> Sektor administracji publicznej charakteryzuje się najniższym poziomem zaawansowania kadry zarządzającej oraz kompetencji w zakresie cyberbezpieczeństwa.

celem jest podniesienie poziomu cyberbezpieczeństwa w Unii Europejskiej, obejmuje przede wszystkim organy szczebla centralnego, na przykład ministerstwa, urzędy i agencje państwowe. W zależności od kraju jest to szacunkowo od stu do kilku tysięcy instytucji[7]. Problem pojawia się jednak na poziomie regionalnym i lokalnym.

Według analiz ENISA sektor administracji publicznej charakteryzuje się najniższym poziomem zaawansowania kadry zarządzającej oraz kompetencji w zakresie cyberbezpieczeństwa. Co trzecia organizacja nie posiada strategii rozwoju kompetencji z tego zakresu, a połowa nie zapewnia szkoleń dotyczących zagrożeń i analizy ryzyka[8]. Poza ograniczeniami finansowymi i kadrowymi, problemem jest również kultura organizacyjna. Jednostki publiczne cechują się dużym poziomem biurokracji. Przywiązanie do istniejących procedur i technologii często skutkuje niechęcią do wdrożenia nowoczesnych rozwiązań, również z obszaru cyberbezpieczeństwa. Jest to szczególnie widoczne na poziomie gmin i powiatów.

Dodatkową barierą są także opóźnienia we wdrożeniu dyrektywy NIS2, z którymi mierzy się wiele krajów członkowskich UE. Jeszcze w maju ubiegłego roku Komisja Europejska wystosowała opinie do 19 państw członkowskich, które nie wdrożyły w pełni dyrektywy NIS28. Wśród nich była również Polska. Sytuacja jednak stopniowo się zmienia. W kwietniu tego roku weszła w życie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC), która implementuje unijne regulacje do polskiego porządku prawnego.

Nowe przepisy zobowiązują podmioty objęte dyrektywą NIS do dokonania wpisu do Wykazu KSC do 3 października albo w przypadku samorejestracji – złożyć wniosek o wpis. Termin wdrożenia wymogów wynikających z nowych przepisów to 3 kwietnia 2027 r. Do tego czasu organizacje będą musiały, m.in. wyznaczyć osoby odpowiedzialne za kontakt z KSC, zweryfikować niekaralność zespołu oraz przygotować i wdrożyć System Zarządzania Bezpieczeństwem Informacji (SZBI), czyli zestaw polityk, procedur oraz zabezpieczeń organizacyjnych i technicznych minimalizujących ryzyko nieuprawnionego dostępu do danych.

1. ENISA, 2026, ENISA NIS360

2. ENISA, ENISA Threat Landscape 2025

3. Jak wyżej

4. Jak wyżej

5. Jak wyżej.

6. World Economic Forum, Global Cybersecurity Outlook 2026.

7. ENISA, 2026, ENISA NIS360

8. Komisja Europejska, Transpozycja dyrektywy NIS 2 w państwach UE

AI zmienia elektroniczny obieg dokumentów. Samo „cyfrowe" już nie wystarczy.

Przez lata elektroniczny obieg dokumentów kojarzył się przede wszystkim z przeniesieniem papierowych procesów do systemu: rejestracją dokumentu, przekazaniem go do odpowiedniej osoby, akceptacją i archiwizacją. Dziś taki model przestaje wystarczać. Firmy nie potrzebują już wyłącznie cyfrowego repozytorium. Potrzebują narzędzi, które potrafią zrozumieć informacje zapisane w dokumentach i wykorzystać je do dalszej automatyzacji procesów.

Właśnie dlatego sztuczna inteligencja staje się jednym z najważniejszych kierunków rozwoju systemów EOD. Dokument coraz rzadziej powinien być traktowany jako plik, który człowiek musi otworzyć, przeczytać i ręcznie opisać. Powinien stać się źródłem ustrukturyzowanych danych, które mogą automatycznie zasilać kolejne etapy procesu.

– Przyszłość elektronicznego obiegu dokumentów nie polega na tym, żeby szybciej przesyłać pliki pomiędzy użytkownikami. Kluczowe jest to, żeby system potrafił zrozumieć, z jakim dokumentem ma do czynienia, jakie informacje są w nim istotne i co powinno wydarzyć się dalej – mówi **Filip Kolendo**, CTO i wiceprezes Primesoft Polska.

Od cyfrowego dokumentu do danych, które pracują

Taką zmianę dobrze widać na przykładzie inteligentnego przetwarzania dokumentów, czyli IDP. Rozwiązania tej klasy łączą OCR z mechanizmami AI oraz przetwarzaniem języka naturalnego. W praktyce oznacza to przejście od prostego rozpoznania tekstu do analizy jego znaczenia.

W systemie V-Desk AI może m.in. identyfikować i klasyfikować typ dokumentu, wyodrębniać kluczowe dane, oceniać ich kompletność, interpretować kontekst, tworzyć podsumowania oraz automatycznie zasilać workflow. Może także analizować informacje zapisane w tabelach, diagramach czy dokumentach w różnych językach. W obiegu korespondencji sztuczna inteligencja może rozpoznać charakter pisma i skierować je do właściwego procesu, np. reklamację do działu jakości, a wezwanie do zapłaty do windykacji.

– Największa wartość AI pojawia się wtedy, gdy przestaje być dodatkiem do systemu, a staje się elementem procesu. Jeżeli po rozpoznaniu dokumentu dane trafiają bezpośrednio do odpowiedniego rejestru, systemu ERP, CRM czy kolejnego kroku workflow, eliminujemy nie tylko ręczne przepisywanie informacji, ale również znaczną część pracy związanej z ich interpretacją – podkreśla Filip Kolendo.

AI jako część procesu, nie dodatek do systemu

To właśnie ten aspekt będzie decydował o konkurencyjności systemów EOD w kolejnych latach. Organizacje przetwarzają coraz większe wolumeny informacji: faktury, umowy, korespondencję, formularze, dokumenty przewozowe, dokumentację HR czy pisma urzędowe. Im więcej danych, tym mniej efektywny staje się model oparty na ręcznej obsłudze.

AI może w tym przypadku pełnić rolę pierwszej warstwy analitycznej, o ile będzie potrafiło poprawnie odczytać dokument, zrozumieć jego kontekst, wskazać braki, wydobyć najważniejsze informacje i przygotować dane do dalszego wykorzystania. Człowiek pozostaje odpowiedzialny za decyzję tam, gdzie jest ona rzeczywiście potrzebna, ale nie musi wykonywać każdej czynności technicznej prowadzącej do jej podjęcia.

– Dojrzały system EOD nie powinien już tylko odpowiadać na pytanie: „Gdzie znajduje się dokument?". Powinien również odpowiadać: „Co z niego wynika i co należy z nim zrobić?". Sztuczna inteligencja daje dziś technologiczną możliwość, żeby właśnie w tę stronę rozwijać elektroniczną wymianę danych w przedsiębiorstwach – podsumowuje Filip Kolendo.

Dlatego przyszłość EOD należy nie do systemów, które wyłącznie digitalizują dokumenty, lecz do platform, które zamieniają ich treść w dane, a dane w automatyczne działania. AI nie zastępuje elektronicznego obiegu dokumentów. Staje się jego naturalnym kolejnym etapem.

materiał partnera