

Wydawnictwo Cyfrowe **poswojsku.pl**

BEZPIECZEŃSTWO INFORMACJI

Gołębiowski Dariusz

Audytor Wiodący Systemu Zarządzania
Bezpieczeństwem Informacji ISO 27001

CYBER AI KSC NIS2 SZBI

Moduł 3

DOKUMENTACJA, KTÓRA MA SENS

AKADEMIA BEZPIECZEŃSTWA GDDM

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

Ebook przygotowany z przyjacielskim wsparciem AI.

Wszelkie prawa do zawartości tej książki są zastrzeżone.

Nieautoryzowane przez autora rozpowszechnianie całości lub dowolnego fragmentu niniejszej publikacji w jakiegokolwiek 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

Spis treści

Wstęp: Manifest Praktyka.....	12
Lekcja 3.1 Po co w ogóle dokumentować?.....	16
Rola lekcji.....	16
Cel lekcji 3.1.....	18
Dlaczego dokumentacja ma złą reputację.....	19
Najważniejsze tezy tej lekcji.....	21
Dokumentacja jako przedłużenie myślenia ryzykiem	23
Przykład – „mamy procedury, ale...”	25
Trzy prawdziwe cele dokumentowania.....	27
Uporządkowanie decyzji.....	27
Przypisanie odpowiedzialności.....	28
Zapewnienie powtarzalności.....	28
Błąd organizacji: dokumentacja „na zapas”	30
Dokumentacja w kontekście NIS2.....	31
Case – „kopiuj-wklej”	32
Kiedy dokumentacja zaczyna działać.....	33
Ćwiczenie refleksyjne.....	34

Puenta lekcji 3.1.....	35
Co dalej.....	35
Lekcja 3.2 Co dokumentować w SZBI.....	36
Rola lekcji.....	36
Cel lekcji 3.2.....	37
Dlaczego dokumentowanie „wszystkiego” nie działa	38
Najważniejsza zasada tej lekcji.....	40
Trzy pytania, które decydują, czy coś dokumentować.....	40
Co dokumentować w SZBI – bezwzględnie.....	42
Decyzje dotyczące ryzyka.....	42
Role i odpowiedzialności.....	43
Zasady postępowania w sytuacjach krytycznych.	44
Zasady korzystania z kluczowych zasobów.....	44
Uzasadnienia decyzji.....	45
Czego NIE dokumentować i dlaczego.....	46
Oczywistości.....	46
Rzeczy jednorazowych.....	47

Szczegółów technicznych.....	47
Dokumentów „na wszelki wypadek”	48
Case – organizacja, która dokumentowała za dużo. 49	
Dokument jako narzędzie, nie archiwum.....	50
Ćwiczenie praktyczne: Analiza wartości dokumentu	52
Przykład analityczny: Polityka Hashingu Hasła.....	53
Puenta lekcji 3.2.....	55
Co dalej.....	55
Lekcja 3.3 Dokumentacja jako mapa odpowiedzialności	
– kto, za co i kiedy.....	57
Rola lekcji.....	57
Cel lekcji 3.3.....	58
Najczęstszy problem organizacji.....	59
Najważniejsze tezy tej lekcji.....	60
Odpowiedzialność a wykonywanie zadań.....	61
Pułapka: „IT się tym zajmuje”	63
Obszary, które dokumentacja musi jasno pokazywać	
.....	64
Odpowiedzialność w kontekście KSC i NIS2.....	65

Pułapka „wszyscy byli zaangażowani”	66
Dokumentacja, która faktycznie porządkuje.....	67
Gdzie najczęściej dochodzi do rozmycia odpowiedzialności?.....	68
Ćwiczenie praktyczne.....	70
Puenta lekcji 3.3.....	71
Co dalej.....	71
Lekcja 3.4 Jak dokumentować ryzyko, a nie strach.....	72
Rola lekcji.....	72
Cel lekcji 3.4.....	73
Dlaczego większość rejestrów ryzyka nie działa.....	75
Najważniejsze tezy tej lekcji.....	76
Co odróżnia zapis ryzyka od zapisu strachu.....	77
Przykład – to samo zdarzenie, dwa zapisy.....	78
Cztery elementy dobrego zapisu ryzyka.....	80
1. Kontekst organizacyjny.....	80
2. Skutek (a nie tylko zdarzenie).....	81
3. Decyzja.....	81
4. Odpowiedzialność.....	82

Błędne określenia: „wysokie, średnie, niskie”	83
Jak audyt i NIS2/KSC czytają ryzyko.....	85
Jak uprościć dokumentowanie ryzyka.....	86
Ćwiczenie praktyczne: Transformacja zapisu.....	87
Przykład pomocniczy.....	88
Puenta lekcji 3.4.....	90
Co dalej.....	90
Lekcja 3.5 Procedury, które pomagają, a nie przeszkadzają.....	91
Rola lekcji.....	91
Cel lekcji 3.5.....	93
Dlaczego ludzie nie lubią procedur.....	94
Najważniejsze tezy tej lekcji.....	96
Kiedy procedura jest naprawdę potrzebna.....	97
Przykład – procedura, która pomaga.....	99
Częsty błąd: procedury pisane „pod audyt”	100
Czego procedura NIE powinna robić.....	101
Jak powinna wyglądać dobra procedura.....	102
Struktura dobrej procedury.....	103

Procedury w kontekście NIS2.....	104
Case: „procedura, która była, ale nikt o niej nie wiedział”	105
Ćwiczenie praktyczne.....	106
Puenta lekcji 3.5.....	107
Co dalej.....	107
Lekcja 3.6 Dokumentacja w praktyce – jak audyt i NIS2 ją czytają.....	108
Rola lekcji.....	108
Cel lekcji 3.6.....	109
Najważniejszy mit do obalenia.....	110
Najważniejsze tezy tej lekcji.....	112
Jak audytor czyta dokumentację?.....	113
1. Skuteczny system daje spójność.....	113
2. Dokumentacja a decyzje.....	114
3. Wszyscy to brak odpowiedzialności.....	114
4. „Żywy dokument” daje realność działania.....	115
Czego audyt i NIS2/KSC NIE oczekują.....	116
Czego audyt i NIS2/KSC OCZEKUJĄ.....	117

Case: „kontrola, która niczego nie znalazła”	118
Jak przygotować dokumentację „do obrony”	119
Pytania, które warto sobie zadać PRZED audytem..	120
Ćwiczenie końcowe.....	121
Puenta lekcji 3.6.....	122
Co dalej.....	122
Lekcja 3.7 Podsumowanie MODUŁU 3 – od dokumentów do działania.....	123
Rola lekcji.....	123
Jak MODUŁ 3 domyka MODUŁ 2.....	125
Co organizacja realnie zyskuje dzięki dokumentacji	127
Stabilność operacyjna i ciągłość wiedzy.....	127
Skuteczność w sytuacjach kryzysowych.....	128
Ochrona prawna i dowód świadomego zarządzania	128
Transparentność i zaufanie.....	129
Dokumenty jako wsparcie, a nie zastępstwo.....	130

Przygotowanie do kolejnego etapu: Od projektowania do działania.....	132
Puenta MODUŁU 3.....	134
PODSUMOWANIE.....	136
DODATEK – PRZYKŁADOWE PROCEDURY.....	138
Informacje o prawach autorskich i moich utworach. .	157
ZAPROSZENIE.....	158
Zostańmy w kontakcie!.....	161
Ebooki poswojsku.pl.....	162
Prawa autorskie i znaki towarowe.....	166

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 checkliście 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”. Zaczynij 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:

- jasne,
- powtarzalne,
- możliwe do obrony.

W świecie wysokich standardów bezpieczeństwa (takich jak NIS2) nie liczy się to, czy masz spisany proces, ale to, czy potrafisz udowodnić, że proces ten został przemyślany, wdrożony i że ktoś bierze za niego odpowiedzialność.

Jeśli dokument:

- nie pomaga podejmować decyzji w sytuacjach kryzysowych,
- nie wyjaśnia precyzyjnie, kto i za co odpowiada w konkretnym procesie,
- nie jest używany w praktyce operacyjnej,

to nie jest on dokumentacją bezpieczeństwa. To jest artefakt biurokratyczny – martwy zapis, który jedynie zajmuje miejsce w systemie plików.

Dokumentacja jako przedłużenie myślenia ryzykiem

W MODUŁE 2 skupiliśmy się na fundamentach: nazwaliśmy ryzyka, przeanalizowaliśmy ich skutki, ustaliliśmy priorytety działań i zrozumieliśmy odpowiedzialność biznesową. To był etap myślenia i projektowania.

Dokumentacja nie zaczyna tego procesu od zera. Dokumentacja nie służy do tego, by „wymyślać” zasady na nowo. Jej rolą jest zamknięcie i utrwalenie procesu, który został już przeprowadzony w fazie analizy.

Dokumentacja to zapis Twojego myślenia o ryzyku.

W ten sposób powstaje logiczna ciągłość:

- dokumentacja przed ryzykiem = fikcja (tworzysz zasady, których nie potrzebujesz, bo nie wiesz, z czym walczysz),
- dokumentacja po ryzyku = narzędzie (opisujesz mechanizmy, które mają mitygować konkretne, zdefiniowane wcześniej zagrożenia).

Przykład – „mamy procedury, ale...”

Większość organizacji popełnia ten sam błąd: posiadają rozbudowane zasoby dokumentacji, które nie mają ze sobą żadnego związku. Organizacja posiada:

- politykę bezpieczeństwa,
- regulaminy pracy,
- instrukcje techniczne.

Jednak w momencie wystąpienia problemu (np. incydentu bezpieczeństwa) okazuje się, że:

- nikt nie wie, które ryzyka z listy są kluczowe dla działania firmy,
- decyzje o zmianach w systemach są podejmowane „w biegu”, bez odwołania do spisanych zasad,
- odpowiedzialność jest rozmyta, bo dokumenty nie wskazują konkretnych ról,

- dokumenty nie pomagają w kryzysie, bo są zbyt ogólne, by móc z nich wyciągnąć konkretne kroki działania.

Problemem nie jest brak dokumentów. Problemem jest brak sensu i spójności, które mogłyby połączyć poszczególne elementy w działający system zarządzania.

Trzy prawdziwe cele dokumentowania

Uporządkowanie decyzji

Dokumentacja jest historycznym zapisem procesów decyzyjnych. Pokazuje ona:

- jaką decyzję podjęto,
- dlaczego została ona podjęta w takim, a nie innym kształcie (np. ze względów kosztowych lub technicznych),
- kto za tę decyzję odpowiadał.

Bez dokumentacji decyzje znikają wraz z odejściem kluczowych pracowników. Organizacja traci zdolność do wyciągania wniosków z błędów lub sukcesów, co prowadzi do powtarzania tych samych błędów w przyszłości.

Przypisanie odpowiedzialności

W cyberbezpieczeństwie nie ma miejsca na domysły.
Dokumentacja musi odpowiadać na kluczowe pytania:

**Serdecznie dziękuję za to, że poświęciłeś/aś
swój czas na zapoznanie się z początkowymi
stronami mojego poradnika.**

**Zapraszam do skorzystania z pełnej wersji
ebooka:**

***BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC
SZBI ISO 27001 NIS 2 Moduł 3 DOKUMENTACJA,
KTÓRA MA SENS***

***Szczegóły oferty znajdziesz na stronie firmy
Wydawnictwo Cyfrowe poswojsku.pl***

Informacje o prawach autorskich i moich utworach

W poradniku wykorzystano:

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

DZIĘKUJĘ ZA UWAGĘ

Autor poradnika:

DARIUSZ GOŁĘBIEWSKI

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 spisanych przez ostatnich 30 lat - przygotowywane jest łącznie kilkanaście Ksiąg.

SAGA CYBERJESTESTWA

WSZECZŚWIAT WSZECHRZECZY

Start

Książki

Kroniki

Komiksy

Wszechświat

Postacie i rasy

Artefakty

Gra

Multimedia

Więcej

PL

EN

DE

BIBLIOTEKA UNIWERSUM

Książki 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 tę 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 WSZECZŚWIATA

SKRYPTIUSZ RDZENNY

primordium.pl

KRONIKA 0

Uniwersum Prawdziwego Kosmosu

Szersze spojrzenie na fundamenty uniwersum.

Poznaj tę publikację →

KRONIKA 1

WSZECZŚWIAT WSZECHRZECZY

SAGA CYBERJESTESTWA

SKRYPTIUSZ RDZENNY

primordium.pl

KRONIKA 1

Wszechświat Wszechrzeczy

Odkryj świat poza głównym wątkiem fabularnym.

Poznaj tę publikację →

MODUŁ 3 DOKUMENTACJA, KTÓRA MA SENS

32

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 budujemy
bezpieczniejszy i bardziej świadomy świat cyfrowy!**

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 Ci 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 NISZ dla szkoły publicznej — Część 1

SZKOŁA PUBLICZNA · KSC · SZBI

Poradnik dla dyrekcji, informatyków, IOO-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 2026

CYBERBEZPIECZEŃSTWO · AI

Rozszerzane wprowadzenie do cyberbezpieczeństwa i AI dla zwykłych użytkowników.

[Zapytaj o publikację](#) [Google Play Books](#) [Ebookpoint](#)



Twoje bezpieczeństwo w świecie cyber i AI 2026 — Część 2: Cyberhigiena

CYBERHIGIENA · KONIA · URZĄDZENIA

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 2026 — Część 3: Dziecko i Ty

RODZINA · DZIECKO · AI

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.