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

DLA SZKOŁY PUBLICZNEJ

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 i opracowaniem poradnika: ***BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC ISO 27001 SZBI NIS 2 dla SZKOŁY PUBLICZNEJ Część 1***. Poradnik powstał na bazie aktualnych przepisów oraz materiałów doradczo-szkoleniowych GDDM i poswojsku.pl, w tym szkoleń on-line dostępnych na portalu Akademia Bezpieczeństwa GDDM&poswojsku poswojsku.com.pl

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:

www.poswojsku.pl, bok@poswojsku.pl

ul. Paprocka 86, 98-220 Zduńska Wola

ISBN: 9788368360301

Copyright © poswojsku.pl 2026

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC ISO 27001 SZBI NIS 2 dla SZKOŁY PUBLICZNEJ Część 1

Poradnik powstał na bazie wewnętrznych materiałów szkoleniowych i doradczych właściciela firmy GDDM www.gddm.com.pl będącego certyfikowanym Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001



Spis treści

WPROWADZENIE.....14

1. Nowa Era Bezpieczeństwa.....15

2. Rola Prawa: uKSC, NIS2 i KRI jako podstawa podejmowanych decyzji.....17

3. Co to jest SZBI? Rozbiór Terminologii.....21

4. Mity vs. Rzeczywistość: Dlaczego nie kupimy „szablonu”?.....24

A. Brak kontekstu ryzyka (Risk-Based Approach).....25

B. Różne środowiska operacyjne.....26

C. Dokumentacja jako dowód.....26
D. Zgodność z uKSC 2026.....27
5. Rozpoczęcie Działania: Pierwsze kroki dla Dyrektora/Dyrektorki szkoły.....28
Różnica między „starym" a „nowym" podejściem do raportowania.....31
Podsumowanie.....32
Dodatek: CISO w kontekście SZBI i uKSC dla szkół publicznych.....33
1. Rozwinięcie Akronimu: CISO.....34
2. CISO w szkole publicznej – realia organizacyjne.....35
3. Kogo możemy powołać na omawianą funkcję w szkole? 37
4. Dlaczego to jest kluczowe dla uKSC 2026 i NIS2?.....39
5. Checklista Implementacji Roli (CISO).....41
ROZDZIAŁ 1: Czy szkoła publiczna podlega KRI, uKSC i NIS2?.....43

1. Cel i założenia rozdziału: De-mitologizacja prawa cybernetycznego.....45

2. Szkoły jako podmioty publiczne: Obowiązki wynikające z KRI i uKSC.....48

A. Podstawa prawna:.....49

Dlaczego szkoła publiczna (a np. prywatne?) musi zarządzać bezpieczeństwem?.....49

B. Konsekwencja: Obowiązek SZBI.....51

3. Zrozumienie uKSC/NIS2: Od "Podmiotu Kluczowego - Ważnego" do zarządzalnych obowiązków.....52

A. Koncepcja "Podmiotu Kluczowego lub Ważnego".....53

B. Uwaga Praktyczna: Zasada Proporcjonalności.....54

4. Praktyczna synteza: Łączenie Prawa, Standardów i Procesów.....56

5. Checklisty Decyzyjne dla Dyrekcji Szkoły....58

ROZDZIAŁ 2: Jak System Zarządzania Bezpieczeństwem Informacji przekształca prawo w działanie.....60

1. Definicja i rola SZBI: Od zbioru zasad do ciągłego procesu zarządzania ryzykiem.....62

2. Motor działania: Cykl PDCA – Fundament procesowego myślenia o bezpieczeństwie....72

Plan-Do-Check-Act (PDCA).....73

🟢 PLAN (planowanie).....73

🟡 DO (wykonywanie).....74

🔵 CHECK (sprawdzanie).....75

🟣 ACT (działanie naprawcze).....76

3. Mapa Tłumaczenia Prawnego (Legal-to-Process Mapping).....77

4. Governance i Zasoby Ludzkie: Kto jest odpowiedzialny? Budowanie kultury cyberbezpieczeństwa.....80

5. Checklista Wdrażania: Trzy najważniejsze kroki dla dyrekcji szkoły.....83

ROZDZIAŁ 3: Najważniejszy problem szkół – „Cyber Chaos Organizacyjny" i jak go usystematyzować.....90

1. Definicja Ryzyka: Czy to tylko bałagan? Nie, to jest systemowa porażka zarządzania ryzykiem.....92

2. Diagnoza Chaosu: Kategoryzacja luk.....94

Najczęstsze rodzaje chaosu w szkołach.....95

A. Chaos Zarządczy (Governance Vacuum).....95

B. Chaos Zasobów i Technologii (Technological Debt) 96

C. Chaos Identyfikacji i Dostępu (Access Control Failure).....98

D. Chaos Procesowy.....99

3. Analiza Konsekwencji: Dlaczego chaos jest najgorszy?.....100

4. Filary Naprawy: Jak SZBI koryguje chaos. 103

5. Wniosek dla Dyrektora/Dyrektorki: Od gaszenia pożarów do budowania odporności 106

ROZDZIAŁ 4: Co jest REALNIE najważniejszym zagrożeniem w szkole?.....110

1. Phishing.....113
2. Przejęcie konta nauczyciela/ki.....113
3. Brak MFA.....114
4. Prywatne laptopy nauczycieli/ek.....114
5. Ransomware.....115
6. Brak sensownych backupów.....115
7. Chaos uprawnień.....116
8. Jedno Wi-Fi dla wszystkich.....117
9. Zewnętrzny informatyk bez kontroli.....117
10. Papier pozostawiony „na wierzchu”.....118

1. Wprowadzenie: Zagrożenie nie jest zewnętrzne, jest systemowe.....119

2. Klasyfikacja Zagrożeń: Trzy filary ataku…121

Podstawowe filary ataku.....122

I. Filar Ludzki (The Human Element) – Najsłabsze ogniwo, ale w wyniku odpowiednich działań wewnętrznych - powinno ewoluować w kierunku najmocniejszego ogniwa cyberbezpieczeństwa danej organizacji.....122

II. Filar Techniczny (The Infrastructure) – Luka sprzętowa i systemowa.....123

III. Filar Zarządzający (The Governance) – Brak kontroli i odpowiedzialności.....125

3. Analiza Top Szczegółowa analiza krytycznych luk.....126

🔥 TOP PRIORYTET: Phishing i Przejęcie Konta.....127

💣 TOP KRYTYCZNOŚCI: Ransomware i Brak Backupów.....129

🛠️ TOP PORZĄDKOWOŚCI: Chaos uprawnień i Zewnętrzny Informatyk.....131

4. Scenariusz Ataku Kaskadowego: Jak to działa razem.....133

5. Checklista Defensywna: Pierwsze 3 miesiące 136

ROZDZIAŁ 5: Wprowadzenie do zagadnienia „Minimalne realistyczne SZBI dla małej/średniej szkoły”.....138

SZBI szkoły NIE może być „korporacyjne”....139

1. Co powinno być ABSOLUTNYM minimum? 140

ORGANIZACYJNIE.....140
TECHNICZNIE.....141

2. Najbardziej realistyczny model bezpieczeństwa dla małej szkoły publicznej 143

3. Największy problem przyszłości.....146

brak ludzi i kompetencji.....146

4. Najkrótsze podsumowanie.....148

PODSUMOWANIE Architektura Odporności i Nowa Rola Liderów Edukacji.....151

Podróż od zagrożenia do zarządzalnego procesu.....153

Synteza Źródeł Ryzyka: Jak wszystkie elementy się łączą? 155

Nowa Rola Liderów: Od menedżera do Architekta Bezpieczeństwa Cyfrowego.....157

3. Ostateczny Plan Działania: Zasada Priorytetowości.....161

Podsumowując: Zobowiązanie do ciągłej poprawy (filozofia Kaizen).....164

Co będzie w Części 2?.....170

ZAPROSZENIE.....172

📚 Poznaj inne książki poswojsku.pl.....174

🎓 Szkolenia i Webinary.....178

🌟 Zostańmy w kontakcie!.....180

✨

WPROWADZENIE

Fundamenty Bezpieczeństwa w Szkole Publicznej

podstawowa kwestia:

czy każda szkoła publiczna musi stworzyć, wdrożyć oraz utrzymywać tzw. SZBI?

Czyli:

System Zarządzania Bezpieczeństwem Informacji

1. Nowa Era Bezpieczeństwa

W dobie cyfryzacji edukacji szkoła nie jest już jedynie instytucją wychowawczą, ale też operatorem skomplikowanych systemów teleinformatycznych. Przechowujemy w nich dane uczniów, kadry zarządzającej i procesy administracyjne o wysokiej wartości. Współczesne środowisko zagrożeń cybernetyczne wymusza całkowitą zmianę podejścia do bezpieczeństwa – nie możemy już polegać na tym, że „nic się nie wydarzy”.

Znajdujemy się w kontekście nowych ram prawnych, które *nakładają obowiązki na każdy podmiot przetwarzający dane publiczne*. W ramach ebooka „Cyberbezpieczeństwo Informacji CYBER AI KSC ISO 27001 SZBI dla szkoły publicznej", rozpoczynamy od najważniejszego fundamentu: ***dlaczego szkoła publiczna musi mieć System Zarządzania Bezpieczeństwem Informacji (SZBI)*** i ***jak zbudować go zgodnie z nowymi wymaganiami***. Czyli już zapewne zrozumiałeś/aś:

na dzień pisania tego poradnika interpretacja jest taka, że ***każda szkoła publiczna musi:***

- ***stworzyć,***
- ***wdrożyć,***
- ***utrzymywać,***

tzw. SZBI !!!

2. Rola Prawa: uKSC, NIS2 i KRI jako podstawa podejmowanych decyzji

Pytanie retoryczne dla każdego dyrektora/ki szkoły brzmi: „Czy nasza placówka jest bezpieczna?". Odpowiedź musi być zgodna z obowiązującym prawem. W kontekście polskim kluczowe są dwa filary prawne:

1. **uKSC czyli Ustawa o Krajowym Systemie Cyberbezpieczeństwa (oparta na NIS2):**

   Nowelizacja polskiej uKSC oraz europejska Dyrektywa NIS 2 - definiują szkoły publiczne jako podmioty, które muszą (przymus prawny) wykonywać działania w zakresie zarządzania ryzykiem bezpieczeństwa cybernetycznego (ang. cybersafety). Nie ma wyboru – jest to **obowiązek ustawowy**.

2. **Krajowe Ramy Interoperacyjności (KRI):**

   Zgodnie z obowiązującym prawem, każda szkoła publiczna właściwie podlega KRI. Dlaczego?

Ponieważ:

- Jest jednostką sektora finansów publicznych.
- Realizuje zadania publiczne.
- Przetwarza informacje o charakterze publicznym.
- Wykorzystuje systemy teleinformatyczne do realizacji w.w. zadań.

Kluczowe wnioski z kontekstu prawnego:

Szkoła nie jest w tym przypadku tylko "obiektem edukacyjnym", ale podmiotem zobowiązanym do:

- Zarządzania bezpieczeństwem informacji (SZBI).
- Stosowania środków organizacyjnych i technicznych.

- Wykonywania regularnych analiz ryzyka.
- Zabezpieczania systemów i danych osobowych uczniów oraz kadry.

Ignorowanie tych wymagań to nie tylko brak bezpieczeństwa, ale ***naruszenie ustawy o Krajowym Systemie Cyberbezpieczeństwa*** (uKSC 2026), co:

może skutkować odpowiedzialnością osób zarządzających oraz nałożeniem kar administracyjnych lub karnych.

3. Co to jest SZBI? Rozbiór Terminologii

Dla Dyrektora/ki, Wójta czy Burmistrza oraz osoby zajmującej się cyberbezpieczeństwem (często fachowo określaną jako tzw. CISO), pojęcie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zwykle brzmi zbyt technicznie. Zatem przełóżmy to na język praktyki.

SZBI to nie jest „teczka z dokumentami". To proces ciągły (tworzenia, wdrażania, udoskonalania, utrzymywania), oparty na podejściu **Plan-Do-Check-Act (PDCA)**.

- **Plan:**
  Definiujemy cel (np. ochrona danych uczniów), analizujemy ryzyko i ustanawiamy cele bezpieczeństwa.
- **Do:**
  Wdrażamy środki – politykę hasłową, antywirusy, szkolenia, szyfrowanie.
- **Check:**
  Monitorujemy skuteczność – audyty, monitorowanie incydentów, różnego rodzaju przeglądy.

- **Act:**

  Działamy naprawczo, gdy coś się zepsuje lub zmienią warunki (np. nowy atak ransomware).

Zgodnie z normą ISO/IEC 27001:2022, SZBI musi być dostosowane do specyfiki organizacji. Szkoła to nie bank i nie firma produkcyjna – jej środowisko operacyjne, zagrożenia i aktywa informacyjne są unikalne.

4. Mity vs. Rzeczywistość: Dlaczego nie kupimy „szablonu”?

Wiele placówek wyraża chęć zakupienia gotowego wzorca SZBI lub szablonu dokumentacji z oferty zewnętrznej, aby spełnić wymogi formalne bez nakładania kosztów na personel IT. Jako Audytor ISO 27001 i Ekspert ds. Cyberbezpieczeństwa muszę stanowczo odradzić ten krok. Oto dlaczego:

A. Brak kontekstu ryzyka (Risk-Based Approach)

Niestety, standardowe wzorce nie uwzględniają specyfiki danego podmiotu. Gotowy szablon zawiera środki kontroli dla sektora finansowego lub ochrony danych wrażliwych, które są przesadzone dla typowej szkoły podstawowej lub wręcz przeciwnie – pomijają krytyczne luki. Bezpieczeństwo musi być proporcjonalne do ryzyka (zasada ISO 27001), a nie arbitralnie wysokie.

Szacowanie ryzyka powinno odnosić się do faktycznych zasobów danej organizacji, w tym przypadku – szkoły.

B. Różne środowiska operacyjne

Szkoła używa systemów edukacyjnych, platform LMS, chmury oraz lokalnej sieci. Gotowy szablon nie uwzględni specyfiki konkretnych urządzeń (np. interaktywne tablice, terminali czy drukarek w sali), które mogą być wektorami ataku.

C. Dokumentacja jako dowód

Organ nadzorczy (CSIRT poziomu krajowego lub inne) będzie wymagał dokumentowania decyzji: „Dlaczego zaimplementowaliśmy ten środek?". Gotowy szablon nie zawiera uzasadnienia w kontekście analizy ryzyka konkretnej szkoły.

Wniosek:

SZBI musi być **oparty na faktycznych potrzebach oraz możliwościach danej szkoły**. Musi odzwierciedlać rzeczywistość – m.in.:

- budżet,
- zasoby kadrowe (w tym kadrę IT),
- technologiczną infrastrukturę.
- specyfikę procesów nauczania.

D. Zgodność z uKSC 2026

Nowelizacja uKSC (uwzględniająca standardy NIS2) wymaga, aby system bezpieczeństwa był skalowany i dopasowany do kategorii obiektu kluczowego/ważnego. Szkoła publiczna jest istotnym podmiotem, a „gotowiec" nie uwzględni specyfiki ochrony danych osobowych w kontekście RODO oraz kryteriów KRI.

5. Rozpoczęcie Działania: Pierwsze kroki dla Dyrektora/Dyrektorki szkoły

Aby spełnić wymogi uKSC 2026, NIS2 i ISO 27001, szkoła musi podjąć następujące działania wdrożeniowe (Checklista Startowa):

1. **Ustalenie odpowiedzialności:**

   Wyodrębnienie odpowiedzialnej/ych za bezpieczeństwo informacji osoby/osób (CISO szkolny lub delegowane przez organ, CISO = Chief Information Security Officer czyli Kierownik Zarządzania Bezpieczeństwem Informacji). Na końcu wprowadzenia znajdziesz szczegółowe wyjaśnienie pojęcia CISO w kontekście szkolnym.

2. **Ocena stanu posiadania:**

   Spisanie listy aktywów informacyjnych (laptopy, tablice, bazy danych) i wrażliwych zasobów.

3. **Analiza ryzyka:**

   Przeprowadzenie pierwszej analizy zagrożeń pod kątem uKSC – kto atakuje? Co może stracić szkoła (przerwane zajęcia, dane uczniów)?

4. **Określenie zakresu SZBI:**

   Wytyczenie granic systemu (np. czy obejmuje to serwery lokalne, platformy zewnętrzne, telefony pracowników?).

5. **Opracowanie dokumentacji podstawowej:**

   Zamiast gotowca – polityki bezpieczeństwa dostosowane do kultury szkoły i procedury reagowania na incydenty (RAPORTOWANIE).

Różnica między „starym" a „nowym" podejściem do raportowania

Dawniej reagowano na incydent dopiero po .. tak, tak, szkoły to właściwie nie robiły zwykle nic. No chyba, że zostały zmienione oceny w dzienniku elektronicznym ;).

W nowym paradygmacie uKSC/NIS2 **obowiązuje** zgłaszanie do CSIRT i organu nadzorczego w określonym terminie (zgodnie z klasyfikacją zagrożenia). SZBI musi zawierać procedury raportowania dostosowane do tych wymagań, a nie „zamiatanie pod dywan".

Podsumowanie

Każda szkoła publiczna jest zobowiązana prawem do posiadania sprawczo działającego systemu bezpieczeństwa. Kupno gotowego wzorca nie spełnia wymogów normy ISO 27001 ani ustawy uKSC, ponieważ ignoruje zasadę proporcjonalności i specyfikę środowiska szkoły. Bezpieczeństwo informacji w szkole to nie koszt, a inwestycja w ciągłość edukacji i ochronę danych uczniów.

W następnym rozdziale przejdziemy do szczegółowego omówienia kluczowych wymagań ISO 27001:2022 pod kątem sektora edukacyjnego oraz konkretnych narzędzi technicznych, które należy zaimplementować w ramach SZBI dla szkoły publicznej.

Dodatek: CISO w kontekście SZBI i uKSC dla szkół publicznych

W tym ebooku, termin **„CISO szkolny”** jest używany jako funkcjonalny standard branżowy. Aby zapewnić pełną klarowność prawną i operacyjną w środowisku polskiej administracji publicznej, poniżej znajduje się szczegółowe rozwinięcie tego pojęcia dostosowane do specyfiki szkół i wymagań uKSC/NIS2.

1. Rozwinięcie Akronimu: CISO

CISO = Chief Information Security Officer (Kierownik Zarządzania Bezpieczeństwem Informacji).

W profesjonalnym środowisku cyberbezpieczeństwa - CISO to funkcja strategiczna, odpowiedzialna m.in. za:

- definicję polityk bezpieczeństwa,
- nadzór nad zgodnością z regulacjami (RODO, uKSC, NIS2),
- zarządzanie ryzykiem informacyjnym.

2. CISO w szkole publicznej – realia organizacyjne

Warto odnotować istotne rozróżnienie między **tytułem** a **funkcją**, które jest kluczowe w kontekście polskiej administracji i uKSC:

- **Tytuł:**

  W statucie szkoły rzadko znajdziesz pozycję „CISO". Jest to funkcja korporacyjna, często spotykana w dużych firmach IT.
- **Funkcja (Role):**

  Zgodnie z wymogami Dyrektywy NIS2 oraz art. 6a ustawy o Krajowym Systemie Cyberbezpieczeństwa, podmiot musi ustanowić wyraźnie określoną odpowiedzialność za bezpieczeństwo.

Wniosek praktyczny:

Szkoła nie musi zatrudniać oddzielnego pracownika z nowym tytułem „CISO”, jeśli budżet to nie pozwala. Jednak **musi być wyznaczone** ..

Życzę inspirującej lektury i wielu pomysłów, które pomogą budować bezpieczniejszą szkołę.

Dariusz Gołębiowski

Audytor Wiodący Systemu Zarządzania

Bezpieczeństwem Informacji ISO 27001

Zakup i pytania:

bok@poswojsku.pl poswojsku.pl

A gdybyś był/była zainteresowany/a szkoleniami z tematów omawianych w tym poradniku i/lub wdrożeniem SZBI w Twojej organizacji

serdecznie zapraszam do kontaktu z moją firmą:

biuro@gddm.com.pl , gddm.com.pl

Co będzie w Części 2?

Jeżeli chcesz szybki dostęp do Części 2 poradnika BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC ISO 27001 SZBI dla szkoły publicznej Część 1

napisz maila do Wydawnictwa Cyfrowego poswojsku bok@poswojsku.pl a jak tylko będzie dostępny – dostarczymy stosowną informację :).

W następnej części:

- nauczysz się **tworzyć SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)**,
- przykładowe – wzorcowe dokumenty związane z wdrożeniem uKSC 2026 i NIS2,
- mnóstwo niezbędnej fachowej wiedzy podanej w przystępny, zrozumiały sposób.

SERDECZNIE ZAPRASZAM CIEBIE

AUTOR Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

Dariusz Gołębiowski

ZAPROSZENIE

Seria wydawnicza:

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001

Moduł 1 PODSTAWY

a już wkrótce kolejne moduły.

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. szkolenia elearnig zakończonego certyfikatem Audytora Wewnętrznego na portalu Akademia Bezpieczeństwa GDDM - poswojsku.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

Poznaj inne książki poswojsku.pl

Jeśli spodobał się Tobie ten poradnik i chcesz dalej rozwijać swoją wiedzę o cyberbezpieczeństwie, technologii i świadomym korzystaniu z internetu, oto moje inne książki, które mogą w tym pomóc. Każda z nich powstała z myślą o osobach, które szukają praktycznych wskazówek, konkretnych przykładów i języka zrozumiałego dla każdego.

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 1: Praktyczny poradnik nie tylko dla nauczycieli

Sztuczna inteligencja to nie tylko moda, ale i realne narzędzie, które może usprawnić naukę i pracę. W tej książce pokazuję, jak korzystać z AI w prosty sposób – od generowania treści, przez wspieranie kreatywności, po automatyzację codziennych zadań. Idealna dla edukatorek/edukatorów i osób, które chcą poznać podstawy nowoczesnych technologii.

AI w edukacji – Część 2: Praktyczne pomysły na kreatywną edukację

Kontynuacja pierwszej części – pełna inspiracji, scenariuszy zajęć i ćwiczeń. Dowiesz się, jak prowadzić warsztaty i lekcje, które łączą AI z rozwojem kompetencji cyfrowych, logicznego myślenia i twórczego podejścia do nauki. Świetna pozycja dla wszystkich, którzy szukają konkretnych narzędzi i gotowych rozwiązań.

Stwórz Grę Mobilną

Praktyczny przewodnik dla osób, które marzą o stworzeniu własnej gry na smartfon. Od absolutnych podstaw programowania w JavaScript i React Native, przez projektowanie rozgrywki, aż po publikację gry. Jeśli chcesz uczyć się kodowania w sposób ciekawy i namacalny, to ta książka będzie Twoim drogowskazem.

Saga CyberJestestwa

Powieść science fiction dla tych, którzy chcą oderwać się od codzienności i zanurzyć w refleksyjnej historii o sensie istnienia, wolności i relacjach w obliczu zmian. To opowieść o ludziach i technologii, o wyborach i konsekwencjach – dla miłośniczek/miłośników literatury, którzy cenią głębsze przesłanie i oryginalny klimat.

Wszystkie moje ebooki możesz nabyć na:
📍 stronie wydawnictwa cyfrowego **poswojsku.pl**

Szkolenia i Webinary

Jeśli chcesz pogłębić wiedzę, zdobyć praktyczne umiejętności i od razu wprowadzić je w życie – zapraszam Cię na moje szkolenia i webinary. Każde z nich zostało przygotowane tak, aby w przystępny sposób przekazać konkretne rozwiązania i pomóc Ci działać od zaraz.

Bezpieczni w sieci – Jak chronić siebie i rodzinę przed cyberzagrożeniami

Szkolenie, w którym krok po kroku omawiam zagrożenia najczęściej dotykające rodziny – od fałszywych wiadomości i wyłudzeń danych, po ochronę urządzeń domowych i zabezpieczanie dzieci w internecie. Idealne dla rodziców, opiekunów i osób, które chcą działać świadomie.

Cyberbezpieczeństwo dla małych organizacji i firm

Praktyczny warsztat dla właścicieli firm, fundacji i urzędów, którzy chcą nauczyć się chronić dane pracowników i klientów bez kosztownych wdrożeń. Omawiam darmowe narzędzia, procedury bezpieczeństwa i sposoby budowania kultury cyberhigieny w zespole.

AI w życiu codziennym – od podstaw

Webinar pokazujący, jak sztuczna inteligencja może ułatwić pracę, naukę i organizację codziennych spraw. Dowiesz się, jak korzystać z AI do tworzenia treści, automatyzacji zadań i rozwijania nowych umiejętności – nawet jeśli nie masz doświadczenia technicznego.

Szyfrowanie danych – dyski, pliki, poczta

Szkolenie wprowadzające w świat szyfrowania, pokazujące krok po kroku, jak zabezpieczyć swoje dane prywatne i firmowe za pomocą bezpłatnych narzędzi. Idealne dla każdego, kto chce uniknąć utraty poufnych informacji.

Cyfrowe bezpieczeństwo dziecka – jak mądrze wspierać młodych użytkowników internetu

Spotkanie dla rodziców i nauczycieli, którzy chcą dowiedzieć się, jak rozmawiać z dziećmi o zagrożeniach online, jak ustawiać kontrolę rodzicielską i jak budować zaufanie w cyfrowym świecie.

Aktualne terminy szkoleń i webinarów znajdziesz na stronie: poswojsku.pl

a webinarów: www.poswojsku.com.pl

Zapraszam również do kontaktu – chętnie pomogę dobrać szkolenie odpowiednie dla Twoich potrzeb.

Zostańmy w kontakcie!

Jeśli chcesz być na bieżąco z nowymi książkami, szkoleniami i inspiracjami o cyberbezpieczeństwie, technologii i AI – zapraszam Cię do obserwowania moich profili. Dzięki temu nie przegapisz premier, promocji i wartościowych materiałów które tworzę: często, prosto, przystępnie i z humorem.

- ***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!