



Ako rozbehnúť pilotný projekt s umelou inteligenciou pre výrobný podnik?

Ťažko by sme hľadali odborné podujatie či podnik, kde by sa v nejakej forme nehovorilo o umelej inteligencii. Mnohí v nej vidia záchranu ľudstva, iní naopak jeho prekliatie. A ako to už väčšinou býva, pravda je niekde uprostred. Schopnosť UI spracovať, analyzovať a vyhodnotiť obrovské množstvá údajov, upriamiť pozornosť človeka na ťažko zachytiteľné súvislosti či upozorniť na problémy skôr, ako sa zmenia na katastrofu. To sú skvelé možnosti, ktoré už teraz UI ponúka a ktoré môžu priniesť pre priemyselné podniky reálne zlepšenia. Ako teda začať využívať UI v produktívnej prevádzke? Odpovede sme hľadali v exkluzívnom interview so Svetlanou Margetovou, špecialistkou na zavádzanie umelej inteligencie vo výrobných podnikoch zo spoločnosti Pulsar Solutions, s. r. o.

Ak by ste zhrnuli svoje doterajšie skúsenosti s možnosťami a prínosmi UI, odporučili by ste zaoberať sa touto témou aj priemyselným podnikom? Aký by mal byť taký najsilnejší argument, aby vedenie podniku uvoľnilo finančné a ľudské kapacity na realizáciu projektov využívajúcich UI v ich podniku?

Jednoznačne áno. Prínosy zavedenia UI sú v priemyselných podnikoch reálne a potenciál je veľký. Firmy, ktoré pred rokmi začínali s digitalizáciou a digitálnymi dvojčatami, majú dnes zozbierané obrovské množstvo dát a práve tu UI dokáže priniesť konkrétnu hodnotu. Najsilnejší argument závisí od use case, ale takmer vždy je tu jeden spoločný menovateľ. Prvým benefitom, ešte pred samotným nasadením UI, je príprava dát. Podnik si pri nej zjednotí dátové sety, odhalí slabé miesta vo svojich procesoch a začne

s nimi systematicky pracovať. Firma teda získava hodnotu už v momente, keď sa na projekt len pripravuje.

Následne prichádza úspora času. UI dokáže prevziať ťarchu monotónnych a opakujúcich sa činností, čím sa uvoľní kapacita ľudí na kreatívnu prácu a inovácie. V praxi to vidíme napríklad pri automatickom vyhľadávaní v technickej dokumentácii a manuáloch, kde technik namiesto hodín listovania dostane odpoveď v sekundách, alebo pri kontrole kvality, kde UI zachytí odchýlky, ktoré ľudské oko v rýchlosti prehliadne. A napokon to najpodstatnejšie z dlhodobého hľadiska, vo firme vzniká nový tím ľudí, ktorí pracujú s UI, automatizujú procesy a stávajú sa motorom inovácií v celom podniku.

Začiatky vo všetkom novom bývajú ťažké a rozpačité. Pozrime sa teda na úvod, ktoré konkrétne procesy v priemyselnom podniku sú najvhodnejšie na nasadenie umelej inteligencie a aké prínosy možno po nasadení UI, napr. pri kontrole kvality, prediktívnej údržbe, riadení spotreby energií, znižovaní nákladov a pod., očakávať?

Naozaj to závisí od podniku, ale najčastejšie ide o oblasť riadenia kvality, automatizáciu reportov a odchýlok, ďalej o digitalizáciu údržby a spracovanie dát zo strojov a snímačov. Sú to procesy, kde existuje veľa dát a zároveň veľa opakujúcej sa ľudskej práce, takže návratnosť je tam najrýchlejšie viditeľná.

Pokiaľ ide o prínosy, na prvom mieste je úspora času a posun k dátovo riadenému rozhodovaniu. UI dokáže nájsť súvislosti, ktoré by sme bežne neodhalili, napríklad opakujúci sa vzor v objednávkach, v nekvalite alebo v reklamáciách. Práve takéto skryté vzory bývajú kľúčom k znižovaniu nákladov. Druhým výrazným prínosom je zjednodušenie rozhrania pre operátorov. Hlasoví asistenti, predvypíňané informácie a inteligentné navrhovanie hodnôt nielen uľahčujú prácu, ale zároveň normalizujú dátové sady, ktoré vo fabrike zadávajú ľudia. Tým sa postupne zvyšuje kvalita dát a celý systém sa stáva spoľahlivejším.

Musí podnik, ktorý sa rozhodne implementovať UI vo svojich procesoch, urobiť „inventúru“ svojich technologických a IT systémov? Inými slovami aké technologické požiadavky musí podnik splniť pred implementáciou UI riešení a aké HW a SW nástroje bude podnik pri nasadení UI vo svojej prevádzke potrebovať?

Áno, určite musí, ale rozsah tej „inventúry“ závisí od use case. Niekedy stačí zvalidovať dokumentáciu k strojom, inokedy ide o milióny dát zo senzorov, niekedy je kľúčová otázka integrácií, teda či sa systémy vôbec dajú prepojiť. Práve pri tomto kroku sa veľmi často odhalia duplicity. Rôzne systémy vo firme totiž zbierajú tie isté dáta, len v inom formáte, a podnik o tom často ani nevie. Toto zmapovanie má samo osebe veľkú hodnotu ešte predtým, než sa nasadí samotná UI.

Technologické požiadavky sú rovnako variabilné. Z pohľadu hardvéru opäť všetko závisí od use case. Bežné ML aplikácie si vystačia s CPU hardvérom v cenovej úrovni rádovo desiatok tisíc, GPU pre vyšší výkon sa začína približne na 12-tisíc eurách, no nie je potrebné vždy. Veľká časť praktických nasadení sa zaoberá aj bez neho. Z pohľadu softvéru je dôležitejšie než konkrétne nástroje to, aby firma mala poriadok v dátach a jasne definované, kde a v akej kvalite vznikajú. Technológia sa potom prispôsobí use case, nie naopak.

Podľa sa teraz podrobnejšie pozrieť na to, ako by mala implementácia UI v priemyselnom podniku prebiehať. Jednou z prvých otázok určite bude, ako vybrať ten správny proces/aplikáciu, ktorú chceme s UI podporiť, a druhou, ako správne odhadnúť náklady (aj keď len na pilotný projekt), ktoré s tým budú súvisieť?

Toto je komplexná téma, ktorá sa nezačína technológiou, ale na úrovni biznisu, teda zmapovaním požiadaviek. Manažment musí v prvom rade vedieť, kde má najväčšie náklady alebo čo chce zefektívniť z pohľadu návratnosti. Až potom má zmysel hovoriť o konkrétnej aplikácii. Pri výbere procesu sa oplatí riadiť niekoľkými kritériami naraz. Ideálny pilotný proces zapadá do cieľov firmy, je čo najmenej zložitý a má aspoň čiastočne pripravené dáta, prípadne nie je ťažké ich získať. Zároveň je dobré vybrať oblasť, kde bude najmenší odpor zo strany ľudí. Ak ľudia na danom oddelení už pracujú s nejakou technológiou, UI projekt sa tam nasadí výrazne ľahšie a má vyššiu šancu na úspech.

Samotné mapovanie pritom nie je otázka dní. Pokojne môže zaberať aj tri až šesť mesiacov, kým sa vyberú tie správne use cases. Práve tu sa veľmi vyplatí prizvať externistu vidiaceho súvislosti, ktoré už firma pre-

hliada, pretože nemá odstup od svojich zaužívaných procesov. Pokiaľ ide o odhad nákladov, ten ide ruka v ruku s týmto mapovaním. Bez jasne zadaného procesu a stavu dát je akýkoľvek odhad len číslom vo vzduchu. Preto pri pilotných projektoch odporúčam najprv investovať do dôkladnej analýzy a až na jej základe stanoviť rozpočet, ktorý potom zodpovedá realite a neprekvapí v polovici projektu.

Nemenej zásadnou otázkou z pohľadu ekonomiky a efektivity projektu bude aj definovanie, aké oddelenia podniku by mali byť zapojené do zavádzania UI technológií?

Povedala by som, že to nie je najmenej zásadná, ale práve naopak, jedna z najzásadnejších otázok vôbec. Z mojej skúsenosti totiž všetky riešenia, či už s UI alebo bez nej, v konečnom dôsledku stoja a padajú na ľuďoch. Preto je kľúčové od úplného štartu jasne komunikovať, prečo daný projekt robíme, a zapojiť ľudí do procesu plánovania. Platí jednoduchá pravda: ľudia oveľa menej sabotujú riešenie,

na ktorom sa sami podieľali. Ak majú pocit, že im niečo nasilu spadlo zhora, prirodzene sa tomu bránia. Ak naopak cítia, že boli pri tom a ich názor mal váhu, stávajú sa z nich spojenci. V praxi to znamená zapojiť nielen IT a manažment, ale najmä koncových používateľov z prevádzky, teda operátorov, technikov a vedúcich zmien, ktorí s riešením budú reálne pracovať každý deň. A nezabúdať ani na tých, ktorí dáta vytvárajú a spravujú. Správne nastavenie ľudskej stránky projektu je pritom rovnako dôležité ako výber správnych dát. Jedno bez druhého nefunguje.

Aj keď je UI silný nástroj pre rôzne činnosti, stále budú minimálne v procese finálneho prijímania rozhodnutí (a aj inde) prítomní aj ľudia. Aké znalosti a kompetencie potrebujú zamestnanci pri práci s UI systémami?

Možno to prekvapí, ale v praxi sa ukázalo, že žiadne extra špecializované znalosti väčšina zamestnancov nepotrebuje. Závisí to však od konkrétnej úlohy. Ak ide o dátových analytikov, ktorí pripravujú dáta pre UI, tí by mali v prvom rade chápať biznis požiadavku, teda rozumieť tomu, čo a prečo riešime. Samotnú technológiu a programovanie je naopak ideálne nechať na externistu, ktorý sa na to

špecializuje. Nie je efektívne, aby firma budovala takúto expertízu interne pri prvých projektoch.

Pri koncových používateľoch je to ešte jednoduchšie. Tí by nemali potrebovať prakticky žiadne špeciálne znalosti, postačí im bežné narábanie s webom a mobilom. A práve v tom spočíva celé tajomstvo úspechu. Správne navrhnutý systém je totiž taký, pri ktorom používateľ prirodzene vie, čo má robiť, a používa ho pri práci bez toho, aby nad tým musel rozmýšľať. Ak si systém vyžaduje školenia a manuály na základné používanie, niečo je zle navrhnuté. Úspech projektu sa neskrýva v tom, ako veľmi sa ľudia prispôbia technológii, ale v tom, ako veľmi sa technológia prispôsobí ľuďom.

Aplikácie využívajúce UI silne závisia od údajov. Ich množstvo, dostupnosť a kvalita do značnej miery určujú, aké výsledky/výstupy z UI budú vychádzať. Ako teda začať so zberom údajov? Postačia snímače a meracia technika aktuálne nainštalovaná v prevádzke, alebo sa z vašich skúseností ukazuje, že väčšinou je potrebné doplniť/inštalovať aj nové snímače či systémy na zber a prenos údajov?

Aj tu platí, že veľa závisí od konkrétneho use case, no všeobecne platí jedno pravidlo. Pre akýkoľvek UI projekt je potrebný väčší objem predovšetkým správnych dát. Kvantita totiž automaticky neznamená kvalitu a práve to býva najčastejší omyl. Preto je dôležité začať už pri mapovaní požiadaviek takzvaným dátovým auditom. Pri ňom sa odhalia skryté a slabé miesta, dáta sa zvalidujú a výsledkom je jasná odpoveď na otázku, či sú dostatočné, či treba nejaké pridať a akým spôsobom ich prečistiť.

V praxi sa pritom ukazuje, že firmy majú dáť zvyčajne dosť. Problémom nie je ich množstvo, ale ich stav. Proces čistenia a takzvaného labelovania, teda označovania dát, je časovo najnáročnejšou časťou celého projektu a pokojne môže zaberať aj 90 % celkového času zavedenia UI. To je realita, ktorú firmy na začiatku často podceňujú.

Čo sa týka samotných snímačov, odpoveď je opäť individuálna. Niekedy je potrebné doplniť nový senzor, systém alebo manuál, prípadne previesť dáta z papierovej podoby do digitálnej. Inokedy úplne stačí to, čo už v prevádzke nainštalované je. Vždy záleží na tom, čo konkrétny use case skutočne vyžaduje, a nie na tom, koľko technológie dokážeme do prevádzky pridať.

Ak už máme dostatok údajov k dispozícii, čo s nimi ďalej? Stačí ich „nahrať“ do aplikácie využívajúcej UI a počkať si na výstup?

Nestačí a to je asi najčastejšia mylná predstava o tom, ako UI funguje. Najprv musíme dáta zvalidovať, teda overiť, či sú správne a použiteľné. Až potom prichádza na rad takzvaný ETL proces. Je to skratka z anglických slov Extract, Transform, Load, teda extrahovanie dát z rôznych zdrojov, ich pretransformovanie do jednotného a použiteľného formátu a následné nahranie do cieľového systému. Zjednodušene povedané, je to fáza, keď surové a často nesúrodé dáta upravíme tak, aby s nimi UI vôbec dokázala pracovať.

Treba si tiež uvedomiť, že UI aplikácia má v zásade dve úrovne. Prvou je tréningovanie, ktoré beží lokálne počas vývoja, a druhou je samotná produkcia, kde už systém dávkuje pracuje s novými, reálnymi dátami z prevádzky. A čo je možno najdôležitejšie, nejde o jednorazovú činnosť, ale o nekončiaci sa proces. Až po reálnom zavedení UI sa totiž naplno ukáže množstvo chýb a špecifických situácií, ktoré sa vopred nedali predvídať. Dáta sa preto validujú a upravujú aj za behu, úplne bežne počas ostrej prevádzky. Nasadenie UI teda nie je cieľová páska, ale skôr štart do ďalšej etapy.

Dôveruj, ale preveruj – to je v prípade UI ešte v súčasnosti aktuálne. Ako sa dá skontrolovať, či sú výstupy z UI urobené „zodpovedne“ a vierohodne do takej miery, aby sme na nich mohli postaviť ďalšie rozhodovanie?

Aj tu platí, že odpoveď závisí od konkrétneho use case, ale existuje niekoľko osvedčených princípov. Pri LLM aplikáciách, teda tých, ktoré sú postavené na jazykových modeloch, je veľmi dôležité vždy ukázať zdroj, z ktorého bola odpoveď vygenerovaná. Používateľ tak nedostáva len holé tvrdenie, ale môže si ho okamžite overiť priamo v origináli, napríklad v konkrétnom manuáli alebo dokumente. To je základ dôvery.

Pokiaľ ide o plne autonómnych agentov, ktorí by konali samostatne bez dozoru, tých zatiaľ do produkcie neodporúčam. Jednoducho ešte nie sú v takom stave, aby sa dali spoľahlivo a jednoducho kontrolovať, riziko je tam stále priveľké. Pri bežných ML aplikáciách funguje overovanie priamo cez používanie. Používateľ za behu validuje dáta jednoduchým rozhraním a tieto dáta sa potom raz za čas použijú na pretrénovanie modelu. Systém sa tak prirodzene zlepšuje vďaka samotnej práci s ním.

A nad tým všetkým stojí jeden princíp, ktorý sa nám osvedčil najviac. Vždy začíname tým najmenším možným use case a nové veličiny pridávame až postupne. Takto má firma celý proces neustále pod kontrolou, dokáže priebežne overovať výsledky a buduje si dôveru v systém krok za krokom, namiesto toho, aby naslepo spustila niečo veľké a komplexné naraz.

Jednou z vlastností systémov podporovaných UI je ich schopnosť učiť sa, resp. trénovať sa. Aby to však bolo možné zabezpečiť, je potrebné do UI posilať nielen tie správne, ale aj chybné príklady/výsledky/údaje. Ako sa to dá v spojitosti bežiacich prevádzkach zabezpečiť, keď má podnik snahu vyrábať v čo najvyššej kvalite a s minimálnou chybovosťou?

Hneď na úvod treba uviesť jednu vec na pravú mieru. Predstava plne samoučiacich sa systémov je do veľkej miery mýtus. UI sa v produkcii takmer nikdy nezlepšuje sama od seba, bez zásahu dodávateľa alebo programátora. Skôr naopak, jej výkon má časom tendenciu klesať, pretože sa mení charakter reálnych dát v prevádzke. Zlepšenie nepríde automaticky, ale až vtedy, keď model na nových dátach cielene pretrénujeme.

Pokiaľ ide o chybné príklady, tie sú na tréningovanie naozaj potrebné, pretože model sa musí naučiť rozoznať nielen to, ako vyzerá správny stav, ale aj ten chybný. Tieto dáta sa štandardne dodávajú vo fáze tréningovania, ešte pred nasadením do produkcie. Problém je v tom, že chybové stavy sa veľmi ťažko umelo nasimulujú. V kvalitnej prevádzke ich navyše prirodzene nie je veľa, čo je síce dobrá správa pre výrobu, ale komplikácia pre tréning.

Práve preto sa nám osvedčil iný prístup. Namiesto zložitého simulovania chýb je oveľa efektívnejšie zbierať reálne chybové prípady postupne, počas demo testu alebo pilotnej prevádzky a algoritmus na ich základe priebežne upravovať a doladovať. Pilot teda neslúži len na overenie funkčnosti, ale je aj cenným zdrojom presne tých chybových dát, ktoré by sme inak v laboratórnych podmienkach len ťažko získavali.

Ako dlho trvá natréňovať UI, aby prinášala zmysluplné a dôveryhodné výsledky? V akej podobe sú výsledky/výstupy z UI k dispozícii?

Ako už býva pri UI zvykom, aj tu platí, že všetko závisí od konkrétneho use case. Vo všeobecnosti sa však bavíme o rozmedzí zhruba od troch mesiacov až po jeden rok, kým systém začne prinášať skutočne zmysluplné a dôveryhodné výsledky. Práve preto opäť zdôrazňujem, že je dobré začať tým najmenším možným use case a dobre pripravenými dátami, pretože to celý proces výrazne urýchľuje.

V praxi to zvyčajne vyzerá tak, že približne tri mesiace zaberie lokálne tréningovanie modelu. Nasledujú ďalšie tri až šesť mesiacov validácie a zlepšovania priamo v praxi, teda v pilotnej alebo demo prevádzke, kde sa model konfrontuje s reálnymi dátami. Potom je tu ešte obdobie rádovo jedného až dvoch rokov postupného doladovania, kým sme s výsledkami naozaj spokojní a systém je úplne usadený. Netreba sa toho však zľaknúť, pretože hodnotu prináša už počas tohto obdobia, nie až na jeho konci.

Čo sa týka podoby výstupov, tá je veľmi rôznorodá a prispôsobuje sa tomu, kto s nimi pracuje. Môže ísť o prehľadné reporty a dashboards pre manažment, o konkrétne upozornenia a odporúčania priamo v systéme, ktorý operátor používa, alebo o odpovede na otázky v prirodzenom jazyku s odkazom na zdroj. Dôležité je, aby výstup dostal používateľ v takej forme, ktorá preňho dáva zmysel a vie ju ihneď použiť pri svojej práci bez nutnosti čokoľvek si prekladať alebo dodatočne spracúvať.

Finančných manažerov a vedenie podniku zaujíma návratnosť investície do nových projektov. Ako môže teda podnik merať úspešnosť implementácie UI?

V prvom rade musí podnik poznať svoje čísla ešte pred štartom projektu. To je úplný základ, na ktorý sa často zabúda. Ak napríklad nevieme, koľko reklamácií máme dnes a aké sú ich príčiny, len ťažko neskôr zvalidujeme návratnosť investície do kontroly kvality. Bez poznania východiskového stavu totiž nemáme s čím porovnávať. Samotná úspešnosť sa potom meria vopred definovanými ROI ukazovateľmi. Môže ísť napríklad o skrátenie času údržby, zníženie chybovosti alebo úsporu nákladov, pričom konkrétne veličiny opäť závisia od use case. Aby však toto meranie vôbec dávalo zmysel, je často potrebné zmeniť aj mindset firmy. Ideálne je mať k dispozícii BI oddelenie (business intelligence), ktoré pozná súčasný stav, rozumie cieľom firmy a dokáže správne nastaviť metriky, ktorými sa bude úspech merať. V praxi zvyčajne stanovujeme dva horizonty. Krátkodobé ROI sledujeme rádovo do šiestich mesiacov a dlhodobé v rozmedzí dvoch až troch rokov. Počas celého tohto obdobia priebežne sledujeme, či sa k stanoveným cieľom skutočne približujeme.

Na záver jedna dôležitá poznámka. Niekedy sa ukáže, že sa k očakávaným číslam nepribližujeme. V takom prípade je úplne v poriadku, ba dokonca žiaduce takýto projekt včas zastaviť. Schopnosť povedať stop hneď na začiatku, kým náklady ešte nenarástli, je rovnako cenná ako schopnosť projekt úspešne dotiahnuť. Nie každý use case sa totiž oplatí a práve poctivé meranie nám to dokáže ukázať veľmi skoro.

Nasadením a otestovaním možnosti UI na pilotnom projekte sa v tom lepšom prípade nemusí skončiť a podnik môže pristúpiť aj k jeho rozšíreniu na ďalšie procesy. Aké úlohy, resp. povinnosti pre podnik sa skrývajú v celom životnom cykle projektu využívajúceho UI?

Najväčšia povinnosť, ktorá sa skrýva v celom životnom cykle UI projektu, sa netýka technológie, ale ľudí a fungovania firmy. Podnik totiž musí byť pripravený zaviesť nové úlohy a postupne aj nové oddelenia. Konkrétne ide o ľudí, ktorí rozumejú procesom, poznajú svoj tím a zároveň chápú možnosti technológie. Patria sem napríklad inovační manažéri, ktorí neustále mapujú požiadavky a hľadajú ďalšie vhodné use cases, dátoví analytici, ktorí sa starajú o kvalitu dát, a už spomínané BI oddelenie, ktoré úzko spolupracuje s finančným úsekom a sleduje návratnosť. Toto prepojenie technickej a ekonomickej stránky je mimoriadne dôležité.

Rovnako dôležitá je však aj ľudská a motivačná rovina. Vo firme by mali byť ľudia, ktorí dokážu ostatných zamestnancov motivovať, aby UI riešenia reálne používali, dôverovali im a sami prinášali nápady na zlepšenie. Práve zdola prichádzajúce podnety bývajú často tým najcennejším zdrojom ďalších inovácií.

Treba si preto úprimne priznať, že nejde o jednorazový nákup technológie, ale o dlhodobý proces, ktorý sa začína zmenou mentality firmy a pokračuje budovaním nových rolí a oddelení. Firma, ktorá toto pochopí a investuje do toho, premení jeden úspešný pilotný projekt na trvalú schopnosť inovovať. A to je v konečnom dôsledku oveľa väčšia hodnota než akékoľvek jednotlivé riešenia.

Vysvetlime ešte výhody/nevýhody lokálne nasadených a cloudových aplikácií/riešení UI? Kedy sa ktorý typ oplatí nasadiť?

To je veľmi dôležitá téma a hneď na úvod poviem, že univerzálna odpoveď neexistuje. Obe riešenia majú svoje pre a proti a voľba vždy závisí od konkrétnych potrieb a obáv klienta. Lokálne nasadené modely majú jednu veľkú výhodu a tou je bezpečnosť v tom zmysle, že dáta zostávajú v sieti klienta a nikam neodchádzajú. To je pre mnohé priemyselné podniky zásadný argument. Treba si však uvedomiť, že táto výhoda so sebou nesie aj viacero nevýhod. Lokálne modely majú spravidla nižšiu kvalitu a nikdy nebudú schopné konkurovať veľkým modelom z cloudu, za ktorými stoja tímy tých najlepších inžinierov na svete. Navyše, aj lokálny model je v zásade softvér, teda kód, a nesie si svoje vlastné bezpečnostné riziká. Trochu ironicky povedané sa oň treba starať ešte viac než o cloudové riešenie, pretože všetka zodpovednosť za jeho prevádzku a zabezpečenie leží na pleciach klienta. K tomu sa pridáva riziko, že lokálny model nemusí nikdy doručiť požadovanú kvalitu výstupov a čas zavedenia sa môže pokojne aj strojnásobiť.

Cloudové riešenia fungujú opačne. Ich nevýhodou je, že dáta sa posielajú do cloudu, no treba povedať, že aj to sa dá veľmi dobre zabezpečiť a v praxi to bežne robíme. Na druhej strane sú tu vyššie prevádzkové náklady, dlhší reakčný čas a takzvaný vendor lock, teda závislosť od jedného dodávateľa. Ak sa napríklad cloudový poskytovateľ rozhodne výrazne zvýšiť ceny, automaticky nám narastú náklady a v krajnom prípade môžeme byť nútení projekt ukončiť. Podobné riziko hrozí aj vtedy, ak by takýto poskytovateľ skrachoval alebo sa rozhodol službu ukončiť. Vtedy by mohlo padnúť celé naše riešenie postavené na ňom.

Zjednodušene sa teda dá povedať, že lokálne riešenie volíme tam, kde je najvyššou prioritou maximálna kontrola nad dátami a ich bezpečnosť, pričom klient je ochotný akceptovať vyššie nároky na prevádzku aj nižšiu kvalitu. Cloudové riešenie naopak volíme tam, kde je prioritou najvyššia možná kvalita výstupov, rýchlosť nasadenia a klient je s otázkou dát v cloude vyrovnaný. V praxi sa pritom čoraz častejšie stretávame aj s kombináciou oboch prístupov, teda s hybridným riešením, ktoré sa snaží využiť silné stránky každého z nich.

Už sme naznačili vyššie, že nasadenie UI je spojené nielen s výhodami a doteraz nevidanými možnosťami, ale aj s obmedzeniami. Ako treba v tomto kontexte vnímať bezpečnosť (údajov, podniku), etické otázky či ďalšie riziká, ktoré môžu s nasadením UI súvisieť?

Aj pri tejto otázke veľmi záleží na konkrétnom use case, pretože riziká pri systéme na spracovanie dokumentov sú úplne iné než pri systéme na spracovanie obrazu z kamier. Pokiaľ ide o bezpečnosť, v zásade platí to isté ako pri akomkoľvek inom softvérovom systéme. Rovnaké pravidlá, rovnaká disciplína. Novinkou sú v podstate len nové typy útakov spojené špecificky s LLM aplikáciami, teda riešeniami postavenými na jazykových modeloch. Aj proti tým sa však dá účinne brániť a exis-

tujú na to osvedčené postupy. Treba tiež dodať, že ak ide napríklad o systém pracujúci so senzormi a kamerami, otázka osobných údajov a súkromia ľudí sa ho takmer netýka, čím veľká časť obáv prirodzene odpadá.

Etická stránka je z môjho pohľadu zaujímavejšia a často podceňovaná. Kľúčové je stavať systémy s UI ako pomocníka pre ľudí, nie ako ich náhradu. A tu treba povedať jednu vec na rovinu. Ľudí v skutočnosti nenahrádza UI, ľudia nahrádza automatizácia ako taká a to platí už desaťročia. UI je len ďalším nástrojom v tomto procese. Vnímať umelú inteligenciu ako strašiaka, ktorý berie prácu, je preto skôr nedorozumenie. Etika je tak v konečnom dôsledku predovšetkým o komunikácii. O tom, ako vedenie firmy dokáže svojim ľuďom férovo a otvorene vysvetliť, prečo dané riešenie zavádza, čo im prinesie a ako sa zmení ich práca. Ak je táto komunikácia úprimná a ľudia cítia, že UI je tu na to, aby im uľahčila prácu a nie ich ohrozila, väčšina etických aj bezpečnostných obáv sa dá zvládnuť oveľa jednoduchšie, než sa na prvý pohľad zdá.

Vývoj v oblasti UI naberá na obrátkach a to, čo je dnes novinkou, o pár týždňov môže byť už zastarané. Napriek tomu sa na záver pozrime do sklenenej gule – aké trendy nás v oblasti využitia umelej inteligencie v prostredí priemyslu čakajú v najbližších rokoch?

Predpovedať vývoj UI na roky dopredu je takmer nemožné, no niekoľko trendov sa už dnes črtá pomerne jasne a som presvedčená, že práve tie budú formovať priemysel v najbližšom období. Prvým je posun od veľkých univerzálnych modelov k menším, špecializovaným modelom nasadeným priamo u klienta. Donedávna platilo, že čím väčší model, tým lepšie. Dnes sa ukazuje, že na konkrétnu, úzku zameranú úlohu úplne stačí menší a lacnejší model, ktorý beží lokálne a dáta neopúšťajú firmu. Pre priemysel je to ideálna kombinácia kontroly a výkonu. V praxi to vidíme napríklad pri vyhľadávaní v internej technickej dokumentácii a manuáloch, pri spracovaní reklamácií alebo pri automatickom triedení a vyhodnocovaní hlásení z prevádzky, teda všade tam, kde model nemusí vedieť všetko o svete, ale musí dokonale rozumieť práve tej jednej firme.

Druhým výrazným trendom bude dôraz na dôveryhodnosť a vysvetliteľnosť výstupov. Už nebude stačiť, že UI dá odpoveď. Bude musieť zároveň ukázať, odkiaľ ju má, a umožniť spätné dohľadanie. To sa stane podmienkou nasadenia najmä v regulovaných odvetviach ako energetika, automotiv či farmácia. Typickým príkladom je systém, ktorý technikovi poradí postup pri poruche a zároveň priloží odkaz na konkrétnu stranu manuálu, z ktorej čerpal, alebo nástroj na kontrolu kvality, ktorý nielen označí chybný kus, ale aj zdôvodní, na základe čoho tak rozhodol. Práve táto dohľadateľnosť bude rozhodovať o tom, či firmy UI dôveru dajú alebo nie.

A do tretice, postupne budú dozrievať takzvané agentové systémy, teda riešenia, ktoré dokážu samostatne vykonať celú postupnosť krokov. Ako som spomínala už skôr, dnes ich do produkcie ešte neodporúčam, pretože sa zatiaľ ťažko kontrolujú. V horizonte niekoľkých rokov sa však pravdepodobne dostanú do stavu, keď budú dostatočne spoľahlivé a transparentné. Vtedy by mohli prevziať napríklad celý proces prípravy podkladov pre objednávku náhradných dielov, automatické generovanie reportov vo viacerých systémoch či samostatné plánovanie údržbových úkonov, vždy však pod dohľadom človeka, ktorý má posledné slovo. Spoločným menovateľom všetkých týchto trendov je jedno. UI sa bude čoraz viac približovať reálnym potrebám priemyslu, bude bezpečnejšia, dôveryhodnejšia a bližšie k ľuďom, ktorí ju používajú. A presne to je smer, ktorý vitam.

Ďakujeme za rozhovor.

Anton Géner