Wydawnictwo Cyfrowe **poswojsku.pl**

BEZPIECZEŃSTWO INFORMACJI

Gołębiowski Dariusz

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001

CYBER AI KSC NIS2 SZBI

Moduł 5

Audyt wewnętrzny i doskonalenie bez strachu

AKADEMIA BEZPIECZEŃSTWA poswojsku&GDDM

Wszelkie prawa do zawartości tej książki są zastrzeżone.

Nieautoryzowane przez autora rozpowszechnianie całości lub dowolnego fragmentu niniejszej publikacji w jakiejkolwiek postaci jest zabronione.

Wykonanie kopii jakąkolwiek z dostępnych metod (m.in.: elektroniczną, kserograficzną, fotograficzną) spowoduje naruszenie praw autorskich niniejszego dzieła.

Pamiętaj proszę:

napracowałem się, uszanuj moje zaangażowanie i godziny pracy spędzone nad napisaniem oraz opracowaniem książki: BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 NIS2 MODUŁ 5 Audyt wewnętrzny i doskonalenie – bez strachu.

Poradnik powstał na bazie usług doradczo-szkoleniowych firmy GDDM gdddm.com.pl oraz projektu edukacyjnego: Akademia Bezpieczeństwa GDDM&poswojsku

Czytaj tylko legalnie kupione egzemplarze.

Autor oraz Wydawnictwo poswojsku.pl

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

Wydawnictwo poswojsku.pl – kontakt:

poswojsku.pl,

bok@poswojsku.pl

ul. Paprocka 86,

98-220 Zduńska Wola

ISBN: 978-83-68360-56-1

Copyright © poswojsku.pl 2026

Materiał edukacyjny oparty na podejściu do zarządzania bezpieczeństwem informacji opartym na ISO/IEC 27001. Nie jest to dokument certyfikacyjny ani oficjalna publikacja ISO.

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 NIS2

MODUŁ 5 Audyt wewnętrzny i doskonalenie – bez strachu

Praktyczny przewodnik dla specjalistów bezpieczeństwa informacji oraz cyberbezpieczeństwa

Autor:

Dariusz Gołębiowski

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001

W poradniku wykorzystano wsparcie AI w analizie i zmianach niektórych fragmentów tekstu.

Od Wydawnictwa Cyfrowego poswojsku.pl

KILKA SŁÓW O FORMACH ŻEŃSKICH I MĘSKICH

Wspaniała Czytelniczko - Drogi Czytelniku

Jak nowoczesnemu wydawnictwu, zależy nam, aby nasz publikacje były przyjazne dla wszystkich osób. Jednocześnie staramy się, aby nasi autorzy pisali w sposób prosty, naturalny i wygodny w czytaniu.

Dlatego w książce czasami używane są formy męskie, a czasami żeńskie. Wszystkie odnoszą się do każdej osoby czytającej tę publikację, niezależnie od płci, wieku, pochodzenia, stanowiska czy sposobu, w jaki sama siebie określa.

Nie stosujemy konsekwentnie zapisów typu „czytelnik/ czytelniczka”, „nauczyciel/ nauczycielka” itp., ponieważ utrudniają one płynność czytania.

Jeżeli ktoś zauważy, że

- liczba końcówek męskich nie zgadza się z liczbą końcówek żeńskich,
- istnieją inne końcówki, które nie zostały użyte,

z góry przepraszamy za nas i naszych Autorów. Nie jest to działanie zamierzone – po prostu poswojsku jest wydawcą książek ;), a nie firmą księgową, dbającą o zgodność liczby końcówek językowych.

Wszystkim

Wspaniałym Czytelniczkom oraz

Drogim Czytelnikom

życzymy przyjemnej lektury tej książki.

Spis treści

WPROWADZENIE DO MODUŁU 5.....14

Kontrola: Od dokumentu przez działania do audytu..15

5.1 Audyt wewnętrzny – po co on naprawdę jest.....19

Rola lekcji.....20

Cel lekcji 5.1.....21

Najczęstsze skojarzenia z audytem.....22

To nie jest prawdziwy audyt.....23

Najważniejsza teza tej lekcji.....23

Czym JEST audyt wewnętrzny.....24

Czym audyt wewnętrzny NIE JEST.....25

Audyt a kontrola – kluczowa różnica.....25

Dlaczego audyt jest potrzebny nawet wtedy, gdy „nic się nie dzieje”.....26

Audyt jako element cyklu SZBI.....27

Co audyt daje organizacji.....28

Przykład praktyczny – „audyt, który zmienił nastawienie”.....29
Audyt a NIS2/KSC.....30
Ćwiczenie refleksyjne.....31
Puenta lekcji 5.1.....32
Co dalej.....33
Lekcja 5.2 Jak przygotować się do audytu bez stresu. 34
Rola lekcji.....35
Cel lekcji 5.2.....36
Najczęstszy błąd w przygotowaniach do audytu.....37
Najważniejsza teza tej lekcji.....37
Co audytor chce zobaczyć na starcie.....38
Co warto zrobić PRZED audytem.....39
Czego NIE robić przed audytem.....40
Jak przygotować ludzi – a nie tylko dokumenty...41
Rozmowa z audytorem – jak się zachować.....42
Co zrobić, gdy audytor znajdzie problem.....42
Audyt a NIS2/KSC – spokojne przygotowanie.....43

Przykład praktyczny – audyt, który „poszedł spokojnie”.....43
Ćwiczenie praktyczne.....44
Przykłady praktyczne.....45
Moment decyzyjny dla kierownictwa.....48
Pytanie, które zmienia rozmowę.....49
SZBI to.....49
Puenta lekcji 5.2.....50
Lekcja 5.3 Jak przeprowadzić prosty audyt wewnętrzny SZBI.....51
Rola lekcji.....52
Cel lekcji 5.3.....53
Kto może przeprowadzić audyt wewnętrzny.....54
Czego audyt wewnętrzny NIE wymaga.....54
Trzy etapy prostego audytu wewnętrznego.....55
Jak zadawać pytania audytowe.....56
Na co patrzeć w pierwszej kolejności.....57
Najczęstsze błędy w audycie wewnętrznym.....57
Audyt jako rozmowa, nie przesłuchanie.....58

Co zapisać po audycie - minimum.....58
Przykład praktyczny audytu, który coś zmienił.....59
Ćwiczenie praktyczne.....60
Przykład rozwiązania powyższego ćwiczenia.....61
Jak odpowie organizacja świadoma.....63
Moment decyzyjny dla kierownictwa.....63
Puenta szkoleniowa.....64
Puenta lekcji 5.3.....65
Lekcja 5.4 Niezgodności, ryzyka i obszary do poprawy – jak to rozróżnić.....66
Rola lekcji.....67
Cel lekcji 5.4.....68
Najczęstszy błąd po audycie.....69
Najważniejsza teza tej lekcji.....69
Niezgodność - co to naprawdę znaczy.....70
Ryzyko – co nim jest, a co nie.....72
Przykład ryzyka.....72
Obszar do poprawy – bardzo niedoceniana kategoria.....74

Rozróżnienie pojęć: Niezgodność, Ryzyko, Obszar do poprawy - jest bardzo ważne.....75
Jak rozmawiać o wynikach audytu.....76
Co robić z każdą kategorią - w skrócie.....76
NIS2/KSC a rozróżnianie obserwacji.....77
Przykład praktyczny – audyt bez paniki.....77
Ćwiczenie praktyczne.....78
Przykład rozwiązania ćwiczenia.....79
Puenta lekcji 5.4.....82
Co dalej?.....82
Lekcja 5.5 Działania korygujące i doskonalenie w praktyce.....83
Rola lekcji.....84
Cel lekcji 5.5.....85
Najczęstszy błąd po audycie: „Naprawmy wszystko naraz”.....86
Najważniejsza teza tej lekcji.....86
Jak reagować na wyniki audytu?.....87
Co poprawiać najpierw?.....87

Jak nie wpaść w spiralę dokumentów?.....89
Doskonalenie jako proces, nie kara.....90
Audyt jako narzędzie wzrostu.....91
Przykład praktyczny – od naprawy do rozwoju.…92
Ćwiczenie praktyczne.....93
Jak odpowie organizacja świadoma.....95
Moment decyzyjny dla kierownictwa.....95
Puenta lekcji 5.5.....96
Co dalej.....96
Lekcja 5.6 Audyt jako element dojrzałości.....97
Rola lekcji.....98
Cel lekcji 5.6.....99
Najważniejsza zmiana perspektywy.....100
Najważniejsza teza tej lekcji.....100
Jak audyt spina cały system.....101
Dojrzałość SZBI – jak ją rozpoznać.....102
Audyt a spokój kierownictwa.....102
Kontrole zewnętrzne i NIS2/KSC – bez strachu. 103

Co naprawdę chroni organizację.....103

Przykład praktyczny – „organizacja spokojna”...104

Ostatnia pętla: ciągłe doskonalenie.....104

Ćwiczenie końcowe.....105

Puenta końcowa kursu.....105

PODSUMOWANIE.....107

DODATEK – różnica między „udawaniem bezpieczeństwa” a „budowaniem odporności”.....111

MODEL BŁĘDNY: Reakcyjny (Audyt jako „Przeszkada” i gaszenie pożarów).....112

MODEL WZORCOWY: Systemowy (Audyt jako „Narzędzie Rozwoju” i budowanie odporności).....114

STUDIUM PORÓWNAWCZE: Przykład praktyczny...116

Dlaczego to jest kluczowe w kontekście KSC/NIS2?.....118

Informacje o prawach autorskich i moich utworach. .120

ZAPROSZENIE.....121

Zostańmy w kontakcie!.....124

Ebooki poswojsku.pl.....125

Prawa autorskie i znaki towarowe.....129

WPROWADZENIE DO MODUŁU 5

Zamiast przygotowywać się do audytu przez

tydzień przed wizytą,

zbuduj system tak solidny, że każdy audyt

wewnętrzny czy zewnętrzny

stanie się dla Ciebie jedynie

potwierdzeniem Twojej doskonałości

w zarządzaniu bezpieczeństwem.

Kontrola: Od dokumentu przez działania do audytu

Moduł 5 serii poradników ***„BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 NIS2”*** - to moment w podróży poprzez bezpieczeństwo informacji oraz cyberbezpieczeństwo, w którym przestajemy budować „papierowy zamek” (czasami zwany „zamkiem z segregatorów”) i zaczynamy sprawdzać, czy stworzone fundamenty naprawdę wytrzymają uderzenie realnego ataku.

Nagły impuls pod wpływem usłyszenia sformułowania „***Audyt nadchodzi***”,

może wywołać myśli:

Schowam wszystkie nieuporządkowane papiery pod biurko, „wyczyszczę” historię przeglądania, skasuję niepotrzebne pliki i … !

Jak myślisz – czy często zdarza się w Twojej organizacji podejście przedstawione powyżej? A Ty? Także masz takie odczucia? Jeżeli tak, to znaczy, że Twoje ciało zareagowało na jeden z najstarszych mitów współczesnego świata korporacyjnego. Dla wielu osób słowo „audyt”:

- brzmi jak zapowiedź wizyty kontrolnej policji lub wezwania do sądu,
- jest kojarzone najczęściej z szukaniem winnych czy wytykaniem błędów oraz stresującym „przesłuchiwaniem” prawie całego personelu.

W tym module porzucamy tę wizję, bo niepotrzebnie i to dość często, mylony jest audyt z kontrolą. W świecie profesjonalnego bezpieczeństwa informacji oraz cyberbezpieczeństwa (i zgodnie z wymogami KSC/NIS2/ISO27001), audyt jest czymś zupełnie innym:

AUDYT JEST TWOIM „BEZPIECZNIKIEM”.

To narzędzie, które mówi Tobie:

„Witam serdecznie, zrobiliśmy analizę i tutaj masz luki. Napraw wykryte problemy jak najszybciej, zanim zrobi to ktoś nieproszony” (a zaraz po naprawieniu otrzymasz certyfikację bezpieczeństwa :)).

W tym module przeprowadzimy proces demistyfikacji. Odrzucimy lęk i zastąpimy go systematycznym, analitycznym spokojem.

Nauczymy się wspólnie:

- jak patrzeć na System Zarządzania Bezpieczeństwem Informacji (SZBI) z dystansu,
- jak rozróżnić błąd techniczny od ryzyka systemowego,
- jak sprawić, by audyt był dla Twojej organizacji nie źródłem ciężkiego stresu, ale powodem do dumy.

Pokażę Tobie, że dobrze przeprowadzony audyt wewnętrzny, to nie jest „polowanie na czarownice”, lecz profesjonalna diagnoza, która daje:

- kierownictwu - spokój,
- pracownikom - jasne zasady działania.

Przygotuj się na zmianę perspektywy. Zamiast przygotowywać się do audytu przez tydzień przed wizytą, nauczysz się budować system tak solidny, że każdy audyt – wewnętrzny czy zewnętrzny – stanie się dla Ciebie jedynie potwierdzeniem Twojej doskonałości w zarządzaniu bezpieczeństwem organizacji.

Zapraszam do modułu, w którym „strach przed audytem" postaramy się wspólnie zamienić na „pewność działania".

Zaczynamy.

Lekcja 5.1 Audyt wewnętrzny – po co on naprawdę jest

5.1 Audyt wewnętrzny – po co on naprawdę jest

...

Rola lekcji

Ta lekcja ma na celu całkowitą zmianę nastawienia do audytu. Chcę, abyś zrozumiała, że:

audyt to „zdrowy przegląd” kondycji organizacji,

analogiczny do okresowych badań profilaktycznych w medycynie.

audyt nie jest egzaminem,

w którym pracownicy mogą zostać ocenieni lub ukarani za błędy techniczne (a przynajmniej tak być nie powinno).

Bez zrozumienia wyżej wymienionych różnic - organizacja wpada w pułapkę strachu, co prowadzi do ukrywania problemów oraz tworzenia „teatru na papierze” – dokumentacji, która wygląda nienagannie dla audytora, ale nie chroni organizacji przed realnymi zagrożeniami.

Cel lekcji 5.1

Zakładam, że po przeanalizowaniu tej lekcji:

- zrozumiesz, czym naprawdę jest audyt wewnętrzny (narzędzie analityczne służące do weryfikacji procesów – a nie projektów);
- dowiesz się, czym audyt nie jest (nie jest to kontrola osobista ani karanie pracowników) oraz dlaczego ta różnica ma kluczowe znaczenie dla budowania zaufania wewnątrz zespołu;
- spojrzysz na audyt jako na merytoryczną rozmowę o procesach, a nie jako na zwykłe przesłuchanie;
- zrozumiesz rolę audytu w cyklu życia SZBI zgodnie z normą ISO 27001 oraz wymogami NIS2;
- przestaniesz traktować audyt jako zagrożenie dla organizacji, a zaczniesz postrzegać go jako wsparcie i okazję na rozwój.

Najczęstsze skojarzenia z audytem

Wiele osób, słysząc słowo „audyt”, automatycznie kojarzy je z:

- kontrolą,
- szukaniem błędów,
- wskazywaniem winnych.

Takie postrzeganie rodzi negatywne skutki, typu:

- stres,
- defensywna postawa pracowników ,
- celowe ukrywanie problemów - udawanie przed audytorem, a często (o zgrozo!) także przed własnym szefostwem,
- „robienie pod audyt”, czyli tworzenie sztucznego obrazu rzeczywistości tuż przed wizytą kontrolną.

Takie podejście sprawia, że organizacja staje się słaba, ponieważ problemy nie są rozwiązywane, a jedynie maskowane tonami papierowych procedur.

To nie jest prawdziwy audyt

Powyższe skojarzenia to jedynie błędne przekonania, które niszczą realną wartość kontroli wewnętrznej. Jeśli audyt jest postrzegany jako koszmarna kontrola, organizacja przestaje być szczera wobec samej siebie. To uniemożliwia autentyczne naprawienie słabych punktów systemu, co w konsekwencji może prowadzić do poważnych incydentów bezpieczeństwa, których „papierowa" ochrona nie powstrzyma.

Najważniejsza teza tej lekcji

AUDYT (WEWNĘTRZNY i ZEWNĘTRZNY)

NIE SŁUŻY DO OCENIANIA LUDZI

AUDYT SŁUŻY DO OCENIANIA SYSTEMU.

Jeśli audyt służy głównie do szukania winnych lub straszenia konsekwencjami, przestaje być narzędziem zarządzania bezpieczeństwem i staje się kontrolą dyscyplinarną. W takim przypadku organizacja traci możliwość na prawdziwe doskonalenie.

Czym JEST audyt wewnętrzny

Audyt wewnętrzny to:

- spokojne spojrzenie z dystansu na procesy organizacji,
- ...

Serdecznie dziękuję za to, że poświęciłeś/aś swój czas na zapoznanie się z początkową częścią mojego poradnika.

Zapraszam do skorzystania z pełnej wersji ebooka:

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 NIS2 MODUŁ 4 Wdrożenie w praktyce – od dokumentów do działania

Szczegóły oferty znajdziesz na stronie firmy Wydawnictwo Cyfrowe poswojsku.pl

Informacje o prawach autorskich i moich utworach

W poradniku wykorzystano:

- własne materiały doradcze,
- w poradniku wykorzystano wsparcie AI w analizie i zmianach niektórych fragmentów tekstu.

DZIĘKUJĘ ZA UWAGĘ

Autor poradnika:

DARIUSZ GOŁĘBIOWSKI

ZAPROSZENIE

Seria wydawnicza:

Saga CyberJestestwa

przygodowe uniwersum fantasy.

Poznaj kolejne Kroniki i Księgi dostępne w wielu księgarniach internetowych.

Szczegóły oraz wsparcie dla rozwoju uniwersum znajdziesz na: poswojsku.eu/dar.html

Obserwuj, jak WszechBogowie Wszechrzeczy szepczą nowe rozwiązania: poswojsku.eu

Możesz także wejść do świata Sagi CyberJestestwa jako gracz!

W bezpłatnej wersji **„Escape from the Seventh Planet”** - czeka na Ciebie pięć grywalnych poziomów. Wyrusz z Astilusem przez Siódmą Planetę, odkrywaj jej tajemnice i sprawdź, czy zdołasz przetrwać drogę wyznaczoną Astilusowi przez Bogów Wszechrzeczy.

Pobierz grę bezpłatnie:

poswojsku.pl lub poswojsku.eu.

Uniwersum Saga CyberJestestwa

składa się obecnie z pozycji:

Kronika 0 Uniwersum Prawdziwego Wszechświata

Kronika 1 Wszechświat Wszechrzeczy

Księga 1 Siódma Planeta

Księga 2 Ziemia

Księga 3 Planeta Faron

Księga 4 Cienie nanoMatrycy

Księga 5 Herosi Historie (w przygotowaniu)

Księga 6 ... (w przygotowaniu)

Seria Saga CyberJestestwa ciągle się rozrasta. Na bazie materiałów spisywanych przez ostatnich 30 lat - przygotowywane jest łącznie kilkanaście Ksiąg.

Zostańmy w kontakcie!

Strona internetowa poswojsku.pl

Facebook facebook.com/poswojsku

YouTube youtube.com/@poswojsku

LinkedIn linkedin.com/in/golebiowski-dariusz

Instagram instagram.com/poswojsku

Threads threads.com/@poswojsku

TikTok tiktok.com/@astilus

Amazon Author Page
amazon.com/author/dariuszgolebiowski

Goodreads goodreads.com/dariuszgolebiowski

Proszę, dołącz do mnie – razem budujmy bezpieczniejszy i bardziej świadomy świat cyfrowy!

Ebooki poswojsku.pl

Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 1: Wprowadzenie

Kompleksowy wstęp do tematyki ochrony danych, prywatności i bezpiecznego korzystania z sieci. To książka dla tych, którzy chcą szybko zrozumieć, na czym polegają najważniejsze zagrożenia i jak zacząć się przed nimi skutecznie bronić – bez skomplikowanego żargonu. Znajdziesz tu przykłady z życia i proste instrukcje krok po kroku.

Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 2: Cyberhigiena

Praktyczny przewodnik po codziennych nawykach, które realnie zwiększają Twoje bezpieczeństwo. Dowiesz się, jak tworzyć silne hasła, chronić urządzenia, wykrywać próby oszustw i przygotować swoją rodzinę na zagrożenia cyfrowe. To pozycja obowiązkowa, jeśli

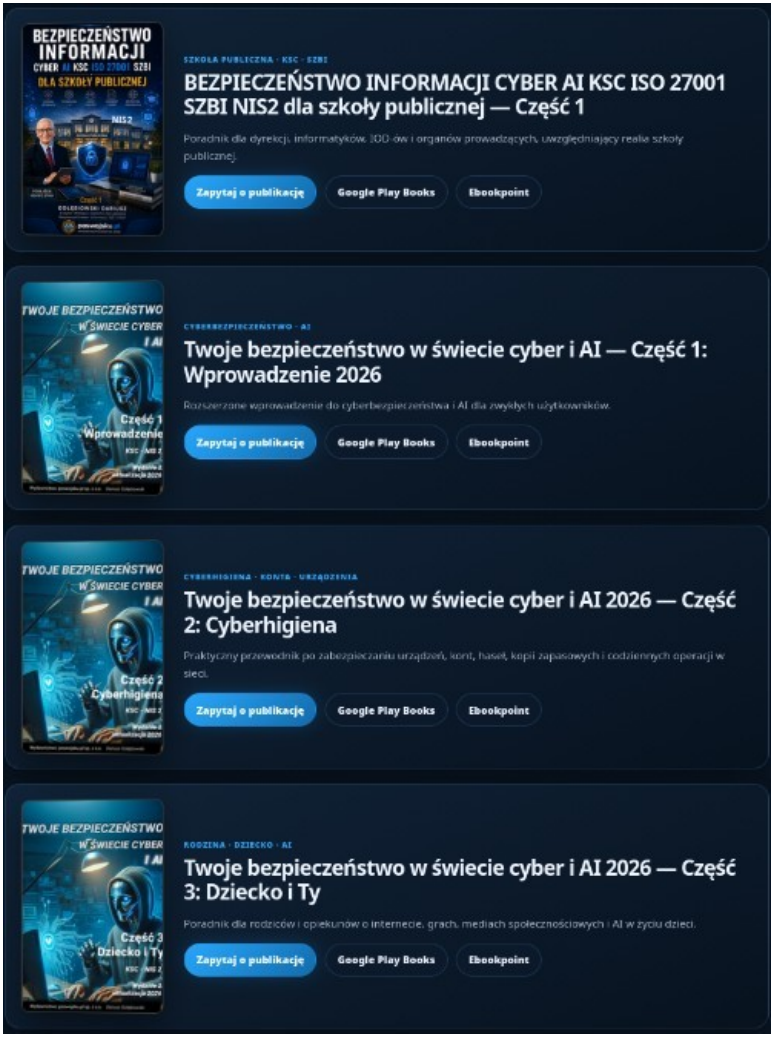
chcesz, żeby cyberhigiena była naturalną częścią Twojego życia.

Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 3: Dziecko i Ty

Poradnik stworzony specjalnie dla rodziców i opiekunów, którzy chcą wprowadzać dzieci w cyfrowy świat z rozsądkiem i spokojem. Znajdziesz tu nie tylko zasady i rekomendacje, ale też gotowe sposoby rozmowy o bezpieczeństwie i budowania zaufania. Ta książka pomoże Tobie chronić najmłodszych bez straszenia i nadmiernej kontroli.

AI W EDUKACJI CZĘŚĆ 2 PRAKTYCZNE POMYSŁY PRAWNE UWARUNKOWANIA dla edukatorów i edukatorek

Poradnik o wykorzystaniu AI w edukacji, z przykładami, ćwiczeniami, podstawami prawnymi.



AI w edukacji Część 1 Praktyczny poradnik od kuchni. Dla edukatorów i edukatorek

Poradnik o wykorzystaniu AI w nauczaniu i uczeniu się, z przykładami i ćwiczeniami.

GODOT ENGINE I GDSCRIPT POSWOJSKU

Część 1: Wprowadzenie do świata gier i pierwsze skrypty

Część 2: Od pustego projektu do pierwszego programu

Praktyczny przewodnik dla osób, które chcą wejść do świata tworzenia gier z wykorzystaniem bezpłatnych narzędzi – Godot Engine i GDScript.

Ebooki możesz nabyć na:

stronie wydawnictwa cyfrowego **poswojsku.pl**

Prawa autorskie i znaki towarowe

Wszystkie wymienione nazwy firm, produktów, usług i logo są znakami towarowymi lub zastrzeżonymi znakami towarowymi ich odpowiednich właścicieli. Nazwy te służą wyłącznie celom informacyjnym i nie oznaczają poparcia ani powiązania z tymi markami.

- **OpenAI** i **ChatGPT** są znakami towarowymi firmy OpenAI.
- **Microsoft**, **Copilot**, **Bing** oraz **Windows** są zarejestrowanymi znakami towarowymi firmy Microsoft.
- **Android**, **Gemini**, **Chrome** są zarejestrowanymi znakami towarowymi firmy Google LLC.
- **Apple**, **iOS** i **macOS** są zastrzeżonymi znakami towarowymi firmy Apple Inc. w Stanach Zjednoczonych i/lub innych krajach.

- **Facebook** jest zastrzeżonym znakiem towarowym firmy Meta Platforms, Inc.
- **YouTube** jest zarejestrowanym znakiem towarowym Google LLC.
- **DuckDuckGo**, **Kiddle.co**, **Swiggle**, **KidRex**, **SPIN Safe Browser**, **Qustodio**, **Kaspersky Safe Kids**, **Norton Family**, **Duolingo**, **Lingokids**, **Smiling Mind**, **Headspace**, **Tayasui Sketches**, **Drawing Desk**, **Khan Academy** i inne wspomniane produkty mogą być znakami towarowymi ich odpowiednich właścicieli.

Wszelkie odniesienia mają charakter edukacyjny i informacyjny.