

# OpenAI and Poland's NASK sign an AI safety and security research agreement

Source copy kept by wheresthe.ai for the story "OpenAI and Poland's NASK sign an AI safety and security research agreement" (<https://wheresthe.ai/d/pl-openai-and-nask-sign-ai-safety-research-agreement-2026-10/>).

Source: <https://www.nask.pl/aktualnosci/jedyna-taka-umowa-w-ue-partnerstwo-nask-i-openai-w-obszarze-bezpieczenstwa-sztucznej-inteligencji>

Text saved 25 Oct 2026 (the page as published).

SHA-256 of the saved text: 59f67470744fdb5404598b85e0a791019c5dc173fff3541db89682dc6610aa4a

---

Aktualność 23 Października 2026 | 4 min. czytania

Jedyna taka umowa w UE. Partnerstwo NASK i OpenAI w obszarze bezpieczeństwa sztucznej inteligencji. Nowe zagrożenia wymagają wspólnego działania. NASK i OpenAI podpisały porozumienie o współpracy w zakresie badań nad bezpieczeństwem AI. Partnerstwo połączy wiedzę i doświadczenie obu organizacji, by szybciej identyfikować zagrożenia związane z tą technologią i lepiej się przed nimi chronić. Pozwoli też skuteczniej weryfikować, jak zaawansowane metody AI mogą pomóc zwiększyć bezpieczeństwo i odporność usług cyfrowych.

Cyberbezpieczeństwo Instytut Sztuczna inteligencja

Sztuczna inteligencja ma coraz większe możliwości. Twórcy technologii i publiczne instytucje badawcze z różnych krajów muszą za nimi nadążyć, dlatego często łączą siły, by lepiej rozumieć ryzyko i opracowywać skuteczniejsze zabezpieczenia. Taka współpraca już przynosi efekty. Wspólne działania OpenAI z amerykańskim Center for Advancing Standards and Innovation for Super Intelligence (CAISSI), brytyjskim AI Security Institute (AISi) i innymi publicznymi instytucjami badawczymi pomogły wykryć i usunąć luki w agentach i modelach AI. Przyczyniły się też do poprawy bezpieczeństwa najbardziej zaawansowanych modeli. Teraz do tego grona dołącza Polska.

Po stronie NASK współpracę poprowadzi Ośrodek Badań nad Bezpieczeństwem Sztucznej Inteligencji, który pełni funkcję polskiego Instytutu Bezpieczeństwa Sztucznej Inteligencji (AISi). Wspólnie z OpenAI będzie badać bezpieczeństwo coraz bardziej zaawansowanych systemów AI. Przeprowadzane analizy pomogą lepiej oceniać te systemy, wykrywać ich słabe punkty i wzmacniać zabezpieczenia.

– Bezpieczeństwa AI nie da się zapewnić w pojedynkę. Dlatego współpraca z OpenAI to ważny krok dla NASK i naszego Ośrodka Badań nad Bezpieczeństwem Sztucznej Inteligencji. Tym bardziej, że to jedyna taka umowa w Unii Europejskiej, co jest dla nas ważnym wyróżnieniem i docenieniem kompetencji naszych specjalistów – mówi dyrektor instytutu, Radosław Nielek. – Badamy nowe zagrożenia, rozwijamy zabezpieczenia i pracujemy nad wykrywaniem treści generowanych przez AI. Sprawdzamy też, jak sztuczna inteligencja może służyć do szkodliwych działań i jak te zagrożenia różnią się w zależności od języka rozmowy. Współpraca z OpenAI pozwoli nam połączyć wiedzę badawczą z doświadczeniem w rozwoju najbardziej zaawansowanych modeli. Dzięki niej będziemy mogli wcześniej rozpoznawać zagrożenia i skuteczniej im przeciwdziałać. Tak buduje się również społeczne zaufanie do AI – poprzez konkretne działania na rzecz jej bezpieczeństwa.

– Polska ma znakomitych naukowców i wyjątkowe talenty technologiczne. Mają one swój udział także w badaniach prowadzonych w OpenAI – dodaje Tom Duff Gordon, wiceprezes i szef polityki publicznej na region EMEA. – AI ma coraz większe możliwości, dlatego potrzebujemy również spojrzenia z zewnątrz. Pomaga nam ono weryfikować nasze założenia, testować systemy i wzmacniać zabezpieczenia. Dzięki porozumieniu z NASK możemy robić to wspólnie i korzystać z polskiego dorobku badawczego w międzynarodowych pracach nad bezpieczeństwem AI.

Bezpieczna AI wymaga wspólnych zasad

OpenAI zaapelowało o współpracę Stanów Zjednoczonych z innymi krajami nad międzynarodowymi standardami technicznymi dla najbardziej zaawansowanych systemów AI. W ich opracowaniu mają pomóc instytuty bezpieczeństwa AI i organizacje normalizacyjne. Wspólne zasady oceny możliwości AI, analizy ryzyka, testowania zabezpieczeń i zgłaszania incydentów ułatwią krajom porównywanie wyników i reagowanie na zagrożenia ponad granicami.

NASK wnosi do tych prac polską wiedzę z badań nad bezpieczeństwem AI, którą na co dzień wykorzystuje do ochrony usług publicznych i polskiej przestrzeni informacyjnej. Udział krajowych partnerów pomaga tworzyć standardy, które odpowiadają na konkretne zagrożenia i uwzględniają lokalne warunki korzystania z AI.

Współpraca, która już przynosi efekty

Podpisane właśnie porozumienie to kolejny etap współpracy NASK z OpenAI. W lipcu zespół CERT Polska, który działa w strukturach instytutu, otrzymał w programie Daybreak dostęp do zaawansowanych modeli OpenAI w zakresie cyberbezpieczeństwa. CERT Polska z ich pomocą wykrył sześć podatności w systemie MikroTik RouterOS. Połączenie części z nich pozwalało przejąć kontrolę nad urządzeniem bez logowania. Producent udostępnił poprawki, a zespół potwierdził, że skutecznie blokują one wykryte metody ataku.

Tematy powiązane Cyberbezpieczeństwo Instytut Sztuczna inteligencja

Udostępnij ten post

Wyróżnione aktualności

Zobacz wszystko

Aktualność 02 Września 2026 | 6 min. czytania

Zanim podatność stanie się incydem. Nowe rozwiązania CERT Polska Nie „czy”, ale „kiedy” – dziś każda organizacja musi być przygotowana na cyberatak. Dlatego NASK uruchamia wiedza.cert.pl oraz rozbudowuje serwis moje.cert.pl. Wszystko po to, by polskie organizacje mogły skuteczniej zapobiegać incydem i szybciej reagować, gdy do nich dojdzie. Eksperti CERT Polska zaprezentowali nowe narzędzia podczas śniadania prasowego.

CERT Polska Cyberbezpieczeństwo

Aktualność 09 Września 2026 | 5 min. czytania

ECSC 2026. NASK trenuje polską drużynę przed cyfrową Ligą Mistrzów Dziesięć osób, różne specjalizacje i jeden cel: jak najlepiej reprezentować Polskę. Już 12 października w niemieckim Bochum rozpocznie się European Cybersecurity Challenge, najważniejsza europejska rywalizacja młodych talentów cyberbezpieczeństwa. Polska drużyna, trenowana przez najlepszych specjalistów z NASK, przeszła właśnie pierwszy wspólny sprawdzian.

CERT Polska Cyberbezpieczeństwo Edukacja

Aktualność 08 Września 2026 | 4 min. czytania

Nie czekaj. Z początkiem szkoły rozmawiaj o zagrożeniach w sieci Nowa klasa, szkolna grupa na komunikatorze i coraz więcej spraw załatwianych online. Powrót do szkoły oznacza również zmiany w cyfrowej codzienności dzieci. To dobry moment, żeby zacząć rozmowę o bezpieczeństwie w sieci. Nie dopiero wtedy, kiedy wydarzy się coś złego.

Cyberprofilaktyka Fundusze Europejskie

Aktualność 26 Sierpnia 2026 | 6 min. czytania

Mocny kurs na cyfrową administrację. EZD-KPO z wynikiem ponad plan Początkowy plan był ambitny: wdrożyć EZD RP w 2 tys. podmiotów i przeszkolić 75 tys. osób. Efekt? 3102 wdrożenia i 206 tys. uczestników szkoleń. Projekt EZD RP realizowany w ramach Krajowego Planu Odbudowy dobiega końca z wynikami znacznie przekraczającymi pierwotne założenia.

EZD RP Fundusze Europejskie Instytut

Informacje Najnowsze aktualności

Zobacz wszystko

Aktualność 23 Października 2026 | 5 min. czytania

Ponad 11 mln euro na cyberbezpieczeństwo firm. Trwa drugi nabór w programie SECURE NASK pomaga firmom przygotować się na nowe unijne wymogi cyberbezpieczeństwa. W ramach programu SECURE przedsiębiorcy mogą ubiegać się o granty na dostosowanie produktów do nowych przepisów. W drugim naborze na ten cel

przeznaczono aż 11,5 mln euro.

Cyberbezpieczeństwo Fundusze Europejskie

Aktualność 22 Października 2026 | 2 min. czytania

Eliza Pogorzelska pokieruje Centrum Projektów Infrastrukturalnych i Edukacyjnych NASK Od lat zajmuje się projektami, które rozwijają cyfrową infrastrukturę Polski. Teraz przed nią kolejne wyzwanie. Eliza Pogorzelska od 1 listopada obejmie stanowisko dyrektorki Centrum Projektów Infrastrukturalnych i Edukacyjnych NASK, zastępując dr Małgorzatę Olszewską.

Instytut Nauka

Aktualność 22 Października 2026 | 5 min. czytania

Zaufanie kosztuje. Jak rozpoznać metody cyberprzestępców? Falszywa wiadomość od firmy kurierskiej, telefon od rzekomego pracownika banku czy prośba o kod do szybkiego przelewu od znajomego. Na pierwszy rzut oka każde z tych oszustw wygląda inaczej. W rzeczywistości jednak cyberprzestępcy bardzo często wykorzystują te same mechanizmy psychologiczne, a różnią się jedynie szczegóły oszustwa. Ekspertki NASK podpowiadają, jak się przed nimi bronić.

Cyberbezpieczeństwo Edukacja Fundusze Europejskie