

BEZPIECZEŃSTWO INFORMACJI

CYBER **AI** KSC SZBI **ISO 27001**



OCHRONA
INFORMACJI



TECHNOLOGIA
I AI



ŁUDZIE
I PROCESY



ZGODNOŚĆ
I NORMY



BEZPIECZNA
ORGANIZACJA



PODEJŚCIE
ISO/IEC 27001

Moduł 2

RYZYZKO I MYŚLENIE AUDYTOWE

GOŁĘBIOWSKI DARIUSZ

Audytor Wiodący Systemu Zarządzania
Bezpieczeństwem Informacji ISO 27001

poswojsku.pl

AKADEMIA BEZPIECZEŃSTWA GDDM

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 i opracowaniem poradnika:

***BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI
ISO 27001 Moduł 2 Ryzyko i myślenie audytowe.***

Poradnik powstał na bazie Modułu szkolenia on-line dostępnego na portalu Akademii Bezpieczeństwa GDDM&poswojsku poswojsku.com.pl

Czytaj tylko legalnie kupione egzemplarze.

UWAGA – AI!

***Grafiki umieszczone w poradniku zostały stworzone przez AI –
na podstawie opisów przygotowanych przez Autora.***

Autor oraz Wydawnictwo Cyfrowe 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 Cyfrowe poswojsku.pl – kontakt:

www.poswojsku.pl, bok@poswojsku.pl

ul. Paprocka 86, 98-220 Zduńska Wola

ISBN: 978-83-68360-34-9

Copyright © poswojsku.pl 2026

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

Od Autora Kilka słów o formach żeńskich i męskich

Wspaniała Czytelniczko - Drogi Czytelniku

Zależy mi, aby moje publikacje były przyjazne dla wszystkich osób. Jednocześnie staram się pisać w sposób prosty, naturalny i wygodny w czytaniu.

Dlatego w książce czasami używam form męskich, a czasami żeńskich. Wszystkie odnoszą się do każdej osoby czytającej tę publikację, niezależnie od płci, wieku, pochodzenia, stanowiska czy sposobu, w jaki sama siebie określa.

Nie stosuję 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, z góry przepraszam. Nie jest to działanie zamierzone – po prostu jestem autorem książek :), a nie księgową ;) końcówek językowych.

**Życzę przyjemnej lektury wszystkim osobom
czytającym tę książkę.**

**BEZPIECZEŃSTWO
INFORMACJI
CYBER AI KSC
SZBI ISO 27001
NIS2 Moduł 2
Ryzyko i myślenie
audytowe**

Poradnik jest kontynuacją ebooka

**BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI
ISO 27001 NIS 2 Moduł 1 Podstawy.**

Poradnik powstał na bazie

**materiałów wewnętrznych firmy doradczo
szkoleniowej Gołębiowski Dariusz Doradztwo
Merytoryczne gddm.com.pl oraz**

szkolenia on-line na portalu poswojsku.com.pl .

**Gdy ukończysz w.w. szkolenie - możesz otrzymać
certyfikat:**

Audytor Wewnętrzny Bezpieczeństwa.

**Drugim sposobem uzyskania w.w. Certyfikatu - jest
egzamin, który przygotowany został na bazie tej serii
poradników.**

**Jeżeli jesteś zainteresowany/a uzyskaniem w.w.
certyfikatu - prosimy o kontakt: bok@poswojsku.pl**



Spis treści

Lekcja 2.1 Czym jest ryzyko w rzeczywistym świecie - bez strachu, bez tabel, bez „ISO-bełkotu”	12
Wstęp: Dlaczego ta lekcja jest fundamentem Twojego bezpieczeństwa?.....	13
1. Rozbijanie mitów: Dlaczego słowo „ryzyko” budzi opór?.....	15
2. Najważniejsza definicja Zasada Złotego Standardu.....	19
3. Ryzyko ≠ Zagrożenie ≠ Strach - Kluczowe idee.....	21
Błąd nr 1: Mylenie ryzyka z zagrożeniem.....	22
Błąd nr 2: Zarządzanie przez strach (Scenariusze Apokaliptyczne).....	24

4. Ryzyko jako narzędzie decyzji - Analiza praktyczna.....	25
Studium przypadku 1: „To tylko mały system”	27
Studium przypadku 2: „Przecież wszyscy sobie ufamy”	28
5. Gdzie w tym wszystkim jest NIS2? -	
Perspektywa polskiego rynku.....	29
Ćwiczenie refleksyjne (5 minut).....	32
Podsumowanie lekcji 2.1.....	33
Lekcja 2.2 Zagrożenie, podatność i ryzyko – dlaczego to NIE jest to samo.....	34
Wprowadzenie: Architektura myślenia o bezpieczeństwie.....	35
Trzy filary Twojego bezpieczeństwa.....	38
Analiza przypadków: Zobacz to w praktyce...44	
Dlaczego to rozróżnienie jest kluczowe dla Zarządu i CISO?.....	48

Kontekst NIS2 i uKSC – Co mówi prawo?.....	51
Podsumowanie lekcji.....	54
Lekcja 2.3 Skutki i priorytety ryzyka – co naprawdę boli organizację.....	55
Dlaczego skutki są kluczowe?.....	58
Definicja skutku w kontekście biznesowym...	60
Błąd nr 1: Skupienie na zdarzeniu zamiast na skutku.....	62
Perspektywa Zarządu a wymagania NIS2.....	66
Skutki bezpośrednie i pośrednie.....	67
Błąd nr 2: Pułapka „wszystko jest krytyczne”. 69	
Ćwiczenie pogłębione: Analiza realnych skutków.....	72
Podsumowanie lekcji 2.3.....	75
Lekcja 2.4 Co zrobić z ryzykiem? Od matematyki decyzyjnej do strategii biznesowej.....	76

Wprowadzenie: Ryzyko jako „menu” możliwości.....	77
1. Cztery filary traktowania ryzyka (Model Decyzyjny).....	80
2. Mechanika Szacowania: Jak mierzymy to, co musimy zarządzać?.....	86
3. Analiza kosztów vs. korzyści (CBA) i zasada proporcjonalności.....	91
4. Pułapka „Bezpłatnej Akceptacji” (Perspektywa NIS2/uKSC).....	93
5. Ścieżka audytowa (ISO 27001 & NIS2).....	95
Podsumowanie lekcji 2.4: Od reaktywności do strategii.....	98
Lekcja 2.5 Jak audytorka / kontroler patrzy na organizację i czego naprawdę szuka.....	100

Wprowadzenie: Audyt to lekarz, nie policjant	
.....	101
Fundament filozoficzny: Odpowiedź systemu zamiast winy jednostki.....	104
Trzy filtry audytora: Jak profesjonalista ocenia organizację	
.....	106
1. Powtarzalność (Systemowość).....	106
2. Decyzje, nie intencje.....	107
3. Spójność (Zasada „Say-Do-Write”).....	108
Analiza przypadków (Case Studies).....	111
Audyt jako lustro kultury organizacyjnej.....	114
Audyt w kontekście uKSC i NIS2.....	115
Refleksja dla liderów, praktyków, a przede wszystkim szeroko rozumianego Szefostwa.....	117
Podsumowanie lekcji 2.4:.....	119
Lekcja 2.6 Jak samodzielnie zauważać ryzyka – w codziennej pracy, bez tabel.....	120
Od „gaszenia pożarów” do budowania bezpiecznej bazy.....	121
Ryzyko to umiejętność obserwacji, nie skomplikowana matematyka.....	124
Pięć pytań diagnostycznych - Twoje narzędzia codziennej uważności.....	125
Analiza przypadków: Ryzyko ukryte w codzienności.....	131

Obsługa Ryzyka jako systematyczne działanie (nawyk), a nie - okresowo celebrowany projekt.....	135
Ćwiczenie pogłębione dla Ciebie:.....	136
Podsumowanie: Ryzyko rzadko krzyczy.....	138
Lekcja 2.7 Podsumowanie MODUŁU 2 i	
przygotowanie do dalszej drogi.....	139
Od Strachu do Strategii: Mapa Twojej Drogi.....	140
Ryzyko jako Tarcza, nie tylko „Problem” (Zarządzanie vs Gaszenie Pożarów).....	142
Analiza Przypadku: Pętla Nieskończona - Incydent bez wartości edukacyjnej.....	144
Kontekst Regulacyjny: Gdzie w tym procesie znajduje się NIS2?.....	146
Rola Dokumentacji: Żywy Organizm a Martwa Dokumentacja.....	149
Podsumowanie i przejście do praktyki.....	151
Co będzie w MODUŁE 3?.....	153
ZAPROSZENIE.....	154
 Poznaj inne książki poswojsku.pl.....	156
 Szkolenia i Webinary.....	160
 Zostańmy w kontakcie!.....	162



Lekcja 2.1 Czym jest ryzyko w rzeczywistym świecie - bez strachu, bez tabel, bez „ISO- bełkotu”

Wstęp: Dlaczego ta lekcja jest fundamentem Twojego bezpieczeństwa?

Fundamenty bezpieczeństwa:

Ryzyko, to nie jest strach przed hakerami.

**Ryzyko, to narzędzie do podejmowania lepszych
decyzji biznesowych.**

Wielu menedżerów i właścicieli firm traktuje cyberbezpieczeństwo jako „projekt IT” lub „kosztowny obowiązek prawny”. To błąd strategiczny, który może kosztować organizację fortunę.

Jeśli nie zrozumiesz istoty ryzyka w Twojej organizacji, każda kolejna procedura (w tym te wynikające z dyrektywy NIS2/KSC czy normy ISO 27001) - stanie się dla:

- Ciebie,
- całego personelu,
- organizacji jako całości,

jedynie martwym zestawem dokumentów – „papierologią”, która ma uspokoić kontrolerkę, udziałowców czy audytora, ale nie chroni realnego biznesu.

1. Rozbijanie mitów: Dlaczego słowo „ryzyko” budzi opór?

**ROZBIJANIE MITÓW:
DLACZEGO SŁOWO „RYZYO” BUDZI OPÓR?**

Ryzyko nie jest wrogiem. Jest informacją, która pomaga podejmować mądre decyzje.

CO MYŚLĄ, ŻE TO JEST:

- "To coś strasznego."
- "To oznacza, że coś nie powinno się wydarzyć."
- "To tylko teoria i ukomplikowane tabele."
- "To wskazuje problemy na ulicy."
- "To dodatkowa burokracja."

CZYM JEST NAPRAWDĘ:

- TO SPŁATZENIE W PRZYSZŁOŚĆ**
Przewiduje infekcję, co może się wydarzyć i zanim się wydarzy.
- TO NARZĘDZIE DO DEKLEJ**
Pomaga wyłuskać najbardziej istotne informacje spośród nadmiarowych danych.
- TO PROFITYT**
Odpowiedzi są na pytania, co naprawdę warto, a nie na co nie warto.
- TO WIEDZA + MOC**
Nie tylko. Rozumienie sytuacji, tym bardziej – skuteczność działania.
- TO INWESTYCJA W SPOKOJ**
Dobre decyzje dają cenną energię firm, naszych ludzi i naszej gospodarki.

**RYZYO TO NIE STRACH.
TO ŚMIAŁE ZARZĄDZANIE PRZYSZŁOŚCI.**
Nie chodzi o to, by nigdy nie spać. Chodzi o to, by wiedzieć, gdzie są kamienie, zanim postawisz krok.

CO ZYSKUJESZ DZIĘKI PODEJŚCIU OPARTEMU NA RYZYKU?

- WIĘKSZE BEZPIECZEŃSTWO**
Wzrost odporności przedsiębiorstwa na wszelkie zagrożenia.
- LUCYFRO WYNIK RÓWNOWAGI**
Wzrost przychodów oraz osiągniętych rezultatów.
- CIĄPANE RELACJE: PARTNERSTW**
Przekazanie, że Wasz zespół jest w zgodzie z innymi.
- ZOBOWIĄZANIE Z PRZESZŁOŚCI**
Jedną z najważniejszych zasad jest: nie powtarzaj błędów.
- WIĘCEJ SPOKOJU**
Wiedza, że wiesz, co możesz w sposób odpowiedzialny realizować.
- LUCYFRO DEKLEJ RÓWNOWAGI**
Reguluje się to samoczynnie. Wtedy plany i fakty są w zgodzie.

**ZARZĄDZAJ RYZYKIEM - NIE DLATEGO, ŻE MUSISZ.
DLATEGO, ŻE CHCESZ PROWADZIĆ FIRMĘ W DOBRYM KIERUNKU.**

W tradycyjnym ujęciu, gdy słyszymy słowo „ryzyko”, nasz mózg automatycznie uruchamia mechanizmy obronne. Ryzyko utożsamiamy ze strachem. Często mylimy je z:

- **„Coś złego”** - katastrofa, awaria
a to wywołuje paraliż decyzyjny.
- **„Odpowiedzialnością”** - kto zawinił? kto pójdzie do sądu?
co z kolei rodzi kulturę strachu i ukrywania błędów.
- **„To jest temat dla informatyków, od tego przecież ich mamy”**

efekt – zarząd (kierownictwo, dyrekcja) deleguje ten temat całkowicie „w dół” organizacji, tracąc kontrolę nad tym kluczowym zagadnieniem.

Zmiana paradygmatu:

W profesjonalnym systemie zarządzania bezpieczeństwem (SZBI), ryzyko nie jest wrogiem.

Ryzyko to informacja.

za którą płacisz:

- **uwagę,**
- **zasoby.**

Jeśli ryzyko jest dobrze zdefiniowane, mówi Tobie dokładnie, gdzie musisz zainwestować środki, a gdzie możesz pozwolić sobie na akceptację stanu obecnego.



Skala Ryzyka – Bilans Decyzyjny

2. Najważniejsza definicja

Zasada Złotego Standardu



Jeśli miałybyś zapamiętać tylko jedno zdanie z tego rozdziału, niech to będzie:

„Ryzyko to prawdopodobieństwo wystąpienia negatywnego skutku oraz wielkość wpływu tego skutku na ciągłość i cele organizacji.”

Z tej definicji wynikają dwa kluczowe wnioski, które odróżniają profesjonalistów od amatorów:

1. Nie wszystko, co może się zdarzyć, jest ryzykiem.

Jeśli coś jest mało prawdopodobne i ma znikomy wpływ na firmę (np. uderzenie meteorytu w biuro), nie poświęcamy na to zasobów.

2. Nie każdy problem wymaga tej samej uwagi.

Ryzyko pozwala nam segregować problemy – od tych, które są „hałasem”, po te, które mogą doprowadzić do upadku firmy.

3. Ryzyko ≠ Zagrożenie ≠ Strach - Kluczowe idee



Wielu praktyków popełnia błędy, bo używa tych słów zamiennie. To tak, jakbyś mylił „burzę” z „zalaniem piwnicy”. Przecież nie każda burza prowadzi do kłopotów wewnątrz piwnicy. Prawda? Ale z drugiej strony – każda burza – potencjalnie - może spowodować kłopoty.

Błąd nr 1: Mylenie ryzyka z zagrożeniem.

- **Zagrożenie (Threat)**

To zewnętrzny lub wewnętrzny czynnik, który **może** wywołać zdarzenie (np. „Phishing”, „Atak Ransomware”, „Awarie sprzętu”).

- **Podatność (Vulnerability)**

To słaba strona Twojej organizacji (np. brak kopii zapasowych, stare hasła, brak edukacji pracowników w zakresie cyberhigieny).

- **Ryzyko (Risk)**

To wynik analizy – co się stanie, gdy **Zagrożenie** uderzy w Twoją **Podatność**.



Równanie Ryzyka

Błąd nr 2: Zarządzanie przez strach (Scenariusze Apokaliptyczne).

Prezentowanie zarządzania ryzykiem jako serii „czarnych scenariuszy” i wizji apokalipsy powoduje, że ludzie zamykają się na dialog. Zamiast analizować realne zagrożenia, zaczynają unikać tematu, bo kojarzy się on z karami.

Podejście pro-biznesowe:

Ryzyko nie mówi „nie różniamy tego”. Ryzyko mówi: „Jeśli wybierzesz tę ścieżkę, musisz być świadomy tych konkretnych skutków i przygotować na nie plan”.

4. Ryzyko jako narzędzie decyzji - Analiza praktyczna

W dojrzałej organizacji zarządzanie ryzykiem służy do zadawania pytań zarządowi (i często także - innym kluczowym osobom w organizacji):

„Czy to jest dla nas ważne? Czy możemy to zaakceptować? Co się stanie, jeśli nic nie zrobimy?”



Studium przypadku 1: „To tylko mały system”

Organizacja korzysta ze starego systemu bazy danych , który nie ma kopii zapasowych, bo „od lat działa bezawaryjnie”.

- **Zagrożenie:**

Awaria sprzętu lub błąd bazy.

- **Ryzyko (biznesowe):**

Całkowity paraliż pracy działu sprzedaży, utrata danych klientów i konieczność ręcznego wpisywania informacji przez kilka tygodni.

- **Decyzja zarządu:**

Czy koszt wdrożenia nowoczesnego systemu jest wyższy niż potencjalny koszt 2 tygodni przestoju firmy?

Studium przypadku 2: „Przecież wszyscy sobie ufamy”

W firmie stosuje się wspólne hasła do systemów i szerokie uprawnienia, bo „pracownicy muszą sobie pomagać”.

- **Zagrożenie**

Błąd człowieka lub nieautoryzowany dostęp.

- **Ryzyko (biznesowe)**

Brak możliwości ustalenia, kto dokonał zmiany w dokumentacji finansowej; utrata kontroli nad integralnością danych; brak możliwości przeprowadzenia audytu.

- **Decyzja zarządu**

Czy „wygoda” wspólnego logowania jest warta ryzyka utraty kontroli nad kluczowymi danymi finansowymi?

5. Gdzie w tym wszystkim jest NIS2? - Perspektywa polskiego rynku

Nowelizacja uKSC oraz Dyrektywa NIS2 nie nakładają na Ciebie obowiązku posiadania „idealnego” zabezpieczenia technicznego. One nakładają na Ciebie **obowiązek zarządzania ryzykiem.**

Państwowe organy nadzorcze (w kontekście polskiego rynku) będą pytać:

.....

**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 2 Ryzyko i
myślenie audytowe***

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

Co będzie w MODUŁE 3?

Moduł 3: Dokumentacja, która ma sens (SZBI i NIS2)

To nie będzie nauka o „papierologii”. To będzie nauka tworzenia narzędzi do dokumentowania decyzji i przypisywania odpowiedzialności, aby system bezpieczeństwa działał skutecznie i spełniał wymogi prawne.

MODUŁ 3 – xxx

ale to już kolejna książka oraz szkolenie na portalu www.poswojsku.com.pl z którego możesz otrzymać certyfikat Audytor Wewnętrzny Systemu Bezpieczeństwa.

ZAPROSZENIE

Seria wydawnicza:

**BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI
ISO 27001**

Moduł 1 PODSTAWY

MODUŁ 2 Ryzyko i myślenie audytowe

a już wkrótce kolejne moduły.

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 Tobie 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 Ciebie na moje szkolenia i webinary. Każde z nich zostało przygotowane tak, aby w przystępny sposób przekazać konkretne rozwiązania i pomóc Tobie działać od zaraz.



Bezpieczni w sieci – Jak chronić siebie i rodzinę przed cyberzagrożeniami

Szkolenie, w którym krok po kroku omawiam zagrożenia najczęściej dotyczące 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 Ciebie 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 budujemy
bezpieczniejszy i bardziej świadomy świat cyfrowy!**