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 2

RYZYKO I MYŚLENIE AUDYTOWE

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 SZBI ISO 27001 Moduł 2 Ryzyko i myślenie audytowe***.
Poradnik powstał na bazie Modułu szkolenia on-line dostępnego na portalu Akademia 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

Materiał edukacyjny oparty jest na podejściu do zarządzania bezpieczeństwem informacji opartym na 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).....110
Audyt jako lustro kultury organizacyjnej.....113
Audyt w kontekście uKSC i NIS2.....114
Refleksja dla liderów, praktyków, a przede wszystkim szeroko rozumianego Szefostwa.....116
Podsumowanie lekcji 2.4:.....118

Lekcja 2.6 Jak samodzielnie zauważać ryzyka – w codziennej pracy, bez tabel.....119

Od „gaszenia pożarów" do budowania bezpiecznej bazy.....120

Ryzyko to umiejętność obserwacji, nie skomplikowana matematyka.....123

Pięć pytań diagnostycznych - Twoje narzędzia codziennej uważności.....124
Analiza przypadków: Ryzyko ukryte w codzienności.....130
Obsługa Ryzyka jako systematyczne działanie (nawyk), a nie - okresowo celebrowany projekt.....134

Ćwiczenie pogłębione dla Ciebie:.....135
Podsumowanie: Ryzyko rzadko krzyczy.....137
Lekcja 2.7 Podsumowanie MODUŁU 2 i przygotowanie do dalszej drogi.....138
Od Strachu do Strategii: Mapa Twojej Drogi.....139
Ryzyko jako Tarcza, nie tylko „Problem” (Zarządzanie vs Gaszenie Pożarów).....141
Analiza Przypadku: Pętla Nieskończona - Incydent bez wartości edukacyjnej.....143
Kontekst Regulacyjny: Gdzie w tym procesie znajduje się NIS2?.....145
Rola Dokumentacji: Żywy Organizm a Martwa Dokumentacja.....148
Podsumowanie i przejście do praktyki.....150
Co będzie w MODUŁE 3?.....152
ZAPROSZENIE.....153
Informacje o prawach autorskich i moich utworach.....155
ZAPROSZENIE.....156
Zostańmy w kontakcie!.....159
Ebooki poswojsku.pl.....160
Prawa autorskie i znaki towarowe.....164

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?



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 miałabyś 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 pracownic 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 rózróżniamy 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?”


RYZYKO JAKO NARZĘDZIE DECYZJI
ANALIZA PRAKTYCZNA
Dobra analiza ryzyka pomaga porównać koszt zabezpieczeń z realnym kosztem przestoju biznesu.
1
ZAGROŻENIE
• Awaria sprzętu lub błąd bazy
Problem techniczny sam w sobie nie jest jeszcze pełnym opisem ryzyka.
2
RYZYKO BIZNESOWE
• Całkowity paraliż pracy działu sprzedaży
• Utrata danych klientów
• Konieczność ręcznego wpisywania informacji przez kilka tygodni
2 TYGODNIE
poswojsku.pl
To właśnie skutek biznesowy pokazuje, jak bolesne może być ryzyko.
3
DECYZJA ZARZĄDU
Czy koszt wdrożenia nowoczesnego systemu jest wyższy niż potencjalny koszt 2 tygodni przestoju firmy?
KOSZT WDROŻENIA
Nowy system
Migracja danych
Szkolenie zespołu
KOSZT PRZESTOJU
Utracona sprzedaż
Praca ręczna zespołu
Utrata danych klientów
Opóźnienia i utrata zaufania
Ryzyko pomaga podjąć świadomą decyzję, a nie działać dopiero po kryzysie.

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:

1. Czy wiedzieliście, jakie ryzyka dotyczą Waszych procesów?
2. Czy podjęliście świadome decyzje dotyczące ich akceptacji lub mitygacji (zmniejszenia)?
3. Czy mieliście procedury na wypadek wystąpienia tych ryzyk?

NIS2 nie pyta, czy ktoś chciał źle. Bo NIS2 nie ma na celu szukać winnych.

NIS2 pyta, czy organizacja posiadała kontrolę nad ryzykiem. Ryzyko jest językiem dialogu między zarządem a regulatorem. Jeśli rozumiesz ryzyko, potrafisz udowodnić, że Twoja firma jest bezpieczna, nawet jeśli nie masz „najdroższych" systemów na rynku.



Most do Zgodności (Compliance Bridge)

Ćwiczenie refleksyjne (5 minut)

Zatrzymaj się na chwilkę i zastanów nad swoją organizacją:

1. Gdyby jutro rano jeden z Twoich kluczowych procesów przestał działać (np. strona internetowa, system płatności, dostęp do bazy klientów), co byłoby największym problemem?
2. Czy ktoś w organizacji **wie** o tym ryzyku? A jeżeli wie, to czy istnieje świadomość potencjalnych problemów związanych z w.w. ryzykiem?
3. Czy podjęto decyzję, że **akceptujemy** to ryzyko lub mamy plan, jak je ograniczyć?

Jeśli odpowiedź na którekolwiek z tych pytań brzmi „nie wiem" – gratuluję. Właśnie znalazłaś punkt startowy Twojej drogi (a nawet Twojej organizacji) do zgodności z NIS2 i standardami ISO.

Podsumowanie lekcji 2.1

- **Ryzyko to narzędzie świadomości**, a nie straszak mający wywoływać panikę.
- **Ryzyko dotyczy skutków (wpływu skutków)**, a nie samych zdarzeń technicznych.
- **Bez zrozumienia ryzyka:**
  - ✗ audyt będzie tylko „odhaczaniem” list,
  - ✗ dokumentacja będzie martwa,
  - ✗ NIS2 stanie się dla organizacji barierą zamiast ramami rozwoju.

Co dalej?

Skoro już wiemy, czym jest ryzyko i dlaczego ma ono znaczenie biznesowe, w kolejnej lekcji przejdziemy do „rozbrojenia” pojęć, które są mylone w 90% organizacji: **Zagrożenie vs Podatność vs Ryzyko.**

Lekcja 2.2 Zagrożenie, podatność i ryzyko – dlaczego to NIE jest to samo



Wprowadzenie: Architektura myślenia o bezpieczeństwie

Zanim wejdziemy w techniczne detale, zatrzymajmy się przy fundamentach.

W cyberbezpieczeństwie precyzja słowa decyduje o skuteczności działań.

MODEL ANALITYCZNY



Fundamentem odporności organizacji nie są technologie, lecz zrozumienie różnicy między tym, co nas atakuje, a tym, co nas „dziurawi". W procesie wdrażania dyrektywy NIS2 oraz nowelizacji uKSC, błąd w definicjach, to nie tylko kwestia semantyki – to ryzyko podjęcia błędnych decyzji inwestycyjnych i operacyjnych.

Jeśli wszystko uznamy za „zagrożenie", stracimy kontrolę nad priorytetami (bo hakerów w sieci jest mnóstwo). Jeśli każdą „podatność" nazwiemy „ryzykiem", zarządzający osłabną emocjonalnie i nie będą wiedzieć, na co muszą reagować „na już".

Zrozumienie tej różnicy to przejście od reaktywnego gaszenia pożarów do proaktywnego budowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z normą ISO 27001:2022.

Trzy filary Twojego bezpieczeństwa

Aby uniknąć chaosu, musimy rozdzielić trzy omawiane pojęcia na osobne obszary i najpierw zająć się każdym z nich oddzielnie. A na końcu trzeba znaleźć powiązania pomiędzy każdym z nich.

1. Zagrożenie (Threat) – Co może się zdarzyć?

głównie: Świat zewnętrzny

Zagrożenie to czynnik, który ma potencjał, by wyrządzić szkody. Mogą to być: „siła natury", działanie podmiotu trzeciego lub nawet .. kogoś z naszej organizacji.

- **Kluczowa myśl:**
  Zagrożenia są zazwyczaj poza naszą kontrolą. Nie możemy sprawić, by hakerzy przestali istnieć, ani by pracownicy nie „knuli" przeciwko orgazniacji czy by nie popełniali błędów. Naszym zadaniem jest odpowiednie: przewidywanie, monitorowanie i przygotowanie organizacji na zagrożenia.
- **Przykłady:**

  Ataki phishingowe, wirusy (ransomware), awarie prądu, kradzież laptopa, wykorzystanie AI do przetwarzania danych bez nadzoru.

2. Podatność (Vulnerability) – Gdzie jesteśmy słabi?

głównie: Świat wewnętrzny

Podatność to słabość w Twoim systemie, procesie lub kulturze organizacyjnej. To „otwarte okno", przez które zagrożenie może wejść do środka. **To tutaj mamy realną kontrolę.**

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 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

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 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,
- wsparcie AI w analizie 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

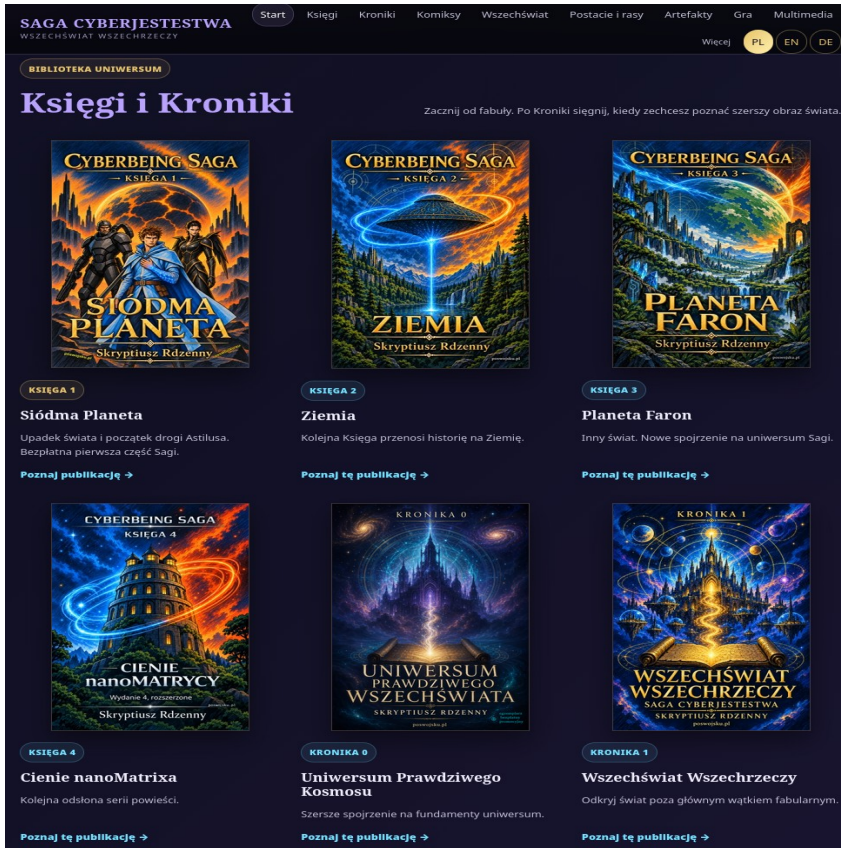
Księga 3 Planeta Faron

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.



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

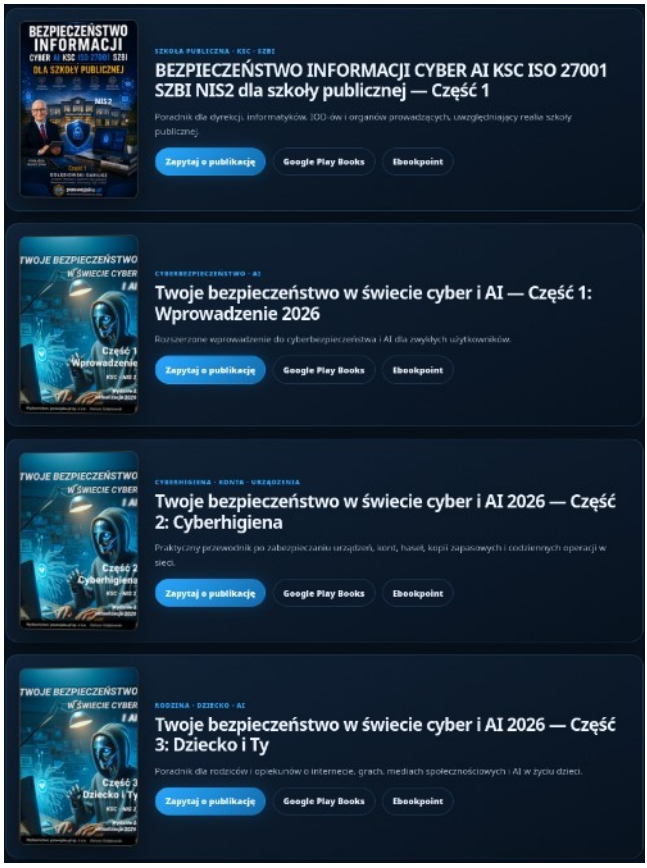
chcesz, żeby cyberhigiena była naturalną częścią Twojego życia.

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
NIS2
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.