

SZTUCZNA INTELIGENCJA W BANKOWOŚCI

Wydawcy raportu



ZWIĄZEK BANKÓW POLSKICH



Centrum Prawa Bankowego i Informacji
www.cpb.pl

BANK

aleBank.pl

SZTUCZNA INTELIGENCJA W BANKOWOŚCI

Patron merytoryczny raportu



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

© Copyright by Związek Banków Polskich

© Copyright by Centrum Prawa Bankowego i Informacji



ZWIĄZEK BANKÓW POLSKICH



Centrum Prawa Bankowego i Informacji
www.cpb.pl

Warszawa, czerwiec 2020

Wydawnictwo Centrum Prawa Bankowego i Informacji



**GFT
POLAND**



BREAKTHROUGH

**Partner
of the Year**

2019

Twój biznes w rękach ekspertów

Szymon Kaczmarczyk
Client Unit Executive Poland & Asia Pacific

Globalne doświadczenie

- 🔧 Rozwiązania technologiczne dla największych banków inwestycyjnych i detalicznych
- 🔧 Zespół 800 ekspertów w Polsce i 6000 w 15 krajach świata
- 🔧 Star Performer wg Everest Open Banking IT Services PEAK Matrix® Assessment 2020

Eksperci najwyższej klasy

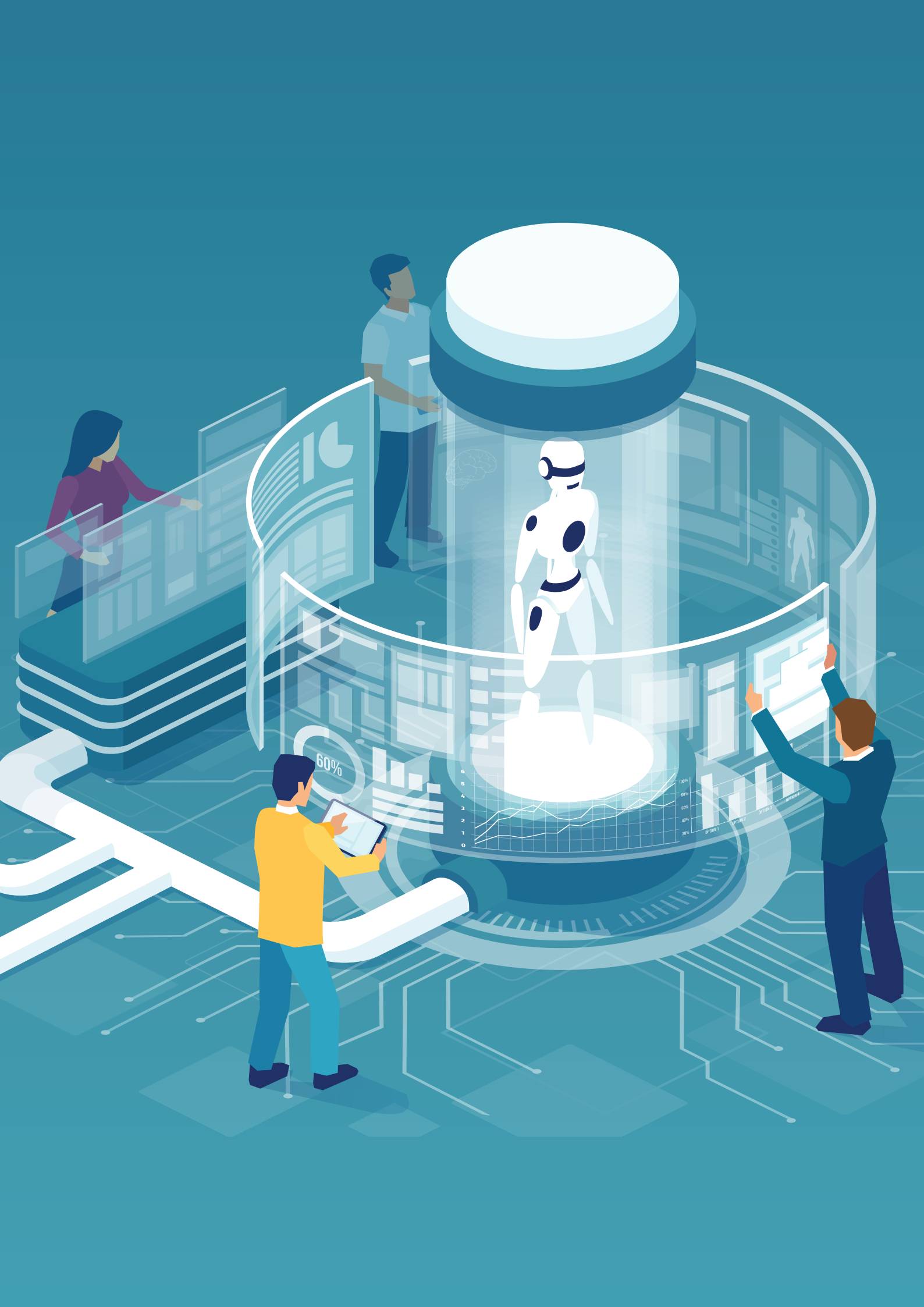
- 🔧 Komercyjne realizacje w obszarach AI, Cloud, Blockchain, Big Data
- 🔧 Niemal 200 certyfikatów AWS, Google i Azure

gft.com/pl

Silne partnerstwa

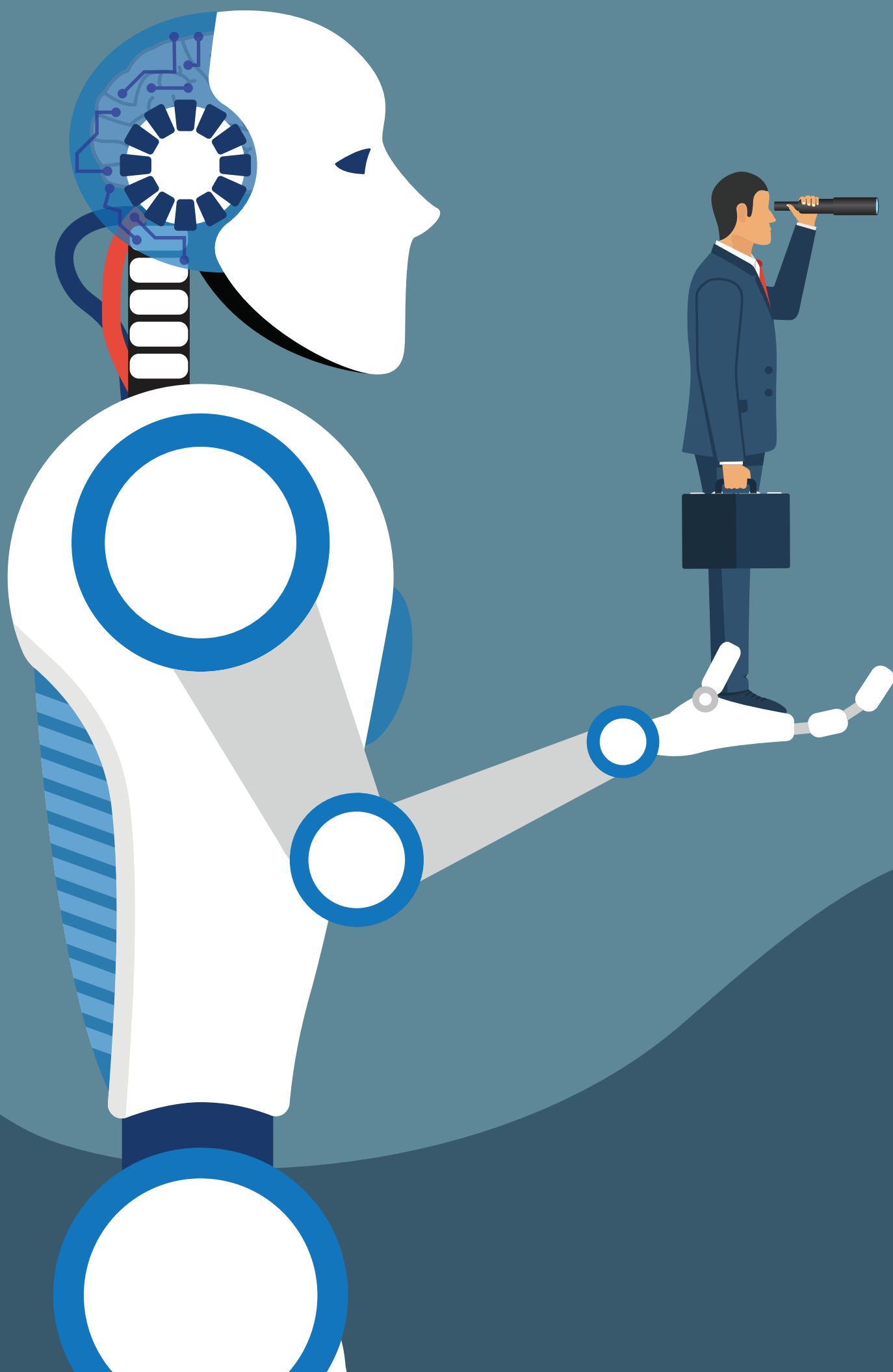
- 🔧 AWS Advanced Consulting Partner
- 🔧 Google Cloud EMEA Breakthrough Partner of the Year
- 🔧 Microsoft Gold Partner

- Optymalizacja i zarządzanie platformami core banking
- Migracja do środowisk chmurowych
- Tworzenie architektury danych
- Zapewnianie zgodności regulacyjnej rozwiązań IT
- Systemy kontroli ryzyka i przeciwdziałania oszustwom
- Kompleksowe narzędzia front office



SPIIS TREŚCI

Wstęp	7
Od wydawcy	9
Sztuczna inteligencja w prawdziwym banku	10
Cloudware Polska: Dlaczego sztuczna inteligencja znajdzie istotne zastosowanie w bankowości?	28
Comarch SA: Czy sztuczna inteligencja może sprawdzić się w walce z przestępstwami w bankach?	32
Dell Technologies: Oczywiste i mniej oczywiste zastosowania sztucznej inteligencji w sektorze finansowym	43
Fortinet: Sztuczna inteligencja jako kluczowy element budowy architektury bezpieczeństwa teleinformatycznego nowej generacji	50
GFT Poland: Biometria z pudełka	57
Microsoft: Analityka danych i uczenie maszynowe kluczem do skutecznej i bezpiecznej bankowości jutra	61
SAS Institute: Jak sztuczna inteligencja zmieniła branżę finansową	68



WSTĘP

Warren Buffett, powszechnie uważany za jednego z najlepszych inwestorów na świecie, powiedział podczas jednego z posiedzeń akcjonariuszy: „nigdy nie inwestuj w biznes, którego nie rozumiesz”. Buffett poświęca wiele czasu i sił, by zrozumieć dogłębnie zasady funkcjonowania spółek, których papiery kupuje. To dlatego wzbraniał się przez wiele lat przed włożeniem do portfela walorów firm technologicznych. Co nie przeszkodziło mu od wielu lat przyjaźnić się z Billem Gatsem.

Tematyka związana ze sztuczną inteligencją może wydawać się czymś tajemniczym, science fiction. Kultura popularna wzbudziła u części ludzi autentyczne obawy o powstanie „superinteligencji”. Z drugiej strony miliony osób codziennie rozmawia z Siri, pytając np. o pogodę. Pewnie niewiele osób przyzna się głośno, że próbowali jej także zadawać pytania egzystencjonalne.

Maszyny są bardziej wydajne niż ludzie. Mogą pracować w systemie 24/7, nie śpią, nie potrzebują przerw, nie nudzą się i praktycznie nie popełniają błędów. Odpowiedzą klien-

tom na czacie nawet w środku nocy. W mgnieniu oka przeanalizują ogromne ilości danych.

Jednak warunkiem wykorzystania potencjału sztucznej inteligencji w sektorze bankowym jest zrozumienie jej działania. Dlatego, pod patronatem Związku Banków Polskich przygotowany został Raport „Sztuczna inteligencja w bankowości”, będący praktycznym kompendium wiedzy na temat technologii i jej zastosowań w sektorze bankowym oraz opisem doświadczeń z wdrożeń. Tworząc publikację, postanowiliśmy połączyć spojrzenie naukowe i praktyczne, dlatego autorem pierwszej części jest dr Konrad Maj – kierownik Centrum Innowacji Społecznych i Technologicznych „HumanTech” na SWPS Uniwersytecie Humanistycznospołecznym, w drugiej znalazły się artykuły czołowych dostawców rozwiązań opartych na sztucznej inteligencji.

Życzę dobrej lektury.

Joanna Barbrich

Zespół Systemów Płatniczych
i Bankowości Elektronicznej,
Związek Banków Polskich



OD WYDAWCY

Sztuczna inteligencja od niepamiętnych czasów wywołuje ambiwalentne odczucia. Wizja myślących maszyn budzi obawy, ucieleśnione najpełniej w legendzie o Golemie, jakoby ludzkość mogła utracić panowanie nad światem za sprawą wytworzonej przez siebie technologii. Po drugiej jednak stronie przemożne lenistwo, będące w równym stopniu grzechem głównym co siłą napędową postępu cywilizacyjnego, skłania nas do tworzenia urządzeń, którym powierzamy coraz bardziej skomplikowane i zaawansowane zadania, wykonywane dotychczas przez „interfejs białkowy”. Dziś trudno byłoby wskazać taki obszar życia, w którym technologia nie odgrywałaby istotnego znaczenia, a w przypadku rynku finansowego wręcz nie sposób wyobrazić sobie jego funkcjonowania w takiej formie, jak to miało miejsce jeszcze u progu XXI stulecia.

Pośród rozlicznych technologii, jakie wspierają nasze funkcjonowanie zarówno w codziennym życiu, jak i na rynku finansowym, szczególnego znaczenia nabiera sztuczna inteligencja i uczenie maszynowe. Podobnie jak imć Jourdain, bohater Molierowskiej komedii „Mieszczanin szlachcicem”, który przez lata nie zdawał sobie sprawy, iż mówi prozą, tak i my nierzadko nie uświadamiamy sobie, jak często naszym codziennym pracom czy decyzjom zakupowym

towarzyszą inteligentne algorytmy. Poczynając od standardowych wyszukiwarek internetowych, poprzez oprogramowanie do obsługi poczty elektronicznej aż po bankowe aplikacje mobilne i chatboty – w każdym z tych przypadków technologia deep learning pozwala na dostarczanie nam odpowiednich wyników, produktów i usług, optymalnie dopasowanych do naszych indywidualnych potrzeb i w czasie rzeczywistym.

Sztuczna inteligencja pozwala nam również poczuć się bezpieczniej we współczesnym zdigitalizowanym świecie. Wbrew apokaliptycznym wizjom, największym zagrożeniem dla współczesnego konsumenta jest nie tyle literacki bunt maszyn, ile „czynnik ludzki”, w postaci świetnie zorganizowanych cyberprzestępców. Bazując na uczeniu maszynowym, złożone systemy, są w stanie doskonale rozpoznać większość technik stosowanych przez sprawców, radząc sobie w sytuacjach, wobec których bezradny bywa najbardziej wytrwały ekspert w dziedzinie bezpieczeństwa. W którym kierunku podążać będzie rozwój tego typu systemów i jak optymalnie wykorzystywać ich możliwości w bankowej praktyce? Próbą odpowiedzi na te pytania jest prezentowany raport.

Karol Mórąwski
Redaktor prowadzący,
„Miesięcznik Finansowy BANK”



SZTUCZNA INTELIGENCJA

w prawdziwym banku

O sztucznej inteligencji słyszało bardzo wiele osób, w biznesie już praktycznie wszędzie można usłyszeć o uczeniu maszynowym, algorytmach czy sieciach neuronowych. W bankowości wiele mówi się o wykorzystaniu tych rozwiązań do automatyzacji procesów operacyjnych czy w bezpośrednim kontakcie z klientem. Instytucje finansowe chcą czym prędzej wdrażać inteligentne rozwiązania, ale tak naprawdę niewiele osób zna pojęcia związane z tym obszarem. Niniejszy tekst ma na celu, w sposób syntetyczny, wyjaśnienie części z nich oraz pokazanie przykładowych zastosowań w bankach.

W listopadzie 2019 r. Centrum HumanTech na Uniwersytecie SWPS przeprowadziło badanie na ogólnopolskiej, reprezentatywnej próbie Polaków, z którego wynika, że większość z nich nie orientuje się w tematyce sztucznej inteligencji, a jedynie 4% „orientuje się bardzo dobrze”. Co jednak ważne, pomimo braku wiedzy na temat, większość Polaków wyraża obawy związane z pracami nad tym obszarem.

Postawy te zapewne wynikają z braku edukacji w zakresie sztucznej inteligencji, a lukę tę zapełnia prawdopodobnie „wiedza” z filmów science fiction, fantastyki naukowej i różnych emocjonalnych ostrzeżeń ze strony przeciwników tego nurtu.

SZTUCZNA INTELIGENCJA

Kultura popularna dostarczyła części ludzi autentycznych obaw o powstanie „superinteligencji”, która zawładnie światem, a część z kolei nabiera nierealistycznych oczekiwań odnośnie rozwiązania problemów świata przez bardzo inteligentne maszyny.

Obie postawy wydają się niewłaściwe i mogą prowadzić do nieporozumień.

Pojęcie „sztuczna inteligencja” (SI, ang. Artificial Intelligence – AI) nie jest wcale nowe. Wprowadził je 1956 r. amerykański informatyk profesor Dartmouth College – **John McCarthy**. Według niego to po prostu maszyna, której działanie przypomina przejawy ludzkiej inteligencji. Współczesne definicje, których jest niezliczona ilość, również krążą wokół podobieństwa do człowieka w zakresie myślenia i podejmowania racjonalnych decyzji. **Krzysztof Ficoń** (2013) podał aż 24 definicje krajowych i zagranicznych teoretyków, samemu opisując ją tak:

Sztuczna inteligencja – pojęcie to odnosi się do interdyscyplinarnej nauki, która dąży do zbadania ludzkiej inteligencji i zaimplementowania jej mechanizmów na maszynach (komputerach).
(Ficoń, 2013).

Ale w istocie można raczej mówić o ześpoleniu różnych technik sztucznej inteligencji. Dodać też należy, że wiele osób poddaje w wątpliwość używanie w ogóle terminu sztuczna inteligencja, uznając, że jest on mocno na wyrost i niepotrzebnie wywołuje porównanie z inteligencją ludzką. Samo uczenie się maszyn czy nawet możliwość rozpoznawania obiektów i podejmowania decyzji nie powinna



Dr Konrad Maj

Psycholog społeczny, adiunkt w Katedrze Psychologii Społecznej, Wydział Psychologii. Kierownik projektu HumanTech Meetings, inicjator oraz kierownik Centrum Innowacji HumanTech, które analizuje najnowsze trendy społeczne i technologiczne, przygotowuje ekspertyzy na podstawie wyników badań i wdrożeń innowacji, a także realizuje projekty we współpracy z biznesem w zakresie komercjalizacji wiedzy. W pracy naukowej i dydaktycznej koncentruje się na zagadnieniach związanych z wpływem społecznym, psychologią mediów oraz innowacjami. Obecnie prowadzi badania w obszarze HRI (Human-Robot-Interaction). W latach 2013–2016 był pełnomocnikiem prorektora ds. nauki w zakresie komercjalizacji wyników badań naukowych i innowacji społecznych. Odbił szereg wizyt studyjnych w ośrodkach zajmujących się innowacjami ISI – Institute for Social Innovation (Carnegie Mellon University, Pittsburgh, USA), ID+ Research Institute for Design, Media and Culture (University of Averoio, Portugal), Design Factory (Aalto University, Finlandia). Na Uniwersytecie SWPS prowadzi zajęcia z zakresu psychologii społecznej, psychologii wpływu społecznego i innowacji społecznych. Jest trenerem występów medialnych, autoprezentacji, negocjacji i komunikacji dla firm i instytucji.

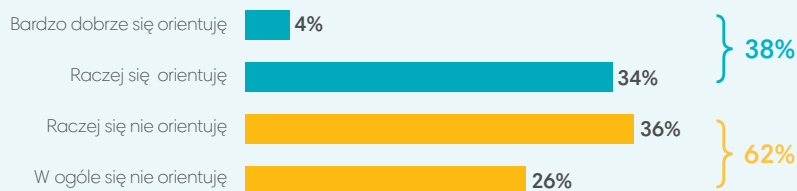
od razu prowadzić do wnioskowania o posiadanej inteligencji.

Stosunkowo łatwo jest zrozumieć sztuczną inteligencję, odnosząc ją do ludzkich procesów uczenia się, przetwarzania informacji oraz podejmowania decyzji. Oczywiście zaznaczając, że raczej nigdy takie pełne odwzorowanie nie będzie możliwe (**patrz tab. 1**).

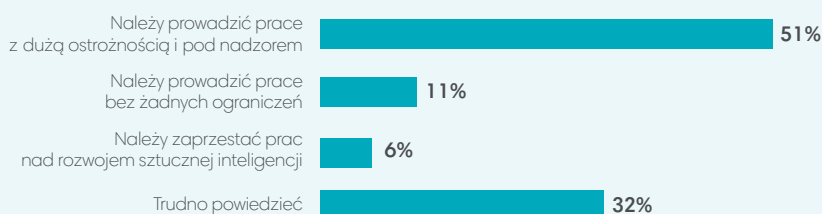
Druga kolumna przedstawia jednocześnie obszary badań i rozwoju sztucznej inteligencji. Poprzez rozwój i integrację różnych technologii kognitywnych dąży się do stworzenia programów działających niezależnie. Nie oznacza to jednak wykształcenia funkcji poznawczych maszyny. Taką perspektywę możemy odłożyć na długie lata.

AI jest obecna już w prawie wszystkich obszarach naszego życia, nie tylko w gospodarce, ale i w naszych domach. Jej zastosowanie jest ogromne, każdy, kto ma smartfon, korzysta z jej rozwiązań. Algorytmy sztucznej inteligencji pomagają nam dotrzeć do

RYS. 1. Na ile orientujesz się w tematyce rozwoju sztucznej inteligencji (AI)?



RYS. 2. Jaki jest Twój stosunek do prac nad rozwojem sztucznej inteligencji (AI)?



Źródło: Badanie Centrum Human Tech, Uniwersytet SWPS pt. „Rozwój sztucznej inteligencji i roboty w życiu społecznym w opinii Polaków”, zrealizowane 22–26 listopada 2019 r. na reprezentatywnej próbie dorosłych Polaków na panelu Ariadna (CAWI, N=1044).

celu (GPS), ale także tłumaczą teksty, rozpoznają choroby, grają w gry, czy prowadzą samochody.

Wzrost popularności AI można wiązać zarówno z coraz większymi możliwościami technologicznymi, jak i sytuacją na rynku, która wymusza stosowanie rozwiązań pomocnych

w realizacji celów biznesowych, które jednocześnie dają przewagę konkurencyjną (**patrz tab. 2**). Wiedza dotycząca sztucznej inteligencji też coraz bardziej się upowszechnia, mówi się o trendzie demokratyzacji AI (ang. *AI democratization*).

Bardzo często można usłyszeć o „słabych” i „mocnych” postaciach sztucznej inteligencji. W pierwszym przypadku mówimy o takim zaprogramowaniu systemu, który jedynie symuluje zachowanie inteligentne, w drugim już o sposobie analizy danych i podejmowania zbliżonym do tego, jak robi to ludzki mózg.

Większość rozwiązań sztucznej inteligencji ma postać słabą. Asystenci głosowi, jak Alexa czy Siri, chatboty czy samochody autonomiczne jedynie wywołują wrażenie rozumiejących ludzkie komunikaty. System gubi się, gdy znajdzie się w nowych warunkach, nie potrafi wykonać zadań innych niż te, do których został zaprojektowany. Wiemy przecież doskonale, że umysł ludzki to coś więcej

TAB. 1 Obszary badań nad inteligencją ludzką i sztuczną

Inteligencja ludzka	Inteligencja sztuczna
Rozumienie języka	Systemy rozpoznawania mowy (speech recognition)
Pisanie i czytanie	NLP (Przetwarzanie języka naturalnego)
Widzenie i przetwarzanie danych wzrokowych	Wizja komputerowa (computer vision), przetwarzania obrazów (image processing)
Poruszanie się w świecie fizycznym	Robotyka
Rozpoznawanie wzorów w procesie uczenia się	Rozpoznawanie wzorów (pattern recognition)
Proces uczenia się, sieć neuronów biologicznych	Uczenie maszynowe (machine learning), głębokie uczenie (deep learning), sztuczne sieci neuronowe
Wnioskowanie, podejmowanie decyzji	Predykcja, klasyfikacja, algorytmy

niż obliczenia, analiza danych i wnioskowanie. Jesteśmy bytami społecznymi i emocjonalnymi, i jak się okazuje emocje oraz umiejętności poruszania się w złożonych interakcjach społecznych pozwalają nam lepiej rozumieć świat i adekwatnie reagować. Stąd właśnie idea tzw. ogólnej sztucznej inteligencji (AGI – *Artificial General Intelligence*), która ma cechować się unikalnością natury ludzkiej, zespołem wartości, ale też repertuarem różnych stanów emocjonalnych. Człowiek jednak, jak wiemy, doskonały nie jest. I tu dochodzimy do pytania, czy sztuczna inteligencja ma być kopią ludzką, czy może być inną inteligencją, a może inteligencją, która poszerza możliwości człowieka, wspierając go w niektórych obszarach?

W tym zakresie niektórzy proponują również mówienie o inteligencji rozszerzonej (ang. *augmented intelligence*), która koncentruje się na wzmacnianiu potencjału ludzkiego. W tym ujęciu uczenie maszynowe ma na celu zwiększenie ludzkich możliwości, a nie zastąpienie człowieka.

Warto zwrócić uwagę, że obecnie bardzo wiele krajów oraz wspólnot międzynarodowych opracowało różne dokumenty omawiające strategie rozwojowe czy wobec rozwoju sztucznej inteligencji. UE ma swoją szeroko rozbudowaną politykę w tym zakresie (*Artificial Intelligence Policy*¹). Wielka Brytania powołała AI Council, czyli niezależny komitet ekspertów, który udziela porad rządowi i kierownictwu wysokiego szczebla w sprawach sztucznej inteligencji. Niedawno również w naszym kraju Ministerstwo Cyfryzacji opracowało dokument „Polityka rozwoju sztucznej inteligencji

TAB. 2 Powody dynamicznego wzrostu badań nad sztuczną inteligencją oraz jej zastosowaniami

Sytuacja technologiczna	Sytuacja rynkowa
Wzrost mocy obliczeniowej komputerów	Wymóg szybkiej obsługi, dostępności 24/h
Uczenie maszyn	Braki specjalistów w wielu obszarach gospodarki
Możliwości gromadzenia wielu zbiorów danych	Potrzeba przetworzenia dużej liczby danych
Systemy – np. biometria, systemy związane z analizą obrazu, wydajne procesy graficzne, jak np. GPU (ang. graphics processing unit)	Konkurencja w zakresie innowacyjności
Rozwój algorytmów	Potrzeba personalizacji usług
Główna współpraca (np. OpenAI, demokratyzacja AI)	Dążenie do optymalizacji czasu i kosztów

w Polsce na lata 2019–2027”². Ma on na celu wspieranie stymulowania rozwoju AI i doprowadzenia do powstania 700 nowych firm wykorzystujących ją.

To, że Unia Europejska oraz poszczególne państwa narodowe przyjmują różne dokumenty strategii czy polityki związane ze sztuczną inteligencją, pokazuje jak ważną ona już obecnie odgrywa rolę i jak mocno myśli się o jej rozwoju w przyszłości.

Wiele różnych danych wskazuje, że w biznesie nasila się zastosowanie AI. Dotyczy to w bardzo dużym stopniu sektora bankowego i finansowego:

- Według prognoz stawianych od kilku lat przez IDC w zakresie rozwoju technologii, w 2021 r. ze sztucznej inteligencji będzie korzystać 75% handlowych aplikacji biznesowych. A do 2024 r.

interfejsy oparte na sztucznej inteligencji zastąpią 30% współczesnych aplikacji ekranowych (za: <https://blogs.oracle.com/poland/rewolucyjna-sztuczna-inteligencja>).

- Wedle raportu tej samej firmy (IDC) pt. *Worldwide Artificial Intelligence Systems Spending* Guide 2019*, który został opracowany na bazie danych z rynku sztucznej inteligencji na całym świecie, wydatki na systemy AI sięgną w 2023 r. 97,9 mld USD, ponad dwa i pół razy więcej w porównaniu do wydatków w 2019 r. (37,5 mld USD), co daje złożoną roczną stopę wzrostu (CAGR) w okresie prognozy na lata 2018–2023 na poziomie 28,4% (za: https://www.idc.com/getdoc.jsp?containerId=IDC_P33198).
- Wedle Raportu Accenture „Sztuczna Inteligencja. Dobre praktyki, aspekty prawne i za-

¹ https://ec.europa.eu/knowledge4policy/online-resource/artificial-intelligence-policy_en

² <https://www.gov.pl/attachment/0aa51cd-5-b934-4bcb-8660-bfecb20ea2a9>

stosowania w sektorze finansowym”, banki, które zainwestują w rozwiązania AI i pochodne, mogą w latach 2018–2022 zwiększyć swoje przychody o 34%, a zatrudnienie o 14%. Wszystko to może do roku 2035 podwoić wskaźnik PKB w krajach rozwiniętych i podnieść ich produktywność o 40%, przy oszczędnościach rzędu 20–25%.

- Wedle badania Accenture Technology Vision 2019 (**patrz rys. 3**), w którym w ankiecie zapytano menedżerów z sektora bankowego o stan zaawansowania wdrożeń rozwiązań opartych na AI w firmie okazało się, że 19,6% dokonało już wdrożeń AI w kilku działach, 23% – w jednym, 26,4% uruchomiło pilot rozwiązania, 21% zaplanowało pilot/wdrożenia rozwiązania, jedynie 8,20% nie planuje lub analizuje pod kątem wdrożenia, 1,8% nie ma zdania (za: https://www.accenture.com/_acnmedia/PDF-94/Accenture-TechVision-2019-Tech-Trends-Report.pdf).
- Wedle siódmej edycji raportu opracowanego przez Polską Agencję Rozwoju Przedsiębiorczości „Monitoring trendów w innowacyjności” nadchodzące lata to czas sztucznej inteligencji. W Polsce, w ciągu pięciu lat, do 2025 r. liczba miejsc pracy dla specjalistów od AI wzrośnie do 200 tys. Do 2025 r. wartość globalnego rynku AI wzrośnie do przeszło 190 mld dolarów, przy średniorocznym tempie wzrostu

na poziomie 36%, a rozwiązania na niej oparte wdroży aż 97% największych międzynarodowych firm. Natomiast już do 2022 r. dzięki nowym technologiom powstanie na świecie 133 mln miejsc pracy. Z kolei stopień rozpowszechnienia inteligentnych robotów domowych na świecie osiągnie 14%. Szacowane jest przy tym, że do końca 2021 r. przedsiębiorstwa wydadzą na badania nad AI ponad 60 mld dolarów³.

³ https://www.parp.gov.pl/storage/publications/pdf/RAPORT_NSI_7_2019.pdf

- Z raportu Genpact „Commercial banking and the customer experience imperative. How industry leaders are using CX and artificial intelligence to overcome disruption” wynika, że aż 97% respondentów (kadra kierownicza w bankach komercyjnych) zgłasza pewien poziom wykorzystywania sztucznej inteligencji (**patrz rys. 4** – za: https://www.genpact.com/insight/report/commercial-banking-and-the-customer-experience-imperative?utm_source=prrl&utm_medium=nsrw&utm_campaign=mult_a_didi_prri_nswr_cont_na_cxoctv_all_bcm-bt_x_bk).



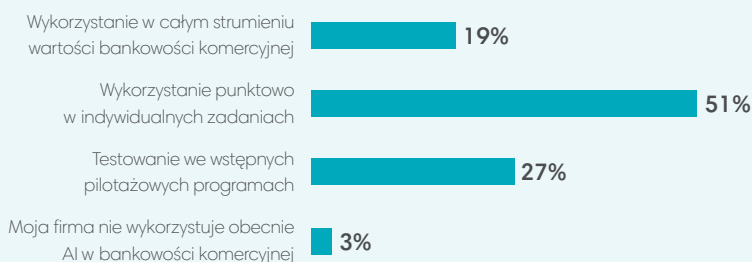
BIG DATA

Sztuczna inteligencja, aby działała poprawnie, potrzebuje paliwa – danych, i to dużej ilości, w czystej postaci. Ale to coraz tańsze i coraz łatwiej dostępne paliwo. Producentem danych jest każdy człowiek, i to nie tylko ten, który prowadzi intensywną aktywność w internecie czy korzysta z określonych aplikacji mobilnych, produktów bankowych czy przejazdów Uberem. Generujemy w ten sposób ogromne ilości informacji. Według szacunków IBM, 90% światowych zbiorów danych zostało wygenerowanych w ciągu ostatnich dwóch lat.

Big data – termin odnoszący się do dużych, zmiennych i różnorodnych zbiorów danych, których przetwarzanie i analiza jest trudna, ale jednocześnie wartościowa, ponieważ może prowadzić do zdobycia nowej wiedzy.

Firma CloudNine, od czterech lat co roku publikuje grafiki pokazujące, co dzieje się w ciągu 60 sekund w internecie. Tak wygląda porównanie roku 2019 i 2020, aktywność internautów rok do roku rośnie wykładniczo. Dane są swoistą karmą dla algorytmów, które dzięki procesom uczenia nabywają coraz większej sprawności (**patrz rys. 5**)

RYS. 4. Wykorzystywanie AI przez banki komercyjne



W roku 2014 ImageNet Large Scale Visual Recognition Challenge (ILSVRC), rozwiązanie Google, zajęło pierwsze w zakresie identyfikacji na zdjęciach ras psów. Algorytm potrafił zidentyfikować około 200 ras, przy zaledwie 6,6% błędzie. Taki wynik może osiągnąć jedynie doświadczony w dziedzinie komputerowy psi ekspert. Warto zauważyć, że rok wcześniej ów błąd był o prawie połowę większy (11,7%), co pokazuje, jak algorytmy uczą się, poprawiając stale swoje wyniki⁴.

⁴ <https://www.entrepreneur.com/article/283990>

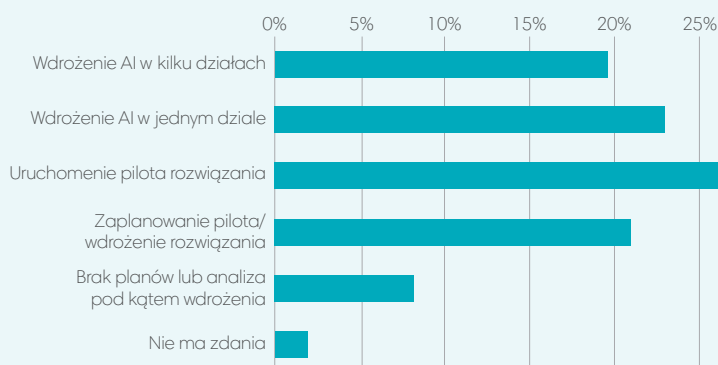
Jedną z pierwszych definicji big data, wprowadzili amerykańscy badacze NASA – **Michael Cox** oraz **David Ellsworth** (1997) w artykule „Managing Big Data for Scientific Visualization”⁵. Autorzy traktują big data jako zbiory danych do analizowania, których liczbę należy maksymalizować w celu wydobycia wartości informacyjnych. Współcześnie można spotkać bardzo często opis big data jako terminu odnoszącego się do dużych, zmiennych i różnorodnych zbiorów danych, których przetwarzanie i analiza jest trudna, ale jednocześnie wartościowa, ponieważ może prowadzić do zdobycia nowej wiedzy.

Data driven business

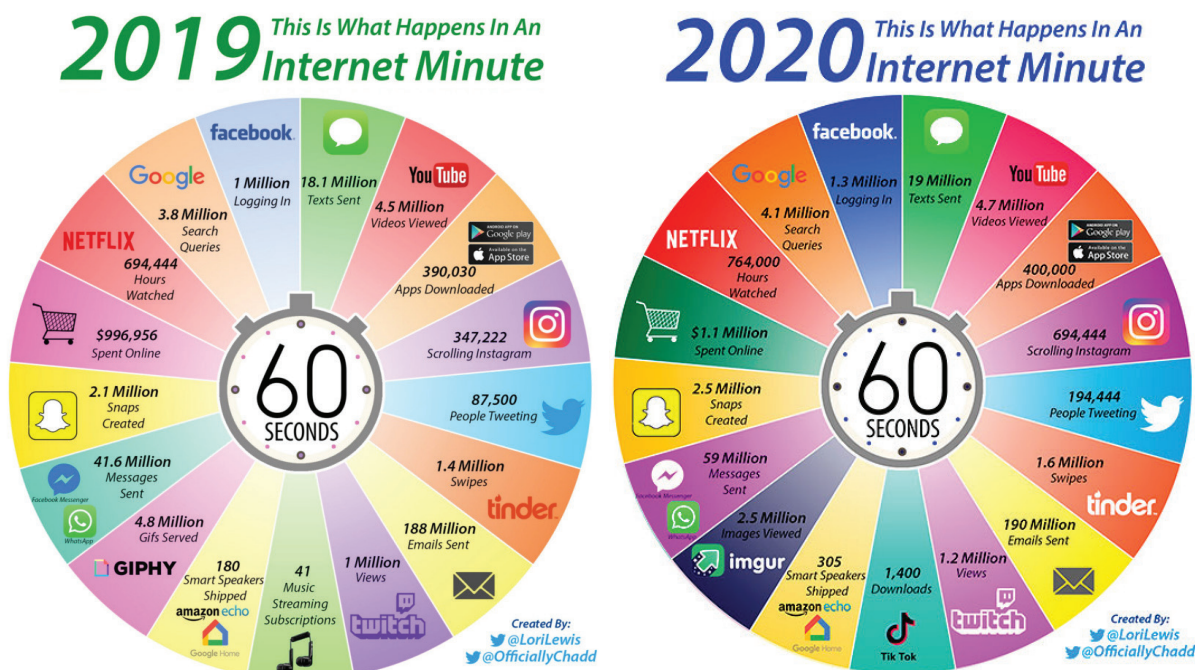
Andrew Ng ze Stanford University, współzałożyciel serwisu Coursera, nazywa AI „nową elektrycznością”, a „The Economist” określił dane cyfrowe „nową ropą”, która stała się źródłem przychodów i rywalizacji.

⁵ https://www.researchgate.net/publication/238704525_Managing_big_data_for_scientific_visualization

RYS. 3. Deklaracja stanu zaawansowania wdrożeń opartych na AI w sektorze bankowym



RYS. 5. Ruch w internecie w popularnych serwisach w ciągu 60 sekund w 2019 i 2020 r.



Organizacje napędzane są w coraz większym stopniu przez dane, których koszty pozyskania stale spadają.

Podejście oparte na danych (ang. data driven business) to wykorzystanie historycznych informacji w celu identyfikacji trendów, optymalizacji procesów, podejmowania decyzji i zwiększenia przychodów. Analizowanie dzięki uczeniu się maszynowemu nieustrukturyzowanych danych pozwala na wyszukiwanie określonych wzorów zachowań, a tym samym na dopasowywanie i personalizację produktów i usług.

Światowa polityka gospodarcza jest w jakimś stopniu oparta na danych, nawet pobranych z takich narzędzi jak Google Trends. To one pokazują nam, czego ludzie szukają w popularnej wyszukiwarce, czy co ich

aktualnie interesuje, jakiego rodzaju pracy poszukują. To daje obraz sytuacji, jeśli chodzi o trendy na rynku pracy, zmiany gospodarcze, rynek turystyczny czy aktualne preferencje żywieniowe. Z tego rodzaju danych korzysta nawet Europejski Bank Centralny, które wykorzystuje do swoich prognoz. Nie jest tajemnicą, że również pod tym kątem analizowany jest Twitter. Dane stanowią zatem ważne zasoby. Są podstawą funkcjonowania globalnych korporacji GAFAM (Google, Amazon, Facebook, Apple, Microsoft).

Oczywiście dane gromadzone są przez firmy od lat, ale z reguły były to zbiory nieuporządkowane, często w postaci analogowej, zbierane niesystematycznie i bez wyraźnego celu. Teraz dzięki wydajnym komputerom oraz uczeniu się maszynowemu systemy potrafią lepiej czytać zbiory danych i dostrzec w nich prawidłowości. Operacje zajmujące obecnie sekundy wymagałyby kilku lat pracy

analityków. Big data pozwala zatem lepiej doradzać klientom przy wyborze produktów finansowych, lepiej zarządzać ryzykiem oraz realizować przeróżne projekty, które wcześniej nie były możliwe.

Nie ma się co dziwić, że tak wiele banków stworzyło centralne rejestry kredytowe dla każdego klienta oraz działy Data Science. Banki wiedzą, na co ich klienci wydają pieniądze, jakie mają nawyki i potrzeby. Mogą dokonywać predykcji co do przyszłych wydatków, a także tworzyć segmentacje oraz spersonalizowane oferty.

Big data pomaga również w określaniu sytuacji na rynkach finansowych. Deutsche Bank korzysta w tym zakresie z platformy opartej na sztucznej inteligencji i machine learning. Alpha-Dig „zna” język naturalny, „czyta” informacje zawarte w prasie, dokumentach regulacyjnych czy w mediach społecznościowych, różne newsy dotyczące danego kraju i na tej podstawie określa sytuację

polityczną. Pomaga to np. inwestorom w podjęciu decyzji, ograniczając ryzyko popełnienia błędu.

Automatyczna analiza dużych i różnorodnych zbiorów danych (big data) możliwa jest dzięki uczeniu się maszynowemu, które zostanie omówione w kolejnym rozdziale.

Uczenie maszynowe

Uczenie maszynowe – umiejętność uczenia się nadana komputerom bez wyraźnego ich zaprogramowania.

(Arthur Samuel, 1959)

Każdy mniej więcej wie, na czym polega proces uczenia się człowieka. Wystarczy przyjrzeć się, jak małe dziecko w trakcie zabawy analizuje różne przedmioty, które są jej elementem, podejmuje jakieś decyzje, stopniowo zdobywa wprawę i doświadczenie, staje się coraz bardziej sprawne w swoich działaniach.

Podobnie robią systemy sztucznej inteligencji, które uczą się, poprzez sprzężenie zwrotne wyciągają różne wnioski z sukcesów i porażek, korygują swoje działania, a jeśli uznają to za konieczne, potrafią też zaadaptować się do nowych warunków. W ten sposób, podobnie jak człowiek, dochodzą stopniowo do wysokiego poziomu efektywności działania.

Ale tutaj ważna uwaga: uczenie się maszyn wydaje się jednak z pewnej perspektywy być bardziej efektywne niż uczenie się człowieka. Ludzie w porównaniu do komputerów uczą się wolniej, niesystematycznie, mają swoje ograniczenia czasowe oraz zniekształcenia. Ponadto zaprogramowane algorytmy komputerowe można wykorzystywać

w różnych kontekstach i zadaniach. Zupełnie inaczej jest z ludźmi – każdy uczy się swoim indywidualnym trybem, a przeniesienie wiedzy z jednego człowieka na innego jest niemal niemożliwe. Wszyscy wiemy, jaki potrafi się pojawić chaos, gdy dana osoba o sporej wiedzy i doświadczeniu, które jest kluczowe dla wykonania zadania, pójdzie na dłuższy urlop, i to nawet jeśli przed swoim urlopem zostawi ona odpowiednią notatkę ze szczegółami – co zostało niedokończonych, co należy zrobić. Z kolei całkowite odejście z pracy takiej osoby powoduje często rozregulowanie całego dotychczasowego systemu pracy.

Nie sposób jest w pełni w maszynie odwzorować sposób uczenia się człowieka. Zresztą być może nie miałyby to sensu. Musielibyśmy przecież wtedy maszynie zaprogramować również różne ułomności, które są częścią procesu przyswajania wiedzy przez

człowieka (zapominanie, tendencyjność, spadki motywacji itd.).

Korzystając z rozmaitych systemów online, bardzo często bierzemy udział w procesie nauczania maszyn. Przykładem jest system captcha. Naszym zadaniem jest rozpoznanie określonych obiektów na zdjęciach, co pozwala nam się zalogować. Pomagamy w ten sposób maszynie „nauczyć się” rozpoznawać obiekty, które nie potrafi rozpoznać w sposób automatyczny. Bierzemy zatem udział w procesie tworzenia oraz doskonalenia systemów identyfikacji rozmaitych obiektów przez sztuczną inteligencję. Bywa, że uczenie maszyn nazywane jest procesem „etykietowania”, gdyż rzeczywiście „uczenie” wydaje się określeniem mocno na wyrost.



Celem uczenia maszynowego w biznesie jest tworzenie algorytmów i modeli, które pozwalają przewidywać wzory podejmowania decyzji przez klientów. Nawet jeśli dojdzie do pewnych zmian w preferencjach i przyzwyczajeniach – następuje szybka aktualizacja kodu oprogramowania.

Uczenie się maszyn przyspieszyło znacząco rozwój innych technologii, jak robotyka czy systemy rozpoznawania mowy. Znalazło zastosowanie wszędzie tam, gdzie ważne jest przewidywanie zachowań ludzi (np. w ubezpieczeniach czy rekrutacji) czy urządzeń (np. wykrywanie awarii maszyn).

Uczenie maszynowe możliwe jest dzięki wykorzystaniu różnego rodzaju algorytmów.

Korzyści z wykorzystania algorytmów machine learning w bankowości:

1. automatyzacja kluczowych procesów,
2. bieżąca komunikacja z klientami (poprzez chatboty),

3. tworzenie unikalnych profili każdego klienta bankowego:

- a. personalizowanie ofert, rekomendacje i dopasowywanie produktów i usług,
- b. tworzenie prognoz dedykowanych dla banków oraz dla klientów,
- c. szybkie ocenianie zdolności kredytowych,
- d. szybkie wykrywanie oszustw, korzystając z biometrii behawioralnej.

Ludzie mogą się uczyć na kilka sposobów. Z maszynami jest podobnie. Wyróżniamy uczenie się nadzorowane, nienadzorowane oraz uczenie ze wzmocnieniem (**patrz rys. 6**). A którą metodą będziemy uczyć nasz program, zależy od danych wejściowych i charakteru rozwiązywanego problemu.

Uczenie nadzorowane

Ten rodzaj uczenia maszynowego (ang. *supervised learning*) nazywany jest też „uczeniem z nauczycielem”, gdyż przypomina sytuację, w której nauczyciel

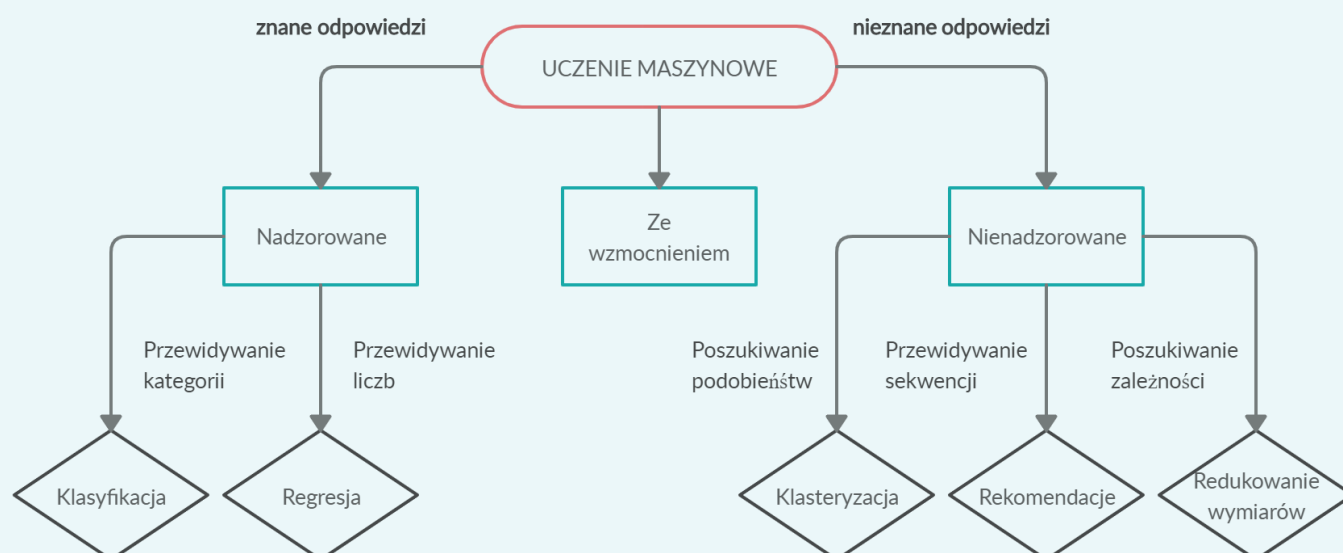
uczy małe dziecko w szkole. Przykładowo – dziecko poznaje figury geometryczne pod nadzorem osoby dorosłej, otrzymuje zestaw prawidłowych nazw określonych figur, a następnie samo już, bez jego pomocy, potrafi poprawnie zaklasyfikować figury, nawet gdy będą się one różniły od pierwotnego zestawu jakimiś cechami (np. wielkość czy kolor).

Weźmy inny przykład. Każdy z nas pewnie składał kiedyś pranie i lokował je w szafie na poszczególnych półkach. Wyobraźmy sobie, że chcemy, aby zrobiła to za nas sztuczna inteligencja. Przyjmijmy jednocześnie, że elementem naszego systemu jest kamera z funkcją rozpoznawania obiektów.

Przygotowujemy zestaw treningowy, pokazując np. różne koszulki. System koduje cechy różnych wersji koszulek.

Po takiej nauce, podobnie jak to bywa w szkole, przychodzi czas na egzamin – zachodzi konieczność sprawdzenia, czy program potrafi generalizować wiedzę w przypadku kontaktu z nowym zestawem. W ramach testu pokazujemy różne ubrania, wśród nich koszulki. System porównuje posiadane

RYŚ. 6. Rodzaje uczenia maszynowego i ich cele



dane wzorcowe z tym, co jest mu pokazywane. Następuje klasyfikacja: koszulka/niekoszulka. Można powiedzieć, że jest to wyjście o charakterze jakościowym, gdzie klasyfikator kwalifikuje obiekt do jednej z dwóch kategorii.

Tego rodzaju uczenie zastosowano np. w filtrach antyspamowych poczty Gmail. Kto pełni rolę nauczyciela w tym przypadku? Sami użytkownicy Gmaila, którzy stale oznaczają podejrzane wiadomości. Ten proces nazywany jest w uczeniu maszynowym – etykietowaniem. Dzięki temu na bieżąco są łatanie luki w systemie. Spam jest rozpoznawany poprzez porównanie pewnych specyficznych cech, które są identyfikowane w e-mailach zaklasyfikowanych jako spam. Ktoś zatem stoi na bramce naszej poczty i wpuszcza, albo kieruje do spamu napływające wiadomości. Coraz częściej żmudny proces etykietowania jest przenoszony na społeczność (tzw. *crowdsourcing*), to dzięki ludziom dane zyskują odpowiednie etykiety. Tak właśnie robi aplikacja Google Crowdsourcing i tak tłumaczy ideę oznaczania różnych zaprezentowanych przez system danych: „Twoja pomoc ma znaczenie”

Gdy używasz Crowdsourcing od Google, sprawiasz, że usługi takie jak Tłumacz Google, Mapy Google czy wyszukiwarka Google są bardziej przydatne dla Twojej lokalnej społeczności.

Crowdsourcing gromadzi odpowiedzi Twoje i osób z całego świata. Pomagają nam one w opracowywaniu usług odpowiadających na potrzeby wszystkich ludzi i kultur. Dziękujemy, że pomagasz nam w tworzeniu usług przeznaczonych dla użytkowników ze wszystkich krajów.

Również Netflix płaci zawodowym oglądaczom filmów będących na jej platformie. Ich zadaniem jest oznaczanie etykietkami poszczególnych filmów.

Oczywiście oddanie do decyzji społeczności co do nadawania określonych etykiet wiąże się z ryzykiem przeniesienia na algorytm określonych skrzywień poznawczych czy tendencyjności człowieka, zwłaszcza gdy rzecz dotyczy obiektów czy sytuacji niejednoznacznych – np. jakiegoś wartościowania obiektów (klasyfikacji emocji, kategoryzowania obiektów jako przyjemnych/nieprzyjemnych itd.)

mentowych. Instytucje, które stosują takie algorytmy, mogą zostać zaalarmowane odpowiednio wcześniej i reagować, mogą też uwzględnić w swojej strategii fakt, że odejście niektórych osób ma charakter nieunikniony (np. zgony).

Uczenie nienadzorowane

Uczenie nienadzorowane (ang. *unsupervised learning*) jest nazywane czasami „prawdziwą sztuczną inteligencją” czy „uczeniem się bez nauczyciela”. W tym przypadku algorytm sam dokonuje analizy danych i znajduje określone prawidłowości. Niepotrzebny jest żaden



Systemy sztucznej inteligencji też się uczą – poprzez sprzężenie zwrotne wyciągają różne wnioski z sukcesów i porażek, korygują swoje działania, a jeśli uznają to za konieczne, potrafią też zaadaptować się do nowych warunków. W ten sposób, podobnie jak człowiek, dochodzą stopniowo do wysokiego poziomu efektywności działania.

Ale algorytm uczenia nadzorowanego może na wyjściu dostarczać dane o charakterze ilościowym – w postaci liczb. Tak jest np. w przypadku algorytmów predykcyjnych, opartych na regresji (czyli określeniu wartości jednej zmiennej na podstawie znanych wartości innych zmiennych). Potrafią one przewidywać stany gotówkowe w oddziałach banku czy prognozować prawdopodobieństwo rezygnacji klientów z danej usługi na podstawie analizy ich zachowań. Prognozowanie rezygnacji (ang. *churn prediction*) jest niezwykle cenne w przypadku modelu biznesowego opartego na posiadaniu klientów długoterminowych abona-

wcześniejszy trening oraz określanie, jaka jest wartość wyjściowa. Jednocześnie sieć nie otrzymuje zewnętrznego sprzężenia zwrotnego. Krótko mówiąc – człowiek nie wie, jaki będzie wynik pracy takiego algorytmu. Można to porównać do uczenia się w wieku niemowlęcym, gdzie spontaniczna eksploracja świata pozwala dziecku porządkować wiedzę o świecie.

Trzymając się przykładu ze składaniem prania, wyobraźmy sobie, że pozwalamy maszynie, aby sama dokonała przeglądu odzieży i podzieliła ją na kupki po względem określonych cech. Powstają wtedy zbiory, którym

my nadajemy etykiety, np. koszulki, spodnie, skarpetki, majtki itd. A zatem cechą charakterystyczną tej sieci jest samoorganizacja.

W tym procesie to maszyna podejmuje decyzję w zakresie stworzenia kategorii. Warto jednak zauważyć, że może to się okazać zupełnie błędnym podejściem – np. maszyna może dokonać podziału wedle kolorów, a nie szeregu elementów kroju. Dlatego ten rodzaj uczenia się maszyn nie zawsze się sprawdza. Zresztą podobnie jest z ludźmi – czasami widzimy, że przyjęta metoda nauczania czegoś naszego podopiecznego przyniosła niesatysfakcjonujący skutek. Pokazuje to jednocześnie, jak ważne jest dobranie odpowiedniej metody nauczania algorytmu.

Uczenie nienadzorowane potrafi być pomocne w generowaniu podpowiedzi klientom sklepów internetowych, rozpoznając mniej oczywiste prawidłowości w potrzebach konsumenckich. Wynika to z faktu, że proste badania marketingowe – wywiady czy deklaracyjne ankiety – mogą w istocie nie pokazywać prawdziwych zachowań w procesie zakupu.

Doświadczony analityk w banku potrafi wydobyć istotne informacje z dokumentów korporacyjnych i podjąć decyzję. Ale dobrze zaprojektowane systemy AI potrafią to już coraz lepiej, a do tego znacznie szybciej, bo w sposób zautomatyzowany, bez konieczności wcześniejszego programowania przez człowieka. Same potrafią znaleźć wzory w danych.

Ten sposób uczenia się potrafi jednak budzić kontrowersje – jest to tzw. problem czarnej skrzynki – mamy dane wejściowe i wyjściowe. Nie wiadomo, co jest w środku, nie wiadomo, jak system

doszedł do wypracowania reguł. Ale część naukowców zajmujących się sztuczną inteligencją nie uznaje tego za poważny problem. Człowiek też nie jest często w stanie opowiedzieć, czym się kierował, podejmując taką czy inną decyzję. Sztuczna inteligencja w tym ujęciu posiada coś w rodzaju sztucznej intuicji. Czarna skrzynka to konstrukt, który przypomina behawioryzm – jest bodziec, po nim następuje reakcja, ale nie wiadomo, jaki proces zachodzi pomiędzy tymi zdarzeniami

Pod wpływem tego rodzaju rozważań narodziła się idea wyjaśnialnej sztucznej inteligencji (ang. *explainable AI* – XAI), czyli zestawu narzędzi i struktur, które pomagają opracowywać interpretowalne i integracyjne modele uczenia maszynowego.

Uczenie ze wzmocnieniem

To uczenie oparte na behawioralnym systemie kar i nagród. Dzieci, sa-

modzielnie eksplorując nieznany im świat, uczą się w taki sposób – dotykają, smakują, wążają i przekonują się (czasami boleśnie), czy takie działanie przynosi przyjemne lub nieprzyjemne doznania. W uczeniu się maszynowym takim dzieckiem jest algorytm określany mianem „agenta”, którego działania uzyskują wzmocnienia pozytywne (nagrody) lub negatywne (kary). Subtelna różnica pomiędzy uczeniem się dziecka a uczeniem się algorytmu sprowadza się jednak do tego, że dla algorytmu ważne jest maksymalizowanie skumulowanej nagrody w dłuższym horyzoncie czasowym (a nie „teraz i tu”). A zatem np. roboty wykorzystujące ten rodzaj uczenia się nabierają stopniowo wprawy i po pewnym czasie zaczynają działać o wiele



dokładniej i szybciej. I co ważne – nie potrzebują żadnego wcześniejszego programowania przez programistę. Uczenie się robotów można też znacząco przyspieszyć poprzez jednoczesne uczenie się kilku urządzeń, zintegrowanie nabytej wiedzy i zwrotny jej transfer do maszyn. W przypadku wielu robotów system może dojść do sprawności w bardzo krótkim okresie, popełniając z czasem coraz mniej błędów.

Przykładem może być program do gry w szachy Alpha Zero. Został on wyposażony w algorytm, który na początku rozegrał miliony partii sam ze sobą, doświadczając zwycięstw i porażek, a następnie po takim treningu podesłano mu prawdziwego rywala – był nim inny program tego rodzaju – Stockfish 8.

Stockfish był wyposażony w strategię oparte na zakodowanej wiedzy na temat kilkuset tysięcy partii rozegranych przez różnych mistrzów szachowych. Zdaniem obserwatorów Alpha Zero, gra zaskakująco, często wydawałoby się irracjonalnie, ale finalnie zdobywa on przewagę nad konkurentem. Pokazuje to siłę treningu w postaci uczenia się ze wzmocnieniem. W podobny sposób nauczono inny algorytm grać w grę Go (AlphaGo).

W tym wypadku składanie prania odbywałoby się pod pewnym „nadzorem”. Zaprogramowane zostaną pewne reguły działania, dzięki czemu maszyna wie, co należy do kategorii np. koszulka, a co do kategorii spodnie czy skarpetki. Za każdym razem otrzymując feedback pozytywny lub negatywny. W ten sposób maszyna powoli dochodzi do wysokiej sprawności.

Algorytmy uczenia maszynowego

Algorytm ma stosunkowo prostą definicję – to inaczej zbiór kroków niezbędnych do wykonania zadania.

Ludzie posiadają algorytmy w odniesieniu do większości wykonywanych przez nas czynności. Np. robienie zakupów czy wychodzenie z domu. Dla komputerów to zbiory kroków dla wykonania przez niego zadania.

Algorytmy uczenia się maszynowego już teraz pomagają w przetwarzaniu ogromnych ilości danych, dokonywaniu analiz w czasie rzeczywistym, a także predykcji. I co ważne – pozwalają znacząco skrócić czas przeprowadzanych operacji. Dąży się do zmaksymalizowania ich wydajności.

Sieć neuronowa

Sztuczne sieci neuronowe (SSN) to w istocie jeden z typów uczenia maszynowego.

Sztuczna sieć neuronowa jest próbą odwzorowania struktury połączeń w ludzkim mózgu (choć zdaniem wielu to gruba przesada, i powinniśmy raczej mówić o symulowaniu mózgu owadów). To swoisty układ nerwowy sztucznej inteligencji.

Ludzie poznają świat za pomocą swoich biologicznych neuronów. Mamy ponad 170 mld komórek nerwowych, ponad 80 mld neuronów, a do tego ok. 100 trylionów synaps. Neuron biologiczny to pojedyncza komórka układu nerwowego, jest ona dość złożona, ale można ją bardzo mocno uprościć

”

Sztuczne sieci neuronowe są wykorzystywane do prognozowania, czy też podejmowania decyzji przez inteligentne rozwiązania, jak np. roboty. W bankowości SSN pozwalają na automatyczne generowanie decyzji kredytowych na podstawie analiz szeregu danych dotyczących klienta. Znacząco przyspieszają szereg procesów w bankach.

i opracować sztuczny odpowiednik, który, podobnie jak ludzki, pobiera dane wejściowe, przelicza je i generuje dane wyjściowe.

Jak pokazuje **rysunek 7**, sztuczny neuron otrzymuje szereg danych wejściowych. Wejścia te są odpowiednikiem dendrytów w ludzkich komórkach nerwowych. Sztuczny neuron sumuje każdy z sygnałów wejściowych, przy czym każdy z nich (W_1 , W_2 , W_3) ma przypisane określone wagi. Są one odpowiednikiem synaps w ludzkich komórkach nerwowych. Podobnie jak w przypadku ludzkiej aktywności – niektóre bodźce odbierane z otoczenia mają duże znaczenie, a niektóre możemy zupełnie zignorować. Wagi ulegają automatycznej modyfikacji (tzw. propagacja wag), których dokonuje algorytm uczenia się w każdym z neuronów sieci.

Wyjście sztucznego neuronu jest odpowiednikiem zakończeń aksonu w komórkach nerwowych. Z kolei blok su-

mujący to coś w rodzaju jądra komórki. Wyjście pojedynczego neuronu stanowi wejście dla kolejnego: neuron przekazuje zagregowane dane dalej. W taki sposób utkana jest sieć neuronowa. SSN mogą posiadać różną architekturę, ale każda posiada dwie warstwy zewnętrzne – wejściową, pobierającą dane i wyjściową generującą wyniki obliczeń, oraz warstwy wewnętrzne (ukryte), które są pomiędzy nimi. Warstw ukrytych może być od kilku do kilkunastu (**patrz rys. 8**).

Sztuczne sieci neuronowe są wykorzystywane do prognozowania, np. ceny nieruchomości czy samochodów, mogą też wspomagać podejmowanie decyzji przez inteligentne rozwiązania, jak samochody autonomiczne czy roboty. W bankowości sieci neuronowe pozwalają na automatyczne generowanie decyzji kredytowych na podstawie analiz szeregu danych dotyczących klienta. SSN znacząco przyspieszają szereg procesów operacyjnych w bankach.

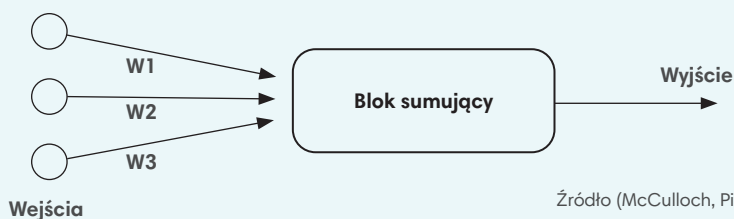
Evan Schnidman, założyciel St. Louis-based Prattle Analytics LCC twierdzi, że ich sieć neuronowa jest w stanie w ciągu 45 sekund przeczytać treść dokumentu o długości 500 słów.

Głębokie uczenie

Uczenie głębokie (ang. *deep learning*) to jedna z technik uczenia maszynowego wykorzystująca sieci neuronowe na głębszym poziomie.

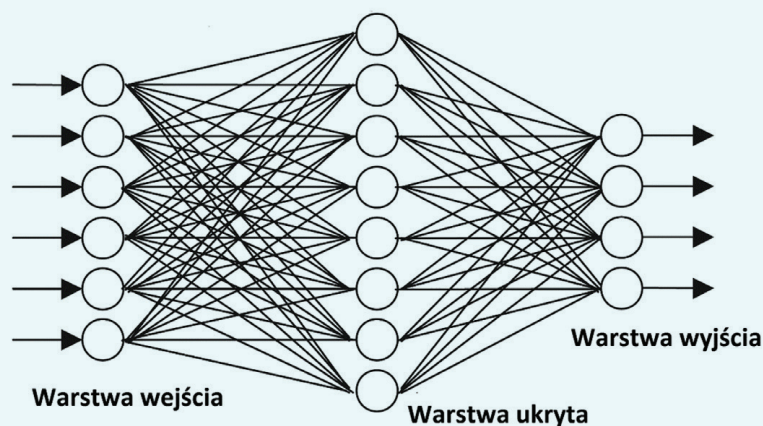
W uczeniu się tego rodzaju dochodzi do zwielokrotnienia liczby „ukrytych warstw” sieci neuronowych. Ich stany zmieniają się wraz z pojawieniem

RYS. 7. Najprostszy model sztucznego neuronu



Źródło (McCulloch, Pitts, 1943)

RYS. 8. Przykładowy model sztucznej sieci neuronowej



Schemat warstwowej sieci neuronowej

Źródło <https://mlodytechnik.pl/technika/29211-czego-sie-ai-nie-nauczytego-terminator-nie-bedzie-umial>

się nowych informacji, umożliwiając systemowi stałe uczenie się. Dzięki temu możliwe jest wyszukiwanie lub kategoryzowanie obrazów czy rozpoznawanie mowy.

ROBOTYZACJA I AUTOMATYZACJA

Połączenie rozwiązań sztucznej inteligencji z robotyzacją powtarzalnych czynności (RPA – *Robotic Process Automation*) daje automatyzację poznawczą (kognitywną). Nie chodzi tu o prostą cyfryzację pracy, ale wsparcie operacyjne pracownika za pomocą inteligentnych narzędzi pracujących w sposób zautomatyzowany.

Automatyzacja tego rodzaju to system bardzo różnych technologii. Roboty pracujące „na zapleczu” dzięki

uczeniu maszynowemu, technologii semantycznej, przetwarzaniu języka naturalnego mogą analizować treść korespondencji z klientami. Narzędzia eksploracji danych (*data mining*) pomagają wyciągać najważniejsze informacje z przesłanych materiałów, systemy wykorzystujące „*text mining*” potrafią wyszukiwać i klasyfikować kluczowe dla banku treści. Pomocna jest tu także technologia optycznego rozpoznawania znaków, OCR (od ang. *optical character recognition*), która pozwala odczytać tekst w zeskanowanych dokumentach, z kolei algorytmy ML pomagają katalogować określone obrazy czy treści w nich zawarte. Wreszcie na koniec specjalne algorytmy umożliwiają kontroling i weryfikację poprawności dostarczonej dokumentacji.

Automatyzacja kognitywna, należy do trzeciej klasy rozwiązań robotyzacji, gdzie inteligentne maszyny nie dokonują prostej syntezy danych (jak w klasie 1 i 2), ale pracują w sposób zbliżony do ludzi, gdzie oprócz porządkowania danych dokonują złożonych analiz i podejmują decyzje.

Automatyzacja tego rodzaju:

- usprawnia obieg dokumentów, porządkuje i przyspiesza prace w systemie 24/7,
- eliminuje szereg potencjalnych (ludzkich) pomyłek przy czytaniu i weryfikacji dokumentów,
- ułatwia i poprawia podejmowane decyzji, zwłaszcza w złożonych przypadkach,
- zapewnia powtarzalny i przejrzysty proces,
- zwiększa zadowolenia klienta,
- generuje olbrzymie oszczędności (odciążenie pracowników i zmniejszenie ich liczby).

Dzięki zaawansowanej robotyzacji i automatyzacji paradoksalnie bank może być bliżej klientów, skupić większą uwagę na budowaniu relacji z nimi. Ów wpływ na zmiany ekonomiczne i organizacyjne w przedsiębiorstwach jest przedmiotem badań i analiz robonomiki (ang. *robonomics* – termin powstał z połączenia słów robotyka i ekonomika).

Instytucje finansowe stosują rozwiązania robotyczne różnej klasy, autorskie



lub oparte na rozwiązaniach. Ayasdi AI czy Zest AI to specjalne platformy oparte na uczeniu maszynowym do analiz i podejmowania decyzji przez instytucje finansowe.

JPMorgan zainwestował we własną platformę Intelligence Contract (COiN), która analizuje dokumenty prawne, bot potrafi w sekundy wykonać operację, które człowiekowi zajęłyby 360 tys. godzin!⁶. Odpowiada to 12 tys. godzin analiz umów kredytowych. Bank uruchomił również wirtualnego asystenta ds. płatności korporacyjnych⁷.

⁶ <https://www.bloomberg.com/news/articles/2017-02-28/jpmorgan-marshals-an-army-of-developers-to-automate-high-finance>

⁷ <https://www.jpmorgan.com/country/PL/en/detail/1320568426081>

W Polsce ING Bank Śląski ma własne rozwiązanie RoboPlatform, a BNP Paribas ma platformę do usprawnień operacji Smart Workforce.

Boty

Nazwa „chatterbot” została po raz pierwszy użyta przez **Michaela Mauldina**, twórcę Verbota w roku 1994, później rozwój technologii spowodował również rozwój nazewnictwa.

Ogólnie mówi się o botach, a najczęściej spotykaną ich formą są boty tekstowe (chatboty), ale od niedawna coraz częściej wdrażane są również boty głosowe, nazywane również voicebotami.

A zatem boty to inaczej asystenci cyfrowi, którzy komunikują się za pomocą wiadomości tekstowych lub głosowo bez udziału człowieka.

Do tworzenia baz wiedzy chatbotów wykorzystuje się język znaczników – AIML. Boty działają, opierając się na różnych rozwiązaniach regułowych oraz na AI, jak i NLP – przetwarzaniu języka naturalnego (ang. *Natural Language Processing*), wraz z NLG (ang. *Natural Language Generation*), czyli silnikami do przetwarzania i generowania języka naturalnego oraz NLU (ang. *Natural Language Understanding*), co pozwala rozumieć intencję rozmówcy, interfejs języka naturalnego (NLI – *Natural Language Interface*), który zapewnia naturalną, mniej standardową interakcję, moduły głosowe ASR (ang. *Automatic Speech Recognition*), które pozwalają zamienić ludzką mowę czy TTS (ang. *text to speech*), system pozwalający zamienić tekst na mowę, aby chatbot mógł odpowiedzieć głosowo), a także systemy analizy rozmów (ang. *Speech Analytics*), czyli aplikacje służące do rozumienia analizy kontekstowej i emocjonalnej zarejestrowanych rozmów.

Za jednego z pierwszych chatbotów w bankowości na świecie uważany jest Ally Assist, wprowadzony przez Ally Bank w 2015 r. Od tego czasu technologia mocno się rozwinęła.

Chatboty wykorzystujące sztuczną inteligencję mają szerokie zastosowanie w bankowości. Ich możliwości komunikacyjne są w zasadzie nieograniczone. Mogą one obsługiwać zapytania potencjalnych klientów oraz już korzystających z usług banku, pełniąc funkcje wirtualnych asystentów czy wirtualnych doradców. Sprawdzają się zarówno na styku z klientem (front office), jak i na zapleczu (back office). Ale stosuje się je coraz częściej w innych obszarach działalności banku, np. w Polsce w procesach rekrutacyjnych (takich rozwiązań używa np. mBank,

TAB. 3. Zalety chatbotów stosowanych w bankowości

Tańsze od pracy człowieka
Praca 24/h
Natychmiastowa reakcja
Systematyczne zbieranie danych, co pozwala stworzyć segmentację behawioralną klientów
Możliwa personalizacja rozmowy (w przypadku zaawansowanych rozwiązań opartych na AI)
Możliwość zintegrowania ze środowiskiem do obliczeń statystycznych oraz wizualizacji danych
Dodatkowy kanał up-sellingowy
Możliwość dokładnego udzielania informacji zgodnie z założonym skryptem
Możliwość szybkiego przekierowania do specjalisty
Wysoka jakość obsługi (Customer Experience)

PKO BP czy BZ WBK) czy też do komunikacji z partnerami (np. PKO BP używa chatbota do komunikacji ze start-upami chcącymi wziąć udział w programie wsparcia) albo też do obsługi programów lojalnościowych (np. Citi Handlowy ułatwia klientom znalezienie rabatów dostępnych u lokalnych partnerów ich programu).

Czy boty zastąpią działy call center? Juniper Research⁸ prognozuje, że do roku 2022 do 93% interakcji z klientami prowadzonych będzie poprzez boty.

⁸ <https://www.juniperresearch.com/analysis/press/july-2017/chatbot-conversations-to-deliver-8bn-cost-saving>

Wyniki badań pokazują, że do 2022 r. zapewnią one oszczędności w wysokości 8 mld dolarów, gdyż pozwalają zaoszczędzić bankom 4 minuty na każdym zapytaniu.

Chatboty wciąż odpowiadają klientom głównie na podstawowe informacje (**patrz tab. 4**), ale rynek botów rośnie, bo wciąż poszerzają się ich funkcje.

Każdy zapewne doznawał uczucia irytacji, gdy człowiek na infolinii potrzebował chwili na poszukanie odpowiedzi w swoich skryptach czy nawet zawieszał rozmowę na jakiś czas. Mimo to ludzie wciąż mają opory przed komunikacją z botami, zamykając wyskakujące okienka chatbotów, gdy się pojawią na różnych stronach internetowych z pytaniem „w czym mogę pomóc”? Jednak nowoczesne, inteligentne boty potrafią być bardziej naturalne, prowadzić wciągające konwersacje, gdyż potrafią rozpoznawać intencję na podstawie kontekstu rozmowy, a nie jedynie poprzez identyfikację słów kluczowych i na tej podstawie generować standardowe odpowiedzi. Coraz częściej można również porozmawiać z chatbotami na różne poboczne tematy. Może się zatem okazać, że szybko oswoimy się z komunikacją botami i przestaniemy tęsknić za ludzkimi asystentami.

Istnieją różne rodzaje chatbotów, te stosowane w biznesie można podzielić na⁹:

- Chatboty oparte na menu (nazywane również buttonowymi):

⁹ <https://chatbotmagazine.com/the-3-types-of-chatbots-how-to-determine-the-right-one-for-your-needs-a4df8c69ec4c>



Są obecnie najbardziej podstawowym rodzajem chatbota na rynku. W większości przypadków są oparte na hierarchii drzewa decyzyjnego, z przyciskami podobnymi do menu telefonu. Od użytkownika wymaga się dokonania kilku wyborów, aby dotrzeć do ostatecznej odpowiedzi. Ten rodzaj chatbotów jest wskazany, gdy klienci powtarzają stale te same pytania.

- Chatboty identyfikujące słowa kluczowe:

Wychwytują słowa kluczowe z tekstów wpisywanych przez użytkownika i odpowiednio reagują. Coraz bardziej spotykane są też chatboty hybrydowe – oparte na rozpoznawaniu słów kluczowych i menu.

- Chatboty kontekstowe:

Najbardziej zaawansowany spośród botów tu omówionych. Wykorzystują uczenie maszynowe i sztuczną inteli-

gencję. „Uczą się” swojego użytkownika podczas każdej rozmowy z nim, w zakresie jego różnych potrzeb i preferencji. Rozumieją kontekst wypowiedzi. Takie boty potrafią angażować się w naturalną rozmowę z klientem przez dłuższy czas.

Wiele banków raportuje bardzo duże korzyści z wykorzystania chatbotów.

Indyjski Bank HDFC jest w posiadaniu pierwszego i największego w Indiach chatbota bankowego zasilanego sztuczną inteligencją o nazwie Eva. Bot ten przetwarza ponad 300 tys. zapytań każdego dnia, łącznie odpowiedział już na ponad 5 mln zapytań od około miliona klientów z dokładnością ponad 85%. Eva udziela odpowiedzi w ułamki sekund. Z kolei

szwedzki bank komercyjny – SEB – stworzył dwa chatboty: Aidę, do obsługi klientów oraz Amelię – dla komunikacji wewnętrznej w sprawach IT dla 15 tys. pracowników. Amelia otrzymuje ok. 300 różnych zapytań dziennie.

W Polsce Alior Bank od 2015 r. wykorzystuje polskiego voicebota Dronn. To robotyczny zaawansowany agent głosowy nagrodzony na wielu prestiżowych konkursach. System oparty na sztucznej inteligencji, biometrii i analizie mowy pozwala na dwustronną komunikację niemal jak z człowiekiem.

Banki adaptują również na swoje potrzeby dobrze znane na rynku rozwiązania głosowe oparte na sztucznej inteligencji. Brytyjski Barclays korzysta z Siri, która pomaga klientom robić przelewy, a amerykański Capital One

TAB. 4 Przykłady zadań wykonywanych przez chatboty w bankowości

wstępna weryfikacja problemu i przekierowywanie do odpowiedniego działu,
weryfikacja tożsamości klientów, np. poprzez zadawanie losowych pytań weryfikacyjnych,
reset haseł,
umawianie spotkań z pracownikami banku,
informacje o najbliższych placówkach banku i godzinach otwarcia,
połączenia tzw. miękkiej windykacji,
zbieranie oświadczeń FACTA (amerykańska regulacja prawna o zgodności z przepisami podatkowymi dla kont zagranicznych),
zbieranie reklamacji
rozmowy o statusie kredytu (sprawdzanie stanu spłaty, najbliższej raty, zamówienie harmonogramu spłaty itd.),
doładowanie kart płatniczych prepaid oraz telefonu,
otwarcie konta,
zamówienie karty,
sprawdzenie stanu konta,
przegląd historii transakcji,
przegląd nadchodzących płatności,
zrobienie przelewów zwykłych,
zrobienie przelewów na telefon,
zapłacenie BLIKIEM,
przewodzenie badań marketingowych

z Alexy, w Polsce PKO BP postawił na integrację z Asystentem Google.

Na potrzeby tworzenia chatbotów wykorzystuje się również często tzw. third-party app, jak np. Facebook Messenger. Jak podaje Facebook, w tym serwisie działa już ponad 300 tys. tego rodzaju asystentów. To rozwiązanie stosuje np. Credit Agricole – KrEdytka oraz mBank – Contact Center.

Funkcje głosowe i tekstowe można też połączyć ze sobą w jedną aplikację. Na tej zasadzie działa asystent Milla Banku Millennium – powstały w 2018 r. pierwszy w Polsce chatbot realizujący transakcje; Talk to IKO – obsługa głosowa aplikacji mobilnej PKO BP czy wdrożone ostatnio rozwiązanie Alia w Alior Banku.

Jest wiele innych rozwiązań platform konwersacyjnych, które mogą być zaadaptowane na potrzeby banków, jak Kai, Abe.ai, Centurysoft, czy Clinic AI.

Dr Johann Hauswald, naukowiec pracujący na Wydziale Informatyki i Inżynierii Uniwersytetu Michigan oraz współzałożyciel firmy Clinic na kongresie Impact fintech'17 w Katowicach zaprezentował Clinic AI – wirtualnego osobistego asystenta, który oprócz dość standardowych funkcji pomaga w analizach dotyczących gospodarowania własnym budżetem domowym, alarmuje, gdy kończą się pieniądze, a nawet pomaga w znajdowaniu najtańszego sklepu w okolicy.

Dzięki rozwiązaniom sztucznej inteligencji funkcje pomocnicze chatbotów będą się rozwijać. Systemy, poznając coraz lepiej swojego użytkownika mogą przecież składać różne oferty partnerów banku – np. wiedząc, że ktoś kupił narty, podesłać oferty wyjazdów narciarskich, albo wiedząc, że ktoś jedzie na koncert, polecić lokalne miejsca noclegowe. Systemy konwersacyjne oparte na rozwiązaniach sztucznej inteligencji stają się coraz doskonalsze i potrafią nie tylko komunikować się językiem potocznym, ale również językiem charakterystycznym dla danej grupy społecznej. Np. do nauczania chatbota IKO PKO wykorzystano 90 tys. zwrotów, proste sprawdzenie stanu konta można zrealizować na ok. 2 tys. sposobów. W przyszłości również voiceboty będą zapewne coraz lepiej rozumieć ludzki głos, wnioskować na tej podstawie o stanie emocjonalnym rozmówcy, następnie dostrajając swój własny głos i składać oferty oraz propozycje adekwatne do zidentyfikowanego nastroju. Te działania nie są wolne od kontrowersji, choć zapewne obecnie również irytujące jest gdy pracownik z call center nie jest w stanie wyczuć, że dzwoni w nieodpowiednim momencie, albo, że klient nie jest w nastroju na rozważanie kredytu na nowy dom, a raczej na pożyczkę na spłatę bieżącego zadłużenia.

Robodoradztwo

Erę robotów – doradców zapoczątkował w 2016 r. Bank of America. Dwa lata później Wealthfront stał się pierwszym doradcą robotycznym, który zaoferował bezpłatne, spersonalizowane planowanie finansowe dla swoich klientów. Business

Insider Intelligence¹⁰ przewiduje, że do 2022 r. cyfrowi doradcy zarządzają będą kwotą 4,6 bilionów dolarów.

Komisja Nadzoru Finansowego tak definiuje robodoradztwo¹¹: „Robo-doradztwo (ang. *Robo-advisors*) jest formą zautomatyzowanego doradztwa finansowego stosowaną m.in. w obszarze usług inwestycyjnych, pożyczek i ubezpieczeń. Rozwiązanie oparte jest na zaawansowanych algorytmach z wykorzystaniem sztucznej inteligencji i narzędzi do analizy dużych zbiorów danych (big data)”.

Komputer, analizując szereg danych historycznych, może dokonywać predykcji w odniesieniu do portfeli inwestycyjnych, może przygotować odpowiedni plan uwzględniający ryzyko inwestycyjne i specyfikę klienta. Następnie, po zatwierdzeniu przez niego, może dokonywać alokacji środków finansowych.

Roboty mogą też pełnić funkcję doradców kredytowych. Zautomatyzowany credit scoring pozwala na zobiektywizowanie reguł przyznawanych pożyczek. Ludzie są podatni na skrzywienia – do jednych czujemy większą sympatię, do innych mniej. Na decyzje analityków mogą oddziaływać różne uprzedzenia

czy tendencja do potwierdzenia własnych tez. Może to doprowadzić do różnych błędów analitycznych. Sztuczna inteligencja jest odporna na subiektywną ocenę.

Zalety wykorzystywania robodoradców w bankowości:

- szeroka dostępność doradców,
- niskie koszty (dla banku oraz klientów),
- sprowadzone rekomendacje finansowe dla konsumentów/inwestorów,
- minimalny udział człowieka (brak tendencji),
- wyniki analiz prezentowane w sposób ustrukturyzowany i powtarzalny.

Oczywiście nie brak zarzutów, że sztuczna inteligencja nie jest wolna od różnych uprzedzeń i może w swojej działalności dokonywać ocen zgodnie z punktem widzenia swojego twórcy. Może też nauczyć się pewnych skrzywień w toku swojej pracy.

Może się też zdarzyć, że część klientów straci zaufanie do banku, gdy zostanie im przydzielony robodoradca. Albowiem wiele osób preferuje kontakt międzyludzki i nie ufa maszynom. Ale jeśli przewidywania i strategię inwestycyjnych doradców robotycznych będą trafne, to zaufanie będzie rosło, a za kilkanaście czy kilkadziesiąt lat w bankach nie będzie ludzkich doradców.

Duże nadzieje należy pokładać we współpracy banków z sektorem technologii finansowych fintech (ang. *financial technology*). Choć nie brakuje rywalizacji, w wyniku takich powiązań

banki będą mogły przygotować klientom dodatkowe oferty zgodne z ich oczekiwaniami i budować ich przywiązanie do banku. Przykładem jest Nuvo, pierwszy brytyjski robotyczny broker kredytów hipotecznych. Chatbot, wykorzystując Messenger Facebook, po uzyskaniu od klientów odpowiedzi na szereg pytań jest w stanie w ciągu kilku minut wybrać najlepszy produkt hipoteczny spośród ok. 50 tys. możliwości.

Inne ciekawe rozwiązanie oferuje koreański Hana Bank. Klienci korzystający z aplikacji tego banku, zainteresowani zakupem danej nieruchomości, mogą otrzymać informację na jej temat oraz warunki pożyczki na jej zakup. Wystarczy tylko skierować kamerę w telefonie na dany obiekt.

Z systemu robo-advisory intensywnie korzysta jeden z największych banków inwestycyjnych na świecie – Morgan Stanley. Wspomaga on armię swoich doradców finansowych (ok. 16 tys.) agentami robotycznymi. Sztuczna inteligencja poprzez algorytmy analizuje sytuację klientów i śledzi na bieżąco różne opcje inwestycyjne. Rola ludzkiego doradcy sprowadza się w zasadzie do omówienia z klientem wygenerowanej propozycji.

Biometria

Dane biometryczne według art. 3 pkt 14 RODO to: „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczne uwierzytel-

¹⁰ <https://www.businessinsider.com/best-robot-advisors?IR=T>

¹¹ https://www.knf.gov.pl/dla_rynku/fin_tech/roboradztwo



nienie lub identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne”.

Procedura należytej staranności w rozpoznaniu klientów banków (KYC, *Know your customer*), unijna dyrektywa unijna PSD2 oraz rejestrowane przez banki coraz częstsze cyberataki nakładają konieczność silniejszej autoryzacji i uwierzytelniania użytkownika bankowości mobilnej i internetowej. Otwiera to drogę do rozwoju i zastosowania technologii biometrycznych w tych obszarach.

Coraz lepsze systemy rozpoznawania i analizy twarzy, które są jednocześnie tańsze we wdrożeniu, pozwalają na wykorzystywanie ich w systemach weryfikacji tożsamości. Bank Citi Handlowy oferuje np. możliwość wzięcia kredytu bez wychodzenia z domu. Identyfikacja odbywa się za pomocą kamery umieszczonej w smartfonie czy komputerze. Wiele banków, takich jak Alior Bank, BZ WBK (dziś Santander Bank Polska), Bank Pekao SA, Credit Agricole Bank Polska oraz Bank Millennium, umożliwia klientom założenie konta

online czy wzięcie pożyczki poprzez zrobienie sobie tzw. selfie i przesłanie zdjęcia dowodu osobistego. Sztuczna inteligencja w procesie weryfikacji sprawdza zgodność biometryczną twarzy na obu zdjęciach. Takie rozwiązanie zabezpiecza przed kradzieżą tożsamości.

Oprócz cech twarzy każdy użytkownik ma swój unikalny sposób posługiwania się komputerem czy telefonem. Ma swoje urządzenia i miejsca, z których się zwykle loguje do serwisów bankowości elektronicznej, ma też swoje charakterystyczne sposoby poruszania się na danej stronie. Mierzenie tego rodzaju unikalnych zachowań nazywa się biometrią behawioralną. Rozwiązania machine learningowe mogą się nauczyć i tworzyć modele dla każdego klienta i odróżniać je od innych. Gdy system zaobserwuje anomalie behawioralne (np. logowanie się z innej niż zwykle przeglądarki), może szybko, w sposób automatyczny powiadomić klienta i prosić np. o potwierdzenie SMS-em tożsamości.

Algorytmy machine learning, które gromadzą wiedzę o przeszłych trans-

akcjach, mogą pomóc w wykrywaniu i zapobieganiu oszustwom transakcyjnym, gdy pojawi się jakaś anomalia (np. gdy z konta danej osoby nagle zaczną być pobierane większe sumy, gdy wcześniej wydawała ona niewiele, czy kupowała tanie produkty).

Obecnie tworzone są całe platformy wykrywania oszustw z wykorzystaniem uczenia maszynowego (*fraud detection*). Przykładowo Bank Informacji Kredytowej ma dwa takie zintegrowane ze sobą rozwiązania: Platformę Antyfraudową (PAF), system do analizy, na bazie danych, ryzyka transakcji kredytowych oraz Platformę Cyber Fraud Detection (CFD), która umożliwia identyfikację urządzenia, z którego loguje się klient, i ocenia ryzyko jego przejęcia przez oszusta. Również Citibank wykorzystuje platformę Feedzai, zasilaną zaawansowanym silnikiem uczenia maszynowego, która analizuje stale szereg danych związanych z klientem i alarmuje go, gdy zachodzi podejrzenie oszustwa.

Nie ma niestety wciąż jednoznacznych regulacji prawnych związanych z biometrią, i nie brakuje już teraz kontrowersji, gdy banki poszerzają zakres jej stosowania przy udziale rozwiązań sztucznej inteligencji. W zeszłym roku Bank PKO BP rozmieścił w części swoich oddziałów specjalne sensory do zliczania uśmiechu pracowników oraz klientów banku. Z kolei ING Bank Śląski w czasie rzeczywistym analizuje obraz z kamer w oddziałach, po to aby monitorować liczbę klientów w poszczególnych działach swoich placówek. Kwestia danych osobowych i etyki powinny być zawsze na pierwszym planie jeśli chodzi o wdrażanie rozwiązań AI, gdyż utrata zaufania klientów oraz szkody wizerunkowe mogą w ogólnym bilansie przynieść więcej szkody niż korzyści danej instytucji finansowej.

DLACZEGO SZTUCZNA INTELIGENCJA

znajdzie istotne zastosowanie w bankowości?

Bez wątpienia jest istotnym wsparciem w realizacji bieżących procesów i działań operacyjnych w instytucjach finansowych. Na dodatek jej potencjał można wykorzystywać tak w projektach realizowanych wewnątrz banku, jak i w relacjach pomiędzy nim a jego klientami oraz wykorzystywaniu danych.

Sztuczna inteligencja zmienia oblicze współczesnego biznesu, głównie poprzez zmiany w trzech obszarach funkcjonowania każdej firmy. Pierwszy dotyczy **kontaktów z klientami** i lepszego dostosowywania oferty sprzedażowej i marketingowej. AI (od ang. Artificial Intelligence – sztuczna inteligencja) pozwala znacznie lepiej i precyzyjniej rozpoznawać potrzeby użytkowników, a także błyskawicznie na nie odpowiadać, dostosowując do nich indywidualną ofertę.

Obszar drugi to **optymalizacja wewnętrznych procesów** obecnych w każdej firmie, bez względu na jej wielkość czy specyfikę. To np. zmiana obiegu dokumentacji z wersji papierowej na cyfrową. Przeznaczone do tego narzędzia nie tylko pomagają porządkować dokumentację, ułatwiają jej przeszukiwanie i analizowanie, ale też odpowiednio ją zabezpieczają. Jest więc taniej, wygodniej, szybciej i bezpieczniej.

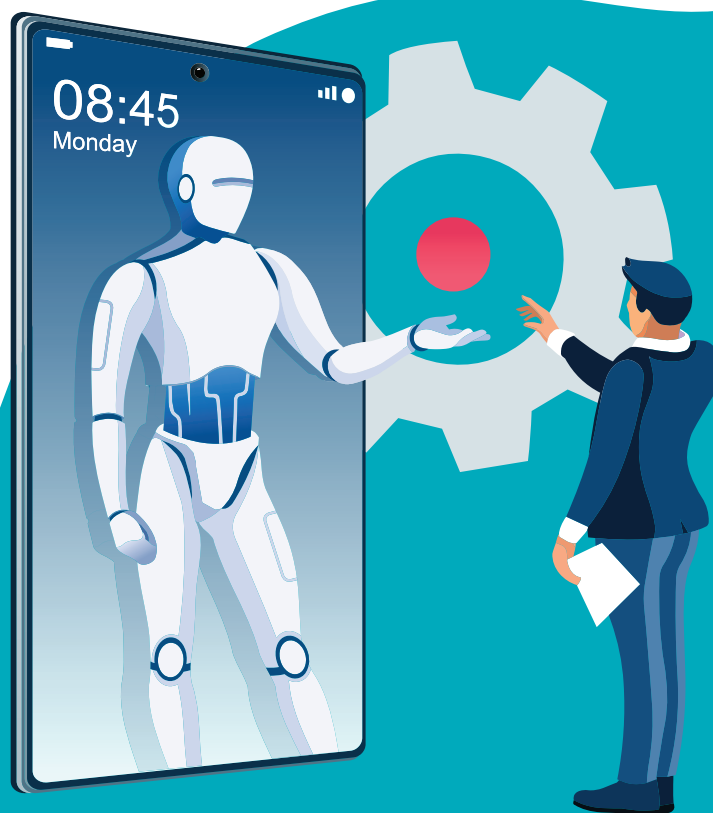
Trzecia sfera dotyczy **wykorzystania danych** gromadzonych w firmach. Informacje pozyskiwane z rynku, z kontaktu z klientami i kontrahentami to dla współczesnych biznesów niezbędny składnik skutecznego działania. Na-

rzędzia wykorzystujące sztuczną inteligencję pozwalają m.in. znacznie przyspieszyć procesy raportowania, a także dają możliwość analizy ogromnych zasobów informacji pod kątem poszukiwania trendów i zależności, które następnie spożytkować można do budowania przewagi biznesowej.

Sztuczna inteligencja to także jeden z wiodących trendów w sektorze bankowym. Zastosowanie rozwiązań opartych na AI ma nie tylko zrewolucjonizować branżę, ale przede wszystkim podnieść jakość świadczonych usług,

a tym samym przyspieszyć pewne procesy biznesowe, zaowocować większym zadowoleniem klientów i zmniejszyć ich odpływ do konkurencji. Banki na całym świecie zaczynają doceniać potencjał płynący z wykorzystania sztucznej inteligencji i chętnie przystępują do wdrażania tego typu rozwiązań.

Jesteśmy świadkami niesamowicie szybkiej zmiany. Celowo nie doprecyzowujemy „co to” to zmiana, bo przez ostatnie miesiące w „codziennym” życiu biznesowym zmieniło się prawie wszystko. Nie da się jednak zaprze-



czyć, że jeśli myśli się o przekonaniu organizacji do wirtualizacji tak wielu procesów, jak się tylko da, to czas kwarantanny i społecznego oddalenia był momentem przełomowym. Dlatego też firmy działające w szeroko pojętej branży IT mają teraz kalendarze wręcz wypełnione projektami, związanymi m.in. z usprawnianiem, ułatwianiem i przyspieszaniem działania procesów wewnątrz organizacji, które mają przy tym wpływ również na klienta końcowego – mówi Grzegorz Gołda, Dyrektor ds. Sprzedaży w Cloudware Polska.

W dzisiejszym świecie banki, jako tradycyjnie rozumiane instytucje, są w pewnym sensie w nietypowym położeniu. Muszą konkurować o zaufanie, a tym samym o pieniądze, nie tylko między sobą, ale też z powiększającą się rzeszą innowacyjnych fintechów. Wiele z tych organizacji, popularyzujących nowe technologie finansowe, promuje się hasłami mówiącymi właśnie o użyciu najnowszych i najbardziej dostępnych rozwiązań, czyli m.in. sztucznej inteligencji. Banki, chcąc zyskać przewagę nad nowymi i pełnymi rewolucyjnych pomysłów graczami, również sięgają do rozwiązań, które mają, dzięki chociażby AI, pomóc im być lepszymi niż ich innowacyjna konkurencja.

Co może sztuczna inteligencja?

Oto przykłady narzędzi: IBM Watson Machine Learning, czyli sztuczna inteligencja autorstwa IBM to system, który pozwala wykorzystać narzędzia i aplikacje oparte na AI do obsługi danych na dowolnej platformie, takiej jak IBM Cloud, AWS, Azure, Google lub własna prywatna chmura danej firmy. Twórcy Watsona zadbali o przygotowanie gotowych do użycia rozwiązań,

które odpowiadają na konkretne problemy przedsiębiorstw w różnych branżach.

Watson Assistant jest platformą konwersacyjną AI, która pomaga w udzielaniu klientom szybkich, prostych i dokładnych odpowiedzi, za pośrednictwem dowolnej aplikacji, urządzenia lub kanału. Dzięki automatyzacji i przyspieszeniu procesu komunikacji Watson Assistant redukuje koszty interakcji z klientami, co dodatkowo pozwala pracownikom skupić się na skomplikowanych przypadkach, a nie na stale powtarzających się wątkach.

Watson Discovery to usługa do przeszukiwania danych korporacyjnych, która dzięki AI przeprowadza analizę ukrytych w nich trendów i zależności. Watson Discovery wykorzystuje m.in. funkcje przetwarzania języków natu-



Zastosowanie rozwiązań opartych na AI ma nie tylko zrewolucjonizować branżę, ale przede wszystkim podnieść jakość świadczonych usług, a tym samym przyspieszyć pewne procesy biznesowe, zaowocować większym zadowoleniem klientów i zmniejszyć ich odpływ do konkurencji.

ralnych, przy czym wyuczenie tego mechanizmu charakterystycznego dla danej dziedziny żargonu nie stanowi problemu. Przewaga rozwiązań IBM tkwi w tym, że tradycyjne wyszukiwarki, nawet klasy korporacyjnej, nie dostarczają pracownikom i klientom precyzyjnych odpowiedzi, ponieważ często nie rozumieją zawiłych sformułowań ani skrótów branżowych i nie są w stanie dokładnie i szybko przeszukiwać skomplikowanych dokumentów.

Watson Speech to Text pozwala na łatwe przekształcanie dźwięku i głosu w tekst pisany, co daje możliwość szybkiego interpretowania treści. Narzędzie umożliwia m.in. spisywanie w czasie rzeczywistym słów wypowiedzianych do mikrofonu, a także np. skomplikowaną analizę tysięcy nagrań z centrum zgłoszeniowego.

Natomiast Watson Tone Analyzer pozwala zrozumieć emocje i styl komunikacji w tekście. Dzięki niemu można analizować znaczenie w internetowych wypowiedziach, takich jak tweety lub recenzje. Narzędzie to wspomaga np. obsługę klientów poprzez rozpoznawanie po stylu komunikacji, czy są oni zadowoleni, czy sfrustrowani.

Korzyści płynące z zastosowania rozwiązań opartych na AI

Korzyści płynące z zastosowania rozwiązań opartych na AI jest wiele i dotyczą one różnych obszarów biznesowych. Przede wszystkim są to korzyści finansowe. Choć na początku może się wydawać, iż wprowadzanie do organizacji nowoczesnych technologii będzie dużą inwestycją, to takie działanie procentuje jednak znacznymi oszczędnościami w przyszłości. Ponieważ konkurencja jest zacięta, jednym z najważniejszych działań jest jak najdłuższe utrzymanie klienta. Banki latami funkcjonowały na zasadzie bezpośredniego kontaktu z interesantami i dzięki temu pięknie rozwija się bankowość internetowa – jednak to nie wystarczy.

Nadal pozostaje sporo spraw, których klient nie jest w stanie sfinalizować przez swój profil bankowy czy infolinię, a to przekłada się bezpośrednio na

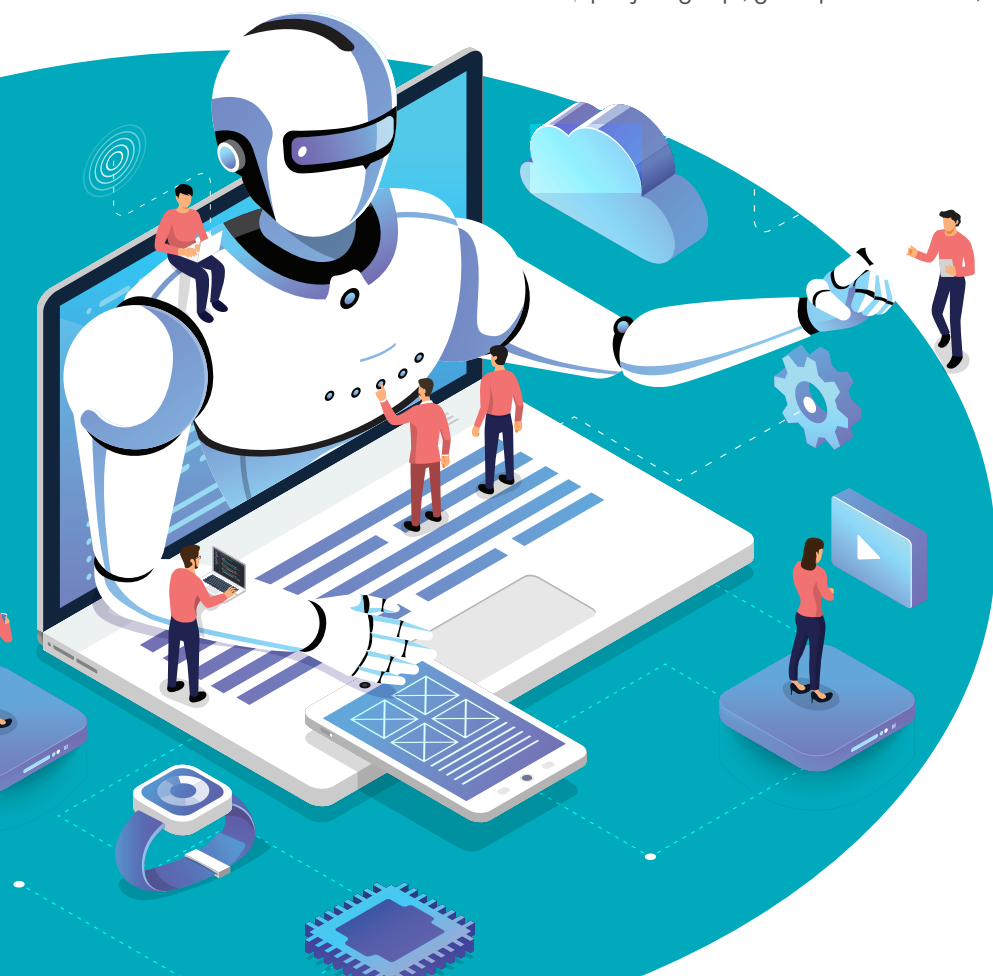
czas realizacji usługi i zadowolenie tegoż konsumenta. Właśnie dlatego wiele procesów, takich jak zakładanie kont, uzyskiwanie informacji ich dotyczących czy udzielanie pożyczek zostaje pierwszymi kandydatami do ulepszenia, a przede wszystkim przyspieszenia procesu dzięki użyciu sztucznej inteligencji. Szybsza i łatwiejsza samoobsługa rachunku bankowego bezpośrednio przekłada się na zadowolenie klienta i tym samym mniejszą ilość klientów odchodzących do konkurencji.

Oprócz poprawienia ogólnych odczuć i zadowolenia klientów względem samoobsługi, banki stosują też rozwiązania AI od „środka organizacji”. Jednym z najlepiej chyba znanych przykładów z naszego kontynentu jest Royal Bank of Scotland (RBS), który dodał do narzędzi dostępnych dla swoich pracowników rozwiązanie oparte na IBM Watson. Dostrzec można wiele zastosowań IBM Watson – chociażby na naszej rządowej stronie pacjent.gov.pl, gdzie polska filia IBM,

pro bono zaimplementowała chatbota, który odpowiadał na najczęstsze pytania dotyczące koronawirusa.

W podobny sposób rozwiązanie oparte na IBM Watson poprawiło jakość i szybkość obsługi klientów banku RBS. Dzięki niemu pracownik podczas rozmowy z klientem mógł szybko odpowiadać na jego pytania lub znaleźć informacje potrzebne do rozwiązania danego problemu. Wystarczyło zadać botowi odpowiednie zapytanie, np. „Mój klient zgubił kartę. Co mam zrobić?”, żeby otrzymać informację zwrotną, kierującą szybko do rozwiązania problemu. Na tym przykładzie widać, że jednym z głównych zagadnień, na których polepszeniu zależy bankom, jest jak najlepsza obsługa klienta. Wysoka jakość obsługi, a przede wszystkim szybkość odpowiadania na prośby, rozwiązywania problemów czy wyjaśniania wątpliwości to jedna z mocnych kart przetargowych, które utrzymują dłużej w danym banku klienta, który posiada duży kapitał i siłą rzeczy powierza danej instytucji fundusze wyższe niż przeciętny Kowalski. O takich klientach banki biją się szczególnie mocno i to właśnie przede wszystkim dla takich klientów warto wprowadzać innowacje oparte na AI.

Możliwość wirtualnego asystenta wykorzystuje też Bradesco – jeden z największych banków w Brazylii (ponad 5200 oddziałów). Asystent AI osiągnął tam wyjątkowy wskaźnik dokładności odpowiedzi na zapytania klientów na poziomie 95%! Watson został przeszkolony w zakresie 62 produktów. Obsługuje 283 tys. pytań miesięcznie, a czas reakcji został skrócony z 10 minut do kilku sekund. Co ważne, Watson ciągle się uczy i, dzięki informacjom zwrotnym, poprawia się.



Co z zapleczem technicznym?

Sprzęt IBM gwarantem jakości narzędzi AI

Narzędzia wykorzystujące sztuczną inteligencję potrzebują superszybkich komputerów, na których mogą pracować. Bezawaryjność, szybkość działania i ogromne moce obliczeniowe to elementy hardware'u, które są podstawą sukcesu AI.

Aplikacje AI analizują ogromne ilości danych i wymagają potężnej mocy obliczeniowej – będącej zdecydowanie poza zasięgiem standardowych procesorów. Serwery IBM z technologią POWER9 zapewniają niezawodność, dostępność i łatwość serwisowania, zautomatyzowane funkcje, odtwarzanie po awarii, znakomitą konfigurację i instalację oraz długi czas dostępności.

Infrastruktura IBM Power Systems for AI pomaga przedsiębiorstwom wykorzystać potencjał technologii sztucznej inteligencji i analiz tak, aby umożliwiać podejmowanie decyzji w jeszcze większym stopniu opartych na danych, uzyskiwać dostęp do pogłębionych informacji, a także budować zaufanie i poczucie bezpieczeństwa. Serwer IBM Power System LC922 został zaprojektowany tak, by spełniał wymagania dotyczące danych i obciążen przetwarzanych przez sztuczną inteligencję. Stworzono go z myślą o intensywnej pracy, dlatego oferuje dużą moc obliczeniową do analizowania i eksplorowania danych, a także dużą pamięć do ich przechowywania.

Gwarancją jakości, bezpieczeństwa i prędkości działania wspomnianych narzędzi są serwery najnowszej ge-

neracji IBM Power Systems – numer 1 w rankingu firmy ITIC dotyczącym niezawodności systemu operacyjnego. Oparte na AI urządzenia zamieniają dane w rozwiązania, nie trzeba więc być analitykiem, by sprawnie używać sztucznej inteligencji. Nowy serwer inferencyjny IBM Power System LC922 wykorzystuje sprzęt i oprogramowanie po optymalizacji, zapewniając komponenty niezbędne do wyciągania wniosków z pomocą sztucznej inteligencji i przejścia od danych do spostrzeżeń. Pozwala wykorzystać modele AI w pracy, a następnie pozyskiwać wartościowe informacje biznesowe.

Wdrożenie rozwiązań opartych na sztucznej inteligencji to nie jest niestety działanie, które można rozpocząć i zakończyć w „jeden dzień”. Dobór, projektowanie i wdrażanie należy zostawić specjalistom, którzy znają dobrze tę

tematykę, prowadzą pogłębione rozmowy z klientem i dokładnie rozumieją potrzeby biznesowe organizacji. Odpowiednio przeanalizowane i dobrane rozwiązanie będzie przecież kluczem do sukcesu i uchroni przed problemami w przyszłości. Dlatego szczególnie ważne jest to, z kim dany bank zdecyduje się taki projekt zrealizować. W Cloudware dbamy nie tylko o to, żeby zapewnić najlepszych specjalistów IT, którzy wdrożenie zrealizują, ale też o to, żeby opiekunowie klienta i nasi specjaliści pre-sales, dokładnie zbadali potrzeby organizacji i dzięki temu optymalnie zaplanowali implementację projektu.

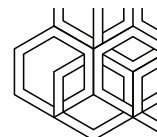
Ważną i chyba zawsze aktualną kwestią w bankowości, jest też ochrona informacji wrażliwych. Regularnie, kilka razy w roku, media informują o wyciekach danych z dużych organizacji, szczególnie często o wyciekach danych bankowych. Wdrażając ulepszenia oparte na sztucznej inteligencji, nie można zapominać o zadbanie o zarządzanie tożsamością. Cloudware wdraża w tym zakresie rozwiązania opracowane przez wiodących inżynierów IBM, np. IBM Identity Access Management. Takie rozwiązanie dotyczące zarządzania tożsamością i dostępem jest szczególnie ważne dla utrzymywania wysokich standardów bezpieczeństwa w organizacji, a właśnie na zabezpieczeniu cyfrowe klienci zwracają dzisiaj coraz większą uwagę.



cloudware

IBM®

Platinum
Business Partner



CZY SZTUCZNA INTELIGENCJA

może sprawdzić się w walce z przestępstwami w bankach?

Przedsiębiorstwa tracą miliardy dolarów rocznie z powodu szeregu oszustw dokonywanych online. Fałszywe płatności, pranie pieniędzy, oszustwa w programach lojalnościowych i incydenty związane z bezpieczeństwem cybernetycznym – to tylko kilka przykładów. To nieuchronnie prowadzi do ogromnych strat finansowych, ale niesie ze sobą także inne poważne zagrożenia, w tym ryzyko utraty reputacji, co jest szczególnie istotne w przypadku instytucji finansowych.

Dotychczasowe metody polegające na badaniu każdego podejrzanego przypadku są niezwykle czasochłonne i generują duże koszty obsługi programu antyfraudowego. Przestępcy idą z duchem

czasu, stosując coraz to bardziej wyrafinowane techniki. To powoduje, że tradycyjne rozwiązania do walki z oszustwami szybko się starzeją, nawet krótko po ich wdrożeniu, przez co wymagają ciągłej aktualizacji. Tutaj z pomocą przychodzi SI – sztuczna inteligencja.

SI – o co w tym wszystkim chodzi?

Artificial Intelligence/sztuczna inteligencja – pewnie słyszałeś ten termin już setki razy. Narosło wokół niego wiele mitów i plotek, które mogą zaburzyć nieco jego prawdziwy obraz oraz znaczenie. Spróbujemy to wyjaśnić w kilku pojęciach:

SI to dziedzina nauki zajmująca się uczeniem komputerów w celu wykonywania zadań, które zazwyczaj wymagają interwencji człowieka. Uczą się one, jak efektywniej wykonywać te rutynowe procesy.

Uczenie maszynowe to automatyzacja pozyskiwania informacji (znanych i nieznanych wzorców) z bazy danych, wyrażanie ich w zrozumiałej formie, tak aby można je było zastosować do przetwarzania nowych i jeszcze nieodkrytych danych w systemie oraz wyciągać wnioski z wyników tych działań.

Głębokie uczenie się idzie o krok dalej, głębiej i można je uznać za podzbiór uczenia maszynowego. Pojęcie głębokiego uczenia się jest czasami nazywane po prostu „sieciami neuro-



nowymi”, gdyż odnosi się do wielu zaangażowanych w ten proces warstw.

A oto najbardziej przełomowe rodzaje uczenia maszynowego:

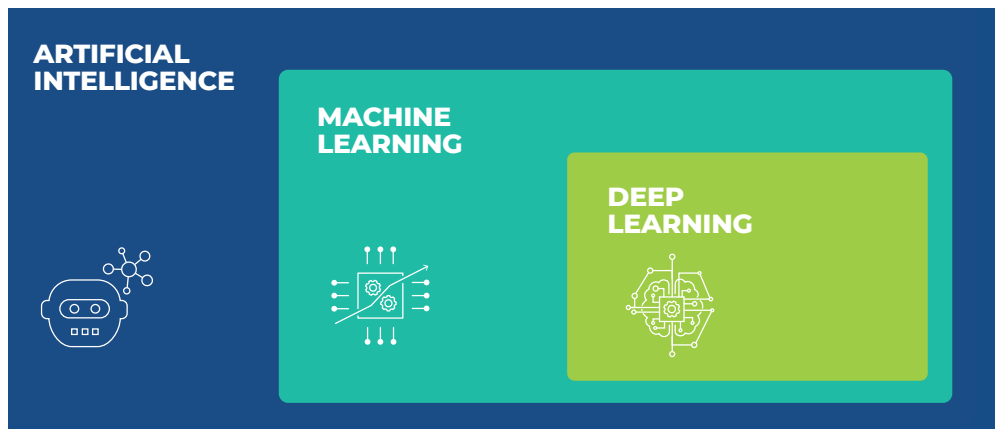
Najważniejszymi technikami, jakie wyróżniamy w zakresie modelowania sztucznej inteligencji, są uczenie nadzorowane (supervised learning) i uczenie się nienadzorowane (unsupervised learning).

- Nadzorowane uczenie wykorzystuje dane historyczne jako materiał wejściowy do uczenia się SI.
- Drugą kluczową techniką jest uczenie nienadzorowane, które daje nam możliwość znalezienia niespójności w analizowanych zbiorach danych.

Sztuczna inteligencja a tradycyjne programowanie

Warto poznać różnice, jakie występują pomiędzy zwykłym programowaniem, a programowaniem z wykorzystaniem narzędzi należących do grupy sztucznej inteligencji.

RYS. 1. Podzbiory sztucznej inteligencji.

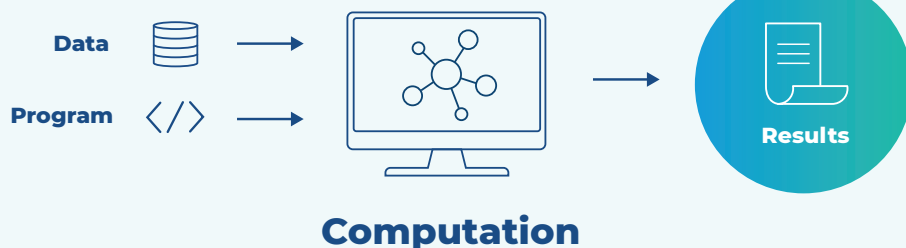


Tradycyjnie, programowanie opiera się na kodzie/programie, który działa na istniejących, zastanych danych, aby zapewnić oczekiwany wynik. Takie podejście jest w wielu obszarach skuteczne. Jednak, gdy mamy do czynienia z bardziej złożonymi zadaniami, istnieje lepsze podejście.

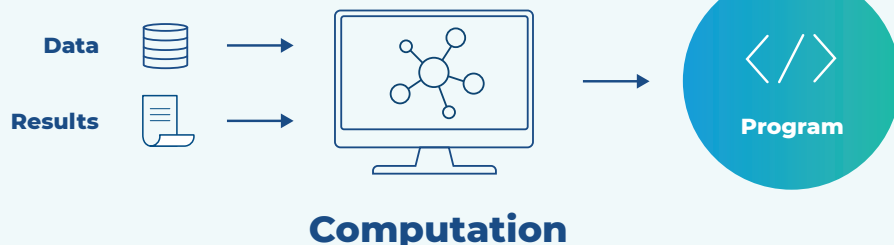
Jeśli mamy zarówno istniejące dane, jak i wyniki (zidentyfikowane jako podejrzane transakcje klientów i ostateczną decyzję co do nich, po sprawdzeniu przez eksperta domenowego) lub gdy mamy do czynienia ze złożonymi problemami, możemy zdecydować się na wykorzystanie uczenia maszynowego. Rezultatem naszych starań jest program, którego możemy użyć do przetworzenia nowych zbiorów danych, w przypadku których nie mamy jeszcze wyników analizy.

RYS. 2. Różnica między tradycyjnym programowaniem, a wykorzystaniem sztucznej inteligencji.

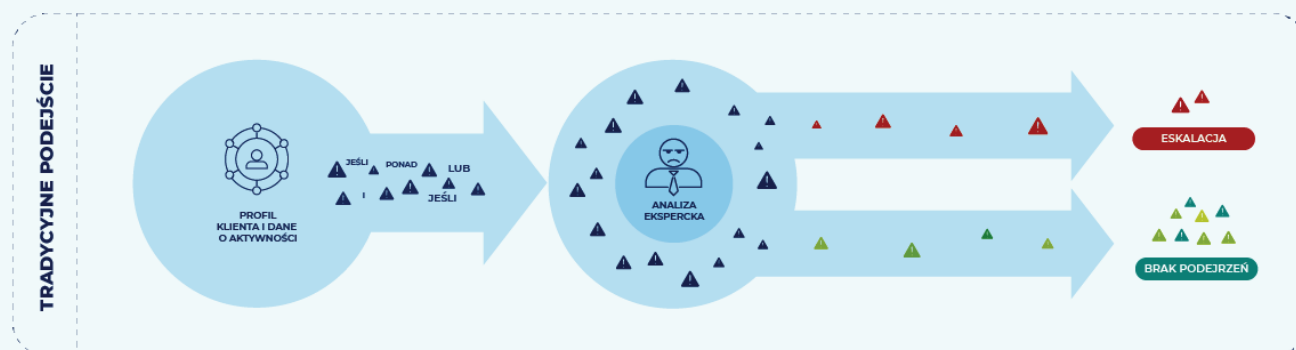
TRADITIONAL PROGRAMMING



MACHINE LEARNING APPROACH



RYŚ. 3. Uproszczony schemat procesu analizy podejrzanej aktywności w działach AML oraz przeciwdziałaniu oszustwom.



Obecnie banki wykazują coraz większe zainteresowanie tematyką uczenia maszynowego i głębokimi sieciami neuronowymi. Dysponują one i procesują mnóstwo informacji na temat swoich klientów i ich transakcji. W takiej sytuacji dobrze sięgnąć po rozwiązania oparte na sztucznej inteligencji i wykorzystać zalety uczenia maszynowego oraz głębokiego uczenia, gdyż w tym przypadku im więcej mamy danych wprowadzonych do systemu, tym zazwyczaj lepsza jest jego wydajność.

Typowe wyzwania działów AML

W tym miejscu warto pokazać, ile sztuczna inteligencja jest w stanie wnieść do codziennej pracy, na przykładzie konkretnego zadania, jakie stoi przed każdym bankiem, czyli przeciwdziałania praniu brudnych pieniędzy i finansowaniu terroryzmu.

Banki podczas budowania swoich programów AML muszą mierzyć się z wieloma wyzwaniami, m.in. z określeniem zbioru zasad i reguł,

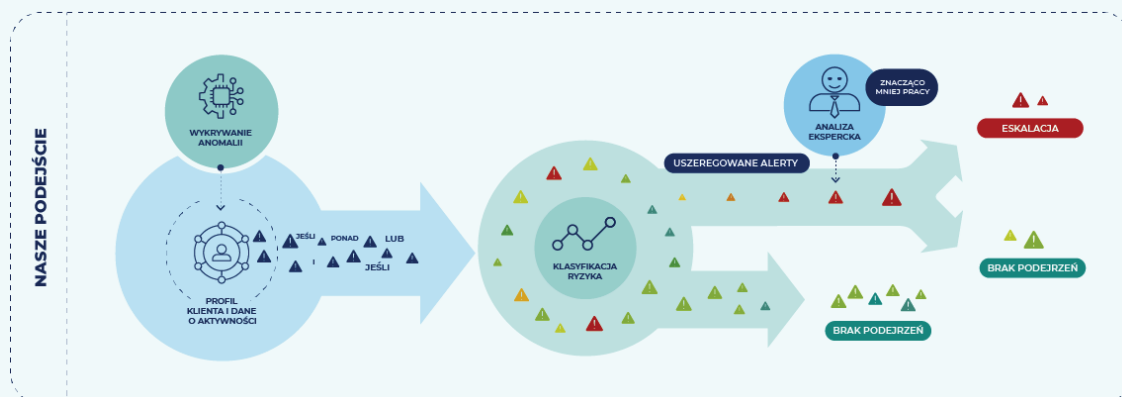
jaka aktywność klientów może być powiązana z działalnością przestępczą i dlaczego. Oczywiście każda instytucja musi sama zidentyfikować ryzyka, na jakie jest narażona oraz wprowadzić adekwatny zestaw narzędzi, procedur i innych środków bezpieczeństwa, aby nie stała się narzędziem do realizacji celów przestępczych.

Każda instytucja finansowa musi zatem sama zmierzyć się z określeniem zasad, kiedy dane zachowanie klienta jest alarmujące i w związku z tym kiedy musi zająć się takim przypadkiem ekspert domenowy.

W idealnym świecie powinny do niego trafiać tylko te przypadki, gdzie rzeczywiście aktywność na koncie wzbudza wątpliwości i konieczne jest zgłoszenie jej do regulatora. W praktyce jednak tak się nie dzieje. Analityków codziennie zalewa cała masa alertów, które nie mają nic wspólnego z żadnym przestępstwem. O takich alertach mówimy, że są fałszywie pozytywne (false positives) – choć system uznał, iż jest to podejrzany przypadek, to analiza ekspercka zamyka go, bez zastrzeżeń, już na wstępnym etapie. Przyjmuje się, że do tej grupy zalicza



RYS. 4. Przykładowe możliwości, jak sztuczna inteligencja może wzbogacić zwykły proces analizy podejrzanego aktywności w działach AML oraz przeciwdziałaniu oszustwom.



się średnio 95% alertów, które systemy regułowe przekazują do weryfikacji. Na ten poważny problem skarżą się instytucje na całym świecie.

Ktoś nieorientowany w temacie mógłby stwierdzić, że wystarczy przecież zmienić zaimplementowane reguły i problem zniknie. Niestety nie da się tak prosto tego rozwiązać.

Jednym ze wspomnianych wcześniej wyzwań programu do walki z praniem brudnych pieniędzy (AML) jest zapewnienie szczelności systemu finansowego na bardzo wysokim poziomie. Pominięcie przez system aktywności klientów, w których rzeczywiście były nielegalne transakcje jest zazwyczaj dużym problemem dla instytucji. Można się spodziewać, iż po wykrytych, podczas kontroli, tego typu przypadkach mogą zostać nałożone kary, nakazy poprawy procesów, poprawa części historycznej już (jak się wydawało) pracy oraz narażenie się na utratę reputacji. W takim wypadku mamy do czynienia z wynikami fałszywie negatywnymi (false negatives) – system błędnie (tj. fałszywie) przyjął odpowiedź na pytanie, czy ma do czynienia z podejrzaną aktywnością i dał odpowiedź negatywną.

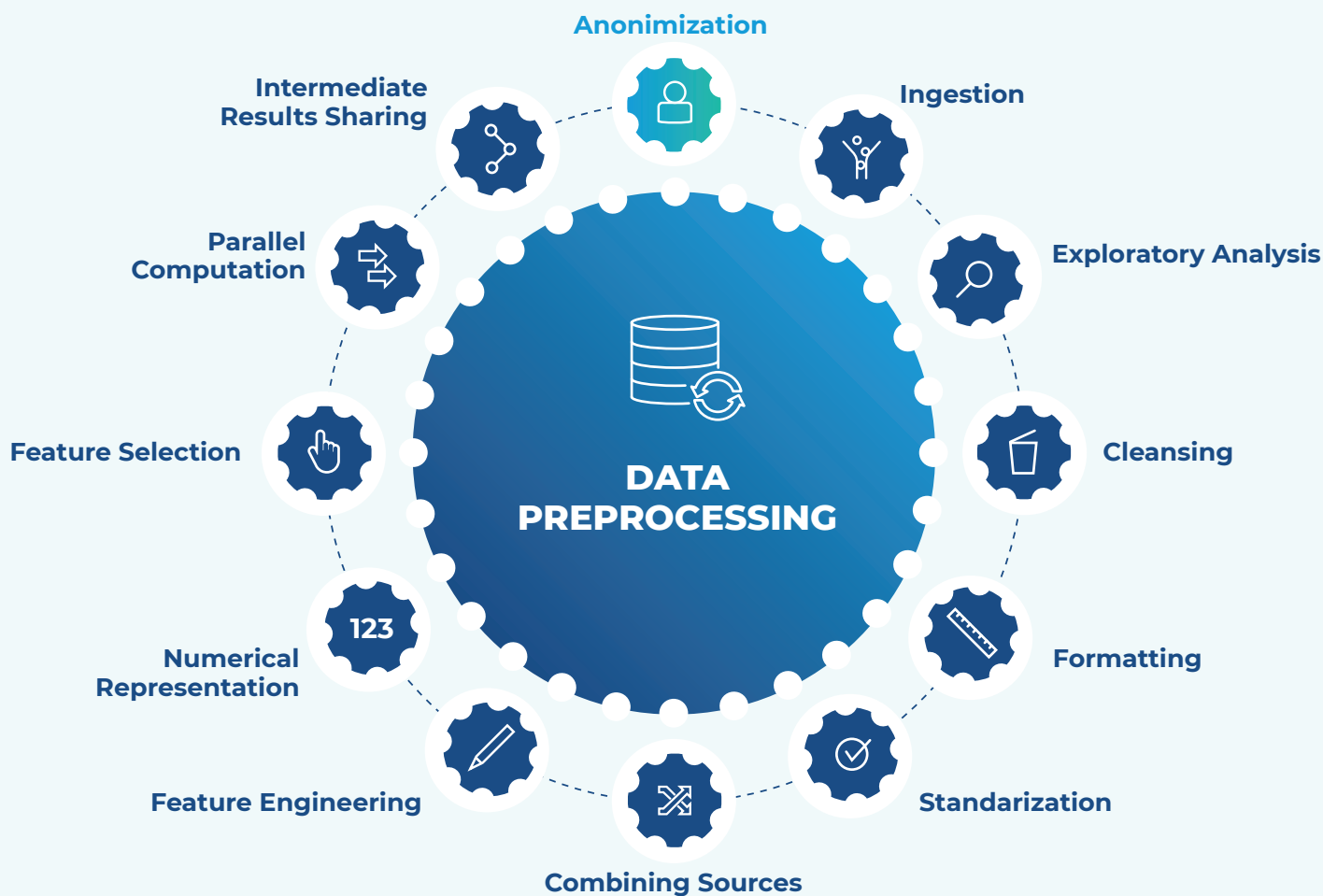
Jak SI realnie może pomóc w rozwiązaniu wyzwań działów AML?

Czas, aby pokazać, na realnym przykładzie, jak z wymienionymi wcześniej wyzwaniami można sobie poradzić, wykorzystując sztuczną inteligencję.

Do Comarchu zgłosił się lokalny oddział jednego z największych banków na świecie z prośbą o pomoc w rozwiązaniu jednego z ich najbardziej palących problemów,

„ Analitików codziennie zalewa cała masa alertów, które nie mają nic wspólnego z żadnym przestępstwem. O takich alertach mówimy, że są fałszywie pozytywne (false positives) – choć system uznał, iż jest to podejrzaný przypadek, to analiza ekspercka zamyka go, bez zastrzeżeń, już na wstępnym etapie. Przyjmuje się, że do tej grupy zalicza się średnio 95% alertów, które systemy regułowe przekazują do weryfikacji.

w dziale odpowiedzialnym za przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu. Zmagali się oni z klasycznym problemem – niską efektywnością pracy, jeśli by wziąć pod uwagę, ile poszczególni analitycy zgłaszają przypadków podejrzenia przestępstwa do Generalnego Inspektoratu Informacji Finansowej (GIIF). Każdego dnia tę żmudną pracę musiało wykonywać kilkudziesięciu pracowników, a wszystko to po to, aby strzec bank zarówno przed przestępcami, jak i karami, które mogłyby zostać nałożone za opóźnienia w pracy lub za zbyt niskie standardy w prowadzonych śledztwach.

RYS. 5. Przykładowe czynności podczas preprocesowania danych.

Tak jak w wielu instytucjach, gdzie praca operacyjna jest rutynowa oraz wymaga utrzymywania oczekiwanych celów jakościowych i ilościowych, tak również i w tym wypadku, kwestia problemu z atrycją wśród załogi stanowiła wyzwanie. Coraz lepsza sytuacja na rynku pracy, a także otwieranie się zagranicznych centrów do obsługi AML, stawiało bank przed coraz większą presją kosztową. Nie można było doprowadzić do braku ciągłości procesu, w przypadku pozyskania zbyt małej liczby pracowników do obsługi wszystkich alertów w wyznaczonych, dla konkretnych jurysdykcji, terminach.

Przekazanie danych wrażliwych

Zanim zespół doświadczonych inżynierów i data scientistów może zacząć pracować, trzeba jeszcze rozwiązać problem z przekazaniem danych tak, aby nie naruszyć żadnych lokalnych przepisów. W tym konkretnym wypadku w pierwszej fazie testowania koncepcji wystarczyło doprowadzić do anonimizacji danych poprzez usunięcie danych wrażliwych klientów, takich jak: imiona, nazwiska, numery dokumentów, nazwiska panieńskie, daty urodzenia czy miejsca zamieszkania. Pozostawienie jednak danych o segmencie do jakiego klient jest zalicza-

ny, flagi ryzyka, czy informacje z jakich produktów klient korzysta oraz kiedy założył konto, nie stanowiło już problemu. Oczywiście nawet przed udostępnieniem takich danych konieczne było podpisanie odpowiednich umów. Gdy tylko kwestie prawne zostały rozstrzygnięte, można było zacząć pracę na otrzymanym zbiorze danych.

Analiza danych

Jak już było wcześniej opisane, uczenie maszynowe nie jest tak prostym rozwiązaniem, jak mogłoby się niektórym wydawać. Wykorzystanie historycznego zbioru danych o aler-

tach oraz przypisanym im ostatecznie wyniku zamknięcia czy eskalacji (SAR, STR) sprawy może jednak pozwolić zidentyfikować wzorce do predykcji dla kolejnych danych.

Do zadań zespołu SI należy analiza otrzymanych danych tak, aby stwierdzić, czy spełniają one określone kryteria. A zatem zanim silnik SI będzie gotów do poprawnej analizy napływających danych oraz wyciągania z nich wniosków, muszą one być odpowiednio przygotowane. Ciężko znaleźć instytutację finansową, której jakość danych można by było określić jako bardzo dobrą. W znakomitej większości, w związku z procesami przejęć innych instytucji czy integracji starych systemów z nowymi, powstają czasami niezwykle kosztowne problemy, przez co obróbka danych staje się nieopłacalna.

Dane są wysokiej jakości, jeśli możemy zawsze oczekiwać, że w zadanym miejscu będzie dokładnie taka informacja, jakiej oczekujemy. Będzie ona

w prawidłowym (zawsze tym samym) formacie, nie tylko w jednym miejscu, ale jeśli ten sam typ danych pochodzi z różnych systemów to, że również między nimi nie będzie co do tego formatu rozbieżności. Podczas eksportu powinny generować się wszystkie dane prawidłowe (bez przesunięć, luk, wad etc.). Do inżynierii danych zalicza się m.in. ich agregację, dekompozycję czy skalowanie. Jeśli ten etap zostanie właściwie przeprowadzony, ma bardzo korzystny wpływ na wydajność całego rozwiązania.

Przygotowanie danych obejmuje wiele iteracji, eksploracji i analiz. Zdarza się, że dopiero na etapie ich analizy można wykryć pewne zaskakujące anomalie lub błędy w danych, które po-

wstały gdzieś na początkowym etapie ich przygotowania do przekazania. Można przyjąć, że w wielu projektach z wykorzystaniem sztucznej inteligencji czas przeznaczony na inżynierię cech to około połowa czasu potrzebnego na realizację całego projektu.

Modelowanie – wybór algorytmu

Choć sztuczna inteligencja jest niezwykle nośnym hasłem, to jak już zostało wcześniej opisane, nie jest ona jedną technologią, a raczej całą grupą rozwiązań opartych na tej samej technologii. Nie wystarczy zatem „wsypać” danych do jednego systemu i oczekiwać, że uzyskamy wszędzie tak samo świetne rezultaty.



Wraz z rozwojem techniki jest coraz więcej algorytmów sztucznej inteligencji, dzięki którym lepiej rozumiemy, które sprawdzają się najlepiej w konkretnych przypadkach (analiza mowy, obrazu etc.).

Nawet w przypadku analizy danych bankowych nie ma złotego rozwiązania, szczególnie gdy będziemy cały czas pamiętać o tym, że każda instytucja finansowa sama definiuje swoje ryzyka, a następnie odpowiednimi środkami zapobiegawczymi je mityguje. Każda ma również swoje procedury i własne definicje ryzyka, co może mieć wpływ na ostateczne zakwalifikowanie danego przypadku jako podejrzanego lub nie. Należy więc znaleźć najlepiej działający algorytm lub kombinację różnych algorytmów, a każdy z nich ma wiele parametrów, które należy przeanalizować. Taka analiza porównawcza wyników i wybranych narzędzi jest nie lada wyzwaniem, które wymaga nie tylko skrupulatności, ale też wiedzy i dużego doświadczenia.

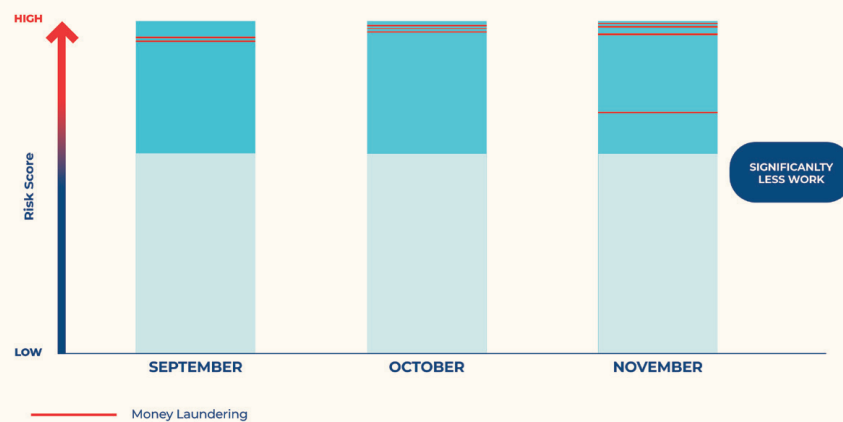
Wyniki zastosowania SI w dziale AML

Najciekawsze wyniki, jakie udało się nam uzyskać, pokazały, że wszystkie, przyjęte przez Generalnego Inspektora Informacji Finansowej, zgłoszenia znajdowały się w 40% alertów o najwyższym ryzyku. Poniżej tej wartości, czyli w pozostałych 60%, nie było żadnego takiego przypadku. Wynik niezwykle obiecujący. Kwestia wybrania poziomu, poniżej którego alerty mogą zostać automatycznie zamknięte, jest oczywiście kwestią indywidualną. Ze strony technicznej zaleca się jednak, aby na samym początku startować z redukcją alertów na poziomie 10–15% i w miarę

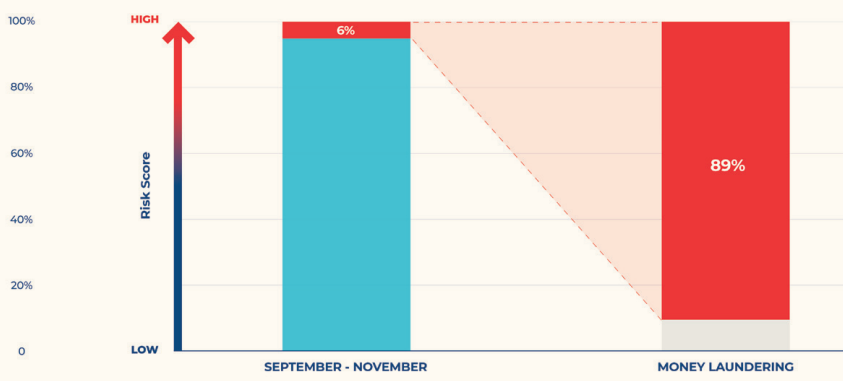
upływu czasu podnosić stopniowo ten poziom. Takie asekuracyjne podejście pozwala upewnić się, że rozwiązanie daje wyniki stabilne w czasie, jak i że w środowisku produkcyjnym wszystko działa perfekcyjnie.

Innym bardzo ciekawym zaobserwowanym przez nas wynikiem było zwrócenie uwagi na 6% alertów o najwyższym ryzyku. Okazało się, że w tej grupie znajdowało się aż 89% wszystkich potwierdzonych przypadków przez GIIF. Jak już wcześniej wspominaliśmy, procesowanie alertów względem ich ryzyka może pomóc przy znacznie szybszej identyfikacji klientów, jakich nikt nie chce mieć w swoim portfolio, czyli przestępców.

RYS. 6. Skuteczność sztucznej inteligencji we wskazywaniu jak ryzykowne są poszczególne alerty.



RYS. 7. Skuteczność sztucznej inteligencji w wykrywaniu przypadków prania brudnych pieniędzy.



Jak oceniać skuteczność rozwiązań wykorzystujących SI?

To, co należy bardzo mocno podkreślić, to powtarzalność wyników. O ile powtarzalność działania modelu w danej instytucji jest oczekiwana i powinna ona występować, to nie da się jej jednak tak prosto zagwarantować między instytucjami. Może dojść do sytuacji, gdzie w jednej instytucji wyniki były bardzo dobre, a w drugiej będą one albo jeszcze lepsze, albo znacznie gorsze. Wynika to z kilku powodów. Wszystkie praktycznie koncentrują się na danych. Mają one różną jakość w rozmaitych instytucjach. Wpływa na to również zakres danych, jaki jest wykorzystywany w ra-

mach uczenia maszynowego. Nie bez znaczenia jest też to, jak skutecznie dotychczas instytucja radziła sobie z przetwarzaniem alertów oraz optymalizacją ich liczby. Z dużą dozą pewności można jednak stwierdzić, że wykorzystanie sztucznej inteligencji pomoże i należy oczekiwać dwucyfrowej redukcji alertów. Jednak jaki to będzie dokładny wynik, należy już weryfikować indywidualnie.

Z racji na to, że wyniki mogą być różne, ważne jest, aby móc przetestować rozwiązanie z wybranym dostawcą, zanim się je wdroży. Zazwyczaj wtedy przekazywany jest do testów pewien ograniczony zakres danych (ale dalej reprezentatywny), tak aby pokazać, że koncepcja działa i daje obiecujące wyniki.

W całym projekcie konieczny jest także balans między „śrubowaniem” wyniku tylko na danym w zbiorze danych (overfitting), a stabilnym działaniem na przyszłych zbiorach danych. Mówiąc obrazowo, nie możemy skupić się i patrzeć tylko na wybrany punkt, bo stracimy obraz całości.

Wydaje się, że najlepszym sposobem na sprawdzanie wyników rozwiązań opartych na SI są testy „podwójnie ślepe próby” (double blind testing). Po tym, jak rozwiązanie zostanie opracowane na zadanym zbiorze danych, najlepiej dać mu do przedstawienia predykcje dla nowego zbioru danych, takich które wcześniej nie były znane zespołowi deweloperów. Po nadaniu odpowiedniej rangi (scoringu), w kolejnym kroku należy je porównać z decyzjami anali-

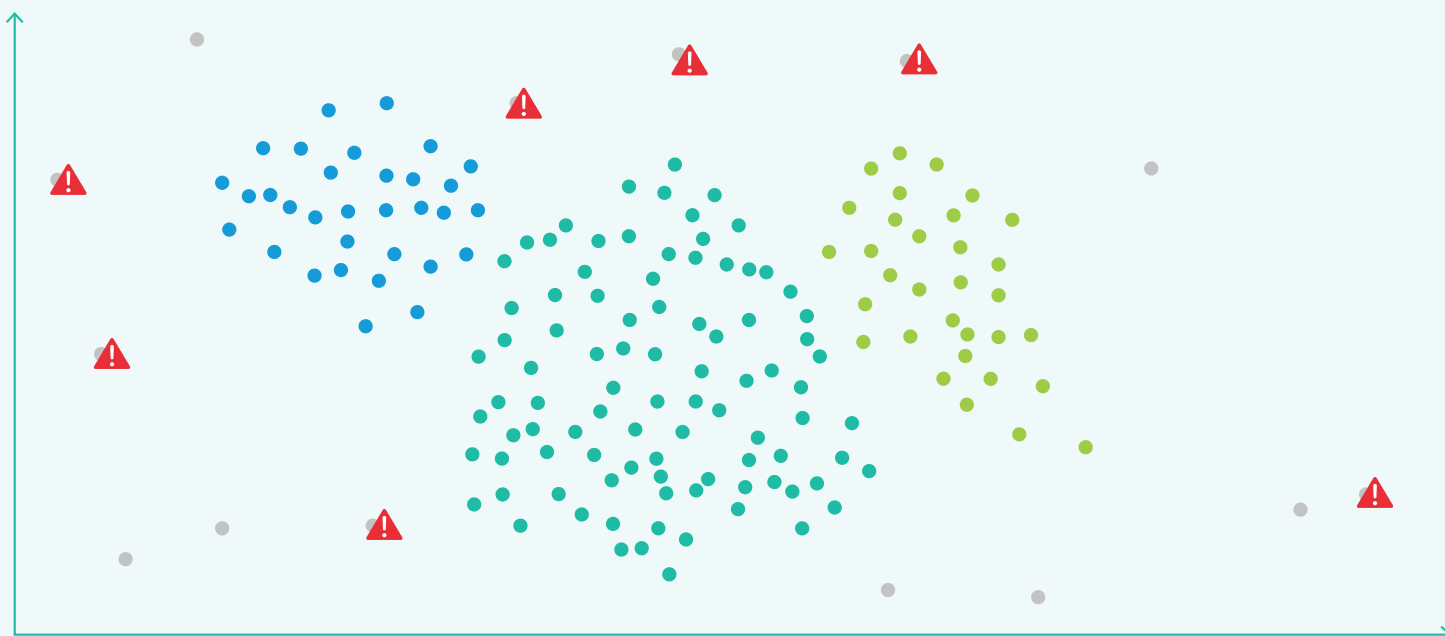
” Atutem wykorzystania technologii SI jest jej ciągła aktualność. Brak reguł w systemie pozwala poruszać się zawsze swobodnie, a nie kroczyć utartymi szlakami.

tyków i ekspertów AML oraz zobaczyć, jakie wartości były przypisywane do alertów według danej instytucji najbardziej istotnych (np. SAR-ów, STR-ów).

Jak poradzić sobie z ryzykiem wyników fałszywie negatywnych (false negatives)?

Pozostaje jeszcze problem wyników fałszywie ujemnych (false negatives). Tutaj również możemy zastosować

RYS. 8. Uproszczony przykład anomalii na dwuwymiarowej płaszczyźnie.



sztuczną inteligencję, ale mechanizm działania będzie zgoła inny. W tym wypadku nie szukamy wzorców, które łączą dane, dotychczas identyfikowane jako podejrzane, oraz tych, które nie zostały zakwalifikowane do tej kategorii. Tutaj zadaniem jest identyfikacja klientów, których aktywność w pewien sposób odbiega od tego, co nazwalibyśmy zachowaniem typowym.

W przypadku zastosowania tak zaawansowanej technologii nie chodzi jednak o zatrzymanie się na prostej analizie, która by wskazywała tylko na największe/najmniejsze transakcje czy aktywności. Zadaniem sztucznej

inteligencji jest znalezienie wielowymiarowych zależności, które wykażą nieścisłości w danych. Oczywiście nie wszystkie anomalie okazują się praniem pieniędzy. Obserwując jednak zachowanie przestępców i, w dużej mierze, ich próby naśladowania zwykłych, tj. uczciwych, użytkowników mogą zostać rozpracowane dzięki wielowymiarowej analizie.

Tak odnalezione nowe schematy mogą oczywiście posłużyć, aby dopracować obecne typy alertów, reguły czy wewnętrzne procedury. Bycie na bieżąco w tym zakresie umożliwia też skrócenie czasu wykonywania remediacji, gdyż nowe podejrzane aktywności mogą być szybciej zidentyfikowane.

Atutem wykorzystania technologii SI jest jej ciągła aktualność. Brak reguł w systemie pozwala poruszać się zawsze swobodnie, a nie kroczyć utartymi szlakami.

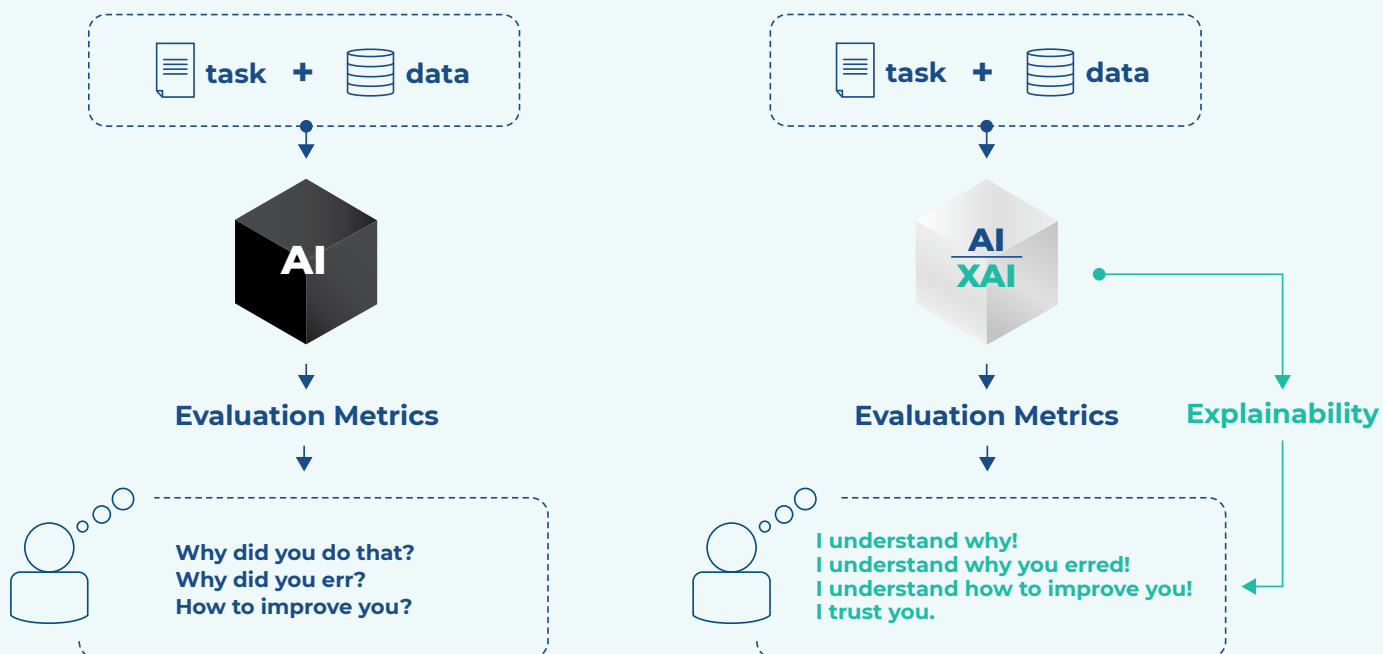
Jak zrozumieć, co stoi za decyzjami sztucznej inteligencji?

Jednym z największych wyzwań jest wyjaśnienie, dlaczego sztuczna inteligencja oznacza jakąś aktywność jako podejrzaną lub dlaczego według niej konkretny przypadek jest mniej podejrzany niż inne. Niestety, to pozornie nie do końca przejrzyste działanie SI może budzić wątpliwości wśród wyższego szczebla kierownictwa, audytorów, organów nadzoru, itp.

Z reguły zawsze lepiej jest wiedzieć więcej niż mniej i właśnie dlatego niektóre firmy decydują się na zastosowanie nowych technologii, bazujących na sztucznej inteligencji, które są w stanie wyjaśnić działanie innych rozwiązań opartych na SI. Mogą one dawać odpowiedzi, dlaczego niektóre przypadki są traktowane jako podejrzane, co wpływa na taki poziom ryzyka czy odpowiedzieć na inne pytania.

” Aby zapobiegać oszustwom i wykrywać je skutecznie, nie wystarczy już stosować zestawu scenariuszy. Pomóc może natomiast sztuczna inteligencja. Korzystając z danych historycznych i uczenia maszynowego, można wykrywać nietypowe zdarzenia znacznie skuteczniej. Co więcej, wraz z upływem czasu i zmieniającymi się wzorcami przestępczości cyfrowej, system Comarch Fraud Protection może na bieżąco douczać się i rozpoznawać zupełnie nowe zachowania przestępców.



RYS. 9. Sztuczna inteligencja versus wyjaśnialna sztuczna inteligencja.

Istnieje wiele możliwych scenariuszy tego, jak prezentować wyniki działania SI oraz do jakiego poziomu szczegółowości je przedstawiać. Temat jest bardzo złożony, jednak jest on w ostatnim czasie niezwykle dynamicznie rozwijany tak przez naukę, jak i biznes na całym świecie.

A co na to Comarch?

Comarch pracuje od dłuższego czasu nad wykorzystaniem najnowszych technologii w branży finansowej, ubezpieczeniowej czy inwestycyjnej. Wykorzystanie SI jest jednym z rozwijanych kierunków działań.

W zeszłym roku Comarch AML (oprogramowanie do wykrywania prania brudnych pieniędzy opartego na SI) zostało wyróżnione w konkursie Hit Roku 2019 „Gazety Bankowej”, który wyłonił najbardziej innowacyjne rozwiązania dla branży finansowej. Comarch AML otrzymało nagrodę w kategorii Hit Roku 2019 – „Bankowość”.

Oprogramowanie Comarch Fraud Protection to platforma oparta na uczeniu maszynowym, gdzie sztuczna inteligencja jest wykorzystywana do tworzenia modeli, które na podstawie danych historycznych mogą z dużą dokładnością określić prawdopodobieństwo wystąpienia określonego zdarzenia mającego znamiona oszustwa. Dzięki temu znacznie zwiększają skuteczność wykrywania podejrzanych zdarzeń, rozszerzając istotnie zakres możliwości rozwiązań opartych tylko na klasycznych regułach. Rozwiązanie pozwala wykrywać pranie brudnych pieniędzy, przestępstwa na kartach kredytowych, w programach lojalnościowych, nadużycia w telekomunikacji oraz w ubezpieczeniach, a także w zakresie cyberprzestępczości.

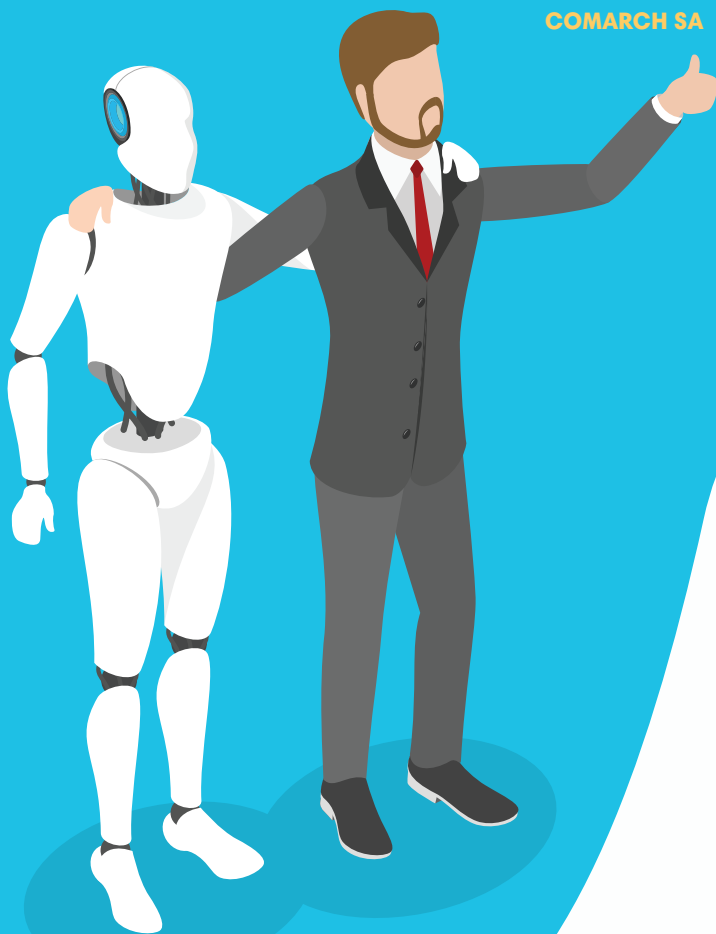
Technologia i nauka stojąca za rozwiązaniem Comarch Fraud Protection

Przez wiele lat stosowanie prostych systemów opartych na regułach było

jedynym i wystarczającym, choć trzeba przyznać, że w wielu przypadkach nieskutecznym, podejściem do wykrywania różnego rodzaju oszustw. Z czasem przestępczość cyfrowa zaczęła szybko ewoluować i wykorzystywać bardziej zaawansowane metody, które pokonują systemy nawet bardzo złożonych reguł.

Aby zapobiegać oszustwom i wykrywać je skutecznie, nie wystarczy już stosować zestawu scenariuszy. Pomóc może natomiast sztuczna inteligencja. Korzystając z danych historycznych i uczenia maszynowego, można wykrywać nietypowe zdarzenia znacznie skuteczniej. Co więcej, wraz z upływem czasu i zmieniającymi się wzorcami przestępczości cyfrowej, system Comarch Fraud Protection może na bieżąco douczać się i rozpoznawać zupełnie nowe zachowania przestępców.

Sztuczną inteligencję często określa się mianem „black box”, czyli systemu, którego logikę działania trudno



koszty. Comarch Fraud Protection zmniejsza to ryzyko dzięki całościowemu podejściu do analizy różnego rodzaju nieuczciwych działań.

Podsumowanie

Sztuczna inteligencja z pewnością nie zastąpi ludzi, jeśli chodzi o rozwiązywanie złożonych problemów. Wizja maszyn, które są w pełni rozumne i mądrzejsze od człowieka we wszystkich sferach jest dalej obszarem science-fiction i prawdopodobnie przez wiele lat nie uda się dojść maszynom do poziomu ludzkiej analizy (niektórzy szacują, że to setki lat, inni, że nigdy do tego nie dojdzie).

Jedno jest jednak pewne – maszyny mogą być lepsze od ludzi w wąskim zakresie najbardziej rutynowych zadań oraz znacznie efektywniej rozwiązywać jasno zdefiniowane problemy. Wykorzystanie sztucznej inteligencji pozwala odciążyć zespół od „bezwartościowych” alertów, a zaoszczędzony czas przeznaczyć na dokładniejszą analizę lub inne zadania.

Obszary, za które odpowiadają bankowe zespoły do walki z przestępczością, ds. bezpieczeństwa czy przeciwdziałania praniu brudnych pieniędzy, mogą z pewnością wiele skorzystać z nowych szans, jakie dziś daje technologia. Lepsze zabezpieczenie przed oszustami oraz możliwość szybszej reakcji w sprawach, gdzie rzeczywiście jest podejrzenie działalności przestępczej, mieści się wysoko na liście celów wielu managerów. Dobrze opracowane narzędzia oparte na sztucznej inteligencji są w stanie te cele jeszcze skuteczniej niż dotychczas osiągać.

jest opisać w formie zrozumiałych dla człowieka formuł. Jednak i na to istnieje rozwiązanie, którym jest XAI (ang. eXplainable AI), czyli „wyłumaczalna” sztuczna inteligencja. Powstało szereg metod, które obecnie pozwalają uzyskać objaśnienie decyzji czy rekomendacji, które wygenerowane zostały przez algorytm SI. Objaśnienie, czyli zrozumiałe i pomocne dla analityka informacje stanowiące uzasadnienie decyzji algorytmu.

Korzyści biznesowe rozwiązania Comarch Fraud Protection

Znacząca redukcja kosztów

Przedsiębiorstwa i instytucje rządowe tracą miliardy dolarów z powodu oszustw. Wdrażając oprogramowanie Comarch do ochrony przed

oszustwami, można spodziewać się wymiernych korzyści – znacznie zmniejszonych strat dzięki najnowocześniejszemu podejściu do wykrywania i zapobiegania oszustwom.

Zwiększona produktywność

Usprawnienie zadań pozwala osiągnąć więcej w krótszym czasie. Zautomatyzowany obieg pracy, zapobiegający oszustwom, zwiększa produktywność pracowników, eliminując obciążenie związane z wykonywaniem rutynowych zadań i finalnie skracając całkowity czas potrzebny na analizę oszustw. To umożliwia pracownikom skupienie się na bardziej wymagających i złożonych wyzwaniach.

Zminimalizowane ryzyko utraty reputacji

Wpływ oszustwa na reputację organizacji jest niewątpliwie negatywny i może narazić firmę na ogromne

OCZYWISTE I MNIEJ OCZYWISTE

zastosowania sztucznej inteligencji w sektorze finansowym

Komputery wcześniej zaczęły wspierać działania rynków finansowych oraz instytucji bankowych. Niezależnie od tego, czy mówimy o księgowaniu operacji, czy też systemach Business Intelligence i big data, technologia przynosi sektorowi finansowemu i jego klientom bardzo wymierne korzyści, pozwala bowiem skrócić czas wykonania pojedynczej operacji i upowszechnia dostęp do bankowości.



Wojciech Janusz

Senior System Engineer
– Dell Technologies
AI/Data Science Champion
Office of the CTO – CTO
Ambassador

Doświadczony architekt odpowiedzialny za projektowanie systemów obliczeniowych dla największych klientów w Polsce i w części Europy.

Pasjonat nowoczesnych technologii, promuje i wspiera wykorzystanie sztucznej inteligencji i zaawansowanej analityki.

Z Dell Technologies (wcześniej Dell EMC) związany od 2013 r., wcześniej pracował m.in. dla Netapp, IBM oraz Onet.pl

Technologia AI w sektorze finansowym

Rynki finansowe zawsze szybko adaptowały zdobycze technologiczne do swoich potrzeb. Nie inaczej rzecz ma się z rozwiązaniami sztucznej inteligencji, zwłaszcza deep learning. Ten typ przetwarzania danych w typowych zastosowaniach bankowych zdecydowanie przewyższa inne metody automatyzacji procesów.

Rozwiązania AI stosuje się m.in. w przygotowywaniu prognoz giełdowych, przy ocenie ryzyka kredytowego czy w procesie wyceny aktywów. Warto jednak pamiętać, że perspektywy, jakie otwiera przed sektorem finansowym wykorzystanie sztucznej inteligencji, są bardziej obiecujące.

Należy do nich m.in.:

- automatyzacja tak skomplikowanych procesów, jak planowanie i wdrażanie zindywidualizowanych i targetowanych akcji marketingowych czy kompletnych strategii zarówno dla konkretnych produktów finansowych i bankowych, jak też i całych brandów;
- zwiększenie bezpieczeństwa transakcji, wdrażane przy równo-

czesnym utrzymaniu elastyczności usług finansowych i bez pogarszania użyteczności narzędzi internetowych oraz jakości obsługi w placówkach;

- przygotowanie złożonych analiz demograficznych w czasie rzeczywistym, bez odciągania uwagi klientów od wykonywanej operacji finansowej;
- analiza zachowań klientów oraz odczuwanych przez nich emocji, na podstawie ich postępowania w sieciach społecznościowych;
- dokładna wycena nieruchomości oraz optymalizacja wyszukiwania nowych lokalizacji dla placówek bankowych.

To tylko kilka z wielu nowych i nieoczywistych możliwości, jakie instytucjom finansowym daje sztuczna inteligencja.



Rola AI w automatyzacji powtarzalnych procesów biznesowych

Najważniejszym z zastosowań sztucznej inteligencji jest automatyzacja procesów biznesowych. Wniosek taki płynie m.in. z wyników badania, przygotowanego i zaprezentowanego przez McKinsey Global Survey¹. Jedną z konkluzji tego opracowania brzmi: automatyzacja procesów biznesowych pozostaje jednym z najważniejszych sposobów poprawy efektywności i wydajności organizacji.

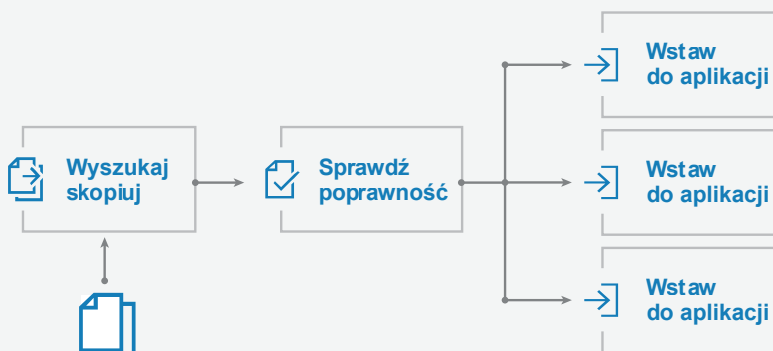
Sprawdza się ona zwłaszcza wówczas, gdy mamy do czynienia z koniecznością wykonania powtarzalnych, czasochłonnych i monotonicznych procesów, wymagających od pracowników ciągłego skupienia uwagi.

Impulsem do stosowania rozwiązań machine learning w automatyzacji takich procesów i w zastępowaniu pracy ludzkiej poprzez algorytmy było głęboko humanistyczne przekonanie, że ludzki czas, zdolności i inteligencję można wykorzystać o wiele efektywniej. Nie można zapominać także o tym, że systemy AI nie męczą się, w związku z czym nie popełniają potencjalnie kosztownych błędów. Można więc zaryzykować twierdzenie, że pełna automatyzacja procesów byłaby dla sektora bankowego rozwiązaniem optymalnym. Na takowy scenariusz będziemy musieli jednak poczekać, głównie z przyczyn natury prawnej, choć i technologia stawia w tym przypadku pewne warunki – m.in. taki, iż automatyzowany proces musi być dobrze zdefiniowany i opisany.

RYS. 1. Pełna automatyzacja procesów



RYS. 2. Proces ręcznego przetwarzania danych



”

Impulsem do stosowania rozwiązań machine learning w automatyzacji procesów i w zastępowaniu pracy ludzkiej poprzez algorytmy było przekonanie, że ludzki czas, zdolności i inteligencję można wykorzystać o wiele efektywniej. Na dodatek systemy AI nie męczą się, w związku z czym nie popełniają potencjalnie kosztownych błędów.

Co i jak może zrobić sztuczna inteligencja?

W przypadku procesów wspomnianych wyżej naturalne wydaje się zastosowanie rozwiązań *Robotic Process Automation*, jednego z wielu mechanizmów, które zawierają się w szerokim pojęciu sztucznej inteligencji.

Przyjrzyjmy się działaniu AI w konkretnym przypadku. Załóżmy, że procesem, który chcemy zautomatyzować, jest kopiowanie danych pomiędzy różnymi miejscami, w których muszą być wykorzystane lub powtarzalne ich uzupełnianie w wielu miejscach systemu. Operacja ta ma jednocześnie sprawdzać podstawową (np. arytmetyczną lub formalną) poprawność wprowadzanych informacji, poprzez weryfikację ich formatu lub sprawdzenie wiarygodności w innych zasobach.

Mogłoby się wydawać, że to tylko przenoszenie informacji z jednego miejsca do innego, a więc proces zbyt banalny, żeby zastosowanie mecha-

¹ <https://www.mckinsey.com/business-functions/operations/our-insights/the-automation-imperative>

zmów AI mogło być efektywne z punktu widzenia biznesowego.

Jednak, jak nadmieniliśmy we wstępie, sztuczna inteligencja sprawdza się właśnie w takich przypadkach. Sam proces wcale nie jest prosty, zaś dzięki zastosowaniu technologii machine learning może być rozszerzony i objąć większą ilość danych, zwłaszcza takich, których przetworzenie bez niego byłoby niemożliwe.

Warto zwrócić uwagę choćby na różnorodność formatów, w jakich mogą występować dane w systemie bankowym. Rozwiązanie *Robotic Process Automation* szybko poradzi sobie z tymi różnicami, unifikując formaty, dzięki czemu system szybciej i dokładniej wykona zadanie. Dzięki AI można wyjść poza informacje występujące w postaci liczb, co sprawi, że zyskamy więcej danych oraz wiedzę o kliencie.

Sztuczna inteligencja:

- traktuje jako dane i umieszcza w systemie także takie informacje, jak nazwy ulic, nazwy miejscowości i kody pocztowe;
- dokonuje konwersji zapisu słownego liczb na cyfrowy i porównuje zapisy;
- rozpoznaje głos i dokonuje konwersji mowy na zapis tekstowy;
- używa mechanizmów NLP (*Natural Language Processing*) do rozumienia kontekstu wprowadzanych informacji i weryfikacji ich poprawności (tzw. *cognitive-based automation capabilities*);
- rozpoznaje obraz, korzystając z rozwiązań *computer vision*, dzięki-



ki czemu może odczytać informacje wprowadzane odręcznie na formularzach papierowych;

- wyszukuje informacje na zdjęciach oraz automatycznie odczytuje numery i symbole zapisane np. na skanach załączonych dokumentów czy na zdjęciach przesyłek.

Każda z informacji, do których zyskałmy dostęp dzięki AI, potencjalnie otwiera kolejne możliwości marketingowe lub łączy procesy działające do tej pory niezależnie bądź osobno.

Gdyby możliwe było wykorzystywanie sztucznej inteligencji bez żadnych ograniczeń, byłaby ona w stanie wprowadzić do sektora finansowego o wiele więcej niż automatyzację. Dostarczyłaby inteligentne wsparcie technologiczne, uwalniając cenne zasoby ludzkie oraz pozwalając na optymalizację kosztów oraz przyspieszenie procesów biznesowych i decyzyjnych.

Zbyt piękne, by mogło być prawdziwe?

Jakkolwiek możliwość pełnej automatyzacji procesów w sektorze finanso-

wym jest kusząca, a jej efekty byłyby biznesowo znaczące, w rzeczywistości jesteśmy w stanie w sposób pełny i bezpieczny zautomatyzować niewiele procesów. Jeszcze mniej spośród nich może być wdrożone w pełnej zgodności z obowiązującym prawem.

Zacznijmy od – być może nieco zaskakującego – stwierdzenia o niemożności wdrożenia pełnej automatyzacji. Wynika ona z dwóch przesłanek:

- procesy, o których niewiele wiadomo (takie, które nie zostały dobrze opisane), nie mogą zostać w pełni zautomatyzowane;
- automatyzacja to proces, z którego człowiek został całkowicie wyłączony, a wszystkie jego zadania przejmują technologie.

Model hybrydowy, w którym występują wyjątki i w którym człowiek aktywnie partycypuje w procesie (najczęściej przez podejmowanie kluczowych decyzji) nie jest nazywany automatyzacją, a *augmentacją* lub *akceleracją*.

Przejdźmy do kwestii prawnych i ich wpływu na zastosowanie AI.

Przepisy RODO określają, które procesy i decyzje mogą zostać w pełni zautomatyzowane, a które muszą posiadać alternatywną (ludzką) ścieżkę. Te same regulacje gwarantują możliwość zastrzeżenia przez klienta prawa do wyłączenia jego sprawy z automatycznego procesowania.

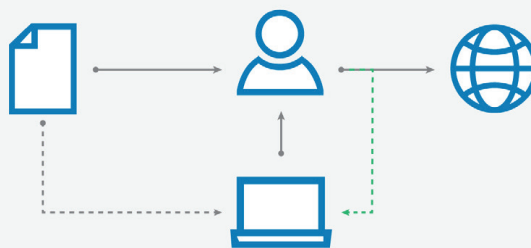
Nie jest to jedyna przeszkoda, na jaką napotyka AI w sektorze finansowym, jednak najlepiej pokazuje, że wdrożenie inteligentnego wsparcia technologicznego procesów może być z punktu widzenia prawnego bardzo trudne, a czasami wręcz niemożliwe.

Zastosowania AI do pełnej automatyzacji procesów zgodne z istniejącym stanem prawnym

Rozwiązaniem wykorzystującym machine learning, na które decyduje się większość firm, jest augmentacja (augmentation). To taki rodzaj inteligentnego wsparcia procesów, który uwalnia pracowników od konieczności wykonywania rutynowych operacji, a dostarcza im dodatkowych danych oraz możliwości działania.

Ciekawym przykładem takiego podejścia jest wdrożony przez Dell Technologies system, wspierający pracę zespołu odpowiadającego za komunikację z klientami.

RYS. 3. Augmentacja procesu



Jak działa rozwiązanie w Dell Technologies?

Wykorzystując technologię ML i NLP (*Natural Language Processing*) zbudowano mechanizm, którego zadaniem jest ocena treści wiadomości wpływających do zespołu, analiza ich ważności i nadanie im odpowiedniej kategorii. Rozwiązanie przygotowano tak, że sugeruje ono szablon odpowiedzi, z którego może skorzystać pracownik. W niektórych przypadkach system proponuje nawet kilka możliwych wersji.

Dzięki AI nie tylko znacząco usprawniono pracę działu, ale i zachowano pełną kontrolę nad kluczowym procesem komunikacji z klientem. Ostatecznie bowiem to człowiek decyduje, czy i w jaki sposób skorzysta z rozwiązań proponowanych mu przez sztuczną inteligencję.

Innym przykładem tego typu hybrydowych rozwiązań mogą być syste-

my analizujące treść dokumentów (np. umów i kontraktów). Technologia wykorzystująca NLP potrafi wychwycić i podkreślić kluczowe fragmenty tekstu, ułatwiając tym samym późniejszą pracę ekspertowi.

Jak nie dać się okraść... inteligentnej palce?

Wśród wielu możliwych zastosowań AI w sektorze finansowym, jedno zostało celowo pominięte. Jest to analiza nietypowych działań użytkowników w kontekście bezpieczeństwa, czyli mówiąc prościej – wykrywanie oszustw.

Tradycyjne modele zabezpieczeń wymagają nie tylko predefiniowania wszystkich sposobów, dzięki którym klient zyskuje dostęp do usług bankowych, ale i tego, by technologia „wiedziała” (dzięki analizie danych dostarczonych jej przez człowieka), jakie są istotne elementy systemu, jak zachowuje się użytkownik i jakie są

RYS. 4. System wspierający komunikację z klientami Dell Technologies



najważniejsze relacje pomiędzy tymi dwoma komponentami.

Takie systemy służące wykrywaniu oszustw mogły się sprawdzać w sytuacjach, gdy liczba kanałów komunikacji z klientem była ograniczona, zaś przestrzeń między instytucją finansową a klientem zdefiniowana i zabezpieczona.

Sprawa się skomplikowała w momencie, kiedy multichannel lub wielokanałowość stały się słowami definiującymi myślenie o usługach i marketingu.

Użytkownicy oczekują dziś swobody w dostępie do wszystkich usług, w tym również finansowych. Pragną dokonywać transakcji jak chcą i gdzie chcą, nie tylko w miejscach i przy użyciu sposobów określonych przez dostawcę. Klient oczekuje także bezpieczeństwa. Sektor finansowy, idąc za trendami technologicznymi i za użytkownikami, stał się nie tylko dostawcą usług, ale i wielokanałowego dostępu do nich.

W szybko zmieniającym się świecie technologii i potrzeb nie ma znaczenia, czy mówimy o fizycznym oddziale banku, stronie internetowej, aplikacji mobilnej czy o domowym asystencie głosowym – każdy z tych kanałów musi posiadać wysoki poziom zabezpieczeń i ochrony przed nadużyciami.

Problem ilości punktów styku, które należy brać pod uwagę, gdy projektuje się i wdraża zabezpieczenia przed oszustwami i kradzieżami, komplikuje coraz większa popularność inteligentnych urządzeń domowych oraz oczekiwanie, że wyręczą one użytkownika w rutynowych zadaniach, opłacanych automatycznie za pomocą dodanej do systemu karty.

RYS. 5. Usługi finansowe dostępne w modelu omnichannel



Jaka jest odpowiedź na problem, który technologia pomogła wykreować?

Pozwólmy jej robić to, w czym jest naprawdę dobra.

W nowym podejściu pozwalamy AI decydować co jest istotne, bez wstępnego definiowania wzorców i relacji w systemie. Pozwalamy też, by sama się uczyła, jak optymalnie wykorzystywać wszystkie dostępne jej informacje, aby zwiększać bezpieczeństwo instytucji finansowych i ich klientów.

W ramach testu takiego podejścia Dell Technologies i firma RSA proponowały i przetestowały nowy model wykrywania nadużyć finansowych.

Stworzenie tego rozwiązania, opartego na ML, wymagało wielu działań, które dla uproszczenia da się sprowadzić do dwóch punktów. Potrzebne było:

- zgromadzenie informacji pochodzących ze wszystkich dostępnych kanałów, jakimi klienci kontaktują się z instytucją;
- zbudowanie na ich podstawie uniwersalnego modelu oceny ryzyka, który uwzględni wszystkie możliwe sposoby dostępu do systemu.

Jeśli myślimy o jednym kanale, wówczas zgromadzenie i opis danych nie stanowią problemu. Sytuacja wygląda zgoła inaczej, kiedy przenosimy się na poziom klienta indywidualnego, korzystającego z jednego lub kilku urządzeń, a niekiedy używającego ich jednocześnie. W tym przypadku niewiadomych jest więcej niż rzeczy, które możemy nazwać z całą pewnością.

AI potrzebuje danych, a my znaleźliśmy się w sytuacji, kiedy nie wiemy, z jakiego rodzaju urządzenia korzysta klient, ani kto je wyprodukował. Co więcej

– nowe urządzenia mogą pojawiać się każdego dnia, zatem nie możemy pozwolić sobie na ręczne dodawanie do systemu każdego z nich.

W takiej właśnie, skomplikowanej rzeczywistości powstawał projekt Dell Technologies i RSA. Samo rozwijający się model miał uwzględniać już zebraną wiedzę oraz wzorce zachowań budowane na podstawie istniejących kanałów dostępu. Miał także przewidywać analogiczne zachowania w przyszłych, nieznanych jeszcze kanałach.

By stworzyć taki model, należało uporać się z wyzwaniem, jakim było opracowanie nowej metody grupowania zdarzeń (rozumianych jako działania klienta w konkretnej aplikacji, na konkretnym urządzeniu lub w konkretnym miejscu) oraz zbudować najbardziej wartościowe kombinacje wszystkich takich elementów systemu.

Budowa modelu była niesłychanie wymagającym zadaniem, ponieważ mówimy o zdarzeniach, które jeszcze nie miały miejsca, urządzeniach i aplikacjach, które jeszcze nie powstały oraz o usługach, które jeszcze nie są oferowane.

Nim AI mogła uporać się z dokonaniem opisanych powyżej predykcji, należało stworzyć podstawę, która działa na zdarzeniach znanych, acz nieoczywistych. Załóżmy, że urządzeniem, dla którego zbudujemy model wykrywania nadużyć finansowych jest inteligentna pralka. Przyjmijmy, że wysyła ona tylko kilka prostych informacji, nie definiując jakich. Dla tych zmiennych możemy zbudować wiele kombinacji, które powinny zostać uwzględnione w naszym modelu, takich jak:

- dni, jakie upłynęły od pojawienia się urządzenia w domu klienta;

- liczba klientów, u których pojawił się ten konkretny model, w ciągu ostatnich 24h;
- łączna kwota transakcji dla danego klienta wykonana przez ten konkretny model pralki;
- liczba transakcji dla tego modelu pralki dla tego klienta w ciągu ostatnich 24h.

Mimo ograniczonej puli danych, jakie gromadzi i wysyła pralka, liczba kombinacji czynników, które powinny być ujęte w modelu może być spora, a to tylko część informacji, na których chcemy oprzeć nasz model. Do gotowego produktu droga daleka, ale widać już doskonale, że człowiek pozbawiony wsparcia AI nie zdołałby jej pokonać, a przynajmniej nie odpowiednio szybko.

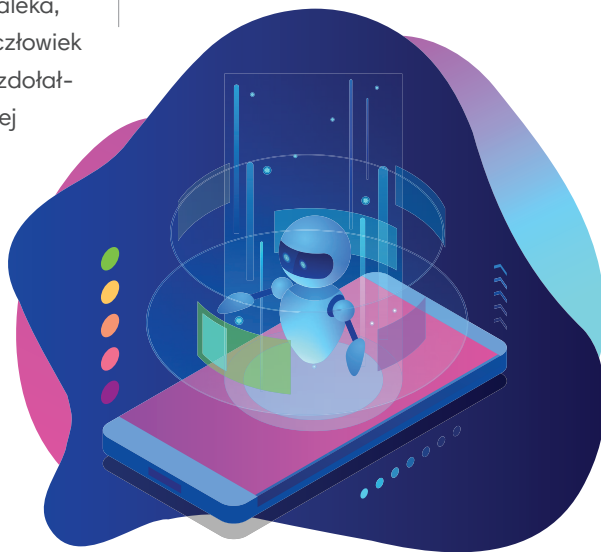
Ocena, które z tych kombinacji będą najbardziej efektywne w ostatecznym modelu, definiowanie relacji pomiędzy dostępnymi danymi oraz powiązanie ich z bezpieczeństwem transakcji finansowych jest zadaniem idealnym dla systemów głębokiego uczenia – deep learning.

Dzięki tej technologii AI radzi sobie z tym, czemu nie podołałby nawet najbardziej utalentowany i najlepiej wykształcony człowiek: jest w stanie szybko powiązać ze sobą ogromną ilość zmiennych, znaleźć zależności, które je łączą oraz zareagować na znalezione w ten sposób nieprawidłowości. Tak właśnie rozwiązania bazujące na sztucznej inteligencji znajdują operacje, które noszą znamiona oszustwa finansowego.

Efektom prac Dell Technologies i firmy RSA było opracowanie nowej metody ochrony operacji finansowych, tzw. *Adaptive Authentication*, umożliwiającej zwiększenie bezpieczeństwa tradycyjnych transakcji oraz przygotowanej na włączenie do analizy zupełnie nowych kanałów dostępu, kiedy takowe się pojawią.

Kilka słów o technologii, która stoi za tego typu rozwiązaniami

Dane występują nie tylko w różnych formatach (liczby, słowa w formie tekstu, słowa w formie zapisu dźwiękowego, emotikony, obrazy, QR cody



i inne), docierają nie tylko z różnych kanałów dostępu (strony www, bankomaty, aplikacje, wearables i urządzenia typu smart), ale i z różnorodnych urządzeń, których producenci działają na własnych lub zmodyfikowanych przez siebie systemach operacyjnych, które mogą stosować inne sposoby zapisu danych i inne ich formaty (Microsoft, Apple, Google, Samsung itp.). Wyzwaniem, przed którym stoją naukowcy i inżynierowie zajmujący się rozwojem AI, jest sposób unifikacji danych.

Na szczęście tę przeszkodę udało się pokonać dzięki tzw. Data Management, a konkretniej dzięki podejściu Data Lake, czyli zunifikowanemu sposobowi przechowywania dokumentów pochodzących z wielu źródeł. Data Lake usprawnia nie tylko przetwarzanie plików zapisanych w różnych formatach, ale i różnorodnych obiektów, a jednocześnie zapewnia niezbędną wydajność i efektywność systemów.

Kolejnym rozwiązaniem umożliwiającym szybką absorpcję danych do systemów AI są platformy integracji lub iPaaS, zewnętrzne rozwiązania oferujące zestaw gotowych narzędzi, dzięki którym można sprawnie budować mechanizmy automatyzacji, mając do dyspozycji konieczne instrumenty technologiczne.

„Proszę, oceń stopień zadowolenia z naszej usługi”

Klienci nie przepadają za dzieleniem się opiniami, szczególnie, gdy nie mają powodów do niezadowolenia z obsługi. Biznes potrzebuje jednak rzetelnej i możliwie obiektywnej informacji o tym, jak są postrzegane świadczone usługi.

Gdyby zatem istniała metoda, która pozwoliłaby bez zadawania pytań dowiedzieć się, co myślą klienci tuż po zakończeniu transakcji, praktycznie w momencie, kiedy odchodzą od okienka w banku!

Okazuje się, że jest to technologia *Human Perception Technology*, która jest jedną z wielu odmian sztucznej inteligencji i zajmuje się rozpoznawaniem zachowań ludzi oraz ich emocji.

Dzisiejsze systemy rozpoznawania obrazu potrafią nie tylko jednoznacz-

nie rozpoznać człowieka na zdjęciu czy obrazie z kamery monitoringu, ale są także w stanie z dużym prawdopodobieństwem określić płeć, przedział wiekowy i rozpoznać podstawowe emocje, ujawnione w mimice i zachowaniu.

Jesteśmy zatem w stanie, używając Human Perception, określić z dużym prawdopodobieństwem, czy klient jest zadowolony, skupiony, czy może zaskoczony.

Oczywiście tego typu systemy nie mogą być stosowane wszędzie, a tam gdzie mogą, muszą być zaprojektowane z myślą o ochronie prywatności i zapewnieniu bezpieczeństwa klientom. Trzeba jednak pamiętać, że sama technologia istnieje, jest przetestowana i gotowa do użycia w postaci kompletnych, łatwych do implementacji rozwiązań.

Zamiast podsumowania

Zadaniem niniejszego raportu było nie tylko pokazanie, że sztuczna in-

teligencja jest obecna w sektorze finansowym od dawna, ale i zaakcentowanie faktu, że szybki rozwój tych technologii wręcz zachęca, by odkrywać ich nowe zastosowania, nie zawsze oczywiste i nie zawsze związane z podstawową działalnością banków.

Kto wie, może niebawem okaże się, że są procesy, które można zautomatyzować całkowicie i dzięki temu uzyskać przewagę konkurencyjną na trudnym rynku usług finansowych? Trudno zgadnąć, jakie nieoczekiwane efekty biznesowe może przynieść augmentacja, czyli włączenie AI do procesów, w których decydentami są ludzie, albo jak duża zmiana może przynieść poprawa zadowolenia klientów lub pracowników banków, szybko i skutecznie oceniana przez sztuczną inteligencję.

Technologia dostarcza narzędzi i rozwiązań, po które wystarczy sięgnąć. Czasem mały krok związany z technologią jest dużym skokiem dla biznesu.



SZTUCZNA INTELIGENCJA

jako kluczowy element budowy architektury bezpieczeństwa teleinformatycznego nowej generacji

Nieustanny wzrost ilości, szybkości i stopnia zaawansowania cyberataków przytłacza zespoły bezpieczeństwa w podmiotach z każdej branży. Na szczęście, architekci bezpieczeństwa teleinformatycznego, chcący odciążyć się od swoich żmudnych codziennych obowiązków, mają do dyspozycji nowe narzędzia, bazujące na technologiach sztucznej inteligencji nowej generacji.

Rozwiązania, takie jak wirtualny analityk bezpieczeństwa, rozpoznawanie zaawansowanych zagrożeń za pomocą wyszkolonej głębokiej sieci neuronowej, czy uczenie maszynowe dla rozpoznawania określonych wzorców, pomagają stawić czoła tym wyzwaniom. Komponenty rozwiązań wykorzystujących sztuczną inteligencję ulokowane w infrastrukturze firmy, czy też serwy dostarczane w postaci chmury obliczeniowej, pomagają analizować nadchodzące zagrożenia w czasie rzeczywistym. Dzięki temu zespoły bezpieczeństwa teleinformatycznego mają możliwość powstrzymania hakerów i złośliwego oprogramowania przed przeniknięciem do ich środowiska.

Zwiększenie liczby, szybkości i złożoności cyberataków

W 2019 r. średni cykl życia kampanii zagrożeń, od rozpoczęcia rozpoznania, do pojawienia się nowego wariantu lub nowej kampanii, często wynosił jeden miesiąc i mniej. Istnieje rozwinięty ekosystem cyberprzestępczości, w którym dostępne są zestawy narzędzi wykorzystujące podatności oprogramowania, Malware-as-a-Service (MaaS), boty do

wynajęcia, i inne, przez co drastycznie skrócił się czas wejścia na rynek dla cyberprzestępców.

Jednocześnie wiele zagrożeń cybernetycznych stało się bardziej wyrafinowanych i nie ograniczają się jedynie do silnie ukierunkowanych ataków na wybrane serwisy w celu ich zablokowania. Działania przestępcze w cyberprzestrzeni wykorzystują m.in. socjotechnikę i prowadzą do powstawania zagrożeń, które stają się coraz trudniej zauważalne dla użytkowników końcowych oraz trudne do wykrycia przez tradycyjne kontrole bezpieczeństwa.

Oczywiście, powtarzanie w kółko tego samego zachowania i oczekiwanie różnych rezultatów jest naiwnością. Aby wygrać tę wojnę, trzeba ponownie przemyśleć swoją strategię bezpieczeństwa, a zmiana paradygmatu bezpieczeństwa wymaga trzech podstawowych podejść:

1. Zaczynaj od bezpieczeństwa. Zamiast budować sieć, a następnie nakładać na nią zabezpieczenia, rozpocznij projektowanie z myślą o bezpieczeństwie. Polityki bezpie-



Wojciech Ciesielski
Major Account Manager,
Fortinet

czeństwa muszą płynnie przechodzić od sieci korporacyjnej do chmury, od sieci przemysłowych do oddziałów oraz pracowników mobilnych, i konsekwentnie być egzekwowane.

2. Wykorzystaj ekonomię cyberprzestępczości. Cyberprzestępcy podlegają takim samym ograniczeniom finansowym jak każda organizacja. Dlatego też większość przestępców woli atakować łatwo dostępne cele przy użyciu znanych metod, ponieważ opracowywanie nowych narzędzi i ataki typu dnia zerowego są kosztowne. Można wyeliminować wiele rodzajów ryzyka, wykonując m.in. następujące działania:

- kontrolę zgodności ze standardami i politykami bezpieczeństwa,
- podnoszenie poziomu świadomości użytkowników w zakresie cyberzagrożeń,
- odkrywanie i usuwanie luk w zabezpieczeniach,

- centralizację logowania zdarzeń i kontroli,
- wprowadzenie ram bezpieczeństwa bazujących na interoperacyjności, wysokiej wydajności i głębokiej integracji,
- segmentację sieci w celu ograniczenia lub spowolnienia poziomego ruchu złośliwego oprogramowania.

3. Zwalczaj ogień ogniem. Zarówno przedsiębiorstwa, jak i cyberprzestępczość działają z prędkością cyfrową. Wiele incydentów w cyberprzestrzeni zaistniało, ponieważ szybkość ataku jest większa niż czas reakcji systemu bezpieczeństwa. Jest to szczególnie zauważalne tam, gdzie na każdym etapie procesu wymagana jest interwencja człowieka. Zamiast tego, krytyczne zdarzenia muszą wywołać natychmiastową reakcję. Oczywiście, automatyka może reagować tylko na znane zagrożenia. Dodanie maszynowego uczenia (machine learning, ML) pozwala zautomatyzowanym systemom lepiej identyfikować nietypowe zachowania i redukować liczbę fałszywych alarmów¹.

Ewolucja sztucznej inteligencji w bezpieczeństwie cybernetycznym

Firmy zajmujące się bezpieczeństwem cybernetycznym od kilku lat wykorzystują uczenie maszynowe

w walce z cyberprzestępcami – przede wszystkim w dziedzinie wykrywania zagrożeń. Algorytmy szkoleniowe stosują uczenie maszynowe, aby umożliwić coraz dokładniejszą identyfikację cech złośliwych plików, a rezultatem jest wykrywanie w czasie rzeczywistym zaawansowanych zagrożeń, w tym ataków dnia zeroowego.

Jednak samo lepsze wykrywanie zagrożeń nie jest wystarczające, aby zespoły odpowiedzialne za cyberbezpieczeństwo czuły się mniej obciążone. Lepsze wykrywanie oznacza jednak jeszcze większą liczbę alarmów, które muszą być obsługiwane. Po-

trzebna jest zatem bardziej rozwinięta automatyzacja – zwłaszcza w zakresie reagowania na zagrożenia.

Postęp zarówno w dziedzinie sztucznej inteligencji (Artificial Intelligence, AI), jak i mocy obliczeniowej pozwala nadążyć za cyberzagrożeniami. Niezależnie od tego, czy celem jest utrzymanie aktualnego stanu wiedzy o globalnych zagrożeniach w cyberprzestrzeni, identyfikowanie incydentów specyficznych dla danej organizacji, zanim staną się one naruszeniami, czy nawet wdrożenie prewencyjnych działań w czasie rzeczywistym, sztuczna inteligencja może być właściwą odpowiedzią.



W przeciwieństwie do automatyzacji i uczenia maszynowego, sztuczna inteligencja próbuje odtworzyć procesy analityczne ludzkiej inteligencji nie tylko po to, aby umożliwić podejmowanie decyzji z prędkością maszyny, ale z czasem może nawet zacząć przewidywać i zapobiegać zdarzeniom związanym z bezpieczeństwem, zanim one wystąpią.

Prawdziwy system sztucznej inteligencji wymaga sztucznej sieci neuronowej (ANN) w połączeniu z modelem głębokiego uczenia się, aby nie tylko przyspieszyć analizę danych i podejmowanie decyzji, ale także umożliwić

sieci adaptację i ewolucję w przypadku napotkania nowych informacji. Ten szeroko zakrojony proces szkoleniowy obejmuje staranne dostarczanie ogromnych ilości coraz bardziej złożonych informacji, dzięki czemu sieć może nie tylko identyfikować wzorce i opracowywać strategie rozwiązywania problemów, ale także dostosowywać te algorytmy w przypadku napotkania nowego wzorca.

Sztuczna inteligencja następnej generacji: głębokie sieci neuronowe

Aby opisać potencjał sztucznej inteligencji następnej generacji dla cyberbezpieczeństwa, pomocne jest precyzyjne zdefiniowanie używanej terminologii:

- **sztuczna inteligencja (AI)** jest ogólnym terminem, który odnosi

się do zdolności maszyny do naśladowania inteligentnego zachowania człowieka,

- **uczenie maszynowe (ML)** jest jednym ze składników sztucznej inteligencji, wykorzystuje dane do rozwiązywania liniowych problemów, takich jak tworzenie przewidywań lub wykonywanie zadań; sztuczne sieci neuronowe (Artificial Neural Networks, ANN) są jedną z powszechnych metod uczenia maszynowego. Używają one sprzętu i oprogramowania do budowania konfiguracji, która jest wzorowana na działaniu neuronów w ludzkim mózgu poprzez szkolenie maszyny uczącej. Modele są na bieżąco zasilane ogromną ilością informacji, a system analizuje te informacje i dostosowuje algorytmy wykorzystując nowe taktyki i możliwości stosowane przez złożone oprogramowanie.

” Firma Fortinet dokonała przełomu w dziedzinie wykorzystania sztucznej inteligencji w obszarze cyberbezpieczeństwa, ponieważ jako pierwsza wprowadziła na rynek, dostępnego do instalacji we własnej infrastrukturze informatycznej, wirtualnego analityka bezpieczeństwa (FortiAI), bazującego na technologii głębokiej sieci neuronowej. De facto jest on drugą generacją samouczącego się systemu detekcji cyberzagrożeń (Self-Envolving Detection System, SEDS) opracowanego i rozwijanego przez Fortinet FortiGuard Lab, który ustawicznie uczy się już od ponad ośmiu lat.



- **głębokie sieci neuronowe** (Deep Neural Networks, DNN), czasami znane jako głębokie uczenie (Deep Learning, DL), są jedną z technik uczenia maszynowego, która wykorzystuje wiele sztucznych sieci neuronowych – z dwoma lub więcej warstwami pomiędzy warstwami wejściową i wyjściową – do modelowania złożonych, nieliniowych relacji.

Poziomy zrozumienia i analizy zapewniane przez głęboką sieć neuronową dają możliwość przeniesienia sztucznej inteligencji na kolejny poziom w zakresie cyberbezpieczeństwa. Kiedy sztuczna inteligencja jest używana tylko do wykrywania zagrożeń, może potencjalnie zwiększyć obciążenie zespołu bezpieczeństwa, ponieważ zwiększa ilość otrzymywanych alarmów. Podnosi to również prawdopodobieństwo, że konkretne zagrożenie nie otrzyma na czas odpowiedzi. Z drugiej strony, jeśli sztuczna inteligencja może być wykorzystana do podejmowania decyzji dotyczących reakcji na zagrożenie, może to zacząć przynosić istotne wsparcie profesjonalistom zajmującym się cyberbezpieczeństwem. Pracownicy mogą nadal koncentrować się na strategii bezpieczeństwa, podczas gdy większość działań podejmowanych w odpowiedzi na zagrożenia jest zautomatyzowana i prowadzona w czasie rzeczywistym przez wirtualnego analityka bezpieczeństwa².

Szkolenie sztucznej inteligencji

Jednym z najbardziej krytycznych elementów dla jakości i skuteczności działania rozwiązania sztucznej inteligencji jest sposób prowadzenia szkolenia. Społeczność AI zaleca, aby

każde rozwiązanie z zakresu sztucznej inteligencji przechodziło trzy etapy szkolenia:

1. **Nadzorowane uczenie się.** Ten początkowy model rozpoczyna się od zasilenia systemu sztucznej inteligencji ogromnym wolumenem oznaczonych danych, w których charakterystyka każdego zestawu informacji jest wyraźnie określona, a decyzje są przewidywalne. Na przykład zespół ds. rozwoju sztucznej inteligencji w Fortinet korzysta z danych opracowanych przez ponad 200 analityków z FortiGuard Lab, którzy obecnie rejestrują ponad 580 tys. godzin badania danych rocznie. Ponadto wykorzystuje on dane zbierane w czasie rzeczywistym z urządzeń i czujników działających na całym świecie oraz dane pochodzące z wielu źródeł wiedzy o zagrożeniach. Ostatecznie to właśnie ten poziom i ilość danych wejściowych pozwalają systemom sztucznej inteligencji na ciągłe doskonalenie poprzez rozszerzanie zestawu oznaczonych wzorców i reakcji.
2. **Nauka bez nadzoru.** W tej kolejnej fazie dane nieoznaczone są wprowadzane powoli, co zmusza system do samodzielnego uczenia się, gdy zaczyna dostrzegać i rozpoznawać nowe wzorce.
3. **Wzmocnienie.** Oba te procesy monitorują działanie systemu za pomocą znanych i nieznanych plików i „nagradzają” system za dobre wyniki. Cykle szkoleniowe pomiędzy tymi trzema strategiami uczenia się odbywają się na bieżąco przez miesiące, a czasami lata, w zależności od złożoności

problemów, które system musi zidentyfikować i rozwiązać.

Ze względu na powtarzające się wymogi procesu uczenia się, każdy system sztucznej inteligencji, który nie wykorzystuje wszystkich trzech z powyższych modeli uczenia się jest niepełny. Każdy model uczenia się pomaga udoskonalić wyniki i poprawić dokładność.

Ponieważ środowisko zagrożeń wciąż się zmienia, modele szkolenia w zakresie sztucznej inteligencji nie mogą pozostawać statyczne. System musi być stale wzbogacany o nowe modele, które bazują na nowych zagrożeniach i technikach ataku, a także o nowe strategie identyfikacji i wykrywania. Należy również stosować stały monitoring jakości rozpoznawania wzorców. Sztuczna inteligencja może zostać niezamierzenie zatruta złymi danymi, tworząc tendencję, która wpływa na jej zdolność do podejmowania dobrych decyzji, lub zostać celowo zatruta w celu ominięcia pewnych rodzajów zagrożeń³.

Wykorzystanie AI do poznania konkretnych organizacji

Aby bardzo przyspieszyć wykrywanie wzrastającej liczby zaawansowanych zagrożeń, wirtualny analityk bezpieczeństwa FortiAI uczy się i dostosowuje do nowych ataków na konkretną organizację, stale ulepszając i optymalizując metody ochrony przed zagrożeniami. W rezultacie wirtualny analityk bezpieczeństwa wspiera personel zespołu bezpieczeństwa poprzez identyfikację i analizę złośliwego oprogramowania niebazującego na plikach, jak i opartego na plikach, oraz identyfikuje zagrożone systemy w całej organizacji ze stuprocentową pewnością

w czasie poniżej jednej sekundy. W tym celu FortiAI wykorzystuje technologię głębokiej sieci neuronowej do podejmowania decyzji, które podejmowałby analityk bezpieczeństwa podczas ręcznego badania ataków, m.in:

- klasyfikacja ataku na konfigurowalne kategorie, takie jak: wymuszenie okupu (ransomware), złośliwe wydobywanie kryptowalut (cryptojacking), robaki (worms), ataki back-door, wycieki danych (data leaks), botnety i przejmowanie kontroli nad urządzeniami (rootkit),

pierwszej” w przeglądarce doszło do złośliwego wykorzystania kodu; w „chwili drugiej” do pobrania trojana do katalogu użytkownika lub katalogu tymczasowego.

Dane opracowane przez wirtualnego analityka bezpieczeństwa FortiAI mogą zostać automatycznie wykorzystane przez inne elementy architektury bezpieczeństwa w organizacji, takie jak zapory sieciowe nowej generacji (NGFW), umożliwiając zablokowanie zidentyfikowanych przez niego zagrożeń. Pracownicy działu bezpieczeństwa teleinformatycznego mogą

generację samouczącego się systemu detekcji cyberzagrożeń (Self-Envolving Detection System, SEDS) opracowanego i rozwijanego przez Fortinet FortiGuard Lab, który ustawicznie uczy się już od ponad ośmiu lat. FortiAI zawiera niezależną, samowystarczającą sztuczną inteligencję, która naśladuje funkcję analityka bezpieczeństwa informacji i, podobnie do człowieka, dostosowuje się do nowych ataków i zdobywa doświadczenie w miarę upływu czasu. Jednak w przeciwieństwie do analityków zajmujących się bezpieczeństwem, robi to z prędkością maszyny. Wirtualny ana-



- dochodzenie do źródła ataku poprzez identyfikowanie pierwotnego miejsca zakażenia i zapewnienie pełnej widoczności rozprzestrzenienia się infekcji od pacjenta zerowego do wszystkich kolejnych narażonych systemów,
- analiza złośliwego oprogramowania pod kątem jego cech i osi czasu incydentu. Przypomina to miniatury model łańcucha ataku (kill-chain), który opisuje w sposób naukowy, co zagrożenie próbowało zrobić krok po kroku, w tym zastosowaną technikę – przykładowo: w „chwili zerowej” nastąpiło pobranie pliku HTML; w „chwili

następnie wykorzystać tę wiedzę do kontroli bezpieczeństwa w całej sieci.

Wirtualny analityk bezpieczeństwa

Firma Fortinet dokonała przełomu w dziedzinie wykorzystania sztucznej inteligencji w obszarze cyberbezpieczeństwa, ponieważ jako pierwsza wprowadziła na rynek, dostępnego do instalacji we własnej infrastrukturze informatycznej, wirtualnego analityka bezpieczeństwa, o nazwie FortiAI, bazującego na technologii głębokiej sieci neuronowej. Wirtualnego analityka bezpieczeństwa FortiAI można de facto określić jako „SEDS 2.0”, drugą

lityk bezpieczeństwa z bardzo wysoką wydajnością wykorzystuje głęboką sieć neuronową do automatyzacji badania incydentów bezpieczeństwa i budowania wiedzy o zagrożeniach w celu przerywania ukierunkowanych ataków.

Model uczenia się bez nadzoru głębokiej sieci neuronowej wykorzystywany w wirtualnym analityku bezpieczeństwa FortiAI, może być tak naprawdę nazwany „przyjazną sztuczną inteligencją” (Friendly Artificial Intelligence, FAI), terminem, który do tej pory był w dużej mierze aspiracyjny. Ze względu na swoje możliwości związane z wykorzystaniem techno-

FORTINET®

SKALA ZAGROŻEŃ JEST WIĘKSZA NIŻ KIEDYKOLWIEK

Reakcja musi być szybka, jak nigdy dotąd

www.fortinet.com

Copyright © 2020 Fortinet, Inc. Wszelkie prawa zastrzeżone.



logii uczenia maszynowego, wirtualny analyt bezpieczeństwa identyfikuje i analizuje zagrożenia z coraz większą prędkością i dokładnością, zwiększając tym samym wydajność pracy całego zespołu odpowiedzialnego za bezpieczeństwo cybernetyczne.

Architektura bezpieczeństwa cyfrowego wsparta sztuczną inteligencją

Firma Fortinet od dawna inwestuje w rozwiązania sztucznej inteligencji (AI), aby sprostać rosnącym wyzwaniom w zakresie bezpieczeństwa cybernetycznego. Modele maszyn uczących się i bardziej zaawansowane sztuczne sieci neuronowe (ANN), szkolone przez analytów zagrożeń w laboratoriach FortiGuard Labs, przetwarzają ogromne ilości danych, pomagając aktualizować wiedzę na temat globalnych cyberzagrożeń. Są one uzupełniane przez podobne systemy sztucznej inteligencji, które mogą być wdrażane w infrastrukturze danej organizacji w celu zapobiegania atakom, wykrywania ich i reagowania na nie. Rozwiązania te obejmują urządzenia końcowe, pocztę elektroniczną, systemy oraz aplikacje, niezależnie od tego, czy znajdują się one w sieci wewnętrznej firmy, chmurze publicznej, czy działają przez internet.

Dzięki temu możliwe jest zbudowanie solidnej architektury cyberbezpieczeństwa sterowanej przez sztuczną inteligencję, która wykorzystuje zalety globalnego scentralizowanego oraz lokalnego rozproszonego uczenia maszynowego. Z zastosowaniem technik sztucznej inteligencji przeszkolonych i zastosowanych na każdym etapie łańcucha ataku, począwszy od prowadzonego rozpoznania,

a skończywszy na realizacji celów, rozwiązania Fortinet są w stanie zarządzać ryzykiem cybernetycznym zarówno zewnętrznym, jak i wewnętrznym, dzięki zaawansowanym funkcjom zapobiegania, wykrywania i reagowania na zagrożenia.

Zasoby, uczenie i integracja wyznacznikiem skuteczności AI

Wiele firm zajmujących się bezpieczeństwem cybernetycznym twierdzi, że wprowadziły do swoich rozwiązań mechanizmy ochrony z wykorzysta-

w izolacji jest bezużyteczna. Im więcej informacji o zagrożeniach jest współdzielonych – czy to z zewnętrznego źródła informacji, czy też ze zintegrowanych systemów bezpieczeństwa rozmieszczonych w sieci rozproszonej – tym skuteczniejsze staną się systemy obronne bazujące na sztucznej inteligencji.

Systemy wyposażone w rozwiązania sztucznej inteligencji zapewniają firmom i organizacjom przewagę nad cyberprzestępcami. Wpłatają one zabezpieczenia w infrastrukturę, identyfikują i reagują na najbardziej

” Sztuczna inteligencja w izolacji jest bezużyteczna. Im więcej informacji o zagrożeniach jest współdzielonych – czy to z zewnętrznego źródła informacji, czy też ze zintegrowanych systemów bezpieczeństwa rozmieszczonych w sieci rozproszonej – tym skuteczniejsze staną się systemy obronne bazujące na sztucznej inteligencji.

niem sztucznej inteligencji. W rzeczywistości jednak większość z nich nie posiada prawdziwej sztucznej inteligencji, ponieważ ich infrastruktura jest zbyt mała lub ich modele uczenia się są niekompletne. Inne odmawiają ujawnienia stosowanych przez nie metod, co budzi obawy co do wiarygodności ich rozwiązań sztucznej inteligencji. Powinny to być czerwone flagi dla każdej organizacji chcącej przyjąć system bazujący na sztucznej inteligencji.

Równie ważne jest, aby nawet jeśli system sztucznej inteligencji spełnia podstawowe wymagania szkoleniowe i infrastrukturalne, nadal musiał współdziałać w ramach istniejącego środowiska bezpieczeństwa. Inteligencja

zaawansowane zagrożenia. Mają działanie odstraszające i zniechęcające cyberprzestępców do podejmowania prób ataków, ponieważ wiązałoby się to z koniecznością opracowania nowych narzędzi i technik, co przekłada się na wysokie po ich stronie koszty⁴.

- 1 Disrupting Cybercriminal Strategy With AI and Automation, Security Week, August 2019
- 2 Using AI to Address Advanced Threats That Last-Generation Network Security Cannot, 2019 Fortinet.
- 3 Disrupting Cybercriminal Strategy With AI and Automation, Security Week, August 2019
- 4 Disrupting Cybercriminal Strategy With AI and Automation, Security Week, August 2019

BIOMETRIA Z PUDEŁKA

Rozwiązania biometryczne nie są niczym nowym na rynku finansowym, co roku zyskują coraz większe zaufanie klientów. Już w 2016 r. ponad 60% Brytyjczyków deklarowało, że uważają biometrię za tak samo bezpieczną, lub nawet bezpieczniejszą, od tradycyjnych metod weryfikacji tożsamości. Według analityków Markets and Markets, wartość globalnego rynku rozwiązań biometrycznych w zakresie rozpoznawania twarzy zwiększy się z 3,2 mld USD w 2019 r. do 7,0 mld USD do 2024 r., przy średniorocznym wzroście na poziomie 16,6%. Rozwiązania tego typu mogą m.in. znacząco upraszczać dokonywanie transakcji oraz przyspieszać obsługę klienta.

W październiku 2019 r. NatWest, jako pierwszy bank na świecie, wydał biometryczną kartę kredytową, wykorzystującą rozpoznawanie odcisków palców w celu uwierzytelnienia tożsamości i umożliwienia dokonywania płatności. Chiny poszły o krok dalej z rozwiązaniem „Smile-to-Pay”, które pozwala użytkownikom płacić za towary, po prostu uśmiechając się do maszyny w punkcie sprzedaży.

Gotowe do wdrożenia

Obecnie na rynku pojawia się coraz więcej rozwiązań pudełkowych typu SaaS, które są gotowe do wdrożenia przez odpowiednich integratorów.

Przykładem rozwiązania z zakresu cyfrowej weryfikacji tożsamości jest pakiet narzędzi firmy Veridas. Hiszpański producent oprogramowania oferuje technologie biometryczne oparte na autorskich algorytmach uczenia maszynowego w trzech zasadniczych obszarach: rozpoznawania twarzy (w tym weryfikacja autentyczności osoby i biometryczny kod QR), głosu oraz weryfikacji dokumentów tożsamości. Silniki biometryczne Veridas zostały

wysoko ocenione przez amerykański Narodowy Instytut Standaryzacji i Technologii (#3 w kategorii rozpoznawanie twarzy w kwietniu 2019 r.), a jednym z rynkowych potwierdzeń jakości jest globalna implementacja w banku BBVA.

– Chcemy, aby nasi klienci mieli dostęp do możliwie największego zakre-

su funkcji i usług za pośrednictwem ulubionych kanałów, o każdej porze dnia i nocy, z zachowaniem wygody i bezpieczeństwa. Veridas udowodnił, że oferuje niezrównaną technologię – będzie teraz dostępna dla naszych klientów niezależnie od lokalizacji – podkreśla **Gonzalo Rodriguez**, szef rozwoju biznesu BBVA w Hiszpanii.

CASE STUDY

BBVA, jako jeden z największych banków komercyjnych świata, poszukiwał nowych technologii umożliwiających wzrost biznesu przez przyciąganie nowych klientów. Wdrażając rozwiązanie Veridas, BBVA stał się pierwszym bankiem w Hiszpanii oferującym w pełni cyfrową rejestrację potencjal-

nych użytkowników. Usługa jest obecnie dostępna w Meksyku, Hiszpanii, Stanach Zjednoczonych i Kolumbii. Narzędzie identyfikacji tożsamości autorstwa Veridas pozwoliło bankowi na cyfrowy onboarding klientów przy zachowaniu maksymalnego poziomu bezpieczeństwa. Rozwiązanie pozwala zastąpić proces kontaktu z agentem banku w czasie rzeczywistym. Zamiast tego, oprogramowanie Veridas, oparte na sztucznej inteligencji, weryfikuje dokument tożsamości klienta i dokonuje porównania biometrycznego twarzy z uwzględnieniem autentyczności osoby (tzw. liveness check) – wszystko odbywa się w ciągu kilku minut i w dowolnej lokalizacji za pośrednictwem urządzeń mobilnych lub strony internetowej.

Zespół Veridas, w ścisłej współpracy z BBVA, opracował modułowe rozwiązania z zakresu onboardingu, zapewniając nowym klientom intuicyjność i satysfakcjonującą obsługę. Zestawy narzędzi programistycznych Veridas zostały zaimplementowane w aplikacjach mobilnych i internetowych BBVA, umożliwiając onboarding za pomocą preferowanego kanału. Interfejsy programowania aplikacji (API) przechowywane w chmurze (Amazon Web Services) umożliwiły dostarczanie usług w dowolnej lokalizacji.

Innym przykładem wdrożenia jest Bankia. Bank zaimplementował rozwiązanie z zakresu wideoidentyfikacji. Narzędzie umożliwia cyfrową rejestrację klientów bez konieczności pojawienia się w placówce banku. Pozwala na zdalne nabywanie produktów i usług finansowych dzięki technologii biometrii twarzy, a także na skanowanie i weryfikację dokumentów tożsamości.

Ważnym czynnikiem sukcesu jest możliwość optymalnego wdrożenia rozwiązania technologicznego. Z tego powodu Veridas podjął decyzję o partnerstwie z GFT Group – doświadczonym integratorem rozwiązań z bardzo mocnym zespołem technicznym. Rozwiązania Veridas funkcjonują w modelu Software as a Service, dzięki czemu dostępne są dla organizacji na całym świecie. Interfejsy programowania aplikacji (API) oraz zestawy narzędzi programistycznych (SDK) dostarczane inżynierom po stronie



Michał Jankowski

Senior User Experience Designer GFT Poland

klienta pozwalają na daleko idącą personalizację i skuteczną integrację z istniejącymi systemami.

– Dzięki rozwiązaniom z zakresu zdalnej identyfikacji i weryfikacji użytkowników, takim jak dostarczane przez Veridas, jesteśmy w stanie uwolnić klientów banków od konieczności odwiedzania placówek. To fantastyczny krok naprzód w poprawie bezpieczeństwa i zwiększe-

nie wygody dla nas wszystkich. W końcu my też korzystamy z usług bankowości na co dzień. Takie rozwiązania podnoszą user experience w bankowości na zupełnie inny poziom – tłumaczy **Michał Jankowski**, Senior User Experience Designer GFT Poland.

Nie ma AI bez analizy danych

Zakup gotowych rozwiązań od dostawcy to pierwszy krok. Kluczem do osiągnięcia pożądanego efektu jest odpowiednie wdrożenie usługi lub produktu oparte o rozwiązania AI. Po pierwsze – wdrożenie wymaga gruntownego zrozumienia sposobu działania narzędzia oraz celów, jakie stawia przed nim klient. W przypadku podmiotów z rynku finansowego potrzeba szczególnej wiedzy – każde narzędzie musi bowiem działać zgodnie z regulacjami danego rynku. Dodatkowo działanie sztucznej inteligencji opiera się na uczeniu maszynowym z odpowiednio przygotowanych danych. AI jest więc narzędziem, które pomaga nauce o danych uzyskać wyniki i rozwiązania konkretnych problemów – niezbędny jest zatem integrator, który potrafi z danymi pracować.

– Sukces projektów opartych na AI w 80% zależy od danych, a nie tylko od doboru odpowiedniego algorytmu. W praktyce wygląda to tak, że wszelkie dane, na których uczymy maszynę rozpoznawać nieoczywiste szablony ukryte w naszych zbiorach, muszą być odpowiednio ustrukturyzowane, zanim przetworzy je algorytm sztucznej inteligencji. W projektach, które dotyczą skomplikowanych systemów sprowadza się to nierzadko do przetworzenia dziennie dziesiątek milionów wierszy z danymi, które dodatkowo pochodzą z wielu heterogenicznych źródeł – trzeba więc

CASE STUDY

Skok wydajności dzięki integracji systemów z narzędziem machine learning

Klient Grupy GFT z rynku funduszy inwestycyjnych wyraził zapotrzebowanie na automatyzację systemu obsługi zapytań telefonicznych, polegającą na zrozumieniu zapytania głosowego i przekierowaniu klienta do odpowiedniego działu organizacji. Zastosowany wcześniej przez organizację model uczenia maszynowego (Latent Dirichlet Allocation) miał umożliwiać redukcję czasu klasyfikacji zapytań, jednak z uwagi na znaczne objętości danych i niedostateczne zrozumienie przypadku, wydajność pozostawała na niezadowolającym poziomie. Okazało się, że niezbędna jest optymalizacja samego modelu, jak i odpowiednia konfiguracja środowiska do przetwarzania danych. Tego rodzaju działania wymagają kompetencji i doświadczenia komercyjnego w integracji środowisk.

Specjalistom Grupy GFT udało się osiągnąć 78-procentowy wzrost wydajności w automatycznej identyfikacji tematów rozmów, a liczba danych procesowanych przez system wzrosła o 2000% (z 500 tysięcy do 10 milionów rekordów w ciągu godziny). Wysokie kompetencje w dziedzinie Cloud DevOps umożliwiły ponadto uzyskanie znacznych oszczędności kosztów działania systemu.

dane po pierwsze uporządkować, po drugie wykryć w nich braki i błędy, a po trzecie – dostarczyć w ujednoliconym formacie do algorytmu sztucznej inteligencji. Z analogicznym procesem wielokrotnie mieliśmy do czynienia przy dostarczaniu danych na temat różnych instrumentów finansowych banku przy pojawieniu się nowych, międzynarodowych regulacji. Tę pracę trzeba wykonać nad wyraz solidnie i ze zrozumieniem zarówno stojącego za tym biznesu, jak i specyfiki projektów zawierających pierwiastek AI. Popętnienie błędu na tym etapie oznacza klęskę, gdyż ze źle podanych danych nawet najbardziej zaawansowany algorytm sztucznej inteligencji wyciągnie błędne wnioski – zaznacza **Maciej Nowicki**, Head od AI Practice GFT Poland.

Identyfikacja twarzy

W przypadku biometrii twarzy popularną metodą identyfikacji jest wytypowanie jej punktów orientacyjnych, które są kluczowe dla rozróżnienia od innych – jeden system identyfikuje ich niemal 70. Numeryczna reprezentacja twarzy opraco-



Maciej Nowicki

Head od AI Practice GFT Poland

wana na podstawie analizy tych punktów porównywana jest z twarzami znajdującymi się w bazach danych, których mogą być miliony – dla przykładu, w 2018 r. FBI miało dostęp do 412 milionów zdjęć twarzy na potrzeby wyszukiwania. Efektywne zarządzanie tak dużymi zbiorami danych i opracowanie odpowiednich interfejsów ma więc kluczowe znaczenie dla efektywności systemów biometrycznych.

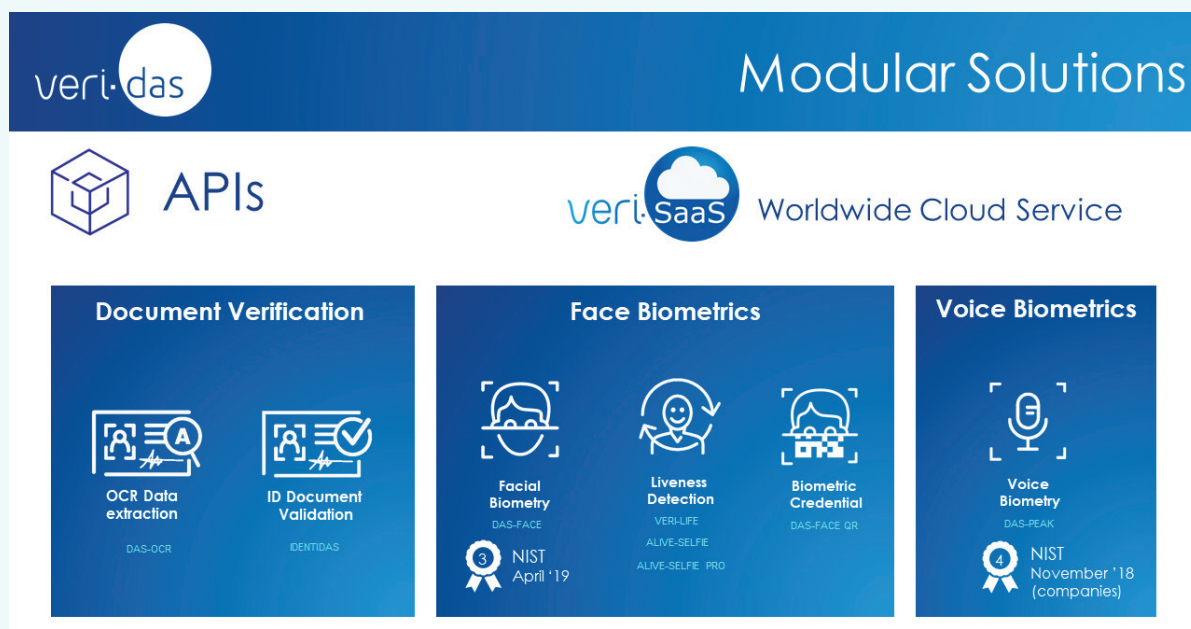
Autorskie algorytmy Veridas oparte są na bardziej zaawansowanych technologiach wykorzystujących sieci neuronowe.

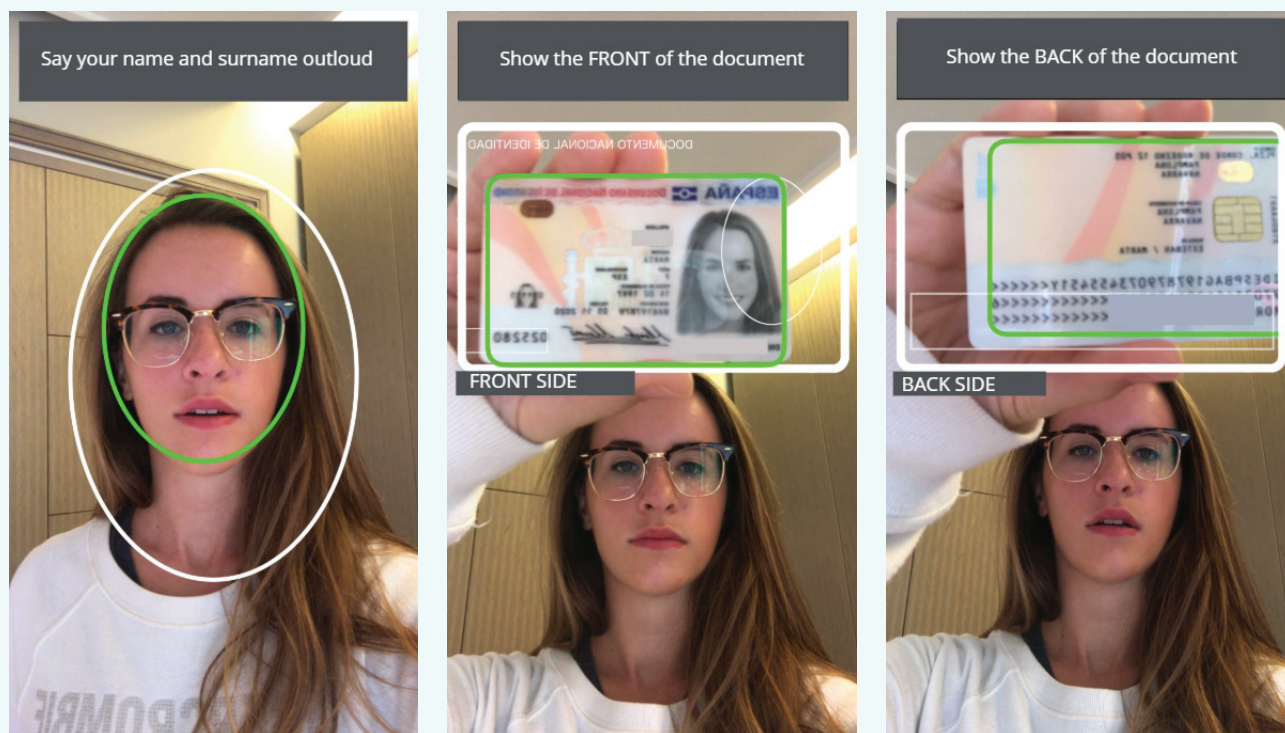
Obraz twarzy przetwarzany jest w mapę nieodwracalnych wektorów matematycznych, na bazie której przyznawany jest współczynnik podobieństwa. W przeciwieństwie do standardowej biometrii opartej na punktach orientacyjnych, system rozpoznawania twarzy Veridas pomija zmiany w ubiorze lub wyglądzie (takie jak okulary bądź zarost), a nawet wpływ procesów starzenia, zapewniając tym samym znacznie wyższą skuteczność. Oba silniki biometryczne Veridas (do rozpoznawania twarzy i głosu) zostały ocenione przez amerykański Narodowy Instytut Standardów i Technologii i wymieniane są w czołówce najlepszych technologii biometrycznych.

Prywatność i bezpieczeństwo danych

Troska o prywatność i pełne bezpieczeństwo danych użytkownika ma kluczowe znaczenie na współczesnym rynku usług bankowych – zwłaszcza w kontekście mechanizmów biometrycznych, które skutecznie identyfikują osobę z jej fizycznymi cechami. Dlatego, z zasady, systemy informatyczne,

Rys. 1. Rozwiązania modularne



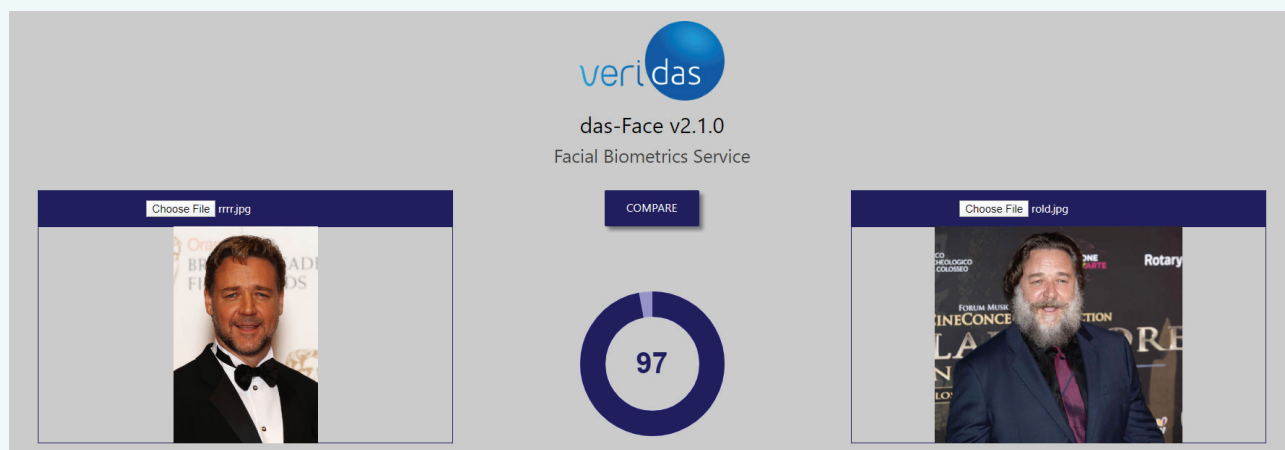
Rys. 2. Procedura wirtualnej weryfikacji klienta

takie jak rozwiązanie opracowane przez Veridas, nie przechowują żadnych danych osobowych klientów. Zaszyfrowany ciąg liczb, będący wzorem danej twarzy, jest przechowywany w miejscu wskazanym przez bank. Na potrzeby powtórnej identyfikacji użytkownika tworzony jest nowy ciąg liczb, porównywany następnie z prze-

chowywanym w bazie. Dzięki temu nie są przechowywane wrażliwe dane użytkownika, co znacząco podnosi bezpieczeństwo rozwiązania.

Oczywiście, społeczeństwo wciąż wymaga edukacji związanej z bezpieczeństwem biometrycznej autentykacji. O ile logowanie do konta banko-

wego czy mikropłatności nie muszą stanowić problemu, o tyle zaciągnięcie kredytu hipotecznego o wysokiej wartości może już spotkać się z pewnymi oporami. Wszystko zależy od tempa adopcji nowych technologii w finansach i idących w parze regulacji, które będą sprzyjały rozwojowi szeroko pojętej oferty banków.

Rys. 3. Ilustracja prezentuje biometrikę twarzy Veridas. System potrafi trafnie rozpoznać osobę niezależnie od powierzchniowych cech wizualnych.

ANALITYKA DANYCH I UCZENIE MASZYNOWE

kluczem do skutecznej
i bezpiecznej bankowości jutra

Cyfrowa transformacja, jaką przechodzi gospodarka, znajduje odzwierciedlenie nie tylko w samej ofercie banków. Dostęp do coraz obszerniejszych zasobów informacji w czasie rzeczywistym, ułatwiony przez upowszechnienie urządzeń mobilnych, przyczynia się do trwałej i gruntownej zmiany potrzeb i oczekiwań użytkowników.

Rezultatem tych tendencji jest rosnąca presja na nowe modele zaangażowania klientów. To dodatkowy czynnik napędzający transformację technologiczną w sektorze finansowym, jako że dotychczas używane, niezintegrowane systemy nie nadążają za aktualnym tempem działalności, przez co nie są w stanie na bieżąco budować doświadczenia klienta. Fundamentalnego znaczenia nabiera sztuczna inteligencja i rozwiązania chmurowe, dzięki którym możliwa jest analiza w czasie rzeczywistym niemal nieograniczonych zasobów danych, zarówno ustrukturyzowanych, jak i nieustrukturyzowanych. Ta zaś jest niezbędna, aby natychmiast reagować na potrzeby i oczekiwania konsumentów.

W cyfrowej transformacji w obszarze rozwiązań chmurowych oraz sztucznej inteligencji uczestniczą także instytucje nadzorcze. Jeszcze do niedawna cloud computing postrzegany był przez KNF jako potencjalne zagrożenie, jednak wskutek pandemii

podejście regulatora ulega przemodelowaniu. – Obecnie obserwujemy potężną zmianę zarówno w percepcji, jak i w praktycznym podejściu do adopcji chmury w sektorach regulowanych. Obecne wydarzenia pokazały, że w przypadku wielu rozwiązań technologicznych potrzeby biznesowe i wymagania klientów mogą przełamać wiele istniejących w „poprzednim” świecie ograniczeń i blokad nowych projektów. Rok 2020 przynosi także przełom

w regulacjach Komisji Nadzoru Finansowego. Komunikat UKNF ze stycznia 2020 r., jest pierwszym przykładem adaptacji do nowych wymagań rozwoju technologii chmurowych – twierdzi **Paweł Jakubik**, członek zarządu Microsoft, przewodniczący Forum Technologii Bankowych.



Marsz sektora bankowego ku chmurze i sztucznej inteligencji będzie coraz silniej determinowany przez ekspansję nietradycyjnych graczy, którzy oferują niższe ceny i lepsze doświadczenia konsumentów. Już dziś 37%¹ klientów „pokolenia Y” korzysta z usług tych właśnie podmiotów, których aspiracją jest stać się interfejsem pomiędzy użytkownikiem a dostawcami różnego rodzaju usług. To poważne wyzwanie dla banków, które, pragnąc uniknąć zmarginalizowania, muszą udostępnić swym klientom porównywalne możliwości. W badaniu przeprowadzonym przez Accenture prawie 90%² dyrektorów bankowych wyraziło opinię, że organizacje muszą wprowadzać innowacje w coraz szybszym tempie, aby nadążyć za rynkiem. Transformacji towarzyszy rosnąca troska o bezpieczeństwo. Reprezentanci co czwartego banku nie mają wątpliwości, że największe zagrożenie dla branży finansowej stanowią wyzwania związane z cyberprzestępczością³. Ryzyko stanowi nie tylko sama aktywność grup przestępczych, ale i sankcje nakładane przez organy regulacyjne w przypadku wycieku danych.

Dane są kluczowe

W obliczu kompleksowych zmian regulacyjnych, szybkiej dezaktualizacji systemów i presji kosztowej instytucje finansowe będą w coraz większym stopniu wykorzystywać duże zbiory danych. Analitycy firmy Mc-

Kinsey & Company przypominają, że w roku 2018 około 15% kontroli ryzyka bankowego przypadało na analizy, natomiast do 2025 r. odsetek ten wzrośnie do 40%⁴.

Stworzenie prognozy przychodów w przedsiębiorstwie wielkości Microsoftu jeszcze niedawno wymagało zaangażowania zespołu tysiąca ludzi przez trzy tygodnie w kwartale. Pomiędzy kompetencjami wykwalifikowanych analityków, uzyskane wyniki cechowały się sporymi rozbieżnościami pomiędzy prognozami a faktami. Tradycyjne metody prognozowania nie były też w stanie wygenerować prognoz „na żądanie” dla różnych użytkowników. Dlatego zespół finansowy Microsoftu wykorzystał wiedzę pracowników do ustalenia możliwości wdrożenia sztucznej inteligencji w całej organizacji. Rezultatem są liczone w setkach godzin miesięcznie oszczędności czasu pracy członków zespołu przy równoczesnym ograniczeniu ryzyka i poprawie skuteczności podejmowania decyzji biznesowych.

Kluczem do sukcesu okazało się wykorzystanie usługi Azure Machine Learning do analizy zasobów big data w celu tworzenia niezwykle dokładnych prognoz. Dane wyjściowe zostały wprowadzone do narzędzia opartego na Power BI, które syntetyzuje dane historyczne z naszego systemu z prognozami z Azure Machine Learning, aby stworzyć obiektywne źródło prawdy dla całej organizacji. Po wdrożeniu machine learning rozbieżność między naszą ogólną prognozą przychodów a wartościami rzeczywistymi zmniejsza się z 3% do 1,5%.

W firmach typu „runrate”, takich jak nasze małe i średnie biura, gdzie występuje większa ilość danych, rezultat ten może być jeszcze bardziej zauważalny. Zburzenie silosów zapewniło nowy poziom przejrzystości, który jest korzystny dla kultury całego podmiotu. Zespół finansowy nadal korzysta także i z tradycyjnych narzędzi prognostycznych, równoległe z machine learning, i w tym obszarze również zauważyliśmy znaczącą poprawę. Różnica między tradycyjną prognozą a rzeczywistością spadła do 2%.

Bezpieczeństwo danych

Bezpieczeństwo danych stanowić będzie jeden z kluczowych czynników, decydujących o wyborze usług chmurowych. Właśnie dlatego Microsoft dokonał znacznych inwestycji w infrastrukturę chmury, aby zapewnić ciągły monitoring, zwiększoną przejrzystość i cyfrową ochronę prywatności. Wraz z ogłoszeniem inwestycji Microsoft w lokalne Data Center, sektor bankowy oraz jego klienci mogą w chmurze analizować i przechowywać krytyczne dane, które dotychczas mogły być elementem tylko lokalnej infrastruktury.

Walka z oszustwami

Dzięki machine learning i rosnącej mocy obliczeniowej, sztuczna inteligencja stanowi coraz skuteczniejszy mechanizm przeciwdziałania wyłudzeniom. Banki korzystają z rozwiązań do wykrywania oszustw w obszarze płatności, wyłudzeń kredytowych, a także aktywności przestępczej na polu socjotechnicznym (phishing). Wykrywanie niespójności lub nieścisłości w danych dotyczących płatności, pożyczek i aplikacji następuje dzięki analizie

1 PWC, 2016 Source: PwC, Global Economic Crime Survey, 2016 <http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf>

2 <https://thefinancialbrand.com/65338/banking-ai-ui-artificial-intelligence-data/>

3 Celent, 2016 Source: CMS Top Emerging IT Trends in Banking Sector,

4 <https://www.mckinsey.com/industries/financial-services/our-insights/analytics-in-banking-time-to-realize-the-value>

predykcyjnej, prowadzonej w wielu kanałach bankowych. Analizując dane za pomocą wstępnie przeszkolonego algorytmu, można skutecznie oszacować transakcję pod kątem ryzyka wyłudzeń. Taki system może być rozbudowany o powiadamianie o wszelkich odchyleniach od normalnego wzorca, informując o różnych rodzajach podatności na oszustwa bankowe. Weryfikacja transakcji na dużą skalę dokonywana jest wówczas w ciągu kilku milisekund, co zmniejsza ryzyko wyłudzenia we współczesnej, omnikanałowej bankowości.

Zaufanie poprzez bezpieczeństwo

Jak pogodzić produktywność i zadowolenie klientów z utrzymaniem odpowiedniego poziomu bezpieczeństwa? Sukces oznacza zabezpieczenie tożsamości, aplikacji, danych, urządzeń i infrastruktury z największą liczbą usług finansowych – gotowym dostawcą chmury.

- **Szybkie wykrywanie:** zapewnienie swojemu zespołowi ds. bezpieczeństwa narzędzi potrzebnych do ochrony banku i pracowników przed coraz bardziej wyrafinowanymi cyberatakami – dzięki analizie w czasie rzeczywistym w celu szybszego wykrywania zagrożeń.
- **Natychmiastowa ochrona:** kontrola w czasie rzeczywistym jest prosta w użyciu, a co ważniejsze, zapewnia właściwą równowagę między wykrywaniem naruszeń a przetwarzaniem płat-

ności od klientów bez zbędnych opóźnień. Intuicyjne narzędzia do zarządzania alertami pomagają usprawnić operacje, a graficzne pulpity nawigacyjne pokazują poziomy ryzyka.

Innym podejściem do ochrony klientów i banku może być weryfikacja behawioralna. Digital Fingerprints tworzy modele uczenia maszynowego, wykorzystując dane pozyskane podczas interakcji człowieka z komputerem (Human-Computer Interaction; HCI).

Taką usługę, polegającą na analizie zachowania klienta podczas korzystania z serwisu transakcyjnego, wdrożył ING Bank Śląski. Zbierane i analizowane są m.in. informacje o tym, jak szybko i często użytkownik klika w poszczególne klawisze na klawiaturze, jak przewija ekran, jak szybko i często klika myszką komputerową oraz jak trzyma urządzenie. Ten zestaw cech pozwala zbudować unikalny, niezwykle trudny do podrobienia profil użytkownika. System używany przez ING Bank Śląski porównuje zachowania użytkownika po

”

Banki korzystają z rozwiązań do wykrywania oszustw w obszarze płatności, wyłudzeń kredytowych, a także aktywności przestępczej na polu socjotechnicznym (phishing). Wykrywanie nieśpójności w danych dotyczących płatności, pożyczek i aplikacji następuje dzięki analizie predykcyjnej, prowadzonej w wielu kanałach bankowych.



każdym logowaniu, dzięki czemu jest w stanie skutecznie wykryć aktywność oszukańczą. Analogiczne rozwiązanie wdrożył mBank, za co wspólnie z firmą HYPERLINK „https://fingerprints.digital/” Digital Fingerprints otrzymał wyróżnienie w rankingu Złoty Bankier 2019 w kategorii **Innowacja fin-tech**.

Budowa kompetencji

Przy usprawnianiu komunikacji wewnętrznej, zarządzania wiedzą i zaangażowaniu pracowników z pomocą przychodzi np. platforma Workai – intranet nowej generacji. Produkt, dostarczany przez Elastic Cloud Solutions, znalazł się wśród dziesięciu najlepszych tego typu rozwiązań na świecie i otrzymał prestiżową nagrodę „Best Intranet Design” od Nielsen Norman Group, za wyjątkowy i zorientowany na użytkownika design.

Workai pozwala na mierzenie oraz analitykę cyfrowych doświadczeń i interakcji pracowników z organizacją (Digital Employee Experience). Umożliwia to znacznie skuteczniejszy dobór działań do celów i potrzeb działów komunikacji wewnętrznej. Dzięki dostępnej w czasie rzeczywistym inteligentnej analityce, firmy mogą mierzyć trendy, wydźwięk wypowiedzi, ścieżki dotarcia, skuteczność kampanii wewnętrznych oraz ROI i ogólne zaangażowanie organizacji na wszystkich kanałach, w których komunikacja wewnętrzna jest prowadzona. Jej personalizacja możliwa jest dzięki sztucznej inteligencji. Na platformie Workai pracownicy mogą otrzymywać sugestie treści i kategorii do subskrybowania na podstawie nie tylko stanowiska, roli czy obowiązków w firmie, ale i interakcji z innymi treściami, ich oceną, zaangażowaniem, sentymentem i innymi czynnikami – dzięki wykorzystaniu inteligentnych algorytmów personalizacji.

Algorytmy takie uczą się z każdą interakcją użytkownika.

Aby umożliwić swobodny przepływ komunikacji w organizacji, platforma Workai umożliwia inteligentną moderację treści dodawanej przez użytkowników – artykułów, postów, komentarzy czy nawet formularzy. Dzięki temu treści mogą być automatycznie filtrowane lub flagowane zgodnie z unikalną polityką firmy. Do klientów z branży finansowej, używających tego narzędzia należą m.in. Deutsche Vermögensberatung AG, eurobank, Getin Noble Bank oraz PKO Bank Polski.

Korzystanie ze sztucznej inteligencji i cyfrowych umiejętności

– *Firmy, w których priorytetem są z jednej strony umiejętności pracowników, z drugiej zaś inwestycje w sztuczną inteligencję, czerpią z tej ostatniej największą wartość* – mówi **Diana Oleksiuk-Szczurowska**, odpowiadająca za budowę kompetencji w ramach Polskiej Doliny Cyfrowej. Zapewnienie pracownikom właściwej ścieżki rozwoju jest kluczem do uwolnienia wartości biznesowej dla

klientów, a firmy, które są bardziej zaawansowane w stosowaniu sztucznej inteligencji wygrywają ten wyścig.

Microsoft dokłada starań, aby każda osoba mogła zdobyć umiejętności i uzyskać dostęp do zasobów niezbędnych do odniesienia sukcesu w gospodarce cyfrowej. AI zmienia sposób prowadzenia biznesu we wszystkich branżach. Aby lepiej zrozumieć możliwości jej zastosowania, stworzyliśmy platformę AI Business School, bezpłatny internetowy kurs, przygotowany wraz z INSEAD. Cykl szkoleń ma na celu przygotowanie kadry zarządzającej do przeprowadzenia ich organizacji przez cyfrową transformację z zastosowania sztucznej inteligencji, dzięki licznym branżowym przykładom i wskazówkom. Dla osób szukających wiedzy bardziej technicznej proponujemy Microsoft Learn, gdzie oferujemy ścieżki z przewodnikiem i poszczególne moduły dla profesjonalistów, którzy chcą nauczyć się nowych umiejętności i pracować z narzędziami Microsoft.



Aplikacje zorientowane na obsługę klienta

W jaki sposób instytucje sektora finansowego mogą wykorzystać sztuczną inteligencję, by zbudować lojalność i poprawić swoje wyniki finansowe? Jednym z przykładów z polskiego rynku jest Edward, narzędzie do automatyzacji procesów sprzedażowych dla „mobilnych” pracowników. Przypomina on o służbowych obowiązkach (np. napisaniu e-maila czy wykonaniu telefonu), pozwala szybko sporządzić notatkę (pisemną lub głosową) po spotkaniu z klientami, wprowadzić raport ze spotkania do systemu CRM, zaplanować swoją pracę, sprawdzić informację o kliencie (np. przypomnieć szczegóły poprzedniego spotkania) czy zeskanować różne dokumenty i automatycznie wysłać je we wskazane miejsce. Edward potrafi wyłowić kluczowe słowa ze sporządzonych notatek i zasugerować dalsze działania w kontakcie z klientem.

Inspiracją dla stworzenia Edwarda była obserwacja pracy doradców klienta i pośredników finansowych, zwłaszcza tych pracujących „w terenie”. Pierwszą dużą instytucją finansową, która wprowadziła inteligentnego asystenta był ING Bank Śląski. Edward znalazł tam „zatrudnienie” w segmencie doradców korporacyjnych. Samo wdrożenie poprzedzone było testami na mniejszej grupie doradców, które wykazały zarówno potrzebę biznesową, jak i dojrzałość techniczną rozwiązania.

Poznanie swoich klientów

Systemy analityczne oparte na uczeniu maszynowym pomagają uzyskać 360-stopniowy widok klienta dzięki modelom, które przewidują i prezentują jego nawyki zakupowe i aspiracje finansowe. Wraz z szybkim rozwojem

technologii cyfrowych w bankowości konsumenci ustanawiają nowe wzorce i oczekiwania, dotyczące zindywidualizowanych usług. Migracja klientów, zwłaszcza tych z młodego pokolenia, do kanałów zdalnych wymusiła zmianę paradygmatu w samych bankach i odejście od filozofii zorientowanej na produkt w kierunku zindywidualizowanego, klientocentrycznego podejścia. Przykładem jest użycie silników rekomendacyjnych do stworzenia najlepszej oferty dzięki personalizacji, ukierunkowanemu marketingowi i segmentacji użytkowników. Aby należycie wykorzystać 360-stopniowy widok klienta, niezbędne staje się zastosowanie analizy predykcyjnej i rekomendacji w czasie rzeczywistym. Dzięki temu można znacząco poprawić lojalność użytkowników.

Wiodący grecki bank ujednotolica usługi omnichannel z Microsoft Azure Analytics⁵

Jedną z największych greckich instytucji finansowych, Piraeus Bank, wprowadziła Microsoft Azure jako sposób na zarządzanie kanałami omnichannel dla dwóch milionów klientów bankowości internetowej. Zakres usług analizy danych, w tym nowsza funkcjonalność Azure Databricks, łączy w sobie to, co najlepsze z platformy analitycznej Apache Spark i platformy Azure usług w chmurze, zapewniając menedżerom wgląd w czasie rzeczywistym.

Microsoft doradził bankowi, aby skorzystał z możliwości najnowszej generacji dostarczanych przez Microsoft Azure usług analizy danych i zarządzania informacjami; pomogłoby to firmie

⁵ <https://customers.microsoft.com/en-us/story/piraeus-bank-financial-services-azure-greece>

” Na platformie Workai pracownicy mogą otrzymywać sugestie treści i kategorii do subskrybowania na podstawie nie tylko stanowiska, roli czy obowiązków w firmie, ale i interakcji z innymi treściami, ich oceną, zaangażowaniem, sentymentem i innymi czynnikami – dzięki wykorzystaniu inteligentnych algorytmów personalizujących.

uzyskać 360-stopniowy widok swoich klientów, a jednocześnie zapewnić nowe, potężne sposoby budowania nowych KPI. W konsekwencji czas na rozwiązywanie incydentów i reakcję na problemy klientów skrócił się niemal o połowę, a korzystanie z usług chmurowych Microsoft **zmniejszyło koszty informatyczne zarządzania informacjami o klientach o prawie 60%**. W Piraeus Banku usługa Azure Application Insights znacząco wspomaga śledzenie zdarzeń, zapewnia także możliwość porównywania i korelowania informacji z poprzednimi danymi i datami. Ponadto system oferuje teraz pełną ścieżkę audytu wszelkich informacji, a także anonimowe dane klientów w razie potrzeby.

Lowell i inteligentny BOT do automatyzacji call center

W tym kontekście warto też przypomnieć doświadczenia Banku Lowell. Ta jedna z największych firm świadczących usługi zarządzania kredy-

tami w Europie chciała usprawnić proces przyznawania finansowania. Skomplikowane procedury windykacyjne w Norwegii sprawiły, że wysoko wykwalifikowani doradcy kredytowi firmy byli zbyt zajęci pytaniami konsumentami, co utrudniało terminowe płatności. W konsekwencji instytucja ta zwróciła się o pomoc w stworzeniu zaawansowanego rozwiązania automatyzacji call center. Lowell we współpracy z firmą Crayon zbudował niestandardowy, inteligentny chatbot przy użyciu Microsoft Bot Framework i Microsoft Azure Bot Service. Do jego przeszkolenia wykorzystano wcześniej zbudowane modele uczenia maszynowego w Azure Cognitive Services, aby mógł on w naturalny sposób komunikować się z konsumentami, odpowiadając tak na skomplikowane, jak i rutynowe zapytania. Wprowadzony chatbot obsługuje 40% wszystkich zapytań, ułatwiając agentom serwisowym dostarczanie klientom większej wartości. To skuteczny sposób na uzyskanie porady, ustalenie planów płatności, znalezienie odpowiedzi na proste pytania i zarządzanie własnym kredytem. Jego wprowadzenie spowodowało 20-procentowy przyrost *first-call resolution*, z 50 do 70%. Tak duży odsetek zapytań jest obsługiwany na poziomie chatbota, bez potrzeby angażowania konsultantów. Jednak gdy problem wymaga wsparcia fachowca, zautomatyzowane centrum obsługi telefonicznej zapewnia płynne przekazanie od bota do agenta. – *Dzięki Azure przenosimy rozmowy z bota na agenta usługowego bez utraty rejestru rozmów, dzięki czemu konsument odbiera całą komunikację z jednego interfejsu. Zastosowaliśmy Azure Cognitive Services, aby stworzyć bardziej inteligentnego, intuicyjnego i użytecznego bota* – mówi **Carl Udvang**, Product Manager w Lowell.

Rys. 1. Sześć zasad etycznego zastosowania sztucznej inteligencji



Wiodący rumuński bank zwraca się do Microsoft AI w celu lepszego obsługi klienta

Banca Transilvania należy do instytucji regularnie wdrażających nowatorskie rozwiązania. Owo dążenie do innowacji zaowocowało nową ofertą dla klientów detalicznych oraz małych i średnich firm w postaci zautomatyzowanej obsługi klienta z użyciem chatbotów opartych na Microsoft Azure, Raul i Livia.

Bank wykorzystuje technologię sztucznej inteligencji (AI) w postaci dwóch nowych chatbotów zbudowanych przy użyciu usługi Azure Bot Service na platformie Microsoft Azure. Jeden z nich dedykowany jest segmentowi detalicznemu, a drugi małym i średnim firmom. To posunięcie znacząco usprawniło obsługę klienta, jednocześnie obniżając koszty bankowego contact center. Obserwowany wcześniej, dziesięcioprocentowy wzrost liczby połączeń w skali miesięcznej został zredukowany dwukrotnie, co przyniosło 50% oszczędności. Fascynującym rezultatem jest nieoczekiwany wgląd w zachowania klientów, takie jak nowe perspektywy dotyczące problemów klientów z bankiem – co pomogło rozwiązać te problemy. Jednocześnie liczba użytkowników i stawki wiadomości rosły codziennie, co jest wyraźnym znakiem, że klienci to zaakceptowali.

Bot, zaprojektowany w celu zaspokojenia specyficznych potrzeb rumuńskich użytkowników MŚP, odniósł duży sukces. Plany na przyszłość obejmują dodanie większej liczby funkcji, z którymi boby mogą pomóc klientom, dostosowanych do większej eksploracji usług AI na platformie Azure.

Etyczna sztuczna inteligencja

We współczesnej gospodarce, która w coraz większym stopniu bazuje na danych, korzyści zapewniane przez AI mają znaczenie kluczowe, sprawiając, że coraz szersza grupa dostawców usług stosuje tego typu rozwiązania. Niemniej jednak technologie AI powstają oraz ewoluują szybko i stanowią wyjątkowe wyzwanie dla instytucji finansowych i ich organów regulacyjnych. Aby uniknąć niezamierzonych konsekwencji, ograniczyć ryzyko i zminimalizować obawy, organizacje muszą w sposób odpowiedzialny wykorzystywać dane i sztuczną inteligencję.

W Microsoft, jesteśmy świadomi zagrożeń i nieustannie rozwijamy technologie oraz praktyki zarządzania, aby je zminimalizować. Mamy nadzieję, że sześć zasad przewodnich wzmocni bezpieczne i odpowiedzialne korzystanie ze sztucznej inteligencji, co ułatwi przekształcenie organizacji na lepsze.

Czy rozwijasz swoje umiejętności, aby odnieść sukces dzięki AI?

Sztuczna inteligencja przynosi satysfakcję z wykonywanej pracy



Pracownicy chcą się uczyć i doskonalić swoje umiejętności



Więcej umiejętności = większe korzyści



Zdaniem profesjonalistów AI:

46% uważa, że ich praca ma większe znaczenie **39%** ma poczucie, że ich praca jest przyjemniejsza

9 na 10 pracowników chce zdobywać nowe umiejętności związane ze sztuczną inteligencją

Większość pracowników uznaje, że wyższy poziom umiejętności związanych z AI pozytywnie wpływa na karierę zawodową

Czy w pełni wykorzystujesz sztuczną inteligencję (AI), aby zapewnić swojej firmie stabilizację, rozwój i sukces w przyszłości?

Pracownicy firm wykorzystujących AI posiadają więcej umiejętności niezbędnych do odniesienia sukcesu



7 na 10 pracowników czuje się odpowiednio przygotowanych do pracy z AI

Więcej umiejętności z zakresu AI = więcej wartości dla biznesu



Rozwój pracowników jest priorytetem liderów AI



Firmy, które są najbardziej dojrzałe pod względem adopcji AI, aktywnie budują umiejętności zespołu lub mają takie plany

Czy wspierasz swoich pracowników i tworzysz wartość biznesową z AI?

Firmy, które są najbardziej dojrzałe pod względem adopcji AI aktywnie budują umiejętności zespołu lub mają takie plany



63% liderów AI aktywnie rozwija umiejętności swoich pracowników, podczas gdy **34%** ma takie plany

Pobudzenie kreatywności pracowników = większa efektywność i innowacyjność



89% profesjonalistów AI ma poczucie, że technologia w wysokim stopniu wpływa na ich efektywność
62% profesjonalistów AI zauważa, że AI pomaga im rozwijać nowe produkty i usługi

JAK SZTUCZNA INTELIGENCJA zmieniła branżę finansową

Postęp technologiczny przyczynił się do przyspieszenia integracji sztucznej inteligencji i modeli nauczania maszynowego z rosnącą liczbą procesów w bankowości. W dzisiejszych czasach instytucje finansowe niewykorzystujące potencjału AI ryzykują pozostanie w tyle za konkurencją, która podejmuje strategiczne decyzje, wykorzystując systemy analityczne. Inteligentne algorytmy uczą się na podstawie przykładów pochodzących z danych historycznych, a następnie są wykorzystywane do odkrywania wzorców trudnych do identyfikacji przez człowieka.

W wykorzystanie uczenia maszynowego w sektorze finansowym nie jest czymś nowym. W praktyce technologia ta jest stosowana przez banki i instytucje świadczące usługi finansowe od dziesięcioleci. Obejmuje ona podstawowe metody i techniki statystyczne, takie jak regresja liniowa i logistyczna czy modelowanie oparte na regułach. Takie tradycyjne metody są względnie

proste, łatwe do zrozumienia, wytłumaczenia i interpretacji. Jednak ceną ich stosowania jest zazwyczaj niższa skuteczność w porównaniu z możliwościami, jakie dają bardziej zaawansowane techniki uczenia maszynowego.

Wraz ze wzrostem mocy obliczeniowej komputerów w ostatnich latach metody analityczne, takie jak sieci neuronowe, algorytmy oparte na drzewach decyzyjnych i inne, stają się coraz bardziej popularne. Metody te ce-

chują się zazwyczaj wyższą skutecznością w porównaniu z klasycznymi metodami statystycznymi, ale sposób ich działania jest bardziej złożony, a wpływ poszczególnych zmiennych wejściowych na końcowy wynik trudniejszy w interpretacji.

Wyzwania, którym branża musi stawić czoła

Biorąc pod uwagę rosnącą zależność codziennych procesów biznesowych i decyzyjnych od modeli analitycznych, ryzyko wiążące się z ich zastosowaniem musi być odpowiednio kontrolowane. Modele AI i uczenia maszynowego wymagają stałego monitorowania, gdyż błędy w ich opracowywaniu, wdrażaniu czy zastosowaniu mogą doprowadzić do strat finansowych lub reputacyjnych.

Ciągłe monitorowanie i okresowy przegląd wydajności modelu analitycznego to krytyczne elementy dobrego zarządzania jego ryzykiem. Powinny one obejmować informacje gromadzone od chwili wdrożenia danego modelu, co pozwala walidacji na potwierdzenie zdolności modelu do realizacji celów, dla których został stworzony. Skuteczne zarządzanie modelami na większą skalę to złożony



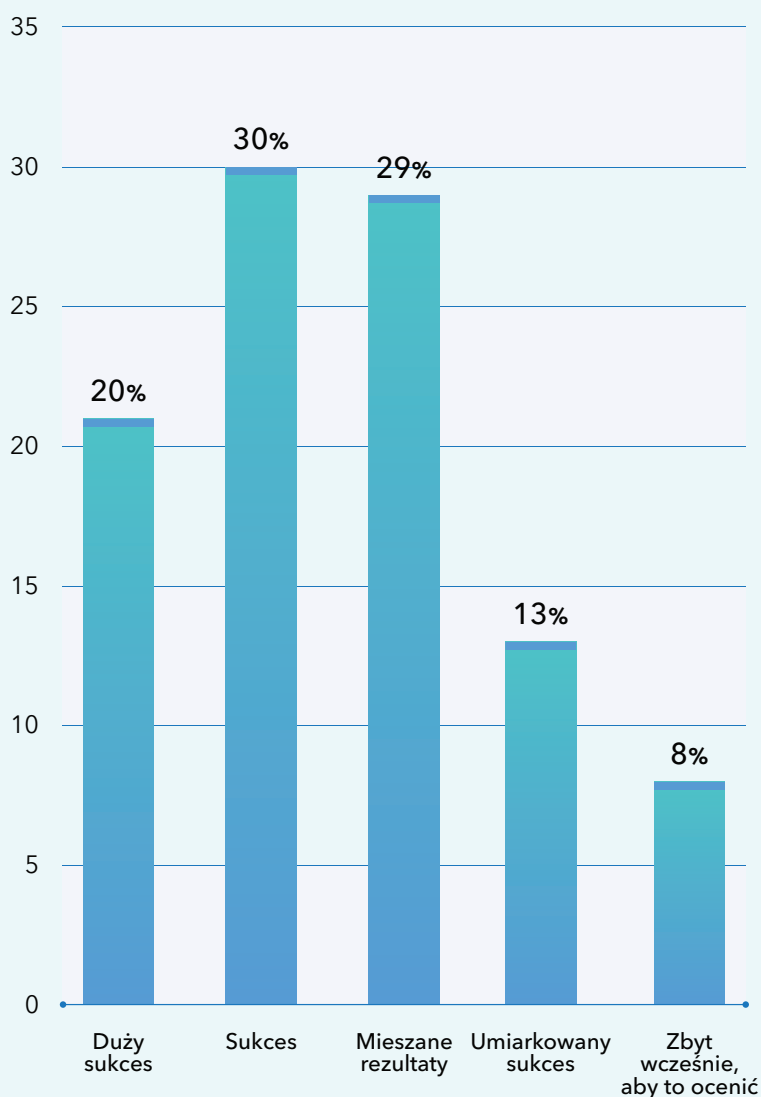
proces, ponieważ w jednej organizacji możemy mieć do czynienia z setkami czy nawet tysiącami modeli.

Wraz ze wzrostem złożoności modeli analitycznych i coraz większą liczbą scenariuszy ich zastosowania obserwujemy wzrost zainteresowania organów regulacyjnych ryzykiem towarzyszącym korzystaniu z tychże modeli. Początek dał temu światowy kryzys finansowy, który uświadomił całej branży, że przynajmniej część z modeli wówczas stosowanych nie odpowiadała swojemu przeznaczeniu, na co nałożył się brak odpowiednich regulacji prawnych. W odpowiedzi na te wydarzenia wzmożono nadzór organów regulacyjnych nad budową, zatwierdzaniem oraz utrzymywaniem modeli.

Produkcyjne wdrożenie modelu w bankowości to złożony czasochłonny proces, który wymaga koordynacji pracy wielu zespołów w obrębie danej instytucji. Mimo że obecnie organizacje są w stanie tworzyć ukierunkowane modele, które przekładają się na istotny wzrost dochodów to jednocześnie, według SAS EYAP Global Survey 2019 i badania Gartnera z 2018 r., mniej niż 50% wytworzonych modeli nigdy nie zostaje zoperacjonalizowanych. Wdrożenie zdecydowanej większości wersji zajmuje ponad trzy miesiące. Większość organizacji nie ma powtarzalnego procesu operacjonalizacji analiz, który szybko przenosi model do produkcji i monitoruje jego wydajność w czasie. Według Gartnera, jest to jeden z głównych powodów, dla których organizacje nie uzyskują wartości biznesowej z zastosowania zaawansowanej analityki.

W odpowiedzi na te wyzwania pojawiają się rozwiązania tworzące ModelOps, czyli holistyczne podejście

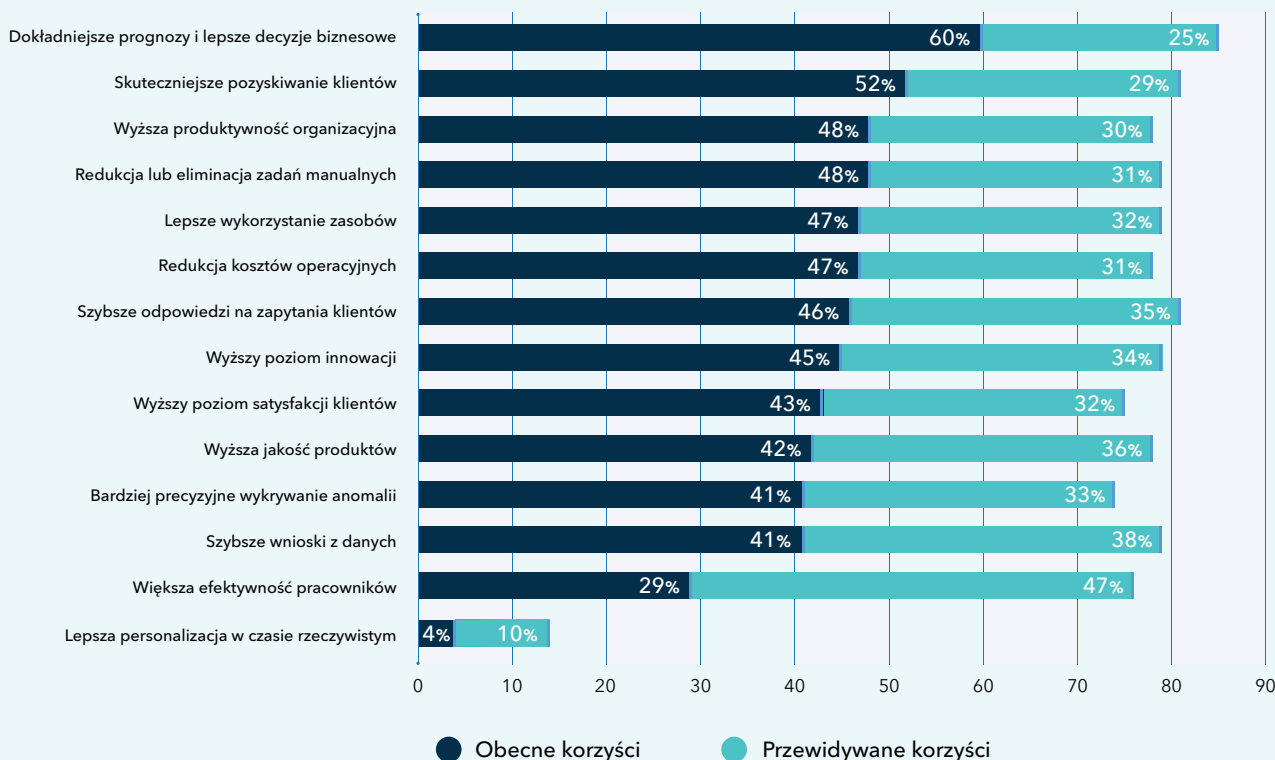
Rys. 1. Oceń wpływ wdrożenia technologii wykorzystujących sztuczną inteligencję w Twojej organizacji



do płynnego zarządzania pełnym cyklem życia modeli analitycznych, dzięki czemu są one wdrażane szybko i zapewniają oczekiwaną wartość biznesową. ModelOps opiera się na podejściu DevOps opracowywanym przez społeczność programistów. Ale tam, gdzie DevOps koncentruje się na rozwoju aplikacji, ModelOps koncentruje się na przenoszeniu modeli z fazy eksperymentów poprzez fazy walidacji, testowania i wdrażania tak szybko, jak to możliwe, przy jednoczesnym

zapewnieniu wysokiej jakości wyników. Koncentruje się również na bieżącym monitorowaniu i ponownym trenowaniu modeli, jeżeli ich skuteczność spada poniżej akceptowalnego poziomu. Poprzez zapewnienie krótkiego czasu wdrożenia organizacje nie muszą już martwić się o to, gdy ich model ze względu na szybko zmieniające się zachowania klientów ulega degradacji, ponieważ ponowne uczenie modelu nie musi już wiązać się ze żmudnym, wielomiesięcznym procesem.

Rys. 2. Jakie korzyści dostrzegasz lub spodziewasz się dostrzec w wyniku zastosowania sztucznej inteligencji w Twojej organizacji?



Cykl życia modelu analitycznego możemy podzielić na osiem etapów:

1. Przygotowanie danych.
2. Trenowanie modelu.
3. Walidacja modelu – selekcja modelu.
4. Testowanie i przygotowanie do wdrożenia.
5. Zatwierdzenie i wdrożenie.
6. Wykorzystanie.
7. Monitoring skuteczności modelu.
8. Ocena wpływu wyników modeli na ryzyko i sprzedaż.

Mimo że sztuczna inteligencja jest mocno osadzona w branży finan-

sowej, zdaniem 52% respondentów badania „*Artificial Intelligence in Banking and Risk Management*” przeszkodą stojącą na drodze do jeszcze powszechniejszego wykorzystania tej technologii jest brak odpowiednich umiejętności. Ankietowani wskazali kolejno: małą dostępność i niską jakość danych (59% odpowiedzi), brak zrozumienia, czym jest AI wśród kluczowych interesariuszy (54% odpowiedzi) oraz problemy z interpretacją modeli analitycznych wykorzystywanych w projektach sztucznej inteligencji (47% odpowiedzi). Dwie ostatnie kwestie są ze sobą powiązane, ponieważ brak możliwości interpretacji, a co za tym idzie czerpania korzyści z wyników analiz sprawia, że osoby z departamentów biznesowych będące odbiorcami modeli nie mają do nich zaufania.

Proces zmiany tego stanu rzeczy nazywamy demokratyzacją analityki, co oznacza szerszy i łatwiejszy dostęp do narzędzi analitycznych wewnątrz organizacji. Aby to było możliwe, interfejs systemu analitycznego powinien być intuicyjny i prosty w obsłudze, dzięki czemu również osoby, które nie są wyspecjalizowanymi data scientist, są w stanie z niego korzystać. Niezwykle istotny jest rozwój obszaru xAI (explainable AI) – wytłumaczalnej sztucznej inteligencji, w ramach której rozwijane i implementowane są metody służące do interpretacji złożonych modeli uczenia maszynowego.

Niezwykle ważnym aspektem, nad którym powinna skoncentrować się branża finansowa, jest etyka wykorzystania sztucznej inteligencji. Badanie SAS, Accenture Applied Intelligence, Intela i Forbes Insights wykazało ograniczone

zaufanie do wykorzystania technologii AI w kontaktach z klientami w finansach i bankowości. Jedyny wyjątek stanowił monitoring pod kątem oszustw i innych potencjalnych zagrożeń. Wykorzystanie sztucznej inteligencji do automatyzacji tych procesów akceptuje 59% respondentów. Badani byli najmniej przychylni wdrożeniom AI na potrzeby udzielania rekomendacji dotyczących zarządzania kartami kredytowymi. Ankietowani wyrazili też zdecydowaną niechęć do udostępniania swojej historii kredytowej. Te dane pokazują, że banki powinny niezwykle ostrożnie wdrażać systemy wykorzystujące AI, dbając o odpowiednie procedury i świadomość zespołu.

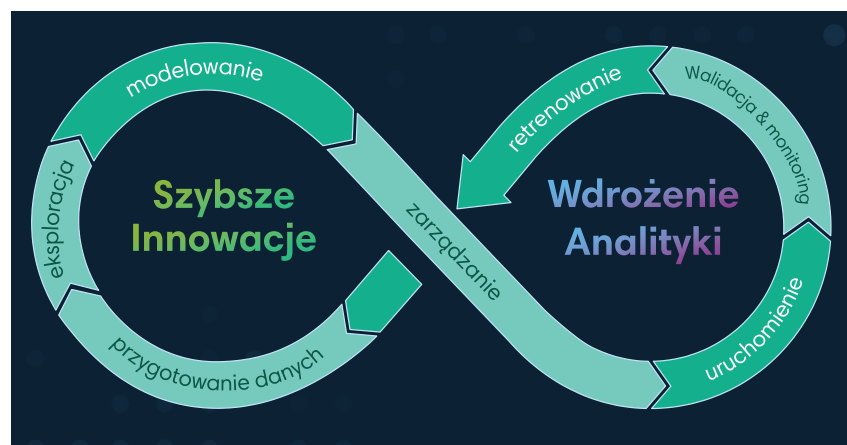
Wysokie oczekiwania wobec AI

Firmy z branży finansowej doskonale rozumieją korzyści wynikające z wykorzystania sztucznej inteligencji. Aż 81% respondentów badania „*Artificial Intelligence in Banking and Risk Management*”, przeprowadzonego przez SAS oraz stowarzyszenie GARP (Global Association of Risk Professionals) wśród organizacji z tego sektora, dostrzega pozytywne efekty implementacji AI.

Dla decydentów z branży finansowej ważnym argumentem przemawiającym za wdrożeniem sztucznej inteligencji jest oszczędność czasu i pieniędzy. Według firmy Bain & Company oszczędności wynikające z wykorzystania AI wyniosą do 2030 r. 1,1 bln USD, co przekłada się na 22-procentową redukcję kosztów operacyjnych.

Oczekiwania względem wykorzystania sztucznej inteligencji są bardzo wysokie. Większość uczestników badania SAS i GARP wierzy, że poprawi ona ich pracę i uczyni bardziej efektywną. Najczęściej wskazywali na wzrost

Rys. 3. Cykl analityczny



produktywności (96% odpowiedzi), szybsze wyniki analizy danych (95% odpowiedzi) oraz większe wsparcie procesów decyzyjnych (95% wskazań). Należy jednak pamiętać, że sukces projektów z zakresu sztucznej inteligencji zależy od bardzo wielu czynników i na drodze do niego trzeba stawić czoła licznym wyzwaniom.

Czym są inteligentne banki?

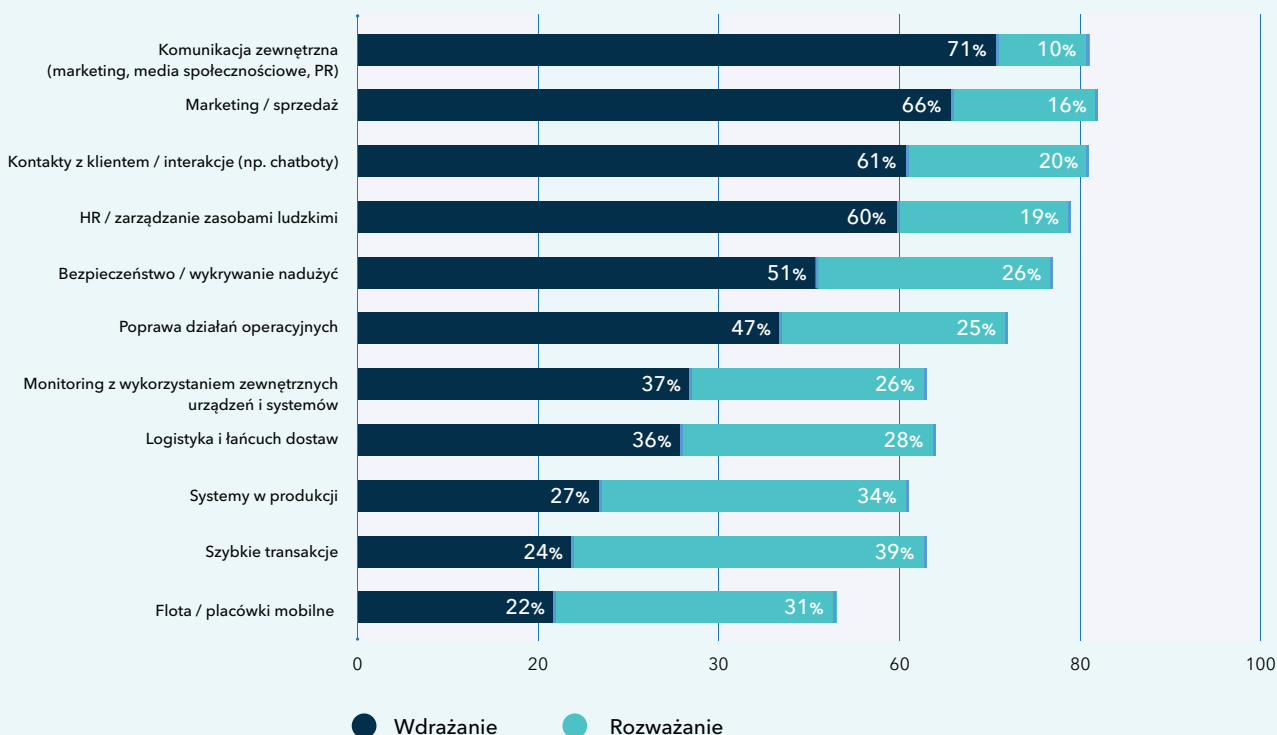
Sztuczna inteligencja ma w branży finansowej wiele zastosowań zarówno w obszarach customer intelligence, nadużyć, compliance, jak i procesów wewnętrznych.

Jak AI pomaga obsługiwać klientów

Klienci mogą mieć styczność z AI już na etapie otwierania konta w banku. Cyfrowy onboarding to obecnie całkowicie zautomatyzowany proces, który stał się standardem w branży finansowej. Każda osoba dokonująca operacji finansowych jest identyfikowana w ramach procesu KYC (ang. Know Your Customer), co pozwala ocenić jej wiarygodność i zapewnić bezpieczeństwo innym uczestnikom transakcji. Tu zyskują na popularności metody sztucz-

nej inteligencji oraz całe spektrum technik analitycznych, takich jak przetwarzanie języka naturalnego służące do znajdowania niespójności w danych czy analiza obrazów wykorzystywana do oceny wiarygodności klienta przez porównanie zdjęcia z dokumentu tożsamości z wizerunkiem z kamery. Działy compliance zajmujące się między innymi przeciwdziałaniem praniu brudnych pieniędzy coraz częściej są zainteresowane zastosowaniem metod uczenia maszynowego do analizy tzw. adverse media – negatywnych informacji do oceny wiarygodności kontrahentów i tym samym ryzyka transakcji.

Również bieżąca komunikacja z klientami może odbywać się z wykorzystaniem sztucznej inteligencji. Szczególnym zainteresowaniem wśród projektów z jej obszaru cieszą się chatboty pozwalające odciążać konsultantów i obniżyć koszty obsługi klienta. Komunikują się z człowiekiem, wykorzystując metody przetwarzania języka naturalnego. Rozwiązania z tego zakresu stanowią podobszar sztucznej inteligencji, za ich sprawą maszyny są w stanie czytać, analizować oraz interpretować i wygenerować język ludzki. Pozwala im to zrozumieć zarówno jego strukturę, jak i znaczenie poszczególnych zdań,

Rys. 3. W jakich obszarach stosujesz sztuczną inteligencję?

a także sformułować odpowiedź, która będzie korespondowała z postawionym pytaniem. Im więcej interakcji chatbota z użytkownikiem, tym więcej maszyna będzie rozumiała, a sama konwersacja będzie bardziej płynna i naturalna. Odpowiedzi na pytania klienta są formułowane na podstawie analizy podobnych zapytań z przeszłości. Również analiza satysfakcji klienta odbywa się z wykorzystaniem sztucznej inteligencji. Stosowane w tym celu głębokie sieci neuronowe analizują jego stosunek emocjonalny w czasie rozmów z pracownikiem call center.

Jak AI pozwala dotrzeć do klientów

Klienci chcą, aby usługi finansowe były dostosowane do ich trybu życia i potrzeb. Niezwykle popularna jest bankowość online, często na urządzeniach mobilnych i w podróży. Klienci chcą

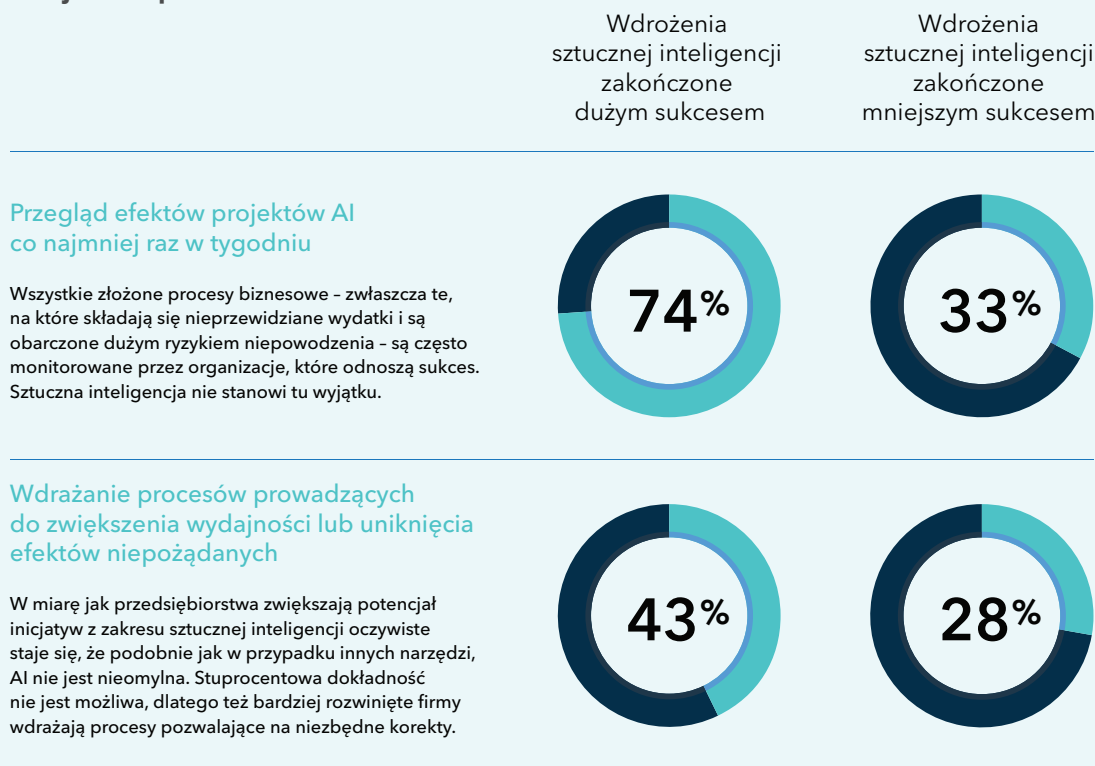
móc sprawdzić saldo przed zakupem, czy łatwo wziąć pożyczkę bez zbędnych formalności. Wszystkie te operacje muszą być możliwe w trybie on-demand i w czasie rzeczywistym. Jednocześnie użytkownicy nie chcą być zalewani ofertami produktów finansowych, których nie potrzebują. Silniki rekomendacyjne umożliwiają, opierając się na danych behawioralnych klientów, oferowanie usług finansowych, takich jak pożyczka gotówkowa czy karta kredytowa w odpowiednim momencie, np. gdy klient odwiedza sklep internetowy i rozważa zakup nowej rzeczy, gdy zabraknie mu środków na koncie lub gdy rozpoczyna działalność gospodarczą.

Jak AI pomaga zwalczać nadużycia

Jak wynika z badania przeprowadzonego przez Association of Certified Fraud Examiners (ACFE) i SAS wyko-

rzystanie sztucznej inteligencji w walce z nadużyciami wzrosło trzykrotnie do 2021 r. Największą korzyścią płynącą z zastosowania metod zaawansowanej analityki i sztucznej inteligencji jest szybsza i bardziej precyzyjna identyfikacja podejrzanych przypadków oraz znaczna redukcja poziomu fałszywych alarmów, a ostatnie ma bezpośrednie przełożenie na sprzedaż i satysfakcję klientów. W przypadku oceny ryzyka zawsze balansujemy między minimalizacją strat finansowych a niewykorzystanym potencjałem sprzedażowym i pozytywnym doświadczeniem klienta, dlatego skuteczność modeli tworzonych w tym zakresie wymaga szczególnej precyzji i kontroli. W zależności od tego, czy mówimy o identyfikacji klientów ryzykownych (customer due diligence), monitorowaniu transakcji pod kątem przeciwdziałania praniu brudnych pieniędzy, czy wykrywaniu nadużyć na wnioskach kredytowych

Rys. 4. Dojrzałość procesu



lub transakcjach w bankowości internetowej oraz mobilnej, zastosowanie mogą mieć różne techniki analityczne – od modeli predykcyjnych wykorzystujących techniki uczenia maszynowego, poprzez modele wykrywania anomalii, analitykę sieci powiązań, aż do analityki tekstu i przetwarzania języka naturalnego (NLP).

Jak AI optymalizuje pracę banków

Sztuczna inteligencja znacznie usprawnia procesy biznesowe wewnątrz instytucji finansowych. Dzięki algorytmom przetwarzania języka naturalnego możliwa jest klasyfikacja korespondencji i dokumentów czy ekstrakcja informacji występujących w kontraktach w określonym kontekście. Inny przykład wykorzystania AI stanowi planowanie zapotrzebowania na pieniądze w bankomatach, w określonych porach dnia, oparte na

analizie zachowań klientów. Również lokalizację samych bankomatów można zaplanować przy wsparciu AI, dzięki czemu użytkownicy będą mogli wygodnie z nich skorzystać.

Przyszłość AI jest w chmurze

Jeszcze kilka lat temu, ze względów bezpieczeństwa, banki umieszczały w środowisku cloud computing jedynie niewielką liczbę niekrytycznych aplikacji. Sposób wykorzystywania systemów analitycznych oraz sztucznej inteligencji uległ jednak diametralnej zmianie. Banki dysponują ogromną ilością informacji o klientach, a starsze systemy uniemożliwiają im szybkie uzyskanie wglądu w te dane, zanim staną się one nieaktualne. Dlatego potrzebują skalowalnych środowisk, które mogą rozbudowywać wraz ze wzrostem potrzeb. Przejście do chmury zapewnia szybkość i elastyczność, a także po-

zwala obniżyć koszty poprzez korzystanie z mocy obliczeniowej na żądanie w zależności od bieżących potrzeb bez utrzymywania kosztownej infrastruktury, ale dla instytucji finansowych wiąże się również z wyzwaniami dotyczącymi bezpieczeństwa i zgodności z regulacjami. To sprawia, że wiele organizacji z tego sektora stosuje chmurę hybrydową, która zapewnia zalety chmury publicznej, uwzględniając jednocześnie specyficzne potrzeby firmy. Przekłada się to na lepsze zaspokojenie oczekiwań klientów, którzy oczekują łatwo dostępnych usług finansowych, które odpowiadają ich potrzebom.

Źródła:

Artificial Intelligence in Banking and Risk Management

Tomorrow's world How will AI transform banking

Anti-Fraud Technology Benchmarking Report



DID YOU KNOW?

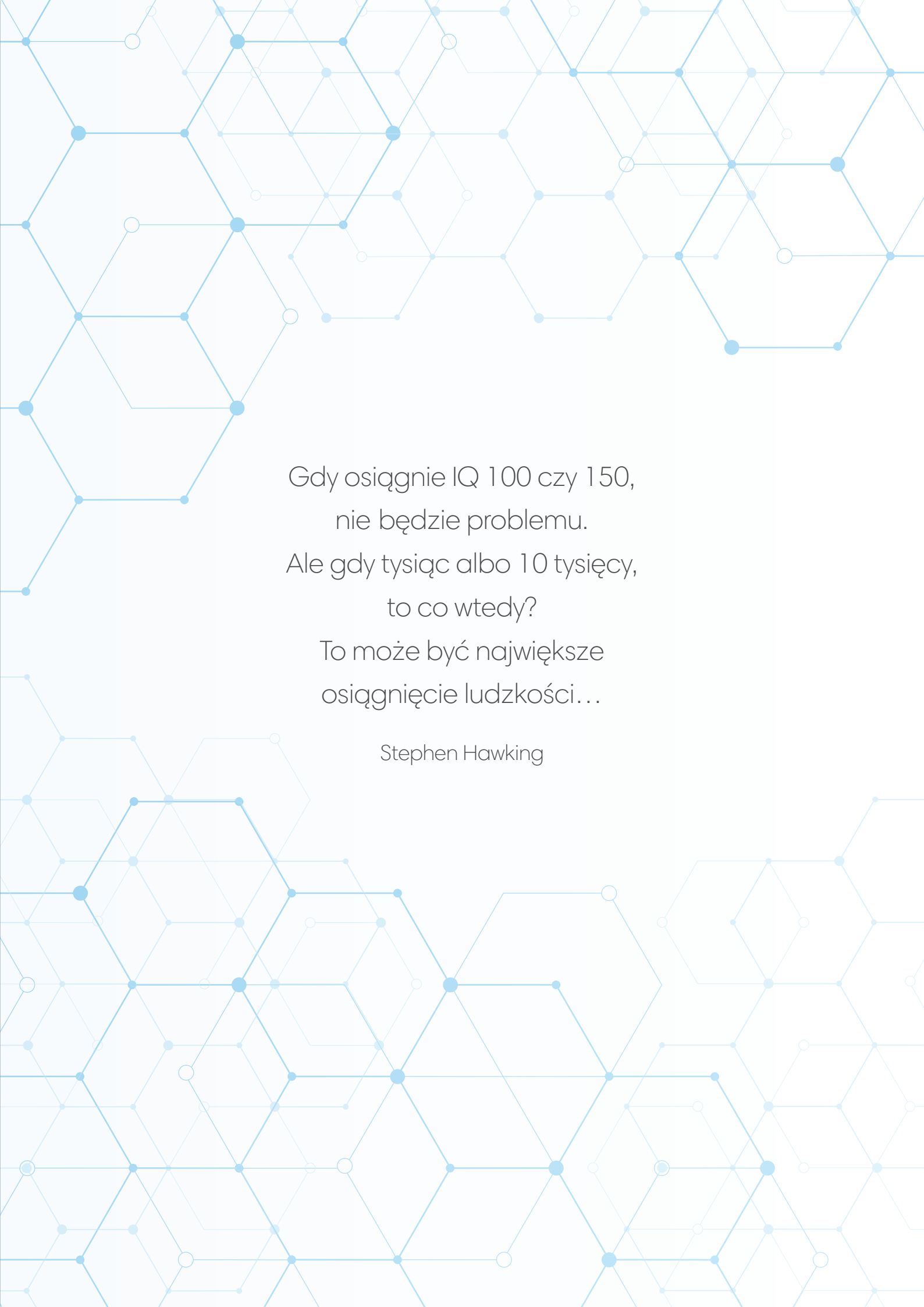
SAS[®] ANTI-MONEY LAUNDERING IS USED BY HUNDREDS OF GLOBAL ORGANIZATIONS.

SAS helps global organizations with enhanced anti-money laundering that uses artificial intelligence and machine learning, allowing them to automate manual tasks and reduce false positives by 50%-70%. All without needing an army of data scientists.

sas.com/aml



SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. © 2020 SAS Institute Inc. All rights reserved.



Gdy osiągnie IQ 100 czy 150,
nie będzie problemu.

Ale gdy tysiąc albo 10 tysięcy,
to co wtedy?

To może być największe
osiągnięcie ludzkości...

Stephen Hawking

