachodząca cyfryzacja i wirtualizacja pieniądza. Bez wdawania się w kwestie przyszłości kryptowalut i ich potencjalnej regulacji wystarczy obserwować rosnące zainteresowanie banków (w tym emisyjnych) wirtualizacją pieniądza. Wydaje się ona logicznym etapem w rozwoju form pieniądza od chwili jego pojawienia się w transakcjach – zamiast bezpośredniej wymiany towarowej – najpierw pieniądza kruszcowego, potem papierowego, a dziś elektronicznego. Na razie pieniądz elektroniczny jest reprezentacją pieniądza tradycyjnego zdeponowanego w bankach lub został wyemitowany na podstawie pieniądza tradycyjnego, ale można prognozować, że światowy sektor bankowy – a zwłaszcza banki centralne i emisyjne – wykorzystają w najbliższych latach niektóre metody „emisji" pieniądza wirtualnego, które pojawiły się kilka lat temu w kryptowalutach. Banki centralne i emisyjne starają się zresztą rozróżniać pieniądz wirtualny (nie akceptowany ani nie wspierany przez banki emisyjne, ale jako kryptowaluty akceptowany i wykorzystywany w transakcjach „pozabankowych", prywatnych) od wstępnych na razie definicji „cyfrowego pieniądza banku centralnego" (CBDC – *Central Bank Digital Currency*)[16].

Obserwując procesy przekształcania się banków w fintechy (poprzez wdrażanie innowacyjnych rozwiązań z obszaru hiperautomatyzacji), przekształcania się fintechów w banki (poprzez uzyskiwanie licencji bankowych), wchodzenia w obszar bankowości z własnymi przedsięwzięciami przez firmy BigTech oraz „wirtualizacji" banków i rozwoju modelu BaaS, można założyć, że wszystkie te zjawiska będą zachodziły równolegle, co będzie dużym wyzwaniem dla nadzoru regulacyjnego rynków finansowych. Dlatego można się spodziewać, że hiperautomatyzacji sektora bankowego i finansowego towarzyszyć będzie wspomniane w p. 6.1 wykorzystywanie w regulacjach sektorowych rozwiązań oferowanych przez firmy RegTech, a więc automatyzacja/robotyzacja organów regulacyjnych.

16 Europejski Bank Centralny, który w 2018 r. odrzucił możliwość wprowadzenia „cyfrowego euro", w lipcu 2021 r. wznowił analizy dotyczące emisji takiego pieniądza. Powołana w tym celu grupa robocza będzie prowadziła te analizy przez 24 miesiące. Wspólny pilotażowy projekt rozliczeń w CBDC prowadziły w 2021 r. Szwajcarski Bank Narodowy [niem. Schweizerische Nationalbank (SNB), fr. Banque Nationale Suisse (BNS), wł. Banca Nazionale Svizzera (BNS), romasz Banca Naziunala Svizra (BNS)] i Banque de France; zaś po eksperymentalnych rozliczeniach z wybranymi miastami wprowadzenie cyfrowego juana podczas Zimowych Igrzysk Olimpijskich w Pekinie w 2022 r. zapowiedział Bank Ludowy Chin – centralny bank ChRL.



Fot. phonlamaiphoto/stock.adobe.com

Robot wspomoże

Robotyzacja procesów biznesowych pozwoli nam pracować mniej. A także więcej wiedzieć o tym, na ile wiarygodni są klienci, z którymi pracujemy.

Fot. Comarch Finance

Paweł Kryszkiewicz
MENEDŻER PRODUKTU AML I KYC
COMARCH FINANCE

Zanim nawiążemy współpracę z klientem, musimy go zweryfikować. Zebrawszy dane o nim, okresowo musimy je aktualizować, a w przypadku podejrzenia o zaangażowanie klienta w działalność przestępczą – zweryfikować go jeszcze raz.

Weryfikacja odbywa się zazwyczaj na kilku poziomach. Od zebrania danych o danej osobie, weryfikacji autentyczności dokumentów, aż po upewnienie się, czy dana instytucja może i chce podjąć z taką osobą współpracę.

Dla przykładu – nie można otworzyć konta osobie, która jest notowana na jednej z setek list sankcyjnych. Takie listy posiadają poszczególne kraje, ma je też wiele instytucji międzynarodowych. Na mocy jednej z takich list, znaczna część rosyjskich oligarchów jest odcięta od systemu finansowego Unii Europejskiej.

Kto, co, czy...

Proces weryfikacji utrudnia fakt, że często istnieje kilka osób o tym samym imieniu i nazwisku. Dodatkowo, w bazach danych nie zawsze widnieje informacja o dacie urodzenia. Kolejna trudność dotyczy problemów z tłumaczeniem imion i nazwisk na inne języki. Imiona te bardzo często występują w kilku wariantach, co może doprowadzić do pominięcia właściwej osoby.

Weryfikacja nie ogranicza się do baz sankcyjnych, ale obejmuje wiele innych elementów, które mają odpowiedzieć na szereg pytań. Kilka najbardziej typowych to:

- Czy dokument, którym klient się posługuje nie został skradziony?
- Czy klient należy do grona PEP-ów (Politically Exposed Person)?
- Czy klient nie jest zaliczany do grona nierzetelnych kontrahentów oraz dłużników?
- W przypadku osoby prawnej, kim jest jej beneficjent rzeczywisty?

Poza analizą klienta za pomocą rządowych oraz komercyjnych baz danych, instytucje finansowe wspierają się informacjami dostępnymi w internecie. Tutaj, jeśli chodzi o prawidłową identyfikację, sytuacja jest jeszcze trudniejsza.

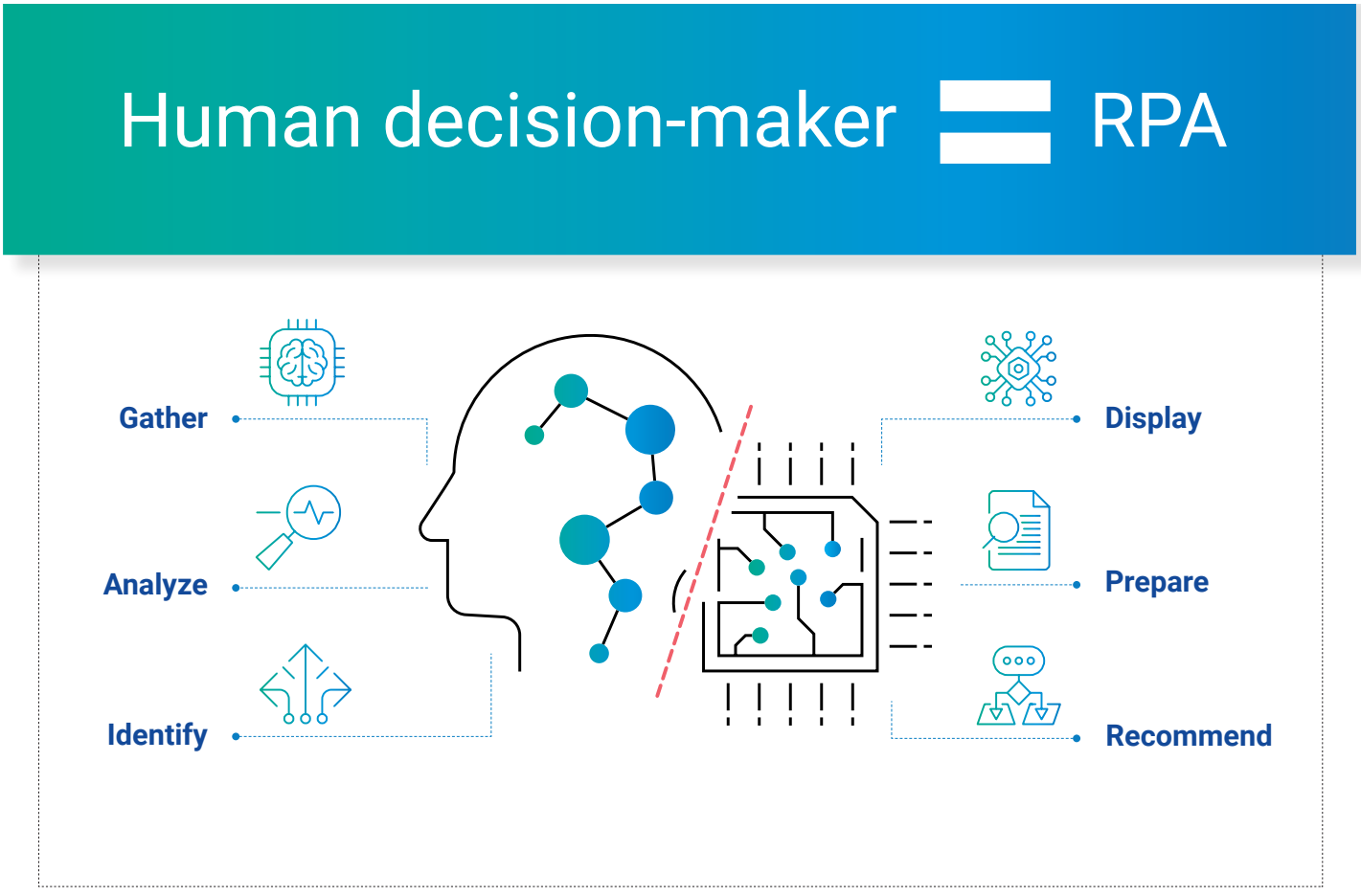
RPA na ratunek

Narzędzia klasy RPA (Robotic Process Automation) nadają się świetnie do automatyzowania standardowych czynności.

ZBIERAJ, TYLKO OSTROŻNIE

Podczas zawierania relacji z nowym klientem najwięcej czasu zajmuje zbieranie danych. Cały proces jest narażony na wiele błędów manualnych, takich jak literówki, źle skopiowane fragmenty tekstu lub braki w dokumentacji. W przypadku kontroli często wymaga się ponownej weryfikacji, a w najgorszym wypadku nakłada kary za jej nierzetelne przeprowadzenie.

Te i inne słabości systemu próbują wykorzystywać przestępcy – w celu nielegalnego wzbogacenia się lub legitymizacji zdobytych nielegalnie środków.



Source: AITE GROUP

Jeśli więc jesteśmy w stanie opisać je lub jasno określić, jak powinien zachowywać się system w przypadku uzyskania konkretnego wyniku, to warto rozważyć wykorzystanie takich narzędzi.

Robot potrzebuje jasnej instrukcji, według której będzie postępował za każdym razem. Wbrew obiegowym opiniom, narzędzia zbudowane w takiej technologii nie muszą się ograniczać tylko do zbierania danych, ale mogą pójść o krok dalej. Potrafią np. wskazać rozbieżności w danych z różnych źródeł. Są dokładniejsze, wielokrotnie szybsze niż człowiek i mniej podatne na generowanie błędów.

Po zebraniu danych kolejnym zadaniem dla RPA może być przygotowanie podsumowania i zaprezentowanie go. Ostatnią kwestią jest umożliwienie generowania rekomendacji przez system. Może on także, na podstawie odpowiedzi zwrotnej od użytkownika, poprawiać trafność swoich sugestii.

Ogromną przewagą systemów RPA jest ich prosta audytowalność, możliwość integracji oraz bezpieczeństwo – w przeciwieństwie do popularnych makr. Systemy te można także monitorować pod kątem działania, wydajności czy użytkowania przez różne osoby.

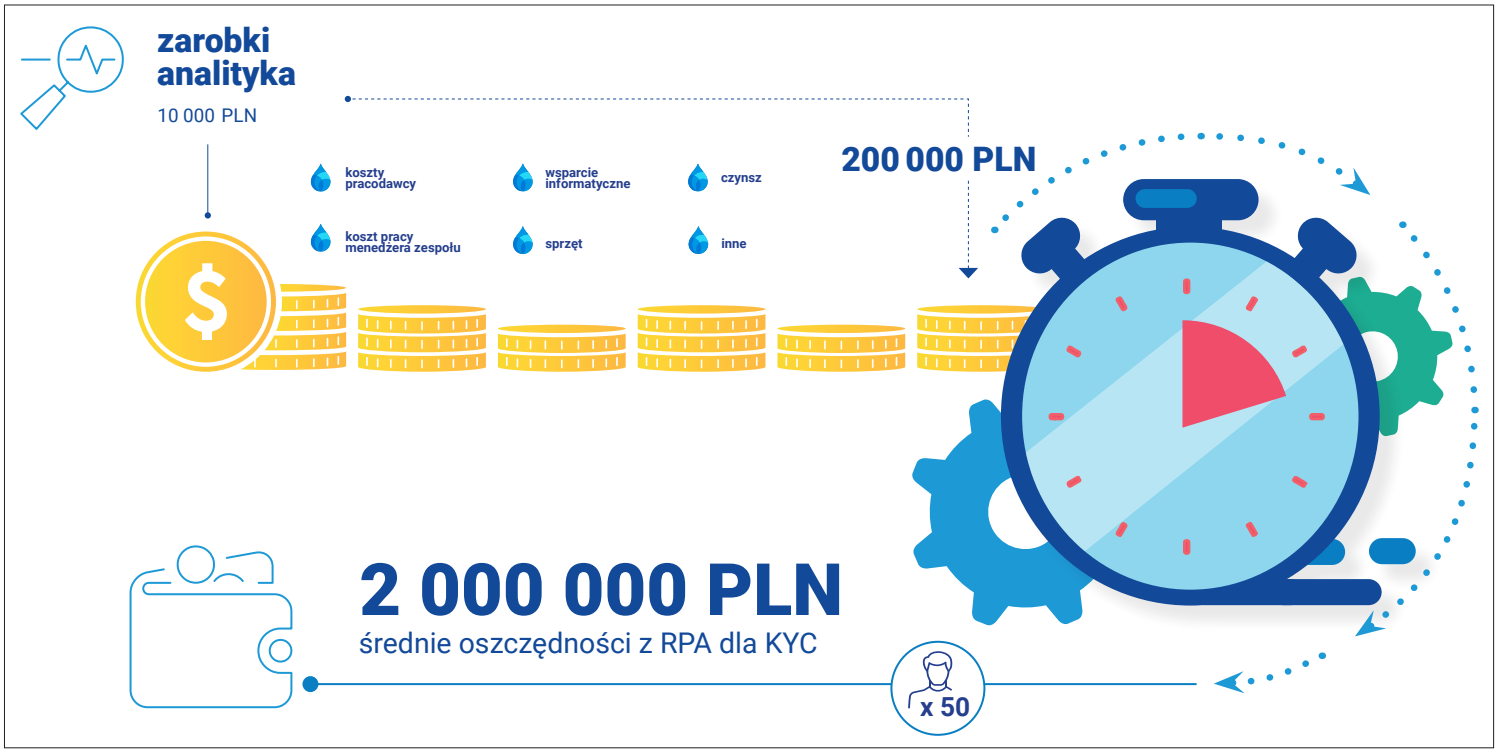
RPA NIE ZAWSZE WYSTARCZY

Działanie narzędzi RPA może znacznie wzbogacić sztuczna inteligencja. Może ona zostać wykorzystana do analizy tekstu ze stron internetowych z zaznaczeniem kluczowych treści, czy wygenerowania podsumowania tekstu. Albo do oceny, czy dana wypowiedź ma wydźwięk pozytywny, negatywny, czy neutralny. Najczęściej badane są wypowiedzi z mediów społecznościowych albo na forach internetowych, co również może być wartością przy analizie klienta. Sztuczna inteligencja może wreszcie przetwarzać informacje ze zdjęć i skanów dokumentów i automatycznie uzupełniać pola w systemach.

Tak przygotowany materiał trafia do finalnego raportu.

Gdzie wykorzystać RPA

Świetnym przykładem zastosowania technologii RPA jest automatyczne zbieranie danych z wielu rozproszonych źródeł. Istnieją firmy udzielające automatycznego dostępu do zbieranych przez siebie danych, a także części publicznych rejestrów. Jednak prawie nigdy nie jest to wystarczające na potrzeby konkretnej instytucji finansowej. Oznacza to, że instytucja ta nie posiada kompletu



informacji w jednym miejscu i jest zmuszona do zbierania brakujących danych z innych źródeł – już na własną rękę.

W takiej sytuacji można stworzyć narzędzie, które pobierze dodatkowe dane. W przypadku rejestrów sytuacja jest dosyć prosta, bo wiemy, w jakim polu powinna znaleźć się konkretna informacja oraz w jakiej formie zostanie zwrócony wynik naszego zapytania. Najprostsze integracje można wykonywać przy użyciu API. RPA potrafi jednak działać na „froncie", to znaczy uzupełniać formularze, w przypadku których prosta integracja nie zadziała.

Weryfikacja informacji w internecie również nie stanowi problemu, gdyż RPA może ocenić wiarygodność zebranych informacji oraz sortować je pod kątem tych najistotniejszych. Dodatkowo, również i w tym wypadku, informacja zwrotna od użytkownika może poprawiać zwracane wyniki.

> ***W działach zajmujących się pozyskiwaniem informacji odnotowuje się wysokie poziomy rotacji pracowników, a także niski poziom zadowolenia z pracy. Dzięki nowym technologiom możemy to zmienić, pozwalając pracownikom czerpać większą satysfakcję z tego, co robią, poprawiając ich efektywność i przynosząc oszczędności.***

Po zebraniu danych z wielu źródeł możemy zlecić narzędziu ich analizę, polegającą na wskazaniu różnic w zdobytych informacjach, określeniu informacji nigdzie nie potwierdzonych, jak też – na podstawie zdefiniowanych parametrów – przeliczać ryzyko dla danego klienta. Tu również jest bardzo duże pole do popisu pod dostosowanie na potrzeby danej instytucji.

Kluczową rolę odgrywa indywidualne podejście do ryzyka każdej z instytucji, wypracowane w oparciu o jej klientów, produkty, zakres działania etc. – stąd bardzo często proces weryfikacji klienta różni się znacząco między organizacjami.

Dzięki takiemu podejściu analityk, czy też inna osoba dokonująca weryfikacji klienta, dostaje podsumowanie wszystkich niezbędnych informacji, umożliwiających podjęcie decyzji, lub w przypadku dostrzeżenia ryzyk, ułatwiające sprawniejsze podjęcie dodatkowych działań.

Czy to się opłaca?

Załóżmy, że – dzięki automatyzacji wyszukiwania informacji – uda się usprawnić procesy o zaledwie 12 minut w każdej godzinie. Jeśli Dział AML/Fraud liczy pięćdziesięciu analityków, może to dawać **oszczędność nawet miliona USD** w skali roku.

Średnie zarobki analityka w krajach zachodnich wahają się między 40–50 tys. USD rocznie. Do tego należy doliczyć koszty pracodawcy, koszt pracy kierownika każdego zespołu, wyposażenie, czynsz, obsługę informatyczną i wiele innych. Bardzo szybko kwota rośnie do 100 tys. USD rocznie.

Jeśli doliczylibyśmy urlopy, zwolnienia chorobowe, czas przeznaczony na szkolenia czy spotkania zespołu, to zwrot z inwestycji jest jeszcze większy.

Oczywiście, nie każda instytucja ma tak duży zespół. W takiej sytuacji warto dokładnie policzyć, jak kształtować się będą wartości. Jeśli założylibyśmy, że uda się zautomatyzować o połowę procesy, to do takich oszczędności możemy dojść przy zaledwie dwudziestoosobowym zespole.

Oszczędności to nie jest jednak jedyne kryterium. Poprawa jakości czy usprawnienie procesu są również nie do przecenienia. Łącząc wszystkie te elementy, bardzo szybko można przekroczyć próg zwrotu z inwestycji.

A co z ludźmi?

Pomimo wielu zalet płynących z wykorzystania technologii RPA w usprawnianiu procesów opartych na danych ze źródeł rozproszonych, nie wydaje się, aby narzędzia te mogły w pełni zastąpić pracę ludzi. Ludzka inteligencja jest w stanie reagować na sytuacje wyjątkowe, które wcześniej nie zostały przewidziane w żaden sposób. Ponadto ludzie są potrzebni do budowania takich systemów na podstawie wiedzy i doświadczenia. Wiele badań nad wykorzystaniem technologii wskazało, że nowe technologie redukują miejsca pracy o niskiej wartości na rzecz prac specjalistycznych, gdzie ludzie przynoszą większe korzyści; tak indywidualnie, jak i dla gospodarki.

W działach zajmujących się pozyskiwaniem informacji odnotowuje się wysokie, przeszło trzydziestoprocentowe poziomy rotacji pracowników, a także niski poziom zadowolenia z wykonywanej pracy. Dzięki nowym technologiom możemy zmienić ten obraz, pozwalając pracownikom czerpać większą satysfakcję z tego, co robią, poprawiając ich efektywność i przynosząc oszczędności.

Brzmi jak fantastyka? Nie, jeśli wspomniane technologie będą odpowiadały na prawidłowo zdiagnozowane potrzeby konkretnej instytucji. **Płaćmy ludziom za myślenie, a robotom – za czas, w jakim wykonują swoje zadania.** •

Platforma PIVOTAL–WINDYKACJA sztuczna inteligencja wspierająca procesy zarządzania należnościami i wierzytelnościami

Zarządzanie należnościami wymaga stałego wyboru optymalnych kroków, dostosowanych do potrzeb wielu zróżnicowanych produktów i szukania strategii przynoszących najlepsze efekty w najkrótszym czasie. Musi uwzględniać zmieniające się ograniczenia formalno-prawne, procedury bankowe oraz indywidualne potrzeby klientów. W praktyce sprowadza się do umiejętnego gromadzenia i analizy ogromnych ilości danych i na ich podstawie wdrażania strategii windykacyjnych.

Tomasz Król
DYREKTOR ROZWOJU RYNKU
PIVOTAL POLSKA
E-MAIL: TKROL@PIVOTAL.PL

WIĘCEJ O PIVOTAL–WINDYKACJA:
HTTPS://PIVOTAL.PL/PL/WINDYKACJA/

Platforma PIVOTAL – WINDYKACJA efekt projektu wdrożeniowego realizowanego przez zespół Pivotal (Centrum Badawczo Rozwojowe Pivotal Polska), ekspertów zewnętrznych (wiodące instytucje badawcze) i instytucje finansowe.

Patrząc z perspektywy obecnych trendów, windykcja to obszar, w którym automatyzacja i wykorzystanie sztucznej inteligencji mają ogromne znaczenie, a ich wdrożenie wydaje się kluczowe dla utrzymania rentowności i wzrostu efektywności procesów. Zarządzanie należnościami bez wsparcia technologii w przyszłości wydaje się trudne, a na pewno bardziej ryzykowne i mniej efektywne.

Big data i machine learning w windykacji postcovidowej

Technologie wspierające procesy zarządzania wierzytelnościami zyskują szczególne znaczenie w nowej, postcowidowej rzeczywistości. Pandemia wpłynęła na pogorszenie sytuacji finansowej firm i klientów indywidualnych. Instytucje finansowe odczuwają znaczny wzrost ilości spraw dotyczących problemów ze spłatą należności i postępowań windykacyjnych. W praktyce oznacza to więcej danych do weryfikacji, więcej procesów do wykonania oraz większe ryzyko błędu i w konsekwencji straty. Dodatkowym utrudnieniem jest wzrost luki pokoleniowej i związany z tym brak specjalistów na rynku pracy. Automatyzacja standardowych zadań, wykorzystanie modeli predykcyjnych do wdrażania strategii naprawczych bez udziału człowieka i wydajna analiza przyrastających baz danych może realnie rozwiązać problem.

Platforma PIVOTAL–WINDYKACJA jest przykładem efektywnego wykorzystania big data i **machine learning** do modelowania, testowania i wdrażania zautomatyzowanych strategii windykacyjnych. Umożliwia standardowe podejście bazujące na dwóch zmiennych: typ produktu i typ klienta. Daje również możliwość rozszerzenia perspektywy i generowania wielopoziomowych podscenariuszy, dostosowanych do indywidualnych wymogów danej sprawy, rodzaju produktu i powstałego zadłużenia oraz aktualnej sytuacji klienta. Eksploracja danych umożliwia definiowanie uogólnionych reguł i wiedzy zawartej w bazach historycznych banków i innych instytucji finansowych, definiowania współzależności, tendencji za pomocą technik statystycznych, matematycznych i rozpoznawania prawidłowości. Umożliwia również koncentrację na kliencie, jego potrzebach i problemach w kontekście spłat należności. Ułatwia prewencję przeterminowania spłat zobowiązań finansowych, a jeżeli już nastąpią, minimalizuje ich negatywne skutki dla klienta i instytucji finansowej (koszty windykacji twardej).

Wielopoziomowe profilowanie klientów i produktów

MODELE KLASYFIKACYJNE

Pierwszym krokiem do tworzenia skutecznych strategii windykacyjnych jest właściwa ewaluacja gromadzonych danych. Platforma PIVOTAL–WINDYAKCJA wykorzystuje modele predykcyjne do **tworzenia klas: klientów i produktów**, definiowania ich atrybutów i poszukiwania zależności między nimi. Pozwala również na analizowanie zachowań i definiowanie możliwych **predykcji behawioralnych** dłużników w określonych okolicznościach. Pracownik obsługujący daną sprawę, może na tej podstawie ustalić optymalne kroki w procesie windykacji, preferowane przez klienta, najskuteczniejsze formy komunikacji lub strategie zapobiegające pojawieniu się zadłużenia, ułatwiające jego spłatę czy przeprowadzenia sprawnej restrukturyzacji itp.

Modele klasyfikacyjne pozwalają zautomatyzować najbardziej pracochłonny etap analizy danych, nie wykluczają jednak udziału człowieka w procesie. Pracownik instytucji finansowej jest

niezbędny, nadaje wskazanym przez algorytmy sztucznej inteligencji klasom etykiety biznesowe, definiuje je i określa przypisane im kroki dotyczące zarówno monitoringu należności, jak i procedur windykacyjnych. Może dowolnie modyfikować strategie windykacyjne i wdrażać je automatycznie lub inicjować manualnie. Platforma umożliwia ich stały rozwój i dostosowanie do nowych, zidentyfikowanych potrzeb lub często zmieniających się wymagań formalno-prawnych dotyczących instytucji finansowych oraz sprzedaży i obsługi produktów finansowych.

Modele predykcyjne zaimplementowane do platformy PIVOTAL–WINDYKACJA umożliwiają również **testowanie i prototypowanie nowych strategii windykacyjnych**. Ułatwiają generowanie **scenariuszy what-if** na podstawie danych historycznych i wstępne oszacowanie prawdopodobieństwa ich skuteczności. Funkcja celu może być dostosowana do wymagań użytkownika platformy, inna dla banków, a inna dla firm windykacyjnych – uwzględniająca cele biznesowe i KPI finansowe.

Dodatkową weryfikację wstępnych założeń umożliwia zaimplementowany do platformy moduł **Champion Challenger**. Pozwala na testowanie na wskazanych danych klienta i dokładne typowanie optymalnych kroków i najlepszych strategii windykacyjnych dla konkretnego produktu czy grupy produktów, jednego lub wielu zdefiniowanych klientów. Zanim strategia zostanie wdrożona, zweryfikowana zostaje jej skuteczność i określone prawdopodobieństwo sukcesu wdrożenia. Champion Challenger daje również możliwość **elastycznego podejścia do zarządzania należnościami** i wierzytelnościami, **szybką odpowiedź na zmieniające się wymagania rynku.**

Wsparcie decyzyjne – kolejki spraw

MODELE SCORINGOWE

Ogromne ilości danych generowane podczas monitorowania stanu spłat należności klientów oraz aktywnych procesów windykacyjnych wymagają priorytetyzacji. Modele klasyfikacyjne ułatwiają ich wstępne klastrowanie, kolejny krok to ustalenie kolejki działań w zależności od aktualnej sytuacji klienta, poziomu zadłużenia. Działania te automatyzują **modele scoringowe**. Każdego dnia działy operacyjne (call center, zespoły windykacyjne itp.) otrzymują **rekomendację kolejki działań** do wykonania, od najpilniejszych wymagających natychmiastowego wdrożenia (wymogi wynikające z: procedur banku, przepisów prawa, strategii minimalizacji ryzyka itp.), po mniej priorytetowe. Kolejki są automatycznie aktualizowane na podstawie stale weryfikowanych danych dotyczących klientów i ich portfela produktów. Modele scoringowe ułatwiają zarządzanie procesami windykacyjnymi. Pozwalają na efektywny podział zadań między pracownikami i skracają czas potrzebny na żmudne analizy, dając możliwość skoncentrowania się na działaniach operacyjnych.

Generowanie optymalnych scenariuszy

MODELE NEXT BEST ACTION

Każda sprawa windykacyjna może mieć kilka możliwych scenariuszy. Kolejne kroki, czas ich wdrożenia i rodzaj zastosowanych narzędzi może być wytypowany przez modele predykcyjne określane w platformie PIVOTAL–WINDYKACJA jako **next best action**. Uwzględniając zdefiniowane atrybuty danego klienta czy

> *Platforma PIVOTAL – WINDYKACJA opracowana została zgodnie z CRISP-DM (Cross-Industry Standard Process for Data Mining). To kluczowa metodologia wspierająca wdrażanie rozwiązań data mining. Uławia eksplorację wielomilionowych repozytoriów danych i prace projektowe w nowym, zmiennym środowisku. Pozwala optymalizować ich efekty poprzez działania w obrębie struktury kilku kroków i jednocześnie zwinnie reagować na ich przebieg i zmiany (iteracja).*

też produktu oraz priorytet wykonania danej sprawy windykacyjnej, system może zarekomendować dedykowane strategie naprawcze i oszacować ich skuteczność. Zespoły operacyjne otrzymują pełen obraz możliwych, rekomendowanych działań. Wskazane scenariusze windykacyjne mogą być wdrażane zarówno automatycznie, jak i manualnie, pod pełną kontrolą użytkowników platformy. Modele predykcyjne next best action pełnią role augmented intelligence (inteligencja rozszerzona), wsparcia strategii generowanych metodą ekspercką. Ułatwiają człowiekowi analizę często wielomilionowych repozytoriów danych windykacyjnych i dają rekomendacje ułatwiające podejmowanie i wdrażanie najskuteczniejszych działań. Poprawiają efektywność procesów windykacyjnych i minimalizują straty, zwłaszcza na poziomie windykacji twardej.

HIPERPERSONALIZACJA i AUTOMATYZACJA obsługi nowego klienta postcovidowego

Dobrze zaprojektowane i zoptymalizowane podczas testów modele predykcyjne ułatwiają nie tylko realizację procesów windykacyjnych, ale również wsparcie nowego klienta postcovidowego. Zawirowania związane z pandemią dały impuls do przyspieszonej cyfryzacji wszystkich obszarów gospodarki. Mocno wpłynęły również na branżę finansową i zaowocowały zmianą dotychczasowych przyzwyczajeń i wymagań klientów. Kanały elektroniczne otworzyły ogólny dostęp do wielu niszy rynków finansowych dla konkurencji, w tym również firm spoza sektora bankowego. Klienci zmuszeni do korzystania z nowych kanałów nie tylko przenieśli tutaj swoją aktywność, ale też zmienili preferencje. Chętnie testują ofertę on-line, chętnie zmieniają dostawcę produktów finansowych i oczekują nie tylko odpowiedzi na zgłaszane potrzeby, ale również ich wyprzedzanie. Takie podejście dotyczy również działań związanych z monitoringiem należności oraz realizacją procedur windykacyjnych. **Empatyzacja potrzeb**, **dostosowanie rozwiązań i komfort** świadczonych usług przy jednoczesnej **gwarancji bezpieczeństwa** to priorytety nowego klienta postcovidowego. Odpowiedź na nie ułatwia cyfryzacja i automatyzacja procesów oraz stałe modyfikowanie strategii dotyczących zarówno prewencji pojawienia się zadłużenia, jak i najszybszego rozwiązywania spraw windykacyjnych klientów.

Algorytmy sztucznej inteligencji zastosowane w platformie PIVOTAL–WINDYKACJA dają odpowiedź na te wymagania. Pozwalają na **hiperpersonalizację działań**: dostosowanie ich do rodzaju klienta i posiadanych przez niego produktów. Uwzględniają jego preferencje dotyczące kanałów i sposobu komunikacji (sms, mail, list), aktualny stan finansów, możliwości zaciągania i spłaty nowych zobowiązań, statusu materialnego rodziny, stanu zdrowia. Umożliwia to proponowanie produktów finansowych dostosowanych do możliwości i minimalizowanie ryzyka zadłużenia, monitorowanie sytuacji, zmiany w czasie i dbanie o bezpieczeństwo. KOMFORT: elastyczna obsługa, ułatwia również automatyzację obsługi klienta na poziomie front office i back office i stały dostęp do informacji (obsługa 24 h). •

Fot. sarayut_sy/stock.adobe.com

Większy poziom cyberbezpieczeństwa dzięki zintegrowanym i zautomatyzowanym rozwiązaniom ochronnym

Rozwój gospodarki bazującej na usługach świadczonych online, tempo wprowadzania cyfrowych innowacji czy postępująca modernizacja infrastruktury IT sprawiły, że sieci współczesnych przedsiębiorstw stały się złożone i rozległe jak nigdy przedtem. Procesy te sprawiają, że brzeg tradycyjnych sieci ciągle się rozszerza, przybywa tym samym nowych obszarów, które powinny zostać objęte ochroną.

Fot. Fortinet

Wojciech Ciesielski
MAJOR ACCOUNTS MANAGER
FORTINET
EMAIL: WCIESIELSKI@FORTINET.COM

W efekcie dostawcy usług i urządzeń ochronnych mogą napotkać trudności związane z zabezpieczaniem całej infrastruktury informatycznej swoich klientów. Z pomocą przychodzą kompleksowe rozwiązania cyberbezpieczeństwa, które w ramach jednolitej architektury integrują narzędzia do ochrony całego środowiska IT. Ważną rolę odgrywają tu zaawansowana sztuczna inteligencja oraz uczenie maszynowe. Wykorzystujące je narzędzia pomagają rozwijać automatyzację procesów zabezpieczających i zwiększają poziom ochrony zasobów IT w firmach, a jednocześnie wspierają analityków, ograniczając ryzyko wystąpienia błędu ludzkiego.

Wielość narzędzi ochronnych

Sieci w przedsiębiorstwach są w coraz większym stopniu używane do obsługi aplikacji o krytycznym znaczeniu dla biznesu. Są wśród nich m.in. wszelkie narzędzia służące do prowadzenia transakcji online, zapewniania łączności z pracownikami wykonującymi obowiązki zdalnie, czy gromadzenia i przetwarzania kluczowych danych. Tempo cyfrowej transformacji sprawiło, że przedsiębiorstwa nie zawsze miały czas, aby wdrażać takie rozwiązania ochronne, które całościowo pokryłyby ich potrzeby doty-

czące bezpieczeństwa. W rezultacie odpowiedzialne za ten obszar zespoły IT często muszą zarządzać ogromną „kolekcją" narzędzi ochronnych pochodzących od różnych dostawców, a jednocześnie utrzymywać odpowiednio wysoki poziom widzialności całej infrastruktury sieciowej.

Sytuacji nie ułatwia rozwój środowiska pracy zdalnej, jaki gwałtownie dokonuje się na przestrzeni ostatnich kilkunastu miesięcy. Pracownicy, którzy wykonują swoje obowiązki z domu, potrzebują dostępu do zasobów firmowych o takiej samej jakości jak ci, którzy mają do nich dostęp z biura. Aby zabezpieczyć to środowisko, przedsiębiorstwa często sięgają po rozwiązania fragmentaryczne, zaprojektowane do ochrony tylko określonego segmentu sieci. Fakt ten został podkreślony w badaniu IBM z 2020 r.[1], które wykazało, że firmy korzystają średnio z około 45 różnych rozwiązań zabezpieczających, zaś do przeciwdziałania skutkom incydentu wymagana była skoordynowana obsługa 19 z nich.

Wszystko to dzieje się w sytuacji, gdy cyberprzestępcy stale poszukują nowych sposobów na ominięcie zabezpieczeń i przedostanie się do sieci ofiary. Ich ataki stają się coraz bardziej wyrafinowane – mają na celu jednoczesne przeniknięcie do różnych obszarów sieci, aby ukryć zastosowane metody i zidentyfikować najłatwiejsze do naruszenia ogniwo w łańcuchu bezpieczeństwa. Rozproszone w różnych miejscach sieci i odizolowane od siebie produkty wdrażane punktowo nie są w stanie rozpoznać tych zagrożeń ani się przed nimi bronić.

Podsumowując, w wielu przedsiębiorstwach zaistniała sytuacja, w której zespoły ds. cyberbezpieczeństwa zmagają się z wykrywaniem coraz bardziej wyrafinowanych i szkodliwych cyberataków, a w tym celu korzystają ze złożonego i w dużej mierze odizolowanego od siebie zestawu narzędzi ochronnych. W sytuacji, gdy personel i tak jest już przeciążony monitorowaniem ruchu w sieci i innymi obowiązkami, może to doprowadzić do powstawania luk w zabezpieczeniach, które cyberprzestępcy wykorzystają do uzyskania nieautoryzowanego dostępu do sieci. Może on skutkować kradzieżą danych, pieniędzy lub kosztownym przestojem w działalności firmy, a w dalszej konsekwencji – problemami prawnymi i wizerunkowymi.

Potrzeba zintegrowanej ochrony

Aby przedsiębiorstwa mogły skutecznie wdrażać zabezpieczenia, muszą mieć zapewnioną szeroką widzialność swojej sieci i kontrolę nad nią. Pierwszym krokiem na drodze do osiągnięcia tego celu jest uproszczenie infrastruktury. Dopiero wtedy możliwe jest wprowadzenie zaawansowanej analityki, badanie korelacji zagrożeń i reagowanie na nie. Przedstawiciele przedsiębiorstw zaczynają rozumieć logistyczne i techniczne wyzwania związane ze złożonością środowisk sieciowych. Z reguły są zainteresowani przejściem od korzystania z usług dziesiątek różnych dostawców i podobnej liczby produktów ochronnych do kilku lub kilkunastu platform zabezpieczających, uzupełnionych w razie potrzeby o produkty wdrażane punktowo.

Chociaż coraz więcej firm stosuje tego rodzaju podejście, to administratorzy wielu platform nadal skupiają się na pojedynczych, odseparowanych od siebie elementach zabezpieczających. Przedstawiciele firm powinni brać pod uwagę, czy rozwiązanie, które zamierzają wdrożyć, rzeczywiście zapewnia kompleksową ochronę całej infrastruktury IT: sieci, urządzeń końcowych i chmury. Odpowiednio dobrana do potrzeb przedsiębiorstwa platforma zabezpieczająca ułatwia skuteczne wdrażanie poszczególnych narzędzi oraz wygodne zarządzanie nimi.

> ***Sieci w przedsiębiorstwach są w coraz większym stopniu używane do obsługi aplikacji o krytycznym znaczeniu dla biznesu. Są wśród nich m.in. narzędzia służące do prowadzenia transakcji online, zapewniania łączności z pracownikami wykonującymi obowiązki zdalnie, czy gromadzenia i przetwarzania kluczowych danych.***

Tego rodzaju podejście pomoże poprawić wydajność infrastruktury ochronnej oraz zapewni niezbędną w obecnych czasach automatyzację procesów, bazującą na zaawansowanej sztucznej inteligencji oraz uczeniu maszynowym. Należy podkreślić, że we współczesnej rzeczywistości oba te mechanizmy są ważniejsze niż kiedykolwiek wcześniej. W konfrontacji z coraz bardziej złożonymi atakami ludzie nie są w stanie reagować wystarczająco szybko i skutecznie. Systemy bazujące na AI oraz ML, często wbudowane w zintegrowane platformy ochronne, zapewniają identyfikację złośliwych narzędzi, ich analizę i reagowanie na nie w czasie rzeczywistym, co pozwala zminimalizować ryzyko wystąpienia incydentu naruszenia bezpieczeństwa sieci.

1 https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue


Fot. Ton Foria/stock.adobe.com

Najważniejsze zasady i praktyki kompleksowego podejścia do bezpieczeństwa

1. Ujednolicona struktura ochronna jest niezbędna do ustanowienia kontroli nad siecią i utrzymywania jej. Musi być w stanie objąć całą rozproszoną i wciąż rozbudowywaną sieć, aby skutecznie wykrywać zagrożenia, prowadzić korelację danych i egzekwować zasady wynikające z polityki bezpieczeństwa. Nie chodzi tu wyłącznie o wybór jednego dostawcy usług, ale raczej o wybór właściwych dostawców. Priorytetowo należy traktować tych, którzy wykorzystują interfejsy programowania aplikacji (API) i przestrzegają standardów dotyczących wspierania interoperacyjności.

2. Wdrożone rozwiązania muszą również mieć dostęp do wspólnych zbiorów danych. Dotyczy to brzegu sieci, urządzeń końcowych i chmury, wzbogaconych o globalne dane wywiadowcze dotyczące zagrożeń. Umożliwia to całościowe analizy stanu bezpieczeństwa sieci i jej wydajności, pomaga identyfikować pojawiające się zagrożenia oraz ułatwia wdrożenie ujednoliconego systemu reagowania w całej firmie.

3. Zintegrowane komponenty bezpieczeństwa muszą zapewniać przeprowadzenie zaawansowanej analizy danych. Powinna być ona połączona z możliwością automatycznego tworzenia nowych reguł reagowania, gdy w trakcie analizy sieci wykryte zostaną nieznane dotąd zagrożenia. System ten powinien funkcjonować autonomicznie w prostszych środowiskach i być połączony z rozwiązaniami służącymi do rozszerzonego wykrywania incydentów i reagowania na nie (XDR), zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) oraz orkiestracji, automatyzacji i reagowania (SOAR) dla coraz bardziej zaawansowanych środowisk centrum operacji sieciowych (NOC) i centrum operacji bezpieczeństwa (SOC).

4. Struktura ochronna musi być w stanie szybko uruchomić skoordynowaną reakcję na zagrożenia w całym ekosystemie w momencie ich wykrycia. Przerywa to sekwencję ataku, jeszcze zanim jego cele zostaną zrealizowane. Wykorzystanie uczenia maszynowego i sztucznej inteligencji sprawia, że jest to możliwe bez spowolnienia pracy infrastruktury i popełniania błędów ludzkich.

5. Ponieważ zmiana jest jedyną stałą w dzisiejszym cyfrowym świecie, struktura zabezpieczeń musi być dynamiczna. Oznacza to, że musi być zapewniona jej skalowalność, w miarę rozwoju chronionej przez nią sieci. Wymaga to głębokiej integracji między zabezpieczeniami a komponentami i funkcjami sieciowymi. Dzięki temu przedsiębiorstwa będą mogły wprowadzać innowacje oraz rozszerzać ekosystemy sieciowe i operacyjne bez opóźnień skutkujących powstawaniem luk w zabezpieczeniach.

Proaktywne podejście do bezpieczeństwa wymaga wykorzystania sztucznej inteligencji i automatyzacji

Sieci stają się coraz bardziej złożone i rozproszone, rośnie też liczba środowisk brzegowych, z których wiele w znacznej mierze funkcjonuje autonomicznie. To powoduje brak wglądu w różne elementy działające w obrębie sieci, a w efekcie brak kontroli nad nimi, co może przekładać się na powstawanie luk w zabezpieczeniach. Co więcej, większość firm boryka się z brakiem specjalistów, którzy mogliby stawić czoła temu wyzwaniu.

Wcześniej cyberataki przebiegały z szybkością ograniczoną przez możliwości człowieka do ich manualnego przeprowadzenia. Stwarzało to realną szansę na wykrycie złośliwego oprogramowania, zanim spowodowało ono poważne szkody. Obecnie cyberprzestępcy wykorzystują innowacje cyfrowe, w tym narzędzia automatyzujące, coraz częściej bazujące na sztucznej inteligencji. Pozwala im to na szybkie tworzenie bardziej wyrafinowanych, wielowektorowych ataków, które są przeprowadzane z prędkością działania maszyn. Umożliwia im to np. aktywne lokalizowanie i wykorzystywanie wielu luk w zabezpieczeniach w jednym czasie, przy jednoczesnym unikaniu wykrycia.

W miarę jak cyberprzestępcy wdrażają zautomatyzowane metody rozpowszechniania złośliwego oprogramowania, członkowie zespołów ds. bezpieczeństwa (oraz stosowane przez nich starsze rozwiązania ochronne) mogą zostać przytłoczeni dużą skalą incydentów i alarmów, które wymagają korelacji i zbadania. Nie ma możliwości, aby skutecznie bronić się przed takimi atakami za pomocą odizolowanych narzędzi ochronnych czy ręcznego reagowania na alarmy.

W rezultacie wiele obserwowanych obecnie przypadków naruszeń bezpieczeństwa IT jest konsekwencją błędu człowieka, niezależnie od tego, czy dotyczył on złej konfiguracji urządzenia,

czy też przeoczenia alarmu. Często jest to po prostu wynik przepracowania specjalistów IT. Nawet najbardziej wykwalifikowani i kierujący się najlepszymi intencjami mogą czasami popełniać błędy, które ostatecznie okazują się niezwykle kosztowne. Z cyberprzestępcami należy walczyć, wykorzystując tę samą broń, z jakiej korzystają i oni. Dzięki automatyzacji procesów i wdrożeniu narzędzi wykorzystujących sztuczną inteligencję, znacznie łatwiej jest identyfikować zagrożenia, usprawniać przepływy pracy oraz spójnie i skutecznie reagować. Zmniejszają one prawdopodobieństwo popełnienia błędu przez człowieka, gdyż eliminują konieczność ręcznego wykonywania zadań.

FortiXDR – od identyfikacji po neutralizację ataku

Mechanizm rozszerzonego wykrywania zagrożeń i reagowania na nie (eXtended Detection and Response, XDR) jest naturalnym rozwinięciem analogicznej koncepcji dedykowanej wyłącznie do urządzeń końcowych (Endpoint Detection and Response, EDR). W obu przypadkach wykrycie podejrzanego kodu inicjuje procedurę jego dalszego badania pod kątem potencjalnie złośliwych lub ryzykownych działań, które wymagają neutralizacji. Pojawia się jednak wyzwanie związane bezpośrednio z podejmowanymi dziś cyberatakami, które polega na tym, że wiele rozwiązań EDR oraz XDR nadal nie jest w stanie prowadzić w pełni zautomatyzowanego rozpoznania, którego skutkiem byłoby szybsze wykrywanie zagrożeń i reagowanie na nie w szerszym zakresie. Poprawę sytuacji firm w zakresie cyberochrony, ale też zmniejszenie obciążenia pracą specjalistów ds. bezpieczeństwa, może zapewnić tylko zastosowanie sztucznej inteligencji.

Rozwiązaniem, które jako pierwsze pozwala na zastosowanie zaawansowanej sztucznej inteligencji (AI) do badania wykrytych zagrożeń, jest stworzony przez Fortinet FortiXDR. Wykorzystuje ono także wiedzę o zagrożeniach zgromadzoną przez FortiGuard Labs. FortiXDR może całkowicie wyręczyć analityków i zautomatyzować procesy ochronne. Dzięki temu jest w stanie szybciej zneutralizować cyberzagrożenia. Jest też niezwykle istotnym elementem architektury Fortinet Security Fabric, działającej w szerokim zakresie, zintegrowanej i zautomatyzowanej platformy bezpieczeństwa, która obejmuje całą infrastrukturę IT przedsiębiorstwa – od urządzeń końcowych i należących do kategorii IoT, przez środowisko sieciowe, po chmurę. Bazuje ona na wspólnej strukturze danych, skorelowanej telemetrii oraz jest kompatybilna z portfolio rozwiązań Fortinet, a także rozwiązaniami firm trzecich, na bazie gotowych adapterów i interfejsu API.

W FortiXDR znalazł zastosowanie mechanizm sztucznej inteligencji, zapewniany przez silnik Dynamic Control Flow Engine. Jest on nieustannie „trenowany" za pomocą danych o zagrożeniach dostarczanych przez FortiGuard Labs, a także rozbudowywany na podstawie doświadczenia ekspertów reagujących na incydenty i analizujących je. W pierwszej fazie działania FortiXDR wykorzystuje informacje udostępniane w ramach Fortinet Security Fabric do korelacji i analizy incydentów bezpieczeństwa, aby wykryć, czy rzeczywiście zaistniała próba przeprowadzenia cyberataku. W kolejnym kroku mechanizm sztucznej inteligencji prowadzi badanie w kierunku ostatecznego sklasyfikowania i oceny skali potencjalnego zagrożenia. Ostatni etap polega na zdefiniowaniu najwłaściwszych metod reagowania na zagrożenie, które mogą być automatycznie uruchomione w celu jego szybkiej neutralizacji. Wszystkie wyżej opisane działania odbywają się w czasie zaledwie kilku sekund. Znakomicie uwidacznia to, na jaką skalę FortiXDR jest w stanie odciążyć analityków, a jednocześnie wyeliminować ryzyko wystąpienia ludzkiego błędu jako przyczyny naruszenia bezpieczeństwa. Należy podkreślić, że jest to rozwiązanie, które mogą wdrożyć u siebie przedsiębiorstwa każdej skali. Polecane jest szczególnie tym, które nie posiadają rozbudowanego zespołu ekspertów, a także nie mają odpowiednich narzędzi ochronnych czy procedur.

Najważniejsze korzyści wynikające z użytkowania FortiXDR

Użytkownicy rozwiązania oferowanego przez Fortinet wskazują, że przede wszystkim pozwala ono znacząco zmniejszyć liczbę alarmów wymagających zbadania, a jednocześnie daje gwarancję, że cyberataki nie zostaną przeoczone. Wszystkie te czynniki sprawiają, że firmy są w stanie skrócić średni czas wykrycia incydentu (*Mean Time To Detection*, MTTD), oraz średni czas reakcji na niego (*Mean Time To Response*, MTTR). Dzięki temu są w stanie zminimalizować wpływ cyberataków na swoją działalność i zachowanie ciągłości biznesowej, a jednocześnie poprawić skuteczność operacji ochronnych oraz wydajność i ogólny stan bezpieczeństwa IT.

Dodatkowo eksperci, którzy wcześniej poświęcali wiele czasu na analizę zagrożeń dotyczących środowiska IT, mogą bardziej skupić się na sprawach strategicznych w kontekście całej firmy. Pomaga to też przedsiębiorstwu skutecznie konkurować na rynku, a jednocześnie, dzięki konsolidacji funkcji obecnych dotychczas w różnych rozwiązaniach, rozwiązuje wcześniej omawiane problemy związane ze wzrostem liczby dostawców narzędzi bezpieczeństwa.

FortiXDR w akcji – najważniejsze przykłady zastosowania

Poniżej prezentujemy kilka reprezentatywnych przykładów podejrzanych zachowań, które uruchamiają „śledztwo" prowadzone przez narzędzia bazujące na sztucznej inteligencji. W wielu

przypadkach są to zachowania, które mogły zostać zablokowane przez istniejące mechanizmy kontroli bezpieczeństwa i ukryte wśród innych informacji o potencjalnych zagrożeniach w logach, pulpitach nawigacyjnych lub alertach.

Nieudane próby logowania. Użytkownicy często zapominają lub błędnie wpisują dane uwierzytelniające, co sprawia, że powtarzające się nieudane próby logowania są powszechnym zjawiskiem. Jednak powtarzające się próby logowania mogą być również związane z atakami typu *brute force* i wymagają dalszej analizy. FortiXDR został przeszkolony do wykrywania takich zdarzeń zgłaszanych przez zapory sieciowe FortiGate, narzędzia uwierzytelniające lub monitorowane urządzenia końcowe. Następnie sprawdza liczbę takich błędnych prób i ich cechy (wraz z adresami IP), później zaś koreluje udane połączenia z usługą weryfikacji tożsamości, jak np. Active Directory. Pozwala to m.in. wykryć anomalie, takie jak niemożliwe do odbycia podróże (biorąc pod uwagę niespójności związane z różnymi strefami czasowymi, w których przebywa logująca się osoba). Jeśli na bazie tej korelacji można wysnuć dowód, że podmiot stanowiący zagrożenie z powodzeniem wprowadził dane uwierzytelniające podczas ataku *brute force*, uruchamiana jest wcześniej zdefiniowana reakcja – od prostego powiadomienia o incydencie, aż po wygaśnięcie danych uwierzytelniających, wymuszone wylogowanie i zresetowanie uprawnień użytkownika.

> ***Dzięki automatyzacji procesów i wdrożeniu narzędzi wykorzystujących AI, znacznie łatwiej jest identyfikować zagrożenia, usprawniać przepływy pracy oraz spójne i skuteczne reagować. Zmniejszają one prawdopodobieństwo popełnienia błędu przez człowieka, gdyż eliminują konieczność ręcznego wykonywania zadań.***

Potencjalny atak phishingowy. Poczta elektroniczna wciąż pozostaje głównym wektorem ataków, a jedno nieopatrzne kliknięcie w złośliwy link z phishingowej wiadomości może mieć poważny wpływ na losy przedsiębiorstwa. W idealnej sytuacji zespoły ds. bezpieczeństwa powinny analizować każdą próbę ataku z wykorzystaniem e-maila (łącznie z tymi, które zostały zablokowane), ale zazwyczaj nie jest to możliwe z uwagi na liczbę takich prób, jakich przeciętna firma doświadcza w ciągu dnia. FortiXDR jest w stanie zastosować rozszerzoną analitykę do każdej wiadomości e-mail oraz do logów bezpieczeństwa sieciowego, aby zidentyfikować te, które zawierają adresy URL prowadzące do złośliwego kodu. Następnie system śledzi te adresy, analizuje pliki hostowane na stronie, inne powiązane strony oraz identyfikuje dodatkowe elementy złośliwej kampanii. W kolejnym kroku jest w stanie wyodrębnić powiązane artefakty, takie jak hashe, adresy IP czy wskaźniki behawioralne. Mając te informacje, FortiXDR wyszukuje wskaźniki mówiące, czy jakikolwiek element kampanii wpłynął na przedsiębiorstwo. Predefiniowane działania obejmują kwarantannę urządzeń, na których zainstalowały złośliwe pliki lub które komunikowały się ze złośliwymi witrynami, aktualizację informacji o zagrożeniach dla złośliwych plików i witryn internetowych itd.

Wykrywanie nieautoryzowanych urządzeń. Inną popularną metodą ataku, wykorzystywaną przez cyberprzestępców, jest infiltracja urządzeń IoT. FortiXDR zapewnia głęboki wgląd w sprzęt tej kategorii i koreluje istotne dane pochodzące z Fortinet Security Fabric. Informacje te są następnie wykorzystywane do wykrywania potencjalnie zagrożonych urządzeń oraz odpowiedniej reakcji z zastosowaniem narzędzi wdrożonych w ramach platformy Security Fabric lub przez strony trzecie. Przykładowo, mechanizm śledzenia kodu może wykryć ruch obejmujący urządzenie końcowe monitorowane przez FortiEDR. Dzięki rozszerzonej komunikacji pochodzącej z Security Fabric, FortiXDR może zidentyfikować źródło aktywności jako np. jedno z urządzeń IoT w sieci. Dalsza korelacja z danymi pochodzącymi z FortiGate może ujawnić podejrzane urządzenie na zdalnym adresie IP, które uzyskuje dostęp do zagrożonego urządzenia IoT. Następnie, wykorzystując funkcje FortiNAC, FortiXDR może automatycznie odizolować urządzenie IoT od sieci i wydać kompleksowy alert.

***

Koncepcja XDR staje się coraz bardziej popularna. Większość obecnych na rynku rozwiązań zapewnia jednak tylko rozszerzone procedury wykrywania zagrożeń. Chociaż są to oczywiście kluczowe elementy, nie mogą być wystarczające, zwłaszcza biorąc pod uwagę niedobór wykwalifikowanych analityków bezpieczeństwa. Na szczęście odpowiednio skonfigurowany system, który bazuje na sztucznej inteligencji, może ujawniać i obsługiwać incydenty szybciej i dokładniej – nie tylko poprawiając sytuację firmy w zakresie ochrony jej zasobów, ale również uwalniając potencjał specjalistów ds. bezpieczeństwa, którzy mogą skupić się na zadaniach wyższego rzędu. Nadszedł odpowiedni czas, aby specjaliści przestali podchodzić reaktywnie do incydentów dotyczących bezpieczeństwa i zaczęli wprowadzać proaktywne zmiany w postawach i strategiach ochronnych. FortiXDR pomaga osiągnąć ten cel. •

Fot. jackykids/stock.adobe.com

Rozszerzenie grupy dyskowej DRAID

W wydanej w lutym 2020 roku kodu w wersji 8.3.1 IBM Spectrum® Virtualize dla IBM FlashSystem®, IBM® SAN Volume Controller (SVC), IBM Storwize® oraz IBM Spectrum Virtualize for Public Cloud pojawiły się nowe funkcjonalności, takie jak: rozbudowa DRAID, replikacja w trzech lokalizacjach (3-site replication), obsługa dysków NVMe Storage Class Memory (SCM) przez EasyTier etc.

Fot. Cloudware

Krzysztof Kowalski
STORAGE & BACKUP SOLUTIONS EXPERT W CLOUDWARE

Funkcjonalnością nad którą chciałbym się teraz skupić jest online'owe rozszerzenie grupy dyskowej DRAID o nowe dyski. Nie jest to nowatorska, nieznana w innych rozwiązaniach funkcjonalność, inne macierze mają takie możliwości, ale w Spectrum Virtualize nie było tej możliwości.

Zanim pojawiła się wersja kodu 8.3.1 wiele osób nie znających rozwiązań IBM było zdziwionych, gdy dowiadywali się, że nie ma możliwości dodania dysku do działającej grupy dyskowej (mdisk) RAID/DRAID. Aby powiększyć mdisk należało zmigrować (online) dane na inną grupę dyskową, usunąć ją i założyć nową z docelową ilością dysków. Nie był to bardzo skomplikowany, ale za to wieloetapowy, długi proces. W przypadku środowisk produkcyjnych które wykorzystują całą

bądź prawie całą przestrzeń dyskową nastręczało to dodatkowych trudności. Oczywiście można było dodać nowy mdisk, ale nie zawsze było to rozwiązanie optymalne.

Nieco teorii

A teraz? Nie dość, że możemy rozszerzać DRAID o nowe dyski, to jednocześnie możemy dodać ich aż 12(!!!) do maksymalnej ilości 128 dysków. Jest fajnie, ale pojawiają się pytania:

- Czy wymagana jest przerwa serwisowa na czas rozbudowy?
- Ile czasu trwa przebudowa grupy?
- Jaki wpływ ma na wydajność macierzy?
- Czy w trakcie przebudowy możemy zmieniać wydajność procesu i co za tym idzie jego ewentualny wpływ na wydajność macierzy?

Skoro już mamy pytania to znajdźmy na nie odpowiedzi:

Ad 1. Pytanie retoryczne – nie jest wymagana przerwa serwisowa, wszystko dzieje się online. I tak być powinno.

Ad 2. Odpowiedź na to pytanie można określić jednym zwrotem: „It depends". Od ilości dysków, które dodajemy (od 1 do 12), ich interfejsu (SAS / NVMe) i wielkości, obciążenia macierzy etc. Wszystkie wymienione parametry mają zasadniczy wpływ na czas przebudowy.

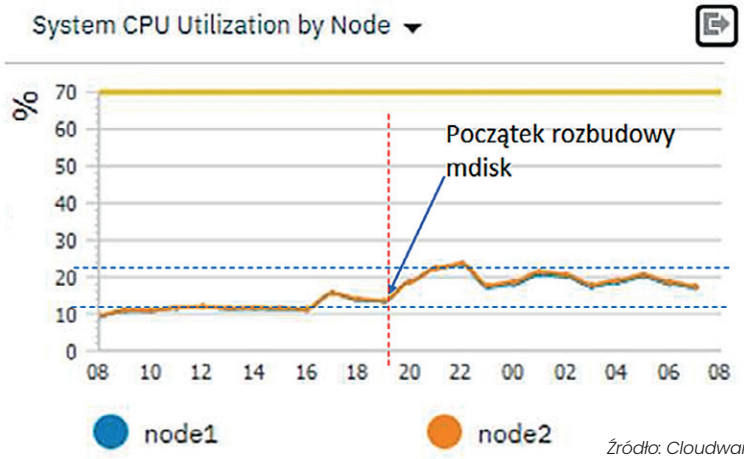
Ad 3. Jedyna informacja na stronach www IBM na temat wpływu rozbudowy na wydajność macierzy w swobodnym przekładzie na język polski brzmi tak: „rozbudowa może mieć wpływ na wydajność serwerów oraz opóźnienia (latency), kiedy jest przeprowadzana na macierzy obciążonej w ponad 50%".

Ad 4. Tak, można zmieniać priorytet procesu rozbudowy i w ten sposób mieć wpływ na wydajność, w skrajnym wypadku można go nawet zastopować.

Szczypta praktyki

Skoro mamy już odpowiedzi na dręczące nas pytania, można przystąpić do działania. Macierz, którą będziemy powiększać o nowe dyski to IBM FlashSystem 9100 z interfejsami „backend" NVMe, rozszerzana rupa dyskowa (mdisk) DRAID6 składa się z 13 dysków IBM NVMe FlashCore Module (FCM) 19.2TB (dyski te mają wbudowaną kompresję, która zazwyczaj jest większa niż 2:1), do tej grupy dyskowej zostanie dodanych kolejnych 11 dysków IBM NVMe FCM 19.2TB.

Grafika 1. Obciążenie CPU macierzy na początku procesu rozbudowy



Źródło: Cloudware

Dlaczego wybieramy powiększenie istniejącego mdisk'a, a nie założenie nowego i oddanie do puli dyskowej?

Przyczyny są prozaiczne: ponieważ rozbudowa istniejącego mdiska pozwala zaoszczędzić przestrzeń dyskową. Ale jak to?

Policzmy dla nowego mdisk'a:

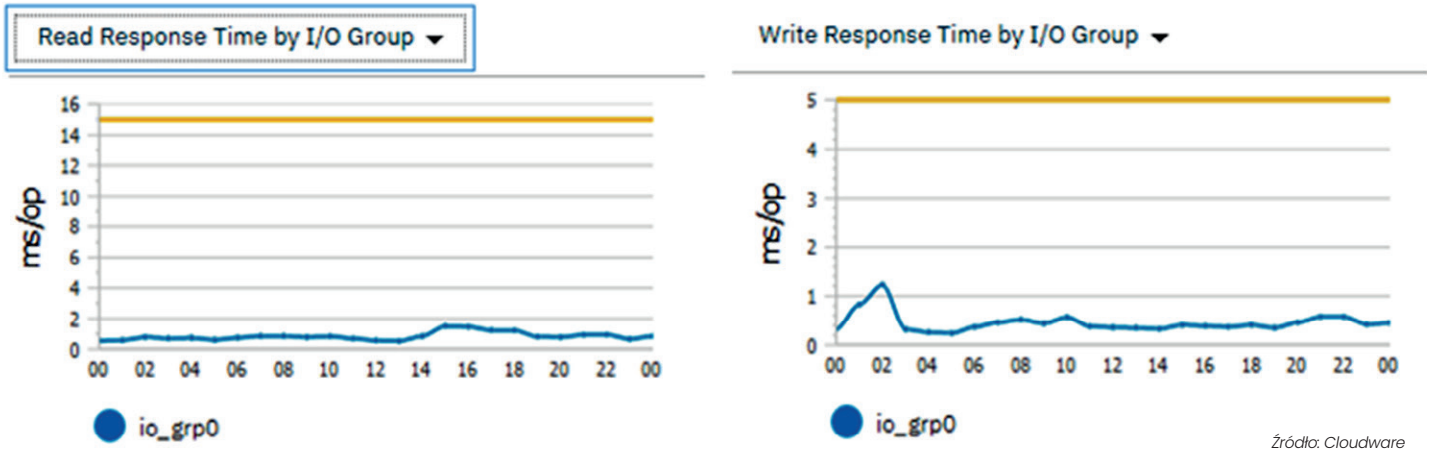
Mamy 11 dysków x 19.2TB (dyski NVMe FCM mają wbudowaną kompresję, ale w tym przypadku nie liczymy jej). Aby założyć grupę dyskową DRAID6 (dwa „dyski" parzystości) z Redundancy Area 1 (odpowiednik HotSpare dla RAID) stracimy dwa dyski na parzystość i jeden jako Hot Spare, użyteczna przestrzeń RAW (bez kompresji) będzie wynosiła 153.6TB (11 – 2 – 1 x 19.2 = 153.6)

A teraz policzmy dla rozbudowy istniejącego mdisk'u:

Aby rozszerzyć grupę dyskową DRAID6 bez zwiększenia Redundancy Area stracimy tylko dyski na parzystość, użytecz-

Fot. shock/stock.adobe.com

Grafika 2. Czas odpowiedzi do systemów produkcyjnych w trakcie procesu rozbudowy



Źródło: Cloudware

na przestrzeń RAW bez kompresji będzie wynosiła 172.8TB (11 – 2 x 19.2 = 172.8).

W przypadku rozbudowy zyskujemy 19.2TB przestrzeni, jeżeli dodamy do tego kompresję (2:1) to otrzymamy 40TB więcej przestrzeni niż w przypadku konfiguracji z nowym mdisk. Warto? Warto!

Wszystko sprawdzone – zatem do pracy

Przed przystąpieniem do prac oczywiście sprawdzono firmware sprzętu, błędy logiczne i fizyczne na macierzy, a skoro nie było przeciwskazań można było przystąpić do prac.

Ponieważ ciągle nie wiadomo było ile czasu zajmie dodanie wszystkich dysków do grupy dyskowej proces przeprowadzono w dwóch etapach:

- etap pierwszy – dodanie sześciu dysków;
- etap drugi – dodanie pozostałych pięciu dysków.

Sam proces dodania dysków można wykonać zarówno z CLI, jak i z graficznego interfejsu zarządzającego macierzy.

Proces rozbudowy DRAID, w etapie pierwszym, o sześć dysków zakończył się po 52 godzinach.

Proces rozbudowy DRAID, w etapie, o pięć dysków zakończył się po 44 godzinach.

Na podstawie powyższych danych można określić, że rozbudowa o jeden dysk NVMe FCM 19.2TB zajmuje 9 godzin, oczywiście w przypadku innej macierzy, innego typu dysków i/lub ich wielkości czas rozbudowy będzie inny.

W obydwu przypadkach rozbudowa przebiegła bez najmniejszych zakłóceń, systemy produkcyjne nie zanotowały żadnych anomalii. Obciążenie CPU macierzy w trakcie rozbudowy wzrosło o 5 do 10%. •

Fot. Cloudware

Grzegorz Gołda
DYREKTOR DZIAŁU SPRZEDAŻY CLOUDWARE

Coraz większe ilości danych wymagają nie tylko przestrzeni na serwerach, ale także możliwości szybkiego do nich dostępu. Ten zapewnia technologia, a konkretnie pamięci masowe flash i nowoczesne interfejsy. Cloudware Polska podchodzi do wspomnianego zagadnienia w organizacjach finansowych w sposób kompleksowy. Oferujemy zarówno doradztwo, jak i dedykowane usługi szyte na miarę. Klientom zapewniamy pełne wsparcie na każdym etapie prac, dlatego nasza oferta obejmuje nie tylko prace analityczne, doradcze czy wdrożeniowe. Naszym klientom staramy się towarzyszyć we wszystkich etapach.

THE FUTURE IS NEXT™

Cloudware Polska jest producentem oprogramowania, integratorem systemów IT, a przede wszystkim partnerem w transformacji technologicznej Klientów.

Budujemy oraz modernizujemy systemy, łączymy nowoczesne technologie z rozwiązaniami czołowych producentów. Od ponad 10 lat tworzymy polską branżę IT.

Wieloletnia współpraca z technologicznymi liderami, pozwoliła nam stworzyć unikalną ofertę wartości, która nie tylko uwzględnia wszystkie potrzeby naszych Klientów, ale przede wszystkim wspiera ich w procesach biznesowych.

10 LAT NA RYNKU

10 LAT WSPÓŁPRACY Z IBM

ISO 9001 i 27001 CERTYFIKATY JAKOŚCI

Największa ilość projektów wdrożeniowych w obszarze IBM Business Automation

Najbardziej dynamiczny wzrost unikalnych kompetencji w obszarze IBM Security

Największa sprzedaż rozwiązań IBM w 2020 roku

Platinum Business Partner IBM

cloudware

Szukasz zaufanego dostawcy usług IT?

DIGITAL BANKING ACADEMY

Organizator

Związek Banków Polskich

Partnerzy

accenture · DELL Technologies · Google Cloud · Microsoft

Patron medialny

BANK

WIEDZA

Sprostaj wyzwaniom ery transformacji cyfrowej w bankach. Poznaj najnowsze trendy. Dowiedz się jakie najnowsze rozwiązania cyfrowe mogą znaleźć zastosowanie w bankowości. Ucz się od liderów z innych sektorów. Daj się zainspirować.

PRELEGENCI

To wybitni eksperci i praktycy reprezentujący czołowe kancelarie prawne, największe banki, wyróżniających się dostawców technologii, pracownicy uczelni, firm doradczych i najbardziej innowacyjne firmy z Polski i świata. Poznaj inspiracje z innych sektorów i kulisy czołowych projektów technologicznych.

TEMATYKA

Zajmujemy się najbardziej aktualnymi i przyszłościowymi zagadnieniami cyfrowymi. Wystąpienia są szczegółowe, pogłębione, długie i przede wszystkim merytoryczne. Otwieramy dyskusję. Dajemy czas na zadawanie pytań. Udostępniamy materiały. Wystarczy przyjść i chłonąć wiedzę.

PERSPEKTYWY

Każdy temat przewodni omawiamy z perspektywy prawnej, regulacyjnej, biznesowej i technologicznej. Dzięki temu w pełni zrozumiesz omawiany obszar poznając korzyści, wyzwania i ograniczenia z kilku perspektyw.

CZAS

Zaoszczędź czas i zdobądź skondensowaną dawkę wiedzy podczas całodziennego, interaktywnego szkolenia online.

Najbliższy warsztat online

„Technologie wspierające kanały sprzedażowe"

28 października 2021 r.

Zaawansowane technologie online okazały się bezcenne w czasie pandemii. Błyskawiczna digitalizacja codzienności dobitnie uświadomiła, że nie ma już bankowości bez nowoczesnych rozwiązań. Technologia służy klientom, ale także doskonalone wspiera kanały sprzedażowe. Jak zoptymalizować jej wykorzystanie, aby oferować klientom produkty dopasowane do ich potrzeb? Porozmawiamy o tym podczas szkolenia.

Dołącz do nas i dowiedz się więcej!

Kontakt: **Katarzyna Cechowska-Jastrzębska**
Centrum Prawa Bankowego i Informacji | e-mail: k.cechowska@wydawnictwocpb.pl | tel. (22) 623 84 53; tel. kom. 885-885-923

Przekonaj się, że warto wiedzieć więcej

„Miesięcznik Finansowy BANK"

Jesteśmy profesjonalnym magazynem środowiska bankowego. Od 30 lat omawiamy zasadnicze problemy rynku finansowego w Polsce. Pomagamy w unowocześnieniu sektora i kształceniu kadr. Współpracujemy z bankami, firmami infrastrukturalnymi i organizacjami środowiskowymi. Organizujemy szereg profesjonalnych konferencji, szkoleń i debat od lat wytyczających rynkowe standardy.

BANK
MIESIĘCZNIK FINANSOWY

www.aleBank.pl/BANK

REDAKCJA	redakcja@miesiecznikBank.pl	DZIAŁ REKLAMY	reklama@wydawnictwocpb.pl
PRENUMERATA	www.alebank.pl/prenumerata	KONFERENCJE I SZKOLENIA	www.alebank.pl/konferencje