

TWOJE BEZPIECZEŃSTWO

W ŚWIECIE CYBER

I AI

Część 2
Cyberhigiena

od kuchni

Wydanie 2
2025r.

NOTA WYDAWCY

Wszelkie prawa do zawartości tej książki są zastrzeżone. Nieautoryzowane przez autora i/lub wydawnictwo poswojsku.pl rozpowszechnianie całości lub dowolnego fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonanie kopii jakąkolwiek z dostępnych metod (między innymi: elektroniczną, kserograficzną, fotograficzną) spowoduje naruszenie praw autorskich niniejszego dzieła.

OD AUTORA:

Pamiętaj proszę- uszanuj zaangażowanie oraz godziny pracy, które spędziłem nad napisaniem oraz opracowaniem książki: Twoje bezpieczeństwo w świecie cyber i AI – używaj tylko legalnie kupiony ebook.

Wydawnictwo poswojsku.pl:

1. dołożyło wszelkich starań, by zawarte w tej książce informacje były kompletne, poprawne oraz rzetelne,
2. nie ponosi żadnej odpowiedzialności za ewentualne szkody, które mogą wyniknąć z wykorzystania informacji zawartych w tej książce.

Wydawnictwo poswojsku.pl – kontakt:

Strona firmowa: www.poswojsku.pl

e-mail: marketing@poswojsku.pl

ul. Paprocka 86, 98–220 Zduńska Wola

ISBN: 978-83-68360-05-9

Copyright © poswojsku.pl 2025

Autor: Gołębiowski Dariusz

TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I AI

CZĘŚĆ 2 CYBERHIGIENA

Autor: Dariusz Gołębiowski

98-220 Zduńska Wola, ul. Paprocka 86, www.gddm.com.pl,
biuro@gddm.com.pl



Szanowny Kliencie,

Wykryliśmy nietypowe połączenie z adresu IP 217.28.147.88.

Co powinieneś zrobić?

Postępuj zgodnie z instrukcjami, klikając poniższy przycisk, aby

Uwaga: Jeśli weryfikacja nie zostanie przeprowadzona w ciągu celów oszustwa.

[Zaloguj się](#)

SPIS TREŚCI

NOTA WYDAWCY	str. 1
SPIS TREŚCI	str. 4
OD AUTORA	str. 6
WPROWADZENIE	str. 11
ROZDZIAŁ 1 PODSTAWOWE ZASADY CYBERHIGIENY	str. 17

Jak rozpoznać, że jesteś ofiarą Cyberataku

Systematyczne szkolenia - profilaktyka cyberbezpieczeństwa

Cyberhigiena - Twój cyfrowy zestaw przetrwania

Metody nieautoryzowanego pozyskania danych - przykłady

Bezpiecznie przetwarzanie danych: szyfrowanie,
przechowywanie, udostępnianie, komunikacja

Czy AI złamie wszystkie nasze hasła?

ROZDZIAŁ 2 NAJCZĘSTSZE CYBERZAGROŻENIA str. 82

Kwestie personalno-mentalnościowe ludzi

Ataki socjotechniczne – charakterystyka

Phishing i jego odmiany

AI – wirtuoz phishingu „czytający nasze zachowania”

Fałszywe strony internetowe

Używanie otwartych sieci WiFi

Złośliwe oprogramowanie - rodzaje, nazewnictwo, opis
przykładowych zagrożeń

PODSUMOWANIE **str. 199**

PRAWA AUTORSKIE I ZNAKI TOWAROWE **str. 206**

OD AUTORA

Witam serdecznie – Ciebie - droga Czytelniczko, wspaniały Czytelniku - w najnowszej wersji poradnika "Twoje bezpieczeństwo w świecie cyber i AI: Część 2 – Cyberhigiena." Ten ebook to drugie wydanie tej pozycji wydawniczej - poprawione i zaktualizowane. Dzięki temu jest zdecydowanie bardziej adekwatny do stanu wiedzy datowanej na 2025 rok. Pisząc go zakładałem, że Ty Czytelniku/czko zapoznałeś/aś się z: "Twoje bezpieczeństwo w świecie cyber i AI: Część 1 – Wprowadzenie" i już ogarniasz obszary:

- fundamenty wiedzy o cyberbezpieczeństwie,*
- bezpieczeństwo a programy komputerowe (systemy operacyjne, przeglądarki internetowe.*

Z tą wiedzą będzie łatwiej zrozumieć wiedzę zawartą w tej części mojej serii poradników.

W obecnym świecie, w którym technologia rozwija się bardzo szybko, kwestia bezpieczeństwa w niezmiernie cyberprzestrzeni staje się równie ważna, jak nasze bezpieczeństwo fizyczne. Wirtualne zagrożenia, z którymi się mierzymy – od wyrafinowanych ataków phishingowych po złośliwe oprogramowanie – wymagają od nas nie tylko zaawansowanych narzędzi obronnych, ale również podstawowej wiedzy, w tym z zakresu tzw. *higieny cyfrowej*.

W tej części skupimy się na praktycznych aspektach cyberhigieny. Zaczniemy od metod rozpoznawania, czy padłeś/aś ofiarą cyberataku. Oczywiście mam na myśli Twoje urządzenia, typu komputer stacjonarny, smartfon, tablet, itd. Zagłębimy się także w profilaktykę cyberbezpieczeństwa, aż po metody ochrony przed coraz to nowszymi zagrożeniami. Wyjaśnię także, jak Twoje dane oraz Twoich bliskich, mogą być pozyskiwane w nieautoryzowany sposób.

💡 Wspólnie rozważymy zagadnienie bezpiecznych połączeń oraz przetwarzania informacji. Zastanowimy się również nad przyszłością bezpieczeństwa naszych haseł w erze sztucznej inteligencji.

Zdjęcie przedstawia wirtualne zagrożenia oraz zabezpieczenia na tle naszego wspaniałego świata rzeczywistego. Grafika została wygenerowana przy dużym udziale AI.



Ten poradnik to także pogłębienie wiedzy o najczęściej występujących cyberzagrożeniach. Odkryjemy ludzkie aspekty stojące za atakami socjotechnicznymi, zrozumiemy mechanizmy stojące za phishingiem oraz zobaczymy, że AI staje się narzędziem w rękach cyberprzestępców.

Moim celem jest wyposażenie Ciebie w wiedzę, dzięki której będziesz bezpiecznie poruszać się w cyfrowym świecie, z pełną świadomością i kontrolą nad własnymi danymi. Niech ten poradnik będzie Twoją tarczą w codziennej interakcji z cyfrową technologią – otaczającą nas dookoła.

Zapraszam do lektury i odkrywania zasad cyberhigieny, które mają za zadanie chronić Twoje cyfrowe "ja".

Do zobaczenia w świecie, gdzie bezpieczeństwo i technologia, w tym sztuczna inteligencja - idą ze sobą ramię w ramię, wspólnie dbając o Twoje bezpieczeństwo.

Dariusz Gołębiowski – Autor poradnika

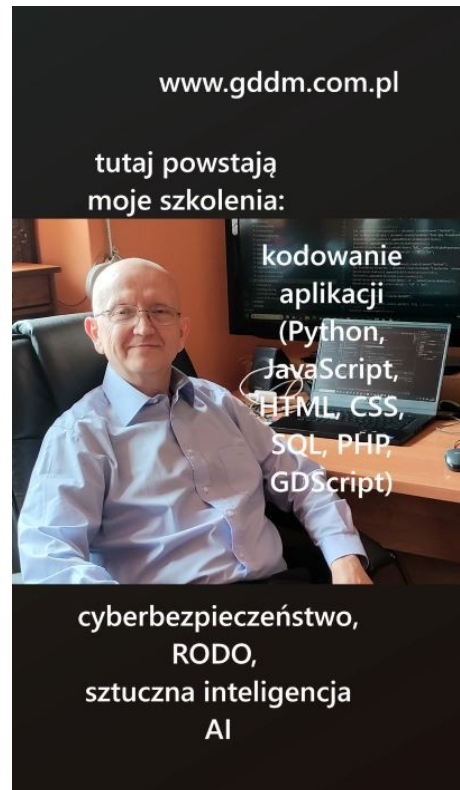
Autor: Dariusz Gołębiowski - www.gddm.com.pl

Zdjęcie – Autor niniejszego poradnika w biurze,
podczas: pisania, kodowania i rozmyślenia ;).

Serdecznie zapraszam do kontaktu.

Znajdziesz mnie bez problemu
poprzez Wydawnictwo poswojsku.pl,
moją stronę [www](http://www.gddm.com.pl), ale także na
popularnych portalach
społecznościowych, m.in.: Facebook,
LinkedIn, [youtube.com/@poswojsku](https://www.youtube.com/@poswojsku) .
Gdybyś szukał/a szkoleń tradycyjnych
czy też on-line dla Ciebie i/lub Twojej
organizacji z omawianych tutaj
tematów - serdecznie zapraszam do
skorzystania z moich usług ;):
www.gddm.com.pl – wspaniale, bo ze
mną - profesjonalne szkolenia oraz
doradztwo z zakresu -

cyberbezpieczeństwo, AI, RODO, programowanie (m.in.: Python,
JavaScript, HTML, CSS, SQL).



WPROWADZENIE



Czy można połączyć cyberhigienę z gotowaniem? Oczywiście, że tak! W końcu zarówno w kuchni, jak i w świecie cyfrowym **zasady (szczególnie związane z czystością 😊) są kluczowe**. A ja, jako osoba, która przepisy - uwielbia tworzyć i stosować (co możecie zobaczyć na moim kanale YT @poswojsku), wiem o tym doskonale.

Przykład? **Cyberbezpieczeństwo to jak przepis na dobre pierogi**. Jeśli:

- masz porządne składniki (odpowiednik w cyberhigienie - silne hasła),
- dobrze wyrobiłeś/aś ciasto (odpowiednik w cyberhigienie - regularne aktualizacje),
- nie dajesz się oszukać podejrzanym „domowym” farszom (odpowiednik w cyberhigienie - phishing i fałszywe strony),




to wszystko powinno wyjść znakomicie, czyli **bardzo smacznie i bezpiecznie 😊** !

Ale jeżeli zignorujesz podstawowe zasady... cóż, zamiast smacznej uczyty możesz skończyć z katastrofą w kuchni, albo zhakowanym komputerem w sieci.

Właśnie dlatego powstał ten poradnik – **żebyś nie serwował w swoim cyfrowym życiu żadnych „zatrutych potraw”**. Moim celem jest pokazanie właśnie Tobie, że cyberhygiena to nie jakiś nudny wykład o hasłach i wirusach, tylko **praktyczna wiedza, którą możesz (i powinieneś/naś!) stosować na co dzień**. A wówczas możesz zostać superbohaterem lub superbohaterką cyfrowego imperium.



Co znajdziesz w środku tego poradnika?

-  Jak rozpoznać, że właśnie stałeś/aś się 😊 cyfrowym „obiadem” dla hakerów .
-  Jak sprawić, żeby Twoje dane były lepiej zabezpieczone niż przepis na sekretny sos babci.
-  Czy sztuczna inteligencja to nowoczesny kucharz ułatwiający życie, czy może szef kuchni rodem z horroru, który już wie, co chcesz zamówić, zanim jeszcze otworzysz menu?

Każdy rozdział to **przystępne, często pełne humoru oraz konkretnych przykładów wskazówki**, które pomogą właśnie Tobie - uniknąć cyfrowych pułapek i cieszyć się bezpiecznym korzystaniem z internetu. Ale spokojnie, jeżeli humoru nie lubisz, nie ma sprawy, aż tak dużo to go tutaj nie ma. Bo najważniejsza jest przecież wiedza zawarta w tym poradniku.

Na kolejnych stronach znajdziesz informacje dotyczące tego, jak nie dać się nabrać na phishing (bo internetowi oszuści to tacy „kelnerzy”, którzy podają Ci danie z haczykiem).

A czy wiesz dlaczego publiczne, otwarte WiFi jest jak **jedzenie sushi w losowym barze przy autostradzie – może być spoko, ale może się też skończyć problemami...** 🌿 💻 I to nie tylko gastrycznymi - no chyba, że z żalu za zhakowanym kontem społecznościowym 😊.

Zadbam też o Twój **cyfrowy lodówko-zamrażalnik**, czyli kopie zapasowe. Jeśli jeszcze nigdy nie straciłeś/aś ważnych plików, to gratuluję, ale uwierz mi, lepiej mieć backup niż nadzieję, że „może jakoś, coś się odzyska”.

Na koniec dowiesz się, jak **mądrze zarządzać swoimi „cyfrowymi składnikami”**, czyli hasłami, aplikacjami i danymi, żeby przypadkiem nie zostawić otwartego konta bankowego tak, jak nie zostawiłbyś gotującego się rosółu na gazie - bez kontroli 🌟 🔥.

💡 Podsumujmy:

cyberhigiena to nic innego jak przepis na życie w sieci bez niestrawności! Czy ta definicja przypadła Tobie do gustu? Mam nadzieję, że tak, no bo kto nie lubi smacznie zjeść?

A jeśli dotrwasz do końca poradnika, to mam głębokie przekonanie, że będziesz lepiej przygotowany/na na cyberzagrożenia niż kucharz na kontrolę sanepidu.

Zatem:

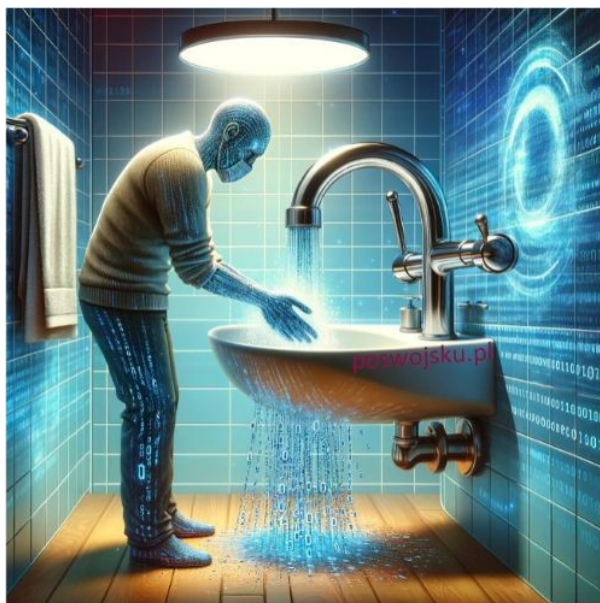
- ***fartuch na siebie, myjemy ręce i.. zaczynamy przygodę w kuchni!*** 🍴🔒🚀
- ***zaktualizuj system, włącz systemy antywirusowe oraz firewall'a i.. zaczynamy przygodę w cyberświecie!*** 🍴🔒🚀

ROZDZIAŁ 1

PODSTAWOWE

ZASADY

CYBERHIGIENY



Wizualizacja:

Cyberhigiena jako codzienne czynności higieniczne człowieka

Analogicznie jak na powyższym zdjęciu powinieneś/nnaś wyobrażać sobie cyberhigienę twojego cyfrowego życia.

Gdy systematycznie stosujesz zasady cyberhigieny, to istnieje mniejsze prawdopodobieństwo, że zachorujesz na jakiegoś wirusa :).

Jak rozpoznać, że jesteś ofiara Cyberataku



Zaczynamy naukę cyberhigieny od ataku hakerskiego na Twój komputer (smartfon, tablet, laptop, itp.). Cóż, ciesz się, że nie na Twoją kuchenkę gazową 😊. Zapewne się zastanawiasz jakie mogą być oznaki, że zostałeś/aś zaatakowany/a?

Wiele osób wyobraża sobie ten stan rzeczy jako niedziałający komputer czy jakieś wyskakujące informacje typu: HACKED. Tak, może tak być. Ale tego typu oznaki są charakterystyczne już dla końcowego etapu bycia zhakowanym, czyli dzieje się tak w trakcie przejścia naszego urządzenia przez tak zwanego haker nieetycznego. Ale zanim do tego dojdzie zwykle możesz mieć do czynienia z innymi oznakami. Mniej czytelnymi, ale za to występującymi na takim etapie, który daje jeszcze nadzieję na skuteczne popsucie zabawy internetowemu przestępcy. Pozwól, że opiszę analogię z dziedziny medycyny - profilaktyki zdrowia człowieka i potencjalnych skutków dla skutecznego wyleczenia, bądź .. no, wiesz zapewne co mam na myśli dla osób zbyt chorych na pomoc :(.

Profilaktyka zdrowia człowieka

Wyobraź sobie u jakiegoś człowieka poważną chorobę, dla przykładu: nowotwór. Jeżeli lekarz wykryje u pacjenta nowotwór w początkowej fazie ataku na ludzki organizm, istnieje duże prawdopodobieństwo całkowitego wyleczenia. Ale jeżeli nowotwór zostanie wykryty, gdy już nawet wizualnie widać, że pacjent jest ciężko chory, może być za późno na skuteczne leczenie i całkowite wyleczenie.

Podobnie może być z Twoim urządzeniem IT:


zagrożenie szybko wykryte - może da się usunąć
ransomware na Twoim komputerze - oznacza konieczność
reinstalacji całego systemu operacyjnego, utratę danych
ewentualnie zapłacenie dużego okupu.

Zatem do rzeczy - możemy mówić o dwóch rodzajach oznak istnienia zagrożenia - wewnątrz Twojego komputera: jawnych i niejawnych. Zatem pozwól, że krótko scharakteryzuję obydwie grupy zagrożeń.

Zagrożenia Jawne

Doprecyzowując myśl z poprzedniej strony - zagrożenia nie są w całym komputerze, tylko - najczęściej - w systemie operacyjnym (Windows, Android, Linux, iOS, itp.). W tego rodzaju przypadkach, może pojawić się na ekranie komputera:

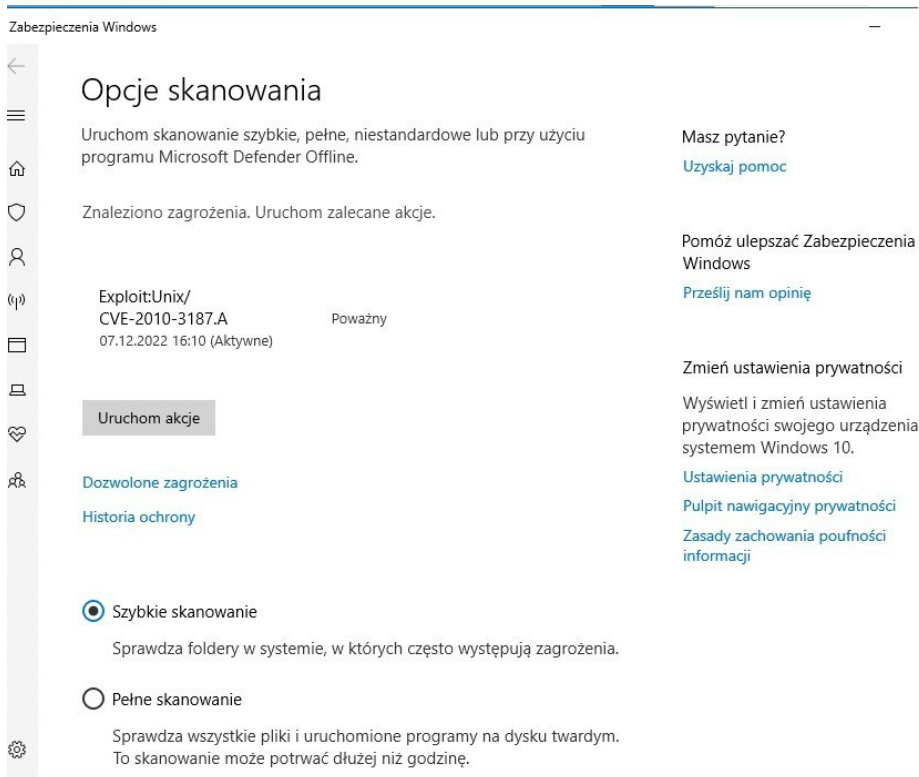
- **Informacja od zabezpieczeń systemowych** posiadanych w komputerze – np. programu antywirusowego, że został znaleziony wirus.

 **Pamiętaj!** Aby znaleźć wirusa trzeba zwykle wykonać działanie – skanowanie komputera (twardego dysku, folderów, plików, itp.).

Czasami niektóre programy działają jak dobry kucharz – same wyłapują „zepsute składniki” (czytaj: wirusy) ukryte na Twoich dyskach. 🍷 🔍 Jednak w większości przypadków to Ty musisz wziąć sprawy w swoje ręce, włączyć cyfrowy „przeгляд lodówki” i zdecydować, co zrobić z wykrytymi nieświeżymi plikami. Wyrzucić? Zamrozić w kwarantannie? A może przyprawić i sprawdzić, czy da się jeszcze coś uratować? Decyzja należy do Ciebie! 😊 🧑🏻💻 🖥️



*Poniższe zdjęcie przedstawia:
Defaultowy program antywirusowy znalazł zagrożenie. Teraz
użytkownik będzie musiał kliknąć właściwy przycisk:
„Uruchom akcje” i podjąć decyzję co dalej:
usunąć zagrożenie czy może skierować zagrożenie do
kwarantanny?*



- **Informacje od potencjalnych napastników**

Na przykład, że został zainstalowany w naszym sprzęcie IT tzw. ransomware, czy też inne zagrożenie cyfrowe.

**SERDECZNIE ZAPRASZAM
DO NABYCIA PEŁNEJ
WERSJI TEGO EBOOKA -
POLECAM:**

AUTOR - DARIUSZ GOŁĘBIOWSKI

Cyberhigiena to nie jednorazowa akcja, ale **codzienny nawyk** – jak mycie rąk po wyjściu z toalety. Jeśli nie chcesz, żeby Twój komputer (albo konto bankowe) zostały „zainfekowane”, stosuj te zasady regularnie.

A teraz idź i szerz tę wiedzę dalej! Bo w cyfrowym świecie każdy bezpieczny użytkownik to mniejsza szansa, że internet zamieni się w postapokaliptyczną krainę pełną oszustów i wirusów.

Dbaj o siebie, **swoje dane i swoje hasła** – i pamiętaj:
świadomy użytkownik to najlepsza zaporę przed cyberzagrożeniami! 🔥🔒

Do zobaczenia po bezpiecznej stronie internetu! 🚀😊

W poradniku wykorzystano:

- własne materiały graficzne,
- prace: Chat GPT4 - zdjęcia,
- cliparty z programu LibreOffice na licencji CC0.

DZIĘKUJĘ ZA UWAGĘ

Autor poradnika: DARIUSZ GOŁĘBIOWSKI

Zapraszam do zapoznania się z innymi książkami, które napisałem lub współtworzyłem, m.in.:

Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji (seria ebooków - poradników):

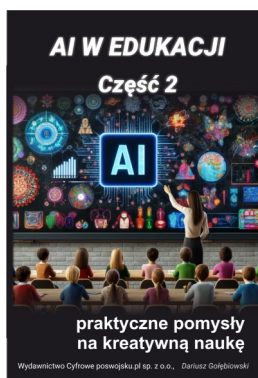
- Część 1 Wprowadzenie
- Część 2 Cyberhigiena
- Część 3 Dziecko i Ty
- Część 4 Sposoby ochrony przed cyber zagrożeniami

SZYFROWANIE BEZPIECZEŃSTWO KRYPTOGRAFIA: CZĘŚĆ 1

Podstawowe pojęcia i koncepcje

CHROŃ I ROZWIJAJ BIZNES- CYBER AI Część 1

Wykorzystanie AI w bezpieczeństwie



AI w edukacji

- Część 1 Praktyczny poradnik nie tylko dla nauczycieli
- Część 2 Praktyczne pomysły na kreatywną edukację

Stwórz Grę Mobilną wydanie 2

NATURALNE ZASADY ŻYCIA Magowie, Hermonianie, Ludzie:

- * TOM I SIÓDMA PLANETA Galaktyki A Ludzie
- * TOM II ZIEMIA Powrót Władcy Magii

Więcej informacji znajdziesz na stronach firmy:

Wydawnictwo Cyfrowe poswojsku.pl , www.poswojsku.pl

Prawa autorskie i znaki towarowe

Wszystkie wymienione nazwy firm, produktów, usług i logo są znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich właścicieli. Nazwy te są używane wyłącznie w celach informacyjnych i nie implikują poparcia ani związku z tymi markami.

Microsoft i **Windows** są zarejestrowanymi znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i/lub innych krajach.

Apple, **iOS** i **macOS** są zarejestrowanymi znakami towarowymi firmy Apple Inc. w Stanach Zjednoczonych i/lub innych krajach.

Android jest zarejestrowanym znakiem towarowym firmy Google LLC.

HarmonyOS jest zarejestrowanym znakiem towarowym firmy Huawei Technologies Co., Ltd.

VirtualBox jest zarejestrowanym znakiem towarowym firmy Oracle Corporation.

Linux jest zarejestrowanym znakiem towarowym Linusa Torvaldsa.

Firefox jest zarejestrowanym znakiem towarowym Mozilla Foundation.

Haiku OS jest zarejestrowanym znakiem towarowym Haiku, Inc.

DuckDuckGo jest zarejestrowanym znakiem towarowym firmy Duck Duck Go, Inc.

Inne wymienione nazwy firm, produktów i usług mogą być znakami towarowymi odpowiednich właścicieli.