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 3

DOKUMENTACJA, KTÓRA MA SENS

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 3 DOKUMENTACJA, KTÓRA MA SENS

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: 978-83-68360-54-7

Copyright © poswojsku.pl 2026

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 NIS2 MODUŁ 3 DOKUMENTACJA, KTÓRA MA SENS

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

Wstęp: Manifest Praktyka.....15

Lekcja 3.1 Po co w ogóle dokumentować?.....19

Rola lekcji.....19

Cel lekcji 3.1.....21

Dlaczego dokumentacja ma złą reputację.....22

Najważniejsze tezy tej lekcji.....24

Dokumentacja jako przedłużenie myślenia ryzykiem 26

Przykład – „mamy procedury, ale…”.....28

Trzy prawdziwe cele dokumentowania.....30

Uporządkowanie decyzji.....30

Przypisanie odpowiedzialności.....31

Zapewnienie powtarzalności.....31

Błąd organizacji: dokumentacja „na zapas”.....33

Dokumentacja w kontekście NIS2.....34
Case – „kopiuj–wklej”.....35
Kiedy dokumentacja zaczyna działać.....36
Ćwiczenie refleksyjne.....37
Puenta lekcji 3.1.....38
Co dalej.....38
Lekcja 3.2 Co dokumentować w SZBI.....39
Rola lekcji.....39
Cel lekcji 3.2.....40
Dlaczego dokumentowanie „wszystkiego” nie działa 41
Najważniejsza zasada tej lekcji.....43
Trzy pytania, które decydują, czy coś dokumentować.....43
Co dokumentować w SZBI – bezwzględnie.....45
Decyzje dotyczące ryzyka.....45
Role i odpowiedzialności.....46
Zasady postępowania w sytuacjach krytycznych.47
Zasady korzystania z kluczowych zasobów.....47

Uzasadnienia decyzji....48
Czego NIE dokumentować i dlaczego....49
Oczywistości....49
Rzeczy jednorazowych....50
Szczegółów technicznych....50
Dokumentów „na wszelki wypadek”....51
Case – organizacja, która dokumentowała za dużo. 52
Dokument jako narzędzie, nie archiwum....53
Ćwiczenie praktyczne: Analiza wartości dokumentu 55
Przykład analityczny: Polityka Hashingu Hasła....56
Puenta lekcji 3.2....58
Co dalej....58
Lekcja 3.3 Dokumentacja jako mapa odpowiedzialności – kto, za co i kiedy....60
Rola lekcji....60
Cel lekcji 3.3....61
Najczęstszy problem organizacji....62
Najważniejsze tezy tej lekcji....63
Odpowiedzialność a wykonywanie zadań....64

Pułapka: „IT się tym zajmuje”.....66
Obszary, które dokumentacja musi jasno pokazywać 67
Odpowiedzialność w kontekście KSC i NIS2.....68
Pułapka „wszyscy byli zaangażowani”.....69
Dokumentacja, która faktycznie porządkuje.....70
Gdzie najczęściej dochodzi do rozmycia odpowiedzialności?.....71
Ćwiczenie praktyczne.....73
Puenta lekcji 3.3.....74
Co dalej.....74
Lekcja 3.4 Jak dokumentować ryzyko, a nie strach 75
Rola lekcji.....75
Cel lekcji 3.4.....76
Dlaczego większość rejestrów ryzyka nie działa.....78
Najważniejsze tezy tej lekcji.....79
Co odróżnia zapis ryzyka od zapisu strachu.....80
Przykład – to samo zdarzenie, dwa zapisy.....81

Cztery elementy dobrego zapisu ryzyka.....83
1. Kontekst organizacyjny.....83
2. Skutek (a nie tylko zdarzenie).....84
3. Decyzja.....84
4. Odpowiedzialność.....85
Błędne określenia: „wysokie, średnie, niskie”.....86
Jak audyt i NIS2/KSC czytają ryzyko.....88
Jak uprościć dokumentowanie ryzyka.....89
Ćwiczenie praktyczne: Transformacja zapisu.....90
Przykład pomocniczy.....91
Puenta lekcji 3.4.....93
Co dalej.....93
Lekcja 3.5 Procedury, które pomagają, a nie przeszkadzają.....94
Rola lekcji.....94
Cel lekcji 3.5.....96
Dlaczego ludzie nie lubią procedur.....97
Najważniejsze tezy tej lekcji.....99
Kiedy procedura jest naprawdę potrzebna.....100

Przykład – procedura, która pomaga.....102
Częsty błąd: procedury pisane „pod audyt”.....103
Czego procedura NIE powinna robić.....104
Jak powinna wyglądać dobra procedura.....105
Struktura dobrej procedury.....106
Procedury w kontekście NIS2.....107
Case: „procedura, która była, ale nikt o niej nie wiedział”.....108
Ćwiczenie praktyczne.....109
Puenta lekcji 3.5.....110
Co dalej.....110
Lekcja 3.6 Dokumentacja w praktyce – jak audyt i NIS2 ją czytają.....111
Rola lekcji.....111
Cel lekcji 3.6.....112
Najważniejszy mit do obalenia.....113
Najważniejsze tezy tej lekcji.....115
Jak audytor czyta dokumentację?.....116
1. Skuteczny system daje spójność.....116

2. Dokumentacja a decyzje.....117
3. Wszyscy to brak odpowiedzialności.....117
4. „Żywy dokument” daje realność działania.....118
Czego audyt i NIS2/KSC NIE oczekują.....119
Czego audyt i NIS2/KSC OCZEKUJĄ.....120
Case: „kontrola, która niczego nie znalazła”.....121
Jak przygotować dokumentację „do obrony”.....122
Pytania, które warto sobie zadać PRZED audytem..123
Ćwiczenie końcowe.....124
Puenta lekcji 3.6.....125
Co dalej.....125
Lekcja 3.7 Podsumowanie MODUŁU 3 – od dokumentów do działania.....126
Rola lekcji.....126
Jak MODUŁ 3 domyka MODUŁ 2.....128
Co organizacja realnie zyskuje dzięki dokumentacji 130
Stabilność operacyjna i ciągłość wiedzy.....130
Skuteczność w sytuacjach kryzysowych.....131

Ochrona prawna i dowód świadomego zarządzania 131

Transparentność i zaufanie.....132

Dokumenty jako wsparcie, a nie zastępstwo.....133

Przygotowanie do kolejnego etapu: Od projektowania do działania.....135

Puenta MODUŁU 3.....137

PODSUMOWANIE.....139

DODATEK – PRZYKŁADOWE PROCEDURY.....141

PROCEDURA 1. NADAWANIE I ODBIERANIE DOSTĘPU DO DOKUMENTACJI MEDYCZNEJ.....142

PROCEDURA 2. REAKCJA NA OTWARCIE PODEJRZANEGO LINKU LUB ZAŁĄCZNIKA.....146

PROCEDURA 3. TWORZENIE KOPII I ODTWARZANIE DANYCH PRODUKCYJNYCH.....150

PROCEDURA 4. BEZPIECZNE PRZEKAZYWANIE DOKUMENTÓW KLIENTA.....154

PROCEDURA 5. KORZYSTANIE Z AI ONLINE PRZY TWORZENIU MATERIAŁÓW MARKETINGOWYCH...158

ZAPROSZENIE.....163

Informacje o prawach autorskich i moich utworach 165
ZAPROSZENIE.....166
Zostańmy w kontakcie!.....169
Ebooki poswojsku.pl.....170
Prawa autorskie i znaki towarowe.....174

Wstęp: Manifest Praktyka

Z wielkim żalem stwierdzam - na podstawie obserwacji otaczającej mnie rzeczywistości, że co najmniej duża część (a może nawet większość) procesów dokumentowania w wielu organizacjach, to nic innego jak **„teatrzyk bezpieczeństwa”**. Mam na myśli żmudne tworzenie setek a czasami nawet tysięcy stron tekstów, których podstawowym (choć często oficjalnie ukrytym) celem jest spełnienie wymogów formalnych (papirologicznych ;( ), a drugim - zadowolenia audytora. Równocześnie – operacja tworzenia dokumentacji bardzo często zupełnie ignoruje rzeczywistość operacyjną organizacji.

Efektem przedstawionego podejścia jest fakt posiadania przez organizację:

- obszernych polityk, których nikt nie czyta,
- procedur, które są omijane „w imię szybkiego, sprawnego działania”
- regulaminów, które powstają tylko po to, by „odhaczyć” kolejny punkt w checklistie KSC/NIS2.

A to oznacza, że nie jest budowany system bezpieczeństwa, tylko archiwum zbędnych papierów, dzięki którym organizacja łudzi się, że będzie bezpieczna. Ale zamiast bezpieczeństwa, uzyskiwane są zupełnie inne skutki:

- Dokumentacja staje się jedynie **uciążliwym obowiązkiem** zabierającym czas specjalistom - zamiast im pomagać.
- **Realny kryzys** – atak ransomware czy poważna awaria prowadzi do **chaosu**, bo nikt nie ma czasu na wertowanie **zbyt dużej ilości stron instrukcji**.
- Zamiast realnej ochrony, dokumentacja staje się **pułapką** tworzącą bardzo złudne poczucie bezpieczeństwa („przecież mamy procedurę”), podczas gdy w rzeczywistości organizacja pozostaje bezbronna.

Moduł 3 napisałem po to, aby pokazać właściwe podejście przy tworzeniu dokumentacji.

Pozwól, iż przypomnę - ten poradnik jest kontynuacją dwóch poprzednich, w których są zawarte odpowiednio: Moduł 1 Podstawy oraz

Moduł 2 Ryzyko i myślenie audytowe.

W poprzednim module - skupiliśmy się (mam nadzieję, że wspólnie) na „mózgu bezpieczeństwa" – analizie ryzyka. Nauczyliśmy się: myśleć, identyfikować zagrożenia i ustalać priorytety. Ale samo myślenie to zbyt mało. Trzeba jeszcze je utrwalić w strukturach organizacji.

Moduł 3 to etap „kodowania i utrwalania".

Nie będę Ciebie uczyć, jak pisać „ładne dokumenty" ani jak kopiować gotowe szablony z sieci, które nie mają żadnego przełożenia na Twoją firmę. Celem nie jest stworzenie kolejnego stosu najbardziej doskonałych papierów, tylko zbudowanie **prawdziwie decyzyjnych narzędzi**.

W tym module nauczysz się, jak stworzyć dokumentację, która:

- **Działa w praktyce**

Jest krótka, konkretna i użyteczna właśnie wtedy, gdy stres sięga zenitu.

- **Definiuje odpowiedzialność**

Kończy z unikaniem odpowiedzi typu „to nie moja decyzja” i „IT się tym zajmuje”.

- **Buduje dowód świadomego zarządzania**

Sprawia, że w oczach regulatora (NIS2/KSC) i audytora - jesteś organizacją, która panuje nad ryzykiem, a nie organizacją, która jedynie „ma papiery”.

Nie budujemy dokumentacji po to, by ją mieć. Budujemy ją po to, by **bezpieczeństwo stało się przewidywalne, a odpowiedzialność – jasna**.

Zapomnij o pisaniu „pod audyt”. Zacznij projektować system, który faktycznie działa.

Zaczynamy.

Lekcja 3.1: Po co w ogóle dokumentować? (i dlaczego większość dokumentacji nie działa)

Lekcja 3.1 Po co w ogóle dokumentować?

(i dlaczego większość dokumentacji nie działa)

Rola lekcji

To jest najważniejsza lekcja całego MODUŁU 3. Nie jest to jedynie wstęp teoretyczny, lecz fundament całego podejścia do zarządzania bezpieczeństwem. Jeżeli uczestnik nie zrozumie głębokiego sensu dokumentowania, całe procesy budowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) ulegną degradacji.

Jeżeli nie zrozumiesz, po co tworzysz dany dokument, to:

- każda polityka będzie „na półkę” – czyli zostanie stworzona raz, a potem całkowicie zignorowana przez pracowników,

- każda procedura będzie fikcją – czyli opis będzie opisywał procesy, które w rzeczywistości w ogóle nie mają miejsca,
- każda kontrola będzie tylko papierem – czyli audytorzy znajdą zapisy, ale nie znajdą w nich żadnej wartości dla bezpieczeństwa,
- NIS2 stanie się straszakiem zamiast ramą – zamiast narzędzia, które pomaga zarządzać ryzykiem, Ty i Twoja organizacja otrzymacie zestaw uciążliwych obowiązków, które głównie - generują stres.

Zrozumienie tej lekcji decyduje o tym, czy będziesz budować system, który działa, czy tylko taki, który „wygląda na działający”.

Cel lekcji 3.1

Po tej lekcji Czytelnik / Czytelniczka:

- rozumie, po co dokumentacja w ogóle istnieje i dlaczego jest niezbędnym elementem procesów biznesowych,
- przestaje traktować tworzenie dokumentów jako „papierologię” i zbędny koszt czasowy,
- widzi w dokumentacji realne narzędzie podejmowania decyzji oraz kluczowe narzędzie definiowania odpowiedzialności,
- rozumie logiczne powiązanie między analizą ryzyka (MODUŁ 2) a dokumentowaniem procesów (MODUŁ 3),
- jest mentalnie gotowy/a na praktyczne wyzwania związane z wdrażaniem standardów w organizacji.

Dlaczego dokumentacja ma złą reputację

Zadaj sobie pytanie: „Z czym kojarzy się dokumentacja w świecie IT i cyberbezpieczeństwa?”

Nie znam Twojej odpowiedzi, ale z obserwacji praktycznych – dokumentacja najczęściej kojarzy się z negatywnymi doświadczeniami:

- papierami tworzonymi wyłącznie „dla audytu” – dokumentami, które mają uspokoić kontrolera, ale nie mają żadnego przełożenia na realne bezpieczeństwo,
- dokumentami, których nikt nie czyta – bo są pisane językiem zbyt skomplikowanym, nieadekwatnym do grupy docelowej lub po prostu zbyt obszernymi,
- kopiowaniem gotowych szablonów z sieci – co prowadzi do tworzenia dokumentacji, która jest całkowicie oderwana od realiów danej firmy,

- uciążliwym obowiązkiem, a nie pomocą – procesami, które zabierają czas specjalistom, zamiast ułatwiać im pracę,
- segregatorem „na wszelki wypadek” – który służy jako magazyn przypadkowych notatek, a nie uporządkowana baza wiedzy.

To nie jest wina braku kompetencji ludzi. To jest wina źle rozumianego celu dokumentowania. Dokumentacja, która nie rozwiązuje żadnego problemu, jest marnotrawstwem zasobów organizacji.

Najważniejsze tezy tej lekcji

Dokumentacja nie powstaje po to, żeby coś było zapisane. Dokumentacja powstaje po to, żeby decyzje były

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 3 DOKUMENTACJA, KTÓRA MA SENS

Szczegóły oferty znajdziesz na stronie firmy Wydawnictwo Cyfrowe poswojsku.pl

ZAPROSZENIE

Seria wydawnicza:

BEZPIECZEŃSTWO INFORMACJI

CYBER AI KSC SZBI ISO 27001

Moduł 1 PODSTAWY

MODUŁ 2 Ryzyko i myślenie audytowe

MODUŁ 3 Dokumentacja, która ma sens

MODUŁ 4 Wdrożenie w praktyce

MODUŁ 5 Audyt wewnętrzny i doskonalenie

MODUŁ 6 Podsumowanie i dojrzałość

Poradniki – materiały edukacyjne dostępne będą w postaci:

A. ebooków dostępnych na poswojsku.pl

B. materiały wdrożeniowe na portalu Akademia Bezpieczeństwa GDDM www.gddm.com.pl

Serdecznie zapraszam do dalszego zgłębiania Twojej wiedzy i podnoszenia kompetencji w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa.

AUTOR: Dariusz Gołębiowski

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

szkolę, doradzam, audytuję, wdrażam i porządkuję obszary: bezpieczeństwo informacji, cyberbezpieczeństwo, RODO i ryzyko informacyjne

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

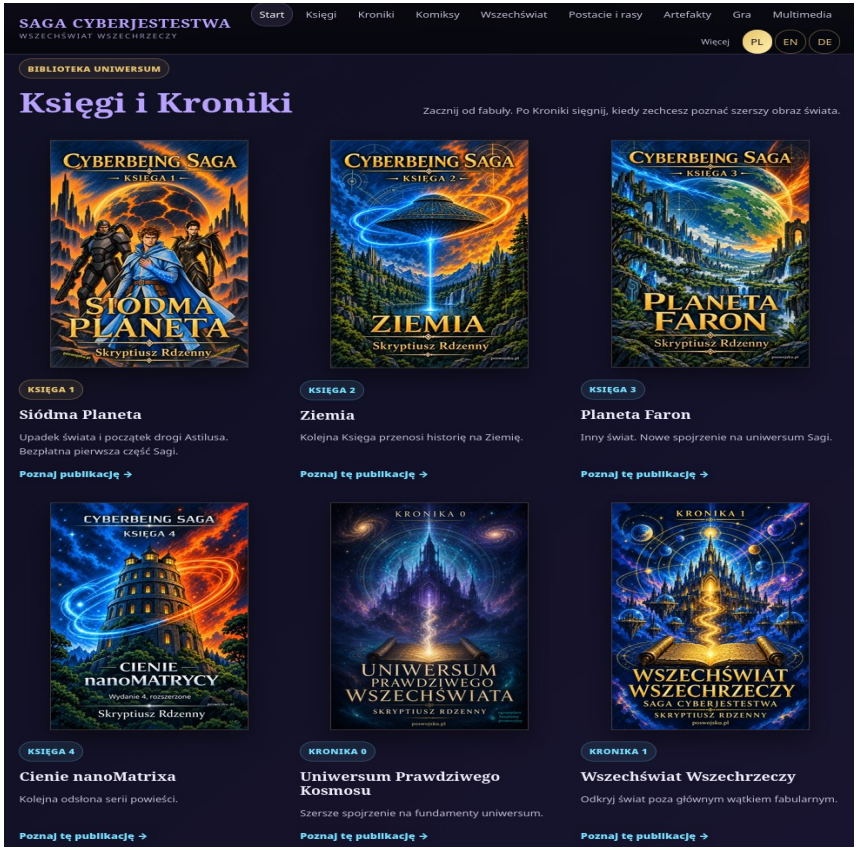
Księga 3 Planeta Faron

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

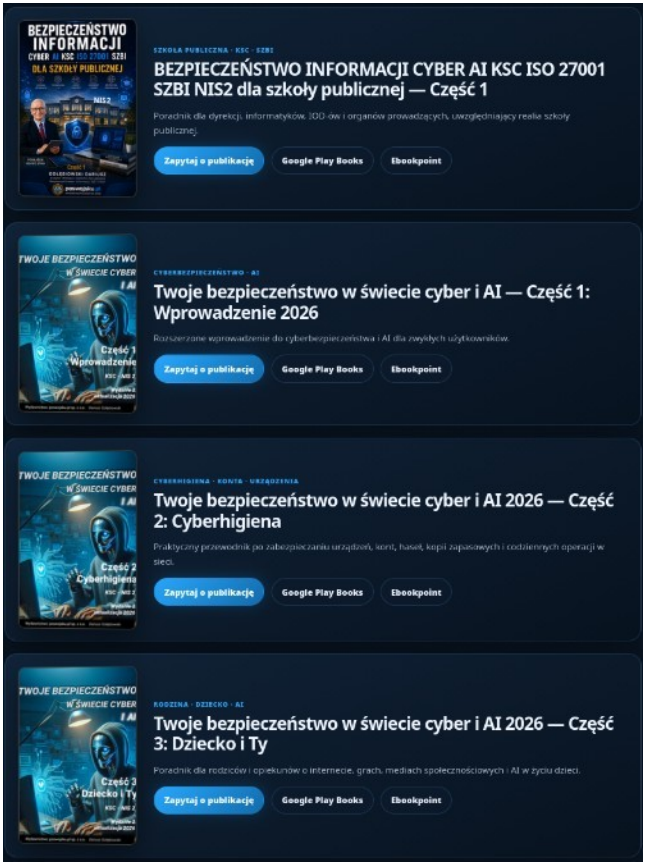
Praktyczny przewodnik po codziennych nawykach, które realnie zwiększają Twoje bezpieczeństwo: jak tworzyć silne hasła, chronić urządzenia, wykrywać próby oszustw i przygotować swoją rodzinę na zagrożenia cyfrowe. To pozycja obowiązkowa, jeśli chcesz, żeby cyberhigiena była naturalną częścią Twojego życia.

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.


BEZPIECZEŃSTWO INFORMACJI
CYBER AI KSC ISO 27001 SZBI
DLA SZKOŁY PUBLICZNEJ
SZKOŁA PUBLICZNA · KSC · SZBI
BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC ISO 27001 SZBI NIS2 dla szkoły publicznej — Część 1
Poradnik dla dyrekcji, informatyków, IOD-ów i organów prowadzących, uwzględniający realia szkoły publicznej.
Zapytaj o publikację
Google Play Books
Ebookpoint
TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I AI
Część 1 Wprowadzenie
CYBERBEZPIECZEŃSTWO · AI
Twoje bezpieczeństwo w świecie cyber i AI — Część 1: Wprowadzenie 2026
Rozszerzone wprowadzenie do cyberbezpieczeństwa i AI dla zwykłych użytkowników.
Zapytaj o publikację
Google Play Books
Ebookpoint
TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I AI
Część 2 Cyberhigiena
CYBERHIGIENA · KONTA · URZĄDZENIA
Twoje bezpieczeństwo w świecie cyber i AI 2026 — Część 2: Cyberhigiena
Praktyczny przewodnik po zabezpieczaniu urządzeń, kont, haseł, kopii zapasowych i codziennych operacji w sieci.
Zapytaj o publikację
Google Play Books
Ebookpoint
TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I AI
Część 3 Dziecko i Ty
RODZINA · DZIECKO · AI
Twoje bezpieczeństwo w świecie cyber i AI 2026 — Część 3: Dziecko i Ty
Poradnik dla rodziców i opiekunów o internecie, grach, mediach społecznościowych i AI w życiu dzieci.
Zapytaj o publikację
Google Play Books
Ebookpoint

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.