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 4

WDROŻENIE W PRAKTYCE OD DOKUMENTÓW DO DZIAŁANIA

AKADEMIA BEZPIECZEŃSTWA 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 4 Wdrożenie w praktyce – od dokumentów do działania

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: 978-83-68360-55-4

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 4 Wdrożenie w praktyce – od dokumentów do działania

Praktyczny przewodnik dla specjalistów bezpieczeństwa informacji i 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 4.....14

Moment Prawdy: Od dokumentu do działania.....15

Dlaczego ten moduł jest kluczowy?.....16

Dla kogo jest ten moduł?.....17

Co musisz zapamiętać na starcie?.....18

Lekcja 4.1 Od dokumentu do działania – co naprawdę oznacza „wdrożenie”.....19

Rola lekcji.....20

Cel lekcji 4.1.....21

Najczęstsza iluzja wdrożeniowa.....22

Najważniejsze tezy tej lekcji.....24

Czym wdrożenie NIE jest.....25

Czym wdrożenie JEST.....26

Przykład – „procedura incydentowa”.....27

Rola kierownictwa w pierwszym etapie.....29

Dlaczego ludzie nie zmieniają zachowań.....32
Co musi się wydarzyć, żeby wdrożenie ruszyło.....34
Wdrożenie jako proces, nie projekt.....36
Ćwiczenie refleksyjne.....37
Puenta lekcji 4.1.....38
Co dalej.....39
Lekcja 4.2 Jak zacząć wdrażanie SZBI – bez rewolucji i bez chaosu.....40
Rola lekcji.....41
Cel lekcji 4.2.....42
Najczęstszy błąd na starcie: „Wielki Wybuch”.....43
Najważniejsza teza tej lekcji.....44
Od czego NIE zaczynać.....45
Od czego zacząć, aby było skutecznie?.....46
Wybór 2–3 obszarów startowych.....47
Szybkie zwycięstwa (Quick Wins).....48
Luźn: Plan pierwszych 30–60 dni - logika działania..49
Rola kierownictwa na starcie.....51
Czy zawsze opór jest naturalny?.....52

Ćwiczenie praktyczne.....54
Puenta lekcji 4.2.....55
Lekcja 4.3 Ludzie, nie dokumenty – komunikacja i kultura bezpieczeństwa.....56
Rola lekcji.....57
Cel lekcji 4.3.....59
Najczęstszy błąd we wdrożeniach: „Technologia zamiast Emocji”.....60
Najważniejsza teza tej lekcji.....61
Dlaczego ludzie omijają zasady?.....62
Kultura bezpieczeństwa w organizacji – co to naprawdę znaczy?.....63
Przykład – dwa odmienne podejścia do tego samego błędu.....64
Rola liderów i kierownictwa.....66
Jak skutecznie komunikować bezpieczeństwo?..67
Małe rytuały, duże efekty.....68
Pułapka - „Szkolenie wystarczy”.....69
Ćwiczenie refleksyjne.....70

Puenta lekcji 4.3.....71

Lekcja 4.4 Wdrażanie procedur w praktyce – jak sprawić, by były używane.....73

Rola lekcji.....74

Cel lekcji 4.4.....75

Najczęstszy mit o procedurach.....77

Najważniejsza teza tej lekcji.....78

Kiedy procedura zaczyna żyć?.....79

Etapy wdrażania procedury.....80

Przykład – „Procedura incydentowa”.....82

Bezwzględna dostępność procedur.....83

Egzekwowanie zamiast poprawy.....83

Jak sprawdzić, czy Twoja procedura działa?.....84

Procedury a wymagania NIS2 / uKSC.....85

Studium przypadku: „Procedura była, ale...”.....86

Ćwiczenie praktyczne.....87

Puenta lekcji 4.4.....88

Co dalej?.....89

Lekcja 4.5 Reagowanie na incydenty w realnym świecie 90

Rola lekcji.....91

Cel lekcji 4.5.....92

Najczęstszy mit o incydentach.....93

Najważniejsza teza tej lekcji.....94

Czym jest incydent w praktyce?.....95

Pierwsze minuty – co jest najważniejsze?.....96

Rola procedury incydentowej.....98

Komunikacja wewnętrzna i zewnętrzna w trakcie incydentu.....98

Incydent a strach ludzi.....99

Wymagania NIS2 / KSC.....100

Co po incydencie – czy Twoja organizacja posiada stosowne procedury?.....101

Studium przypadku: Modelowe działanie systemu zarządzania.....103

Scenariusz: Wykrycie Listerii w partii gotowego dania.....103

Analogia do SZBI - Jak to działa w Cyberbezpieczeństwie?.....105
Ćwiczenie praktyczne.....107
Puenta lekcji 4.5.....108
Co dalej?.....109
Lekcja 4.6 Jak utrzymać SZBI w czasie (a nie tylko „wdrożyć”).....110
Rola lekcji.....111
Cel lekcji 4.6.....112
Najczęstsze złudzenie po wdrożeniu: „Zrobiliśmy to, teraz możemy o tym zapomnieć”.....113
Najważniejsza teza tej lekcji.....115
Co naprawdę oznacza „utrzymanie SZBI”?.....116
Minimalny poziom utrzymania SZBI.....117
Dokumentacja żywa a dokumentacja martwa....118
Rola ludzi w utrzymaniu SZBI.....120
Szefostwo po wdrożeniu: Od „projektu” do „nadzoru” 121
KSC a utrzymanie systemu.....122

Studium przypadku: System, który nie umarł.....123

Ćwiczenie: audyt „żywotności” systemu.....125

Puenta lekcji 4.6.....127

Co dalej?.....127

Lekcja 4.7 Podsumowanie MODUŁU 4: Bezpieczeństwo jako codzienna praktyka.....128

Wprowadzenie: Gdzie kończy się projekt, a zaczyna rzeczywistość?.....129

Co zmienia efektywnie wdrożony SZBI?.....130

Moduł 4 domyka ścieżkę i co dalej?.....132

Wdrożenie to nie koniec – to początek cyklu.....133

Bezpieczeństwo jako element zarządzania, a nie problem IT.....134

Refleksja końcowa - jak sprawdzić, czy odniosłaś sukces?.....135

PODSUMOWANIE.....136

Od dokumentu do działania – bezpieczeństwo, które żyje.....136

Twoje zadanie na teraz.....140

DODATEK - Przewodnik po „żywych” procedurach – porównanie: MODEL BŁĘDNY Biurokratyczny a MODEL WZORCOWY Operacyjny.....141

1. Procedura Reagowania na Incydenty (Dla Zespołu IT/Security).....142

2. Procedura Zgłaszania Podejrzenia Incydentu (Dla Pracownika/Usera).....144

3. Procedura Zarządzania Dostępami (Onboarding / Offboarding).....146

4. Procedura Korzystania z Narzędzi AI (np. ChatGPT) 148

Informacje o prawach autorskich i moich utworach. .150

ZAPROSZENIE.....151

Zostańmy w kontakcie!.....154

Ebooki poswojsku.pl.....155

Prawa autorskie i znaki towarowe.....159

WPROWADZENIE DO MODUŁU 4

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz dostosowanie się do rygorystycznych wymogów dyrektywy NIS2 czyli naszej polskiej implementacji – KSC 2026, to nie projekt informatyczny. To zmiana organizacyjna oparta na procesach.

Moment Prawdy: Od dokumentu do działania

„Mamy dokumenty. I co dalej?” – to pytanie, które słyszę najczęściej od menedżerów, dyrektorów i właścicieli organizacji po zakończeniu procesów analizy ryzyka czy tworzenia polityk bezpieczeństwa.

Wielu liderów wpada w pułapkę, którą nazywamy **„bezpieczeństwem na papierze”**. To iluzja, która powstaje, gdy organizacja wierzy, że posiadanie skomplikowanych plików PDF, podpisanych polityk oraz przeszkolonych (teoretycznie) pracowników, oznacza, że jest bezpieczna. To nieprawda. Prawdziwe zagrożenia nie atakują plików w intranecie – atakują ludzi, procesy i realne, codzienne nawyki.

Dlaczego ten moduł jest kluczowy?

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz dostosowanie się do rygorystycznych wymogów dyrektywy **NIS2** czy nowelizacji **uKSC**, to nie projekt informatyczny. To

projekt zmiany organizacyjnej.

Wiele organizacji popełnia błąd „Wielkiego Wybuchu" – próbują wprowadzić wszystkie procedury, zakazy oraz kontrole naraz. Efekt? Paraliż decyzyjny, opór pracowników i chaos, który sprawia, że bezpieczeństwo staje się postrzegane jako uciążliwy ciężar, a nie wartość.

Ten moduł jest inny. Nie znajdziesz tu nudnych definicji ani technicznego żargonu. To praktyczny przewodnik po „miękkiej" i operacyjnej stronie cyberbezpieczeństwa. Pokażę Tobie, jak:

- **Zamienić dokumentację w realne działania** tak, aby procedury ratowały sytuację w czasie kryzysu, a nie leżały zakurzone na dysku.
- **Wdrożyć bezpieczeństwo bez rewolucji**

jak zacząć od „szybkich zwycięstw” (quick wins), by nie spalić zespołu na starcie.

- **Zbudować kulturę bezpieczeństwa, a nie kulturę strachu**

  jak sprawić, by ludzie zgłaszali błędy zamiast je ukrywać.

- **Utrzymać system w czasie**

  jak sprawić, by SZBI był żywym organizmem, a nie martwym zapisem pod audyt.

Dla kogo jest ten moduł?

Przygotowałem go z myślą o tych, którzy ponoszą odpowiedzialność za organizację i chcą, aby bezpieczeństwo było częścią strategii, a nie „problemem działu IT”. Zatem - najwięcej korzyści powinni z przestudiowania tego poradnika – wynieść:

- **Kadra Zarządzająca**

  aby wiedzieć, jak nadawać kierunek i dawać przykład.

- **Menadżerowie i Liderki**

  aby potrafili wdrażać zmiany w swoich zespołach bez oporu podwładnych.

- **Specjaliści ds. Cyberbezpieczeństwa**
  aby wiedzieli, jak „sprzedać” procedury oraz skutecznie je komunikować.

Co musisz zapamiętać na starcie?

Wdrożenie to nie moment, w którym kończysz projekt.

Wdrożenie to moment, w którym zaczyna się prawdziwa praca.

Jeśli po procesie, który nazywasz „wdrożeniem”, sposób wykonywania zadań w Twojej firmie pozostaje dokładnie taki sam jak wcześniej – to znaczy, że wdrożenia nie było.

Zapraszam do drogi od teorii do działania.

Zaczynamy od najważniejszego:

zrozumienia, czym naprawdę jest realne wdrożenie.

Zaczynamy.

Lekcja 4.1: Od dokumentu do działania – co naprawdę oznacza „wdrożenie”

Lekcja 4.1 Od dokumentu do działania – co naprawdę oznacza „wdrożenie”

Skuteczne wdrożenie SZBI, to moment, w którym cały personel zaczyna działać inaczej, nawet wtedy, gdy nikt nie pilnuje.

Rola lekcji

Ta lekcja ma za zadanie „odczarować” pojęcie wdrożenia, które w wielu organizacjach kojarzy się z nudnym procesem biurokratycznym. Pokażemy, że prawdziwe wdrożenie to nie moment, w którym szef podpisuje stos dokumentów, ale głęboka zmiana sposobu działania całej organizacji.

Bez zrozumienia tej różnicy organizacje wpadają w pułapkę:

- **„Wdrażania na papierze”**

  gdzie system istnieje tylko w plikach PDF, a w rzeczywistości nikt o nich nie pamięta.
- **Martwej dokumentacji**

  gdzie procedury są publikowane raz na rok „dla świętego spokoju” i natychmiast trafiają do cyfrowego archiwum.
- **Pozornego bezpieczeństwa**

  gdzie w obliczu realnego zagrożenia okazuje się, że bezpieczeństwo „nie żyje” w praktyce i nie chroni nikogo.

Cel lekcji 4.1

Po przeczytaniu tej lekcji uczestniczka/uczestnik:

- **zrozumie, czym wdrożenie naprawdę jest, a czym tylko jego złudną imitacją**,
- **potrafi odróżnić realne wdrożenie od „wrzucenia dokumentów na dysk”** (czyli działań administracyjnych od działań systemowych),
- **zidentyfikuje kluczowe warunki**, które muszą zostać spełnione, aby papierowe procedury zaczęły realnie chronić firmę,
- **zrozumie krytyczną rolę kierownictwa** – dlaczego bez „głosu z góry” proces ten zawsze utknie w miejscu,
- **przestanie oczekiwać „efektu od razu”**, rozumiejąc, że budowanie kultury bezpieczeństwa to proces.

Najczęstsza iluzja wdrożeniowa

Wiele organizacji wpada w pułapkę myślenia, że bezpieczeństwo to zestaw zakupionych narzędzi lub spisanych zasad. Pojawiają się błędne przekonania:

- *„Mamy gotowe dokumenty i polityki → jesteśmy bezpieczni”*

  Mit: Dokument to tylko mapa, a nie sama podróż.

- *„Mamy drogie zaawansowane systemy bezpieczeństwa IT → nic złego nam się nie może przydarzyć”*

  Mit: Technologia to tylko jedna warstwa, bez ludzi i procesów jest bezbronna. Może Ciebie to zdziwi, ale niejednokrotnie, to ludzie chronią … aplikacje/systemy bezpieczeństwa cyfrowego.

- *„Opublikowaliśmy procedury w intranecie → ludzie będą je stosować”*

  Mit: Samo udostępnienie informacji nie wymusza zmiany nawyków.

- *„Zrobiliśmy szkolenie z cyberbezpieczeństwa → temat został zamknięty”*

  Mit: Szkolenie to pierwszy, bardzo dobry krok, ale nie jest gwarancją wiedzy w działaniu.

Pamiętaj:

To samo przez siebie - nie działa. Wdrożenie nie dzieje się w momencie kliknięcia przycisku „wyślij” w mailu z nową procedurą.

Wdrożenie zaczyna się następnego dnia – podczas codziennej, rutynowej pracy każdego pracownika/cy.

Najważniejsze tezy tej lekcji

> **Wdrożenie to moment, w którym cały personel zaczyna działać inaczej, nawet wtedy, gdy nikt nie pilnuje. Napisałem cały, bo incydent, to zwykle dzieło jednej osoby.**

Jeśli po procesie, który Ty i Twoja organizacja nazywacie „wdrożeniem”:

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

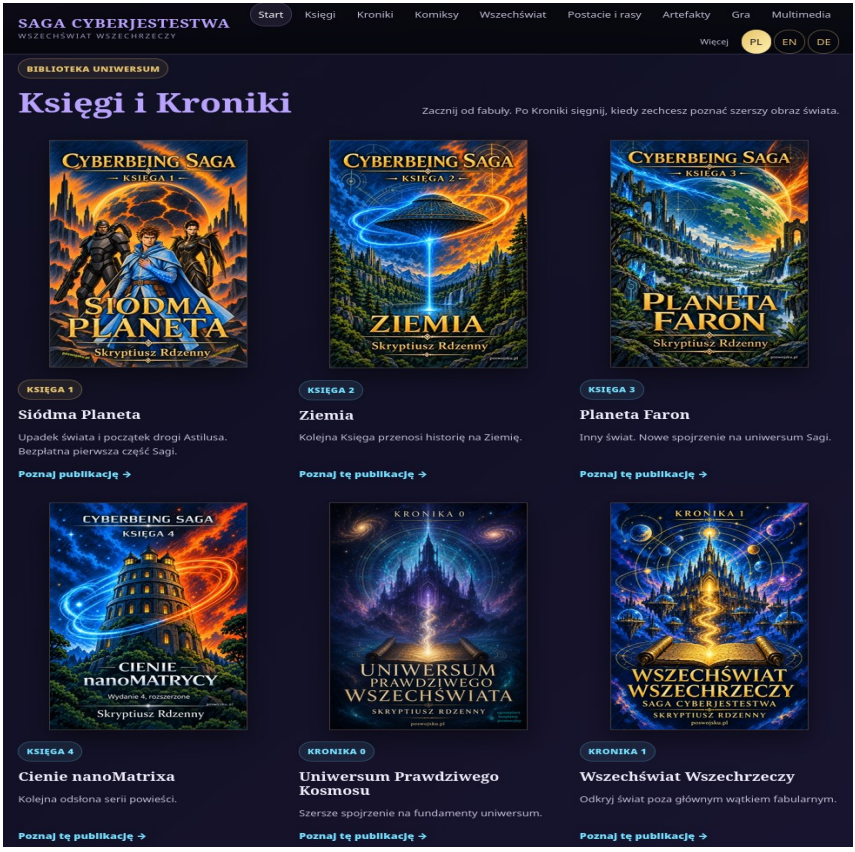
Księga 3 Planeta Faron

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.


SAGA CYBERJESTESTWA
WSZECHŚWIAT WSZECHRZECZY
Start
Księgi
Kroniki
Komiksy
Wszechświat
Postacie i rasy
Artefakty
Gra
Multimedia
Więcej
PL
EN
DE
BIBLIOTEKA UNIWERSUM
Księgi i Kroniki
Zacznij od fabuły. Po Kroniki sięgnij, kiedy zechcesz poznać szerszy obraz świata.
CYBERBEING SAGA
→ KSIĘGA 1 ←
SIÓDMA PLANETA
Skryptiusz Rdzenny
KSIĘGA 1
Siódma Planeta
Upadek świata i początek drogi Astilusa. Bezpłatna pierwsza część Sagi.
Poznaj publikację →
CYBERBEING SAGA
→ KSIĘGA 2 ←
ZIEMIA
Skryptiusz Rdzenny
KSIĘGA 2
Ziemia
Kolejna Księga przenosi historię na Ziemię.
Poznaj tę publikację →
CYBERBEING SAGA
→ KSIĘGA 3 ←
PLANETA FARON
Skryptiusz Rdzenny
KSIĘGA 3
Planeta Faron
Inny świat. Nowe spojrzenie na uniwersum Sagi.
Poznaj tę publikację →
CYBERBEING SAGA
KSIĘGA 4
CIENIE nanoMATRYCY
Wydanie 4, rozszerzone
Skryptiusz Rdzenny
KSIĘGA 4
Cienie nanoMatrixa
Kolejna odsłona serii powieści.
Poznaj tę publikację →
KRONIKA 0
UNIWERSUM PRAWDZIWEGO WSZECHŚWIATA
SKRYPTIUSZ RDZENNY
KRONIKA 0
Uniwersum Prawdziwego Kosmosu
Szersze spojrzenie na fundamenty uniwersum.
Poznaj tę publikację →
KRONIKA 1
WSZECHŚWIAT WSZECHRZECZY
SAGA CYBERJESTESTWA
SKRYPTIUSZ RDZENNY
KRONIKA 1
Wszechświat Wszechrzeczy
Odkryj świat poza głównym wątkiem fabularnym.
Poznaj tę publikację →

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

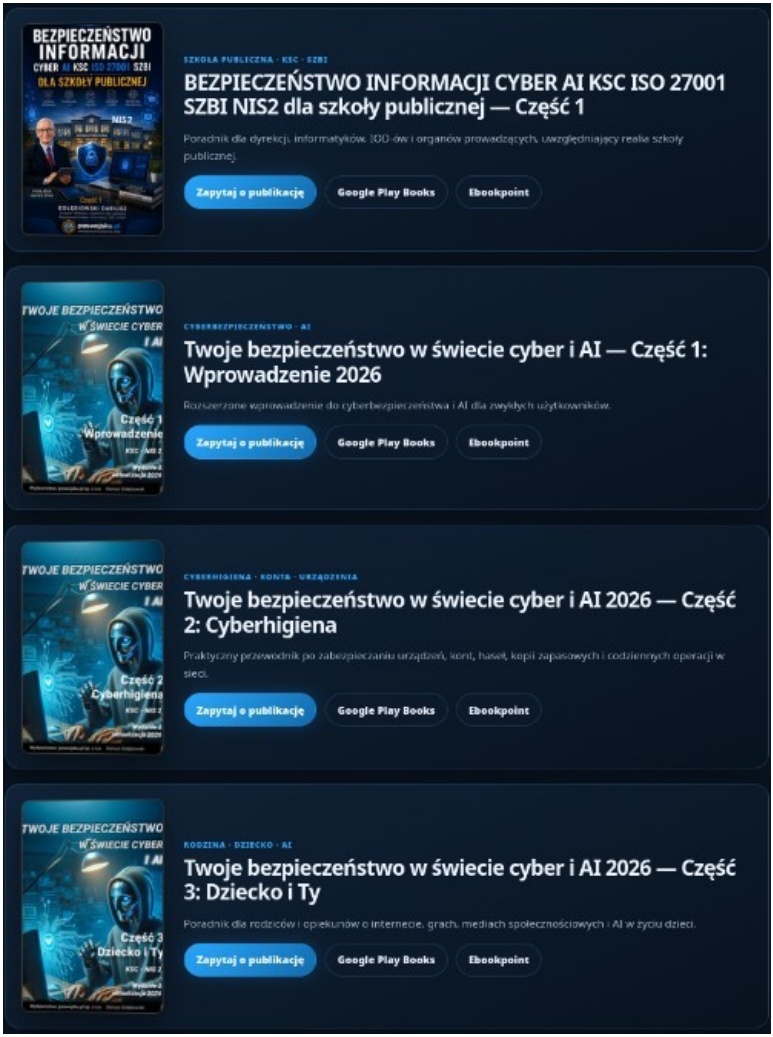
chcesz, żeby cyberhigiena była naturalną częścią Twojego życia.

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.