TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I AI

KSC - NIS 2

Część 2
Cyberhigiena

Wydanie 3 aktualizacja 2026

Gołębiowski Dariusz
Audytor Wiodący Systemu Bezpieczeństwa Informacji ISO 27001

Wydawnictwo: poswojsku.pl sp. z o.o.

NOTA WYDAWCY

OD AUTORA:

Pamiętaj proszę - uszanuj zaangażowanie oraz godziny pracy, które spędziłem nad napisaniem oraz opracowaniem książki: Twoje bezpieczeństwo w świecie cyber i AI Część 2 Cyberhigiena – używaj tylko leganie 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: 978-83-68360-23-3

Autor: Gołębiowski Dariusz

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

TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I AI

CZĘŚĆ 2 CYBERHIGIENA

Autor poradnika:

Dariusz Gołębiowski

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001:

szkoli, doradza, wdraża i porządkuje obszary cyberbezpieczeństwa, RODO i ryzyka informacyjnego oraz.. pisze ciekawe poradniki :).

Kontakt do Autora:

www.gddm.com.pl

biuro@gddm.com.pl

SPIS TREŚCI

Spis treści

OD AUTORA

Witam Ciebie serdecznie - droga Czytelniczko, wspaniały Czytelniku - w najnowszej wersji poradnika "Twoje bezpieczeństwo w świecie cyber i AI: Część 2 – Cyberhigiena." Ten ebook to już trzecie wydanie tego w pewnym sensie legendarnego ebooka - poprawionego i zaktualizowanego.

Dzięki temu jest zdecydowanie bardziej adekwatny do stanu wiedzy datowanej na 2026 rok. Pamiętaj, że ten poradnik jest tworzony z myślą, iż Ty Czytelniku/czko znasz podstawowe zagadnienia związane z cyberbezpieczeństwem. Jeżeli nie – zapraszam do mojego ebooka: "Twoje bezpieczeństwo w świecie cyber i AI: Część 1 Wprowadzenie Wydanie 3". Dzięki temu ogarniesz obszary:

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

Z tą wiedzą będzie łatwiej zrozumieć zawartość tej części mojej serii poradników.

W obecnym świecie technologia rozwija się bardzo szybko, a kwestia bezpieczeństwa w niezmierzonej 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 podstawowe metody ochrony przed coraz to nowszymi zagrożeniami cyfrowymi. 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, poznamy mechanizmy stojące za phishingiem oraz zobaczymy, że AI staje się narzędziem w rękach cyberprzestępców.

Moim celem jest wyposażenie Ciebie w wiedzę, dzięki której będziesz bezpieczne 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. Aby łatwiej zrozumieć omawiane zagadnienia - część z nich przedstawię w odniesieniu do kulinariów (więcej w dziale: Wprowadzenie).

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

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

Serdecznie zapraszam do kontaktu. Znajdziesz mnie bez problemu poprzez WydawnictwonCyfrowe poswojsku.pl, moją stronę www, ale także na popularnych portalach społecznościowych, m.in.: Facebook, LinkedIn, 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 ;): gddm.com.pl – są wspaniałe, 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 uczty ***możesz skończyć z katastrofą w kuchni***, albo ***zhakowanym komputerem w sieci***.

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 IT 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 rosołu na gazie - bez kontroli 💥🔥.

💡 **Podsumujmy:**

cyberhigiena to nic innego jak przepis na życie w sieci bez niestrawności!

Czy powyższa 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 operacyjny, 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 ofiarą Cyberataku

Zaczynamy naukę cyberhigieny od **ataku hakerskiego na Twój komputer** (smartfon, tablet, laptop, itp.). 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 przejęcia 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 tą chorobę w początkowej fazie ataku na ludzki organizm, istnieje duże prawdopodobieństwo całkowitego wyleczenia. Ale jeżeli nowotwór zostanie wykryty w zaawansowanej formie, może być za późno na skuteczne leczenie.

💡 **Podobnie jest z Twoim urządzeniem IT:**

gdy zagrożenie szybko wykryte - może da się usunąć

ale **jak znajdzie się ransomware na Twoim komputerze** - oznacza to konieczność reinstalacji całego systemu operacyjnego i pozostałych aplikacji, utratę lub odzyskanie danych - ewentualnie zapłacenie dużego okupu.

Zatem do rzeczy - możemy mówić o dwóch rodzajach ***oznak istnienia zagrożenia - wewnątrz Twojego komputera***: ***jawnych*** i ***niejawnych***.

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.

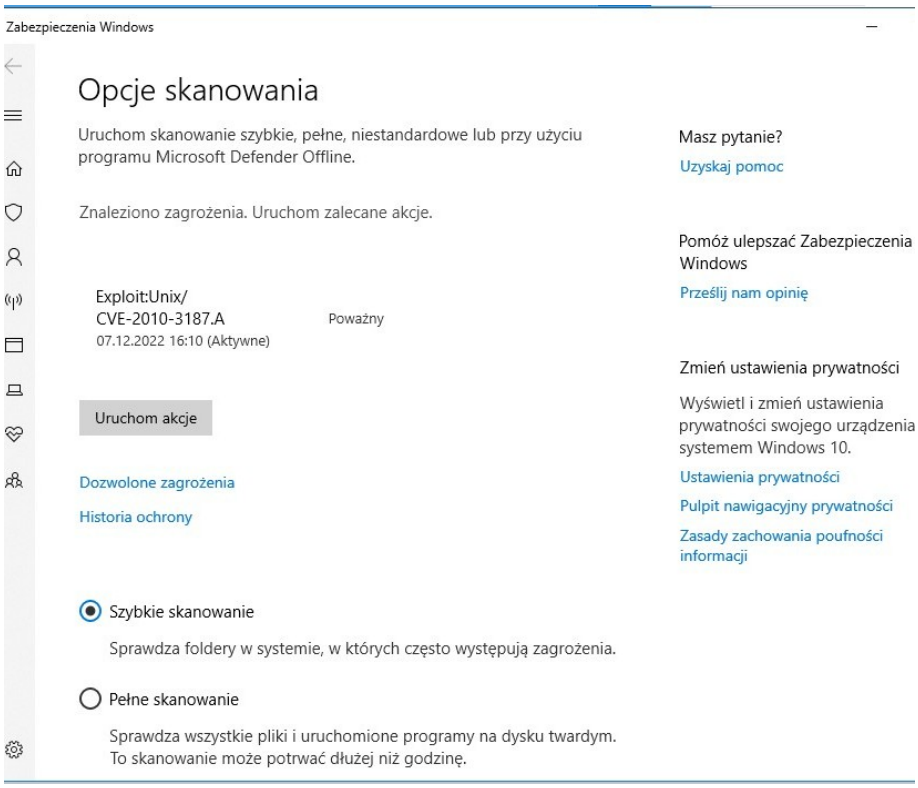
💡 **Pamiętaj! Aby znaleźć wirusa trzeba zwykle wykonać działanie – skanowanie komputera (twardego dysku, folderów, plików, itp.).**

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 „przegląd 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 Twoim sprzęcie IT tzw. ransomware, czy też inne zagrożenie cyfrowe.

  Tutaj może od razu pojawić się żądanie okupu w zamian za usunięcie zagrożenia. W tym przypadku komputer zapewne jest już zablokowany. Możesz jedynie zainstalować od nowa system operacyjny, a potem zgrać dane z kopii zapasowej, o ile ją posiadasz.

  Alternatywnym rozwiązaniem (nie polecam) jest ***podjęcie negocjacji z przestępcami w kwestii odblokowania Twojego sprzętu***. Niestety raczej nie jest to możliwe bez ***zapłaty okupu***.

  Co do zasady "z terrorystami się nie negocjuje", ale niestety co roku firmy i osoby fizyczne płacą (z różnych powodów) co najmniej miliardy dolarów różnego rodzaju okupów dla nieetycznych hakerów.

Zagrożenia Niejawne

W tym przypadku coś dziwnego dzieje się z naszym komputerem, ale nie ma żadnego jawnego komunikatu. Nawet nasze oprogramowanie antywirusowe po wykonanym skanowaniu - zupełnie milczy. Takie sygnały mogą być różnorodne. Do Ciebie należy zachować należytą uwagę i ostrożność w trakcie użytkowania Twojego urządzenia IT.

Sygnały niejawne mogące świadczyć, że właśnie w tej chwili jesteś ofiarą ataku hakerskiego mogą być bardzo różne. Na przykład:

- komputer działa wolniej i/lub często się zawiesza (jak na zdjęciu obok),
- na ekranie pojawiają się dziwne komunikaty, dla przykładu: reklamy jakiegoś produktu, czy strony internetowej,
- na pulpicie Twojego systemu operacyjnego zostały stworzone nowe ikony, a Ty zupełnie nie wiesz skąd się wzięły,
- przeglądarka uruchamia się sama i/lub po jej włączeniu od razu przekierowuje na nieznaną Tobie stronę,
- zmieniła się struktura folderów w posiadanym systemie operacyjnym, powstały nowe foldery czy pliki - bez Twojej wiedzy i/lub zgody,

- przeglądarka ma inny wygląd, np. powstały nowe, nieznane Tobie paski narzędzi, masz wrażenie jakby to nie była Twoja przeglądarka (nie pomyl tego z nową wersją oprogramowania, zmieniającą jego wygląd – o zainstalowaniu nowej wersji, zwykle użytkownik jest informowany stosownym komunikatem),
- reklamy internetowe (w przeglądarkach czy nawet na portalach społecznościowych) nie są dopasowane do Twoich wyszukiwań oraz przyzwyczajeń, całkiem jakby ktoś inny prowadził wyszukiwania na Twoim sprzęcie komputerowym i jego oprogramowaniu.

Wyżej wymienione objawy, zapewne nie są wszystkimi możliwymi, a Ty jako odpowiedzialny użytkownik/czka komputera (stacjonarnego, laptopa, czy też urządzenia mobilnego) powinieneś/nnaś systematycznie analizować, czy danego dnia, wszystko w Twoim sprzęcie działa podobnie jak w dniach poprzednich.

Codzienna czujność oraz spostrzegawczość co do ewentualnych zmian są w tym przypadku bardzo pożądane. Wystarczy tylko (i aż :)) zachować codzienną czujność. Prawnicy zapewne by powiedzieli, że to tak zwana: należyta staranność ;).

Pamiętaj, że to Ty, a nie ktoś inny, jesteś szefem kuchni swojego sprzętu IT! Kucharzem czy adminem? 👨‍🍳💻 Jeśli coś zaczyna działać podejrzanie wolno, nie zakładaj od razu, że „znowu ten złom przypala jajecznicę na patelni”, bo może ktoś właśnie próbuje dodać do Twojego systemu nieautoryzowane przyprawy (czytaj: wirusy). 🦠🧂 Zamiast machnąć ręką, lepiej wrzuć Twój system operacyjny na „cyfrowy ogień” i dokładnie go przeskanuj antywirusem. Lepiej wykryć problem, zanim stanie się on spalonym naleśnikiem Twojej cyfrowej rzeczywistości! 🔥😉

Systematyczne szkolenia - profilaktyka cyberbezpieczeństwa

Dziękuję za przeczytanie wersji PROMO

Zachęcam Ciebie do zakupu pełnej wersji mojego ebooka

Serdecznie polecam i pozdrawiam

Autor Dariusz Gołębiowski

spotkajmy się w sieci :)

PODSUMOWANIE

Podsumowując zawartość drugiej części mojego poradnika - "Cyberhigiena", chciałbym podkreślić głębokie przekonanie, że świadomość i odpowiednie działania mogą znacząco podnieść poziom naszego bezpieczeństwa cyfrowego. Przedstawione tu zasady, praktyki oraz zalecenia - stanowią solidną podstawę, która - jak mam nadzieję - pozwoli Tobie nie tylko rozpoznać i zrozumieć cyberzagrożenia, ale przede wszystkim pozwoli na ich skuteczne ominięcie. Gratulacje! 🎉 Przebrnąłeś/aś przez świat cyberhigieny, a to oznacza, że jesteś teraz bardziej świadomy/a zagrożeń niż 90% internautów, którzy nadal klikają w e-maile o „niespodziewanym spadku” od dalekiego krewnego z Nigerii. 😅

Czy po tej lekturze Twój komputer jest nie do złamania, a Twoje hasła są tak skomplikowane, że sam ich nie pamiętasz? Może jeszcze nie, ale jedno jest pewne – masz solidne fundamenty, które pomogą Ci **unikać cyfrowych pułapek i bronić się przed cyberzagrożeniami**. Wystarczy zastosować się do umieszczonych tutaj porad.

🚀 **A na koniec - minimum, które trzeba zapamiętać:**

✅ **Nie panikuj, ale też nie bądź naiwny** – cyberprzestępcy liczą na Twoją nieuwagę, nie ułatwiaj im zadania!

✅ **Hasło „123456" to nie hasło, tylko zaproszenie** – a jeśli nadal używasz jednego hasła do wszystkiego, to możesz równie dobrze opublikować je na portalu społecznościowym.

✅ **AI już czyha na Twoje dane** (tzn. przestępcy ją używający) – ale spokojnie, teraz wiesz, jak się przed tym bronić!

✅ **Phishing to nie tylko e-maile, to prawdziwa sztuka oszustwa** – i jak każda sztuka, ma swoich mistrzów. Na szczęście po tej lekturze jesteś na nich odporny!

✅ **Otwarte WiFi? Lepiej daj sobie spokój!** Chyba, że chcesz, żeby ktoś inny przeglądał Twoje maile szybciej niż Ty sam/a :).

Czy Twoje życie po przeczytaniu tej książki się zmieni? Możliwe. Czy będziesz bardziej świadomy/a - w co klikasz? **Na pewno!** Czy przestaniesz wreszcie klikać w dziwne linki? No cóż... mam taką szczerą nadzieję 😄 (ale nie - pewność).

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 (i wiele innych) 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 oraz cyfrowych zagrożeń.

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

Do zobaczenia po bezpiecznej stronie internetu! 🚀 😀

W poradniku wykorzystano:

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

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 od podstaw
- 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.