



Zawody przyszłości w przemyśle 5.0

WERYFIKATOR DEEP FAKE'ÓW

Ekspert w zakresie sprawdzania fałszywych treści

www.industryup.pl/zawodyprzyszlosci

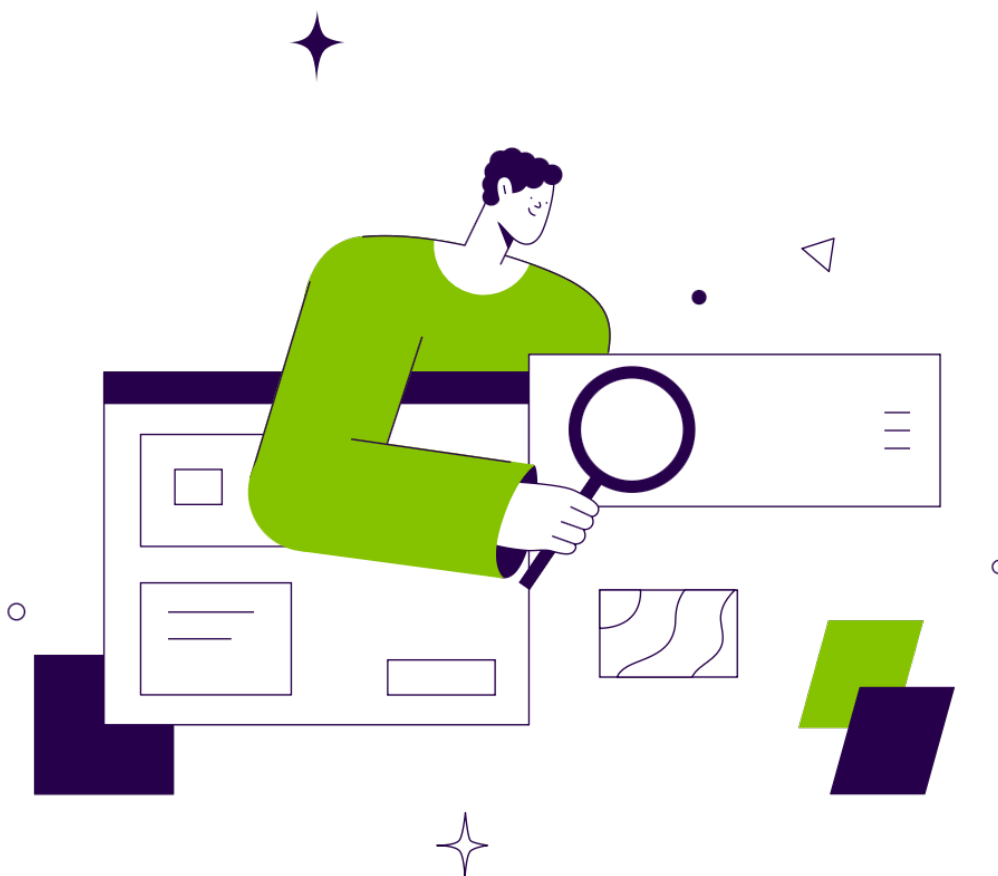
Materiał o etapach kariery jest częścią kampanii edukacyjnej „Zawody przyszłości w przemyśle 5.0”.

Dofinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Fundacji Rozwoju Systemu Edukacji. Unia Europejska ani Fundacja Rozwoju Systemu Edukacji nie ponoszą za nie odpowiedzialności. Wszystkie rezultaty opracowane w ramach projektu „Zawody przyszłości w przemyśle 5.0” są udostępniane na otwartej licencji Creative Commons Attribution – ShareAlike 4.0 International (CC BY-SA 4.0). Dozwolone jest ich nieodpłatne rozpowszechnianie, pod warunkiem wskazania autorstwa oraz źródła finansowania projektu.



Dofinansowane przez
Unię Europejską





NAJWAŻNIEJSZE INFORMACJE

O specjalizacji w skrócie

Główne zadania:

- Wykrywanie i analizowanie fałszywych treści audio, wideo i graficznych (określanych też mianem syntetycznych mediów), aby przeciwdziałać dezinformacji i oszustwom.
- Radzenie sobie z coraz sprytniejszymi atakami twórców deep fake'ów, którzy próbują zmylić systemy wykrywania.
- Sprawowanie kluczowej roli w ochronie prawdy w cyfrowych mediach.

Podstawowe pojęcia:

- Deep fake – odnosi się do mediów syntetycznych, zazwyczaj wideo, audio lub obrazów, tworzonych przy użyciu sztucznej inteligencji w celu

realistycznego odwzorowania wyglądu lub głosu osoby. Funkcją deep fake'a jest wprowadzenie odbiorcy w błąd lub oszustwo.

- Syntetyczne media – treści generowane sztucznie przez algorytmy, często z użyciem sztucznej inteligencji. Nie są rejestrowane w realnym świecie. Twórcy deep fake'ów projektują je tak, aby w swoim wyglądzie, dźwięku i strukturze naśladowały autentyczne materiały tworzone przez ludzi.
- Informatyka śledcza – identyfikowanie, zabezpieczanie, analizowanie i prezentowanie dowodów cyfrowych z urządzeń elektronicznych pod kątem badania naruszeń bezpieczeństwa, oszustw lub innych incydentów z wykorzystaniem danych cyfrowych.

Charakterystyka zawodu

Weryfikator deep fake'ów to nowy i szybko rozwijający się zawód, skoncentrowany na identyfikowaniu oraz ograniczaniu ryzyka związanego z mediami syntetycznymi. Specjaliści tego rodzaju dbają o wiarygodność treści cyfrowych, zwłaszcza w tak wrażliwych obszarach, jak treści informacyjne, dotyczące finansów lub polityki. Głównym zadaniem weryfikatorów jest wykrywanie zafałszowanych lub zmanipulowanych nagrań audio, materiałów wideo i obrazów, aby zapobiegać rozpowszechnianiu fałszywych informacji lub ich wykorzystywaniu w działaniach przestępczych.

W przyszłości rola weryfikatora deep fake'ów może rozwijać się w kierunku takich funkcji, jak specjalista ds. integralności mediów syntetycznych, analityk integralności biometrycznej, czy specjalista ds. kryminalistyki w rzeczywistości immersyjnej.

Twórcy deep fake'ów kontra weryfikatorzy

Jednym z największych wyzwań w tym obszarze jest fakt, że twórcy deep fake'ów stosują często wyrafinowane techniki, które mają na celu zmylenie

systemów wykrywania – to tak zwane atakami kontradyktoryjne (adversarial attacks). Aby im przeciwdziałać, weryfikatorzy wykorzystują zaawansowane metody, które uczą modele machine learningowe rozpoznawać podobne próby obchodzenia zabezpieczeń. Stosują także metodykę zespołową (ensemble approach), czyli używają zestawów współdziałających narzędzi, co zwiększa odporność i dokładność systemów wykrywania.

Innym problemem jest złożoność niektórych narzędzi opartych na sztucznej inteligencji. Nawet dla profesjonalistów bywają one trudne do interpretacji. Dlatego rośnie zapotrzebowanie na modele, które są nie tylko skuteczne, lecz także transparentne i objaśnialne – a zatem potrafiące wskazać, dlaczego podjęły daną decyzję. To z kolei wzmacnia zaufanie do procesu weryfikacji.

Ochrona cyfrowej wiarygodności

Weryfikatorzy deep fake'ów odgrywają kluczową rolę w utrzymywaniu wiarygodności informacji w świecie cyfrowym. Łącząc kompetencje techniczne z krytycznym myśleniem, mierzą się z ze zmieniającymi się wyzwaniami, jakie przynosi rozwój mediów syntetycznych. Specjaliści w zakresie weryfikacji treści pomagają pojedynczym odbiorcom, a także organizacjom ufać lub nie – temu jest publikowane w internecie. W czasie, kiedy treści generowane przez sztuczną inteligencję stają się coraz powszechniejsze, ta profesja nabiera specjalnego znaczenia.

ZAWÓD PRZYSZŁOŚCI

Zero zaufania do cyfrowych treści

Rola weryfikatora deep fake'ów jest jednym z najciekawszych zawodów przyszłości, ponieważ treści cyfrowe nie są już "automatycznie" wiarygodne. W miarę jak generowane przez AI filmy i nagrania audio stają się coraz bardziej realistyczne, trudno odróżniać, co jest prawdziwe, a co fałszywe.

To z kolei stwarza poważne wyzwania w dziedzinach od dziennikarstwa po wymiar sprawiedliwości. Według raportów Deeptrace Labs i Europolu, liczba deep fake'ów w sieci w 2023 roku podwoiła się w porównaniu z rokiem poprzednim, osiągając liczbę około 0,5 miliona materiałów wpuszczonych do obiegu. Gartner prognozuje natomiast, że do 2030 roku aż 90% całej zawartości online może być generowane syntetycznie, co pokazuje, że kompetencje weryfikacyjne w kolejnych latach jeszcze zyskają na znaczeniu.

Tłumienie fałszerstw w zarodku

Administracja publiczna, firmy i media będą polegały na ekspertach, którzy potrafią zatrzymać szkodliwe materiały, zanim te zdążą się szeroko rozprzestrzenić. Wiele organizacji już teraz inwestuje w działania związane z wiarygodnością informacji, traktując je jako kluczowe dla bezpieczeństwa i zaufania.

Lubisz rozwiązywać zagadki?

Weryfikatorzy deep fake'ów to nie tylko eksperci technologiczni – są także kimś w rodzaju "cyfrowych detektywów". Wykorzystują mix narzędzi AI oraz oceny racjonalnej i etycznej, żeby ustalić, czy dany film lub obraz został zmanipulowany. Ich rola jest szczególnie istotna w obszarach takich, jak polityka (np. w czasie kampanii wyborczej), finanse czy bezpieczeństwo międzynarodowe, gdzie jeden fałszywy materiał może wyrządzić duże realne szkody. Podobnie jak w przypadku cyberbezpieczeństwa, które rozwinęło się w odpowiedzi na rosnące zagrożenia online, istotność detekcji deep fake'ów rośnie wraz z nowymi technologiami manipulacji.

Jeżeli lubisz rozwiązywać zagadki, nadążać za szybko zmieniającą się techniką i bronić wiarygodności w świecie cyfrowym, ten zawód może być dla Ciebie doskonałym wyborem.

KOMPETENCJE

Bądź na bieżąco z nowinkami

Weryfikator deep fake'ów jest profesją, która wymaga korzystania z zaawansowanych narzędzi uczenia maszynowego i sztucznej inteligencji do szczegółowej analizy treści cyfrowych pod kątem oznak manipulacji. W konsekwencji musi stale śledzić najnowsze trendy w zakresie metod fałszowania i ich detekcji. Współpracuje ze specjalistami od cyberbezpieczeństwa, tworząc i udoskonalając systemy wykrywania, które potrafią reagować błyskawicznie – często w czasie rzeczywistym lub nawet prewencyjnie. Jednym z największych wyzwań jest fakt, że to nieustanny wyścig: w miarę jak deep fake'i stają się coraz bardziej zaawansowane, narzędzia do ich wykrywania muszą za tymi technikami nadążyć.

Weryfikator stale rozwija swoje kompetencje, aktualizuje oprogramowanie i udoskonala metody pracy. Ponieważ detekcja live wymaga dużych mocy obliczeniowych, coraz większe znaczenie ma rozwój szybkich i energooszczędnych rozwiązań, w tym takich, które mogą działać bezpośrednio w urządzeniu użytkownika – czy, bardziej precyzyjnie, blisko miejsca obliczania, zgodnie z założeniami edge computingu.

Podstawowe umiejętności

Aby pracować jako weryfikator deep fake'ów, potrzebna jest solidna wiedza informatyczna, zwłaszcza z zakresu uczenia maszynowego i sztucznej inteligencji. Niezbędna będzie też znajomość języków programowania, takich jak Python, oraz umiejętność korzystania z narzędzi do deep learningu. Niezbędne jest analityczne myślenie, ponieważ wykrywanie manipulacji często polega na dostrzeganiu bardzo subtelnych szczegółów. Nie można pominąć na tej liście kryminalistyki cyfrowej, analizy metadanych oraz struktury obrazów. Niemniejsze znaczenie ma zdolność jasnego

przekazywania wyników analizy osobom spoza świata technicznego, np. menadżerom, dziennikarzom albo służbom państwowym.

Najważniejsze umiejętności twarde:

- Znajomość uczenia maszynowego – projektowanie i trenowanie modeli zdolnych do wykrywania manipulacji w obrazach, nagraniach wideo i dźwięku.
- Biegłość w językach programowania – umiejętność użycia Pythona lub C++ do budowania lub testowania systemów wykrywania.
- Doświadczenie z frameworkami deep learningowymi – praca z oprogramowaniem takim, jak TensorFlow, PyTorch czy Keras, przy tworzeniu sieci neuronowych.
- Analiza obrazu i przetwarzanie sygnałów – rozpoznawanie wzorców w obrazie i dźwięku w celu wykrycia subtelnych oznak fałszerstwa.
- Techniki informatyki śledczej – analiza metadanych i śladów kompresji w poszukiwaniu ukrytych modyfikacji.
- Znajomość aktualnych trendów – ciekawość i eksplorowanie najnowszych metod tworzenia deep fake'ów oraz sposobów ich wykrywania.
- Ograniczanie błędów systemowych (bias detection and mitigation) – rozpoznawanie i korygowanie uprzedzeń w modelach AI w celu zwiększenia ich sprawiedliwości i dokładności.

Najważniejsze umiejętności miękkie:

- Współpraca zespołowa – efektywna kooperacja z zespołami ds. cyberbezpieczeństwa, analitykami danych i badaczami.
- Szybkie rozwiązywanie problemów – reagowanie na nowe zagrożenia i zapewnianie sprawnego działania systemów.
- Myślenie krytyczne – formułowanie hipotez, testowanie ich i wyciąganie logicznych wniosków na podstawie danych.
- Komunikacja – przekładanie złożonych kwestii technicznych na język zrozumiały dla osób nietechnicznych.

Certyfikaty

Ponieważ chodzi o dziedzinę, która rozwija się wyjątkowo dynamicznie, nauka w tym obszarze nigdy się nie kończy. Pomocnym krokiem kompetencyjnym będzie zdobycie certyfikatów takich, jak np. Multimodal Deepfake Detection, które potwierdzają znajomość najnowszych technik i narzędzi. Warto także współpracować ze specjalistami z innych dziedzin – np. psychologii, medioznawstwa czy socjologii – żeby lepiej rozumieć, jak i dlaczego powstają oraz rozprzestrzeniają się konkretne typy deep fake'ów. Interdyscyplinarna perspektywa udoskonala strategię wykrywania fałszywych treści, bo wzmacnia ich wszechstronność.

ŚCIEŻKA KARIERY

Edukacja i rozwój zawodowy

Rozwój mediów syntetycznych i technologii generowania deep fake'ów stworzył pilną potrzebę pozyskiwania specjalistów, którzy potrafią wykrywać i ograniczać cyfrowe manipulacje. Weryfikator deep fake'ów to ekspert analizujący treści cyfrowe w celu ustalenia ich autentyczności, wykorzystujący połączenie sztucznej inteligencji, uczenia maszynowego, informatyki śledczej oraz wiedzy dziedzinowej. Poniżej przedstawiamy kompleksową ścieżkę edukacyjną i zawodową dla osób aspirujących do pracy w tym nowo powstającym zawodzie.

Krok 0: Wczesne zainteresowania przed podjęciem studiów

Jeszcze przed wyborem uczelni lub szkoły technicznej warto rozwijać zainteresowania w zakresie technologii, mediów lub treści wizualnych. Wielu przyszłych specjalistów zaczyna od eksperymentowania z edycją wideo, nauki podstaw programowania lub śledzenia popularnonaukowych treści o AI. Wiele uczelni i firm technologicznych oferuje bezpłatne lub niedrogie

szkolenia online, webinary i warsztaty wprowadzające w zagadnienia takie, jak edukacja medialna, dezinformacja czy treści generowane przez AI. Dobrym początkiem może być też udział w szkolnych grupach technologicznych lub aktywność w dziedzinowych społecznościach internetowych. Celem na tym etapie jest rozwinięcie ciekawości, myślenia krytycznego i nawyku uczenia się przez całe życie, czyli umiejętności, które okażą się fundamentalne w dalszej karierze.

Krok 1: Edukacja akademicka

Pierwszym krokiem jest uzyskanie tytułu licencjata. Rekomendowane specjalizacje:

- informatyka
- sztuczna inteligencja
- data science
- cyberbezpieczeństwo
- inżynieria systemów komputerowych
- dziennikarstwo.

Najważniejsze przedmioty w trakcie studiów licencjackich:

- programowanie (Python, C++)
- algorytmy i struktury danych
- wprowadzenie do uczenia maszynowego
- przetwarzanie obrazu i sygnałów cyfrowych
- podstawy cyberbezpieczeństwa
- etyka w AI i technologiach.

Warto też angażować się w akademickie projekty dotyczące rozpoznawania obrazów, modeli Generative Adversarial Network czy informatyki śledczej.

Krok 2: Specjalizacja i rozwój umiejętności

Platformy takie, jak Coursera, edX, Udacity czy DeepLearning.AI oferują praktyczne kursy projektowe. Osoby planujące karierę w zawodzie weryfikatora deep fake'ów powinny samodzielnie studiować poniższe obszary:

- modele GAN
- informatyka śledcza i analiza metadanych
- kompresja wideo i artefakty
- psychologia oszustwa i manipulacji medialnej
- nowe trendy w manipulacji z użyciem AI
- etyka AI i zasady odpowiedzialnej sztucznej inteligencji (Responsible AI).

Krok 3: Praktyczne doświadczenie

Wczesne doświadczenie zawodowe ma kluczowe znaczenie. Kandydaci powinni szukać staży lub praktyk w:

- firmach zajmujących się cyberbezpieczeństwem
- organizacjach medialnych posiadających zespoły weryfikacyjne lub fact-checkingowe
- laboratoriach badawczych
- startupach zajmujących się mediami syntetycznymi lub weryfikacją treści
- instytucjach i służbach państwowych, np. w działach bezpieczeństwa lub przestępczości internetowej.

W tego rodzaju środowiskach można współpracować z inżynierami AI, dziennikarzami, analitykami śledczymi i zespołami prawnymi, ucząc się, jak wykrywać i raportować deepfake'i w czasie rzeczywistym.

Potencjalne pierwsze stanowiska:

- młodszy analityk AI

- asystent ds. informatyki śledczej
- analityk zagrożeń cyfrowych
- specjalista ds. weryfikacji (w kontekście mediów lub cyberbezpieczeństwa).

Celem w Kroku 3 jest zdobycie praktycznych umiejętności w pracy z systemami detekcji, pogłębianie wiedzy dziedzinowej oraz rozwijanie kompetencji technicznych i komunikacyjnych.

Krok 4: Rozwój kariery i uczenie się przez całe życie

Technologie deep fake'ów ewoluują niezwykle szybko, dlatego stałe kształcenie się nie jest opcjonalne. Profesjonaliści powinni:

- uczestniczyć w konferencjach takich, jak DEF CON, Black Hat, czy CVPR
- prenumerować czasopisma branżowe, np. Journal of Digital Forensics lub Security and Law
- brać udział w zaawansowanych kursach z zakresu edge computingu, przetwarzania AI w czasie rzeczywistym i wyjaśnialnej sztucznej inteligencji (Explainable AI)
- śledzić dyskusje o etyce AI, prowadzone przez organizacje w rodzaju Montreal AI Ethics Institute czy World Economic Forum
- rozważyć zdobycie stopnia naukowego.

Ukończenie studiów magisterskich lub doktoranckich w dziedzinie uczenia maszynowego, wizji komputerowej czy informatyki śledczej może znacząco przyspieszyć rozwój kariery, zwłaszcza w przypadku osób aspirujących do ról badawczych, kierowniczych lub akademickich.

GŁÓWNE OBOWIĄZKI

W poszukiwaniu śladów manipulacji

Zakres obowiązków weryfikatora deep fake'ów obejmuje techniczne wykrywanie fałszerstw, rozwój systemów detekcji, ocenę ryzyka oraz współpracę interdyscyplinarną. Ta rola wymaga nie tylko zaawansowanych umiejętności analitycznych, lecz też stałego dostosowywania się do nowych form cyfrowych manipulacji.

Wykrywanie i analiza mediów syntetycznych

Specjalista wykorzystuje algorytmy uczenia maszynowego, narzędzia informatyki śledczej oraz techniki rozpoznawania wzorców, aby zidentyfikować anomalie sugerujące ingerencję w materiał. Chodzi o wykrywanie niespójności w oświetleniu, mimice twarzy, modulacji głosu oraz o wychwytywanie artefaktów kompresji.

Tworzenie i optymalizacja systemów detekcji

Konieczne jest trenowanie modeli uczenia maszynowego na zestawach danych zawierających materiały autentyczne i zmanipulowane, w celu zwiększenia dokładności i efektywności detekcji. Weryfikatorzy uczestniczą w tworzeniu systemów wykrywania w czasie rzeczywistym, które muszą łączyć szybkość działania z niskimi kosztami obliczania.

Ocena ryzyka i raportowanie wyników

Weryfikatorzy deep fake'ów oceniają potencjalny wpływ wykrytych manipulacji, zwłaszcza w takich obszarach, jak media, polityka i finanse. Przygotowują szczegółowe raporty opisujące zastosowane metody, poziomy pewności i konsekwencje ustaleń. Raporty muszą być zrozumiałe zarówno dla ekspertów technicznych, jak i osób spoza branży. Weryfikatorzy

doradzają również w zakresie strategii ograniczania skutków manipulacji oraz zasad komunikacji w sytuacjach, gdy spreparowane treści mogą wyrządzić znaczne szkody publiczne.

Współpraca z zespołami interdyscyplinarnymi

Weryfikacja deep fake'ów rzadko odbywa się w izolacji. Weryfikatorzy współpracują z zespołami ds. cyberbezpieczeństwa, dziennikarzami, ekspertami prawnymi i etykami, żeby zapewnić właściwą interpretację i wykorzystanie wyników ich analiz. Praca specjalistów wspiera szersze strategie walki z dezinformacją i oszustwami cyfrowymi, przez integrowanie procesów weryfikacyjnych z procedurami organizacyjnymi.

PODOBNE ZAWODY

Rynek potrzebuje weryfikacji treści

Pojawienie się weryfikacji deep fake'ów jako odrębnej roli zawodowej jest powiązane z trendami widocznymi w pokrewnych profesjach. W podobnych specjalizacjach wyraźnie widać, że rynek szuka kompetencji w zakresie sprawdzania treści, etyki AI oraz informatyki śledczej. A to obszary podstawowe także dla weryfikatora deep fake'ów. Analiza zbliżonych ról pozwala przewidywać, jak dziedzina weryfikacji sztucznych treści będzie się kształtowała w najbliższych latach.

- Analitik informatyki śledczej – bada przestępstwa cybernetyczne, odzyskując i analizując dane z komputerów, sieci i urządzeń pamięci cyfrowej. Często zajmuje się zmanipulowanymi treściami i pomaga w procesach sądowych lub postępowaniach korporacyjnych.
- Analitik integralności mediów – w organizacjach medialnych i firmach technologicznych odpowiada za wykrywanie zmanipulowanych lub wprowadzających w błąd treści, zanim

rozprzestrzenią się w sieci. Wykorzystuje narzędzia śledcze i modele AI do badania obrazów, filmów i dźwięku.

- Specjalista ds. zaufania i bezpieczeństwa - w dużych firmach technologicznych opracowuje polityki oraz prowadzi postępowania w celu usuwania szkodliwych, fałszywych lub zmanipulowanych treści. Monitoruje pojawiające się zagrożenia, w tym deep fake'i i kampanie dezinformacyjne.
- Analitik cyberzagrożeń - skupia się na wykrywaniu i łagodzeniu zagrożeń cyfrowych, w tym syntetycznych mediów używanych do phishingu, oszustw lub ataków socjotechnicznych.
- Specjalista ds. etyki AI - zapewnia, że systemy sztucznej inteligencji, w tym te wykrywające lub tworzące treści syntetyczne, są rozwijane lub wdrażane odpowiedzialnie.
- Analitik OSINT (Open Source Intelligence) - gromadzi, weryfikuje i interpretuje publicznie dostępne informacje, w tym treści z mediów społecznościowych (teksty, filmy i obrazy).
- Analitik ds. zapobiegania oszustwom - w bankowości i ubezpieczeniach bada interakcje cyfrowe i treści w celu wykrycia manipulacji, fałszerstw lub kradzieży tożsamości.
- Badacz dezinformacji - skupia się na mechanizmach powstawania i rozprzestrzeniania fałszywych narracji, w tym manipulacji politycznych wspieranych deep fake'ami.
- Inżynier uczenia maszynowego (o specjalizacji: informatyka śledcza) - projektuje i szkoli modele uczenia maszynowego, które wykrywają anomalie w treściach cyfrowych.
- Moderator treści (o specjalizacji: zmanipulowane treści) - przegląda oznaczone treści pod kątem autentyczności i zgodności ze standardami oraz wspiera systemy AI wykrywające treści syntetyczne.

PODSUMOWANIE

Rola weryfikatora deep fake'ów z dużym prawdopodobieństwem stanie się jednym z najważniejszych nowych zawodów w nadchodzących latach. W miarę jak środowiska cyfrowe stają się bardziej immersyjne, a media syntetyczne – realistyczne, coraz trudniej będzie odróżnić, co jest prawdziwe, a co nie. Mentalność "zero-trust", czyli nawyk domyślnego kwestionowania autentyczności treści cyfrowych, stanie się kluczową umiejętnością, zarówno u ekspertów, jak i u zwykłych użytkowników internetu.

Ważnym tłem jest fakt, że dezinformacja została sklasyfikowana jako jedno z największych globalnych ryzyk już w 2024 roku, a deepfake'i uznaje się za jedno z najgroźniejszych zastosowań AI. Podobnie, jak ma to miejsce od dość dawna w cyberbezpieczeństwie, na polu weryfikacji treści będziemy mieli do czynienia z nieustanną rywalizacją pomiędzy tymi, którzy tworzą deepfake'i, a tymi, którzy je badają i ujawniają manipulacje. W przyszłości weryfikacja deep fake'ów zapewne podejmie klasyczne wyzwanie kryminalistyki: „czy potrafimy być nie jeden krok za oszustami, ale o krok przed nimi?” Być może to dobre wyzwanie właśnie dla Ciebie...

ŹRÓDŁA:

- montreal.ethics.ai/the-state-of-ai-ethics-report/
- <https://www.weforum.org/stories/2024/02/4-ways-to-future-proof-against-deepfakes-in-2024-and-beyond/>
- weforum.org/reports/jobs-of-tomorrow-mapping-opportunity-in-the-new-economy/
- www.coursera.org/specializations/deep-learning
- ainowinstitute.org/
- rand.org/pubs/research_reports/RR4431.html
- nll.ai
- <https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes>