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 1

# PODSTAWY

**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 1 Podstawy***.

Poradnik powstał na bazie usług doradczo-szkoleniowych firmy GDDM gdddm.com.pl oraz projektu edukacyjnego: Akademia Bezpieczeństwa GDDM&poswojsku

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:

poswojsku.pl, bok@poswojsku.pl

ul. Paprocka 86, 98-220 Zduńska Wola

ISBN: 978-83-68360-29-5

Copyright © poswojsku.pl 2026

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

# BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 Moduł 1 PODSTAWY

## Praktyczny przewodnik dla specjalistów bezpieczeństwa informacji i cyberbezpieczeństwa

**Autor:**

***Dariusz Gołębiowski***

**Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001**

W poradniku wykorzystano wsparcie AI w analizie i zmianach niektórych fragmentów tekstu.

## Od Wydawnictwa Cyfrowego poswojsku.pl

## KILKA SŁÓW O FORMACH ŻEŃSKICH I MĘSKICH

### Wspaniała Czytelniczko - Drogi Czytelniku

Jak nowoczesnemu wydawnictwu, zależy nam, aby nasz publikacje były przyjazne dla wszystkich osób. Jednocześnie staramy się, aby nasi autorzy pisali w sposób prosty, naturalny i wygodny w czytaniu.

Dlatego w książce czasami używane są formy męskie, a czasami żeńskie. Wszystkie odnoszą się do każdej osoby czytającej tę publikację, niezależnie od płci, wieku, pochodzenia, stanowiska czy sposobu, w jaki sama siebie określa.

Nie stosujemy konsekwentnie zapisów typu „czytelnik/ czytelniczka”, „nauczyciel/ nauczycielka” itp., ponieważ utrudniają one płynność czytania.

Jeżeli ktoś zauważy, że

- liczba końcówek męskich nie zgadza się z liczbą końcówek żeńskich,
- istnieją inne końcówki, które nie zostały użyte,

z góry przepraszamy za nas i naszych Autorów. Nie jest to działanie zamierzone – po prostu poswojsku jest wydawcą książek ;), a nie firmą księgową, dbającą o zgodność liczby końcówek językowych.

**Wszystkim**

**Wspaniałym Czytelniczkom oraz**

**Drogim Czytelnikom**

**życzymy przyjemnej lektury tej książki.**

# Spis treści

Lekcja 1.1 Dlaczego bezpieczeństwo informacji to nie jest temat IT.....12

Wprowadzenie – obalamy pierwszy mit.....16

Kto naprawdę „dotyka" informacji?.....18

Skąd biorą się realne incydenty?.....19

Przykład 1 – „To tylko mail…".....20
Przykład 2 – „Przecież wszyscy sobie ufamy".....21
Przykład 3 – „Tylko na chwilę wyszedłem".....22

Co z tego wynika?.....23

Nowe spojrzenie – ISO.....24

Ćwiczenie 1 szybka refleksja (2–3 min).....25
Ćwiczenie 2 „kto ma dostęp?" (mini-analiza).....26
Wyjaśnienie do Ćwiczenie 2.....27

Podsumowanie punktu 1.1.....38

Punkt 1.1 – dopasowanie do przykładowych grup odbiorców.....39

WERSJA A: DYREKTORZY / KADRA ZARZĄDZAJĄCA.....40
Przykład poswojsku.....41
Mini-ćwiczenie.....42

WERSJA B: PODMIOTY MEDYCZNE.....43
WERSJA C: NAUCZYCIELE/ NAUCZYCIELKI - SZKOŁY.....45
WERSJA D: URZĘDY / ADMINISTRACJA PUBLICZNA .....48
Finalna myśl do punktu 1.1 - uniwersalna.....50
Most do kolejnego punktu.....50
Lekcja 1.2 Czym jest informacja i dlaczego jest zasobem.....51
Cel tej lekcji.....53
Wprowadzenie – zmiana perspektywy.....54
Kluczowa myśl do zapamiętania.....57
Jakie formy ma informacja?.....58
Rodzaje informacji – nie wszystko jest takie samo .....59
Przykład z życia – „to przecież nic ważnego”.....60
Ćwiczenie.....61
Dlaczego informacja „boli” dopiero po incydencie? .....66
Puenta.....68
„Most” do kolejnej porcji informacji.....69

Lekcja 1.3 Trójkąt bezpieczeństwa informacji (CIA )....70

Trójkąt bezpieczeństwa – tzw. Triada Bezpieczeństwa....71

Cel tej porcji wiedzy....74

Wprowadzenie – trzy pytania, które zawsze wracają....75

Kluczowa myśl - do zapamiętania....76

Element 1: Poufność (Confidentiality)....77

Element 2: Integralność (Integrity)....78

Element 3: Dostępność (Availability)....79

Praktyczne przykłady....80

Dlaczego równowaga jest ważna?....81

Ćwiczenie....82

Puenta tej lekcji....83

Most do kolejnej porcji wiedzy....84

Lekcja 1.4 Bezpieczeństwo informacji w codziennej pracy....85

Cel tej lekcji....86

O czym naprawdę jest ta lekcja?.....87
Typowe sytuacje ryzykowne (wszyscy je znamy).....88
Case Study: „5 minut nieuwagi, 5 lat problemów”.....89
Ćwiczenie.....94
Puenta 1.4.....94

Lekcja 1.5 Najczęstsze błędy organizacji (i ludzi) .....95

Cel.....95
Ważne na start.....96
Najczęstsze błędy (bez oceniania).....96
Przykład „wszyscy wiedzą, jak jest”.....97
Mini-checklista.....98
Puenta 1.5.....102

Lekcja 1.6 Rola człowieka w systemie bezpieczeństwa.....103

Cel lekcji.....104
Człowiek – najsłabsze ogniwo?.....105
Cena Milczenia: Dlaczego strach to największy wróg uKSC/NIS2?.....107
Psychologia Błędu: Dlaczego Twój mózg Cię oszukuje? 110
Świadomość zamiast strachu (Zmiana paradygmatu).....112
Ćwiczenie refleksyjne: Test „Niewidzialnego Pracownika” .....114
Plan działania dla Lidera - Jak budować Human Firewall? .....116
Puenta 1.6.....117

Lekcja 1.7 Podsumowanie MODUŁU 1 i przygotowanie do dalszej drogi.....118

Cel tej lekcji.....119
Co już wiesz po MODUŁ 1?.....120
Dlaczego nie zaczynamy od narzędzi?.....123
Co zmieniło się w Twoim spojrzeniu?.....125
Jedno zdanie, które warto zapamiętać.....126
Domknięcie MODUŁU 1.....127
Most do MODUŁU 2 – naturalny krok dalej.....128
Co będzie w MODUŁE 2?.....129
ZAPROSZENIE.....130
Informacje o prawach autorskich i moich utworach.....132
ZAPROSZENIE.....133
Zostańmy w kontakcie!.....136
Ebooki poswojsku.pl.....137
Prawa autorskie i znaki towarowe.....142

# Lekcja 1.1 Dlaczego bezpieczeństwo informacji to nie jest temat IT

# Informacja to najcenniejszy zasób każdej organizacji.

**Bezpieczeństwo informacji to ochrona procesów biznesowych i wartości organizacji (w tym czynnika ludzkiego), a nie tylko konfiguracja firewalli czy aktualizacja systemów.**

**Skuteczna odporność organizacji na zagrożenia zależy od:**

**ludzi,**

**procedur,**

**odpowiedzialności zarządu,**

**ponieważ technologia jest jedynie narzędziem w służbie zarządzania ryzykiem.**

**Cel tej części poradnika:**

***złamanie mitu, że cyber = informatyk***

Musisz sobie uzmysłowić, że:

- bezpieczeństwo informacji ≠ cyberbezpieczeństwo,
- każdy/a pracownik/pracownica jest „użytkownikiem informacji”,
- incydenty nie zaczynają się zwykle w serwerowni,
- postępowanie typu: „przecież tylko wysłałem/am maila…” czy „to było tylko jedno kliknięcie w link” – może doprowadzić do katastrofy Twojego pracodawcę.

***Mini-refleksja*:**

Wskaż proszę - kto w Twojej organizacji ma dostęp do informacji? Podziel te osoby na dwie grupy:

A. pracujące przy komputerze,

B. nie używające komputera w codziennej pracy.

Przemyślenia koniecznie zapisz w pliku tekstowym lub na papierze, aby móc do nich sięgnąć ponownie, po przejściu przez kolejne części tego poradnika.

# Wprowadzenie – obalamy pierwszy mit

Gdy pada hasło **„bezpieczeństwo informacji”**, większość osób myśli:

- hasła,
- serwery,
- firewalle,
- informatyk/informatyczka „gdzieś tam na zapleczu”.

To naturalne. Ale… **to nieprawda :)**.

Bezpieczeństwo informacji **zaczyna się dużo wcześniej**:

- przy biurku,
- przy telefonie,
- w mailu,
- na czacie.
- w rozmowie,
- w decyzji „komu to wysłać”.

## Kluczowa myśl do zapamiętania

**Jeśli pracujesz z informacją – jesteś częścią systemu bezpieczeństwa. Niezależnie od stanowiska, działu czy wykształcenia.**

**IT dba o systemy**,
**ludzie decydują, co z informacją robią**.

# Kto naprawdę „dotyka” informacji?

Nie tylko dział IT czy księgowość. Informacje mają w rękach m.in.:

- sekretariat,
- kadry,
- księgowość,
- nauczyciele (w placówkach edukacyjnych),
- dyrekcja,
- handlowcy,
- pracownicy administracji,
- stażyści,
- pracownicy/pracownice ochrony,
- osoby sprzątające (tak, one też ;) ).

# Skąd biorą się realne incydenty?

Najczęstsze źródła problemów to:

- mail wysłany **do złej osoby**,
- załącznik otwarty „bo wyglądał normalnie”,
- link kliknięty, bo sprawiał wrażenie, że przyszedł od szefa (wójta, burmistrzyni, prezesa, kierowniczki),
- dokument zostawiony na drukarce,
- rozmowa prowadzona „przy obcych”,
- zdjęcie ekranu wysłane na prywatny komunikator czy adres email,
- pendrive „znaleziony na biurku”.

Żaden system IT tego **nie zatrzyma**.

## Przykład 1 – „To tylko mail…”

Pracownik/ca wysyła listę danych (uczniów, klientów, pacjentów) do osoby o podobnym nazwisku, co pierwotny cel wysyłki.

Efekt:

- naruszenie poufności,
- stres,
- procedura,
- czas,
- możliwe konsekwencje prawne.

**Technicznie wszystko działało poprawnie.**
Problemem była **ludzka decyzja**.

## Przykład 2 – „Przecież wszyscy sobie ufamy”

Hasło do systemu zna kilka osób, „bo tak szybciej”.

W rzeczywistości jest mniej skomplikowanie, ale dużo bardziej niebezpiecznie.

Efekt:

- brak rozliczalności,
- brak kontroli,
- chaos przy incydencie („kto to zrobił?”).

To **nie jest zła wola**, zwykle, choć i tego nie można tak zupełnie wykluczyć. To **brak świadomości**, czyli zapewne brak odpowiednich szkoleń z tzw. komponentem warsztatowym.

## Przykład 3 – „Tylko na chwilę wyszedłem”

Otwarty komputer, działający system,
ktoś przechodzi obok. Pełen dostęp!

Nieuwaga, lekkomyślność, a może
jeszcze coś gorszego?

Efekt:

- dostęp do danych,
- możliwość skopiowania, zmiany, zrobienia zdjęcia.

**System był bezpieczny.**
**Zachowanie – niestety nie było.**

# Co z tego wynika?

Bezpieczeństwo informacji:

- ❌ **nie zaczyna się od jakichkolwiek cyfrowych narzędzi,**
- ❌ **nie kończy się na IT, a nawet nie zaczyna od IT,**
- ✅ zaczyna się od **myślenia każdej osoby w organizacji,**
- ✅ trwa w **codziennych, drobnych decyzjach – w naszych działaniach i ich braku.**

# Filozofia: KSC/NIS2, ISO

W filozofii KSC/NIS2, ISO:

- informacja = **zasób**
- człowiek = **kluczowy element systemu**
- procedury mają pomagać, nie - straszyć

Nie chodzi o:

- karanie,
- podejrzliwość,
- kontrolę „dla kontroli”.

Chodzi o:

- świadomość,
- przewidywanie skutków,
- odpowiedzialność,
- zdrowy rozsądek.

## Ćwiczenie 1 szybka refleksja (2–3 min)

Odpowiedz sobie (na kartce lub w głowie):

1. Z jakimi informacjami **pracuję codziennie**?
2. Które z nich byłyby problemem, gdyby trafiły „nie tam gdzie trzeba”?
3. W którym momencie dnia **najłatwiej o błąd**?

**Nie oceniaj.**

**Rozważ przynajmniej kilka możliwych opcji.**

**Najlepiej spisz wszystkie spostrzeżenia i refleksje. Zachowaj te dane do dalszej analizy.**

## Ćwiczenie 2 „kto ma dostęp?” (mini-analiza)

Wypisz:

- jedną informację,
- kto ma do niej dostęp **oficjalnie**,
- kto ma do niej dostęp **w praktyce**.

**Różnice bywają bardzo ciekawe.**

## Wyjaśnienie do Ćwiczenie 2

Przykłady informacji podlegających ochronie zgodnie z normą ISO 27001 i System Zarządzania Bezpieczeństwem Informacji (SZBI).

Ważne jest zrozumienie, że informacja w kontekście SZBI to nie tylko dane cyfrowe, ale wszystko, co ma wartość dla organizacji i wymaga ochrony. Nawet to co jest tylko w Twojej głowie, ale dotyczy organizacji, w której pracujesz.

Oto kilka przykładów informacji z wyjaśnieniami, podzielone na kategorie, aby lepiej zobrazować różnorodność. Pamiętaj, że konkretne informacje wymagające ochrony będą zależeć od specyfiki działalności Twojej organizacji.

Poniżej przedstawiam przykłady informacji z wyjaśnieniami, podzielone na kategorie, aby lepiej zobrazować różnorodność. Pamiętaj, że konkretne informacje wymagające ochrony będą zależeć od specyfiki działalności Twojej organizacji.

**Informacje związane z działalnością biznesową:**

- **Plany strategiczne i cele biznesowe:**
  Wyjaśnienie: Ujawnienie tych informacji mogłoby dać konkurencji przewagę, osłabić pozycję rynkową firmy lub umożliwić nieuczciwe działania.
- **Strategie marketingowe i kampanie reklamowe:**
  Wyjaśnienie: Ujawnienie planowanych działań marketingowych mogłoby pozwolić konkurencji na zneutralizowanie ich efektu, a nawet wykorzystanie ich do własnych celów.

- **Informacje o nowych produktach/usługach** (ale także pomysły będące dopiero w fazie rozwoju – np. jedynie w głowie jakiejś pracownicy)**:**
  Wyjaśnienie: Kradzież informacji o niepremiowanych produktach mogłaby doprowadzić do utraty przewagi konkurencyjnej i kosztownych strat finansowych.
- **Umowy handlowe, kontrakty z dostawcami/klientami:**
  Wyjaśnienie: Ujawnienie warunków umów może naruszyć poufność transakcji, osłabić pozycję negocjacyjną i potencjalnie doprowadzić do roszczeń prawnych.
- **Cenniki i polityka cenowa:**

  Wyjaśnienie: Udostępnienie cenników konkurencji może prowadzić do wojny cenowej i obniżenia rentowności firmy.

**Informacje o klientach/użytkownikach:**

- **Dane osobowe klientów (imię, nazwisko, adres, numer telefonu, e-mail):**
  Wyjaśnienie: Zgodnie z RODO i innymi przepisami dotyczącymi ochrony danych osobowych, te informacje podlegają szczególnej ochronie. Ujawnienie lub wyciek może prowadzić do poważnych konsekwencji prawnych i finansowych.
- **Dane logowania klientów (zakładam, że odpowiednio zabezpieczone przed nieuprawnionym dostępem - login, hasło):**
  Wyjaśnienie: Bezpieczne przechowywanie i zarządzanie danymi uwierzytelniającymi jest kluczowe dla ochrony kont użytkowników przed nieautoryzowanym dostępem.

- **Historia zakupów czy też korzystania z usług:**
  Wyjaśnienie: Te dane mogą być wykorzystane do profilowania klientów, ale również są wrażliwe i wymagają ochrony przed wyciekiem.

- **Preferencje i opinie klientów:**

  Wyjaśnienie: Informacje o preferencjach klientów mogą być cenne dla celów marketingowych, ale ich ujawnienie mogłoby naruszyć prywatność i zaufanie.

**Informacje finansowe:**

- **Dane dotyczące rachunków bankowych:**
  Wyjaśnienie: Ujawnienie tych danych może prowadzić do kradzieży środków.
- **Wewnętrzne raporty finansowe, bilanse, prognozy finansowe:**
  Wyjaśnienie: Udostępnienie tych informacji konkurencji lub osobom nieupoważnionym mogłoby wpłynąć na wartość akcji firmy i jej pozycję rynkową.
- **Informacje o budżetach i wydatkach:**

  Wyjaśnienie: Ujawnienie planowanych wydatków może pozwolić konkurencji na przewidzenie działań firmy i wykorzystanie tego do własnych celów.

**Informacje techniczne:**

- **Kod źródłowy oprogramowania:**
  Wyjaśnienie: Kradzież kodu źródłowego mogłaby doprowadzić do utraty własności intelektualnej i przewagi konkurencyjnej.
- **Schematy sieci, konfiguracja serwerów:**
  Wyjaśnienie: Ujawnienie tych informacji może ułatwić atakującym dostęp do systemów informatycznych firmy.
- **Dokumentacja techniczna, instrukcje obsługi:**
  Wyjaśnienie: Udostępnienie dokumentacji technicznej osobom nieupoważnionym mogłoby umożliwić im manipulowanie systemami i urządzeniami.

- **Klucze szyfrujące, certyfikaty cyfrowe:**

  Wyjaśnienie: Bezpieczne przechowywanie i zarządzanie kluczami szyfrującymi jest niezbędne do ochrony poufności danych.

**Informacje prawne i regulacyjne:**

- **Dokumentacja prawna, opinie prawne:**
  Wyjaśnienie: Ujawnienie tych informacji mogłoby naruszyć poufność procesów prawnych i osłabić pozycję firmy w sporach.
- **Informacje dotyczące zgodności z przepisami:**

  Wyjaśnienie: Utrata kontroli nad informacjami o zgodności może prowadzić do kar finansowych i utraty reputacji.

## Jak to się odnosi do ISO 27001?

- **Identyfikacja aktywów informacyjnych:**
  Norma ISO 27001 wymaga, aby organizacja zidentyfikowała wszystkie swoje aktywa informacyjne, czyli te informacje, które wymagają ochrony.
- **Klasyfikacja informacji:**
  Po identyfikacji, aktywa powinny być sklasyfikowane według poziomu poufności i krytyczności. To pozwala na zastosowanie odpowiednich środków bezpieczeństwa oraz na właściwe zarządzanie.
- **Ocena ryzyka:**
  Kolejny krok, to dokonanie analizy ryzyka związane z utratą poufności, integralności lub dostępności tych informacji (czyli tzw. Triada CIA – wyjaśnienie znajdziesz w dalszej części tego opracowania).

- **Wybór i wdrożenie kontroli:**

  Na podstawie oceny ryzyka, organizacja wybiera i wdraża odpowiednie kontrole bezpieczeństwa (zgodne z normą ISO 27001) w celu minimalizacji ryzyka.

**Podsumowanie:**

Powyższe przykłady pokazują, że zakres informacji podlegających ochronie w SZBI jest bardzo szeroki. Kluczem do skutecznego wdrożenia ISO 27001 jest dokładna identyfikacja i klasyfikacja aktywów informacyjnych oraz dostosowanie środków bezpieczeństwa do specyfiki działalności organizacji i poziomu ryzyka.

**Ważne:**

**Opisana powyżej lista - nie jest wyczerpująca. Każda organizacja powinna przeprowadzić własną analizę, aby zidentyfikować wszystkie informacje wymagające ochrony w kontekście skutecznego działania biznesowego.**

# Podsumowanie punktu 1.1

- bezpieczeństwo informacji to **temat ludzi**, nie tylko IT
- większość incydentów zaczyna się od **drobnych decyzji**
- każdy/a pracownik/pracownica jest **częścią systemu bezpieczeństwa**
- świadomość oraz zdrowy rozsądek to **najtańsze i najskuteczniejsze zabezpieczenia**

# Punkt 1.1 – dopasowanie do przykładowych grup odbiorców

**WERSJA A: DYREKTORZY / KADRA ZARZĄDZAJĄCA**

**WERSJA B: PODMIOTY MEDYCZNE**

**WERSJA C: NAUCZYCIELE / SZKOŁY**

**WERSJA D: URZĘDY / ADMINISTRACJA PUBLICZNA**

# WERSJA A: DYREKTORZY / KADRA ZARZĄDZAJĄCA

Bezpieczeństwo informacji to
**zarządzanie ryzykiem**, a nie problem informatyka.
Dyrektor odpowiada nie za serwery –
tylko za **konsekwencje:**

- odpowiedzialność formalna i wizerunkowa
- pytanie: *„kto za to odpowiada?”*
- brak świadomości jako **realne ryzyko biznesowe**

## Przykład poswojsku

Incydent nie wydarzył się dlatego, że system był zły. Wydarzył się dlatego, że **nikt nie ustalił zasad** – albo nikt ich nie znał.

A tak na marginesie – myśląc o incydentach - pamiętaj także o mnie – Autorze tego poradnika i szkoleń: Jako Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001 - szkolę, doradzam, audytuję, wdrażam i porządkuję obszary: bezpieczeństwo informacji, cyberbezpieczeństwo, RODO i ryzyko informacyjne.

Pracuję z kadrą zarządzającą oraz zespołami, pokazując jak chronić: dane, ludzi i reputację Twojej organizacji - w praktyce, a nie tylko na papierze – zapraszam Ciebie i Twoją organizację do współpracy: gddm.com.pl .

## Mini-ćwiczenie

Zadaj sobie pytania:

1. Czy w mojej organizacji **wiadomo**, kto odpowiada za informację?
2. Czy w razie incydentu potrafił/a bym powiedzieć:
    - co się stało,
    - kto ma zareagować,
    - komu to zgłosić?

***To nie problem IT - to problem zarządczy*.**

# WERSJA B: PODMIOTY MEDYCZNE

W ochronie zdrowia **informacja jest równie wrażliwa jak pacjent**. Czasem nawet bardziej – bo zostaje na zawsze:

- dane medyczne = dane szczególnej kategorii
- zaufanie pacjenta
- realne skutki błędów (nie tylko „kary”)

**Przykład z życia**

Wyniki badań:

- wydrukowane,
- zostawione na biurku,
- ktoś robi zdjęcie „bo myślał, że to jego”.

**System działał poprawnie.**

**Zawiodła organizacja pracy.**

## Ćwiczenie

Odpowiedz:

- gdzie w Twojej placówce **najczęściej „leżą dane”**?
- kto ma do nich dostęp „przy okazji”?
- co się dzieje z dokumentacją po godzinach?

# WERSJA C: NAUCZYCIELE/ NAUCZYCIELKI - SZKOŁY

## Jak mówić, żeby nie straszyć

**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 1 PODSTAWY***

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

# Co będzie w MODUŁE 2?

W następnym module:

- nauczysz się **patrzeć na organizację oczami audytora**,
- zrozumiesz, czym naprawdę jest ryzyko,
- dowiesz się, jak je zauważać **bez tabel i straszenia**,
- zobaczysz, że audyt to nie kara, tylko narzędzie porządkowania.

**MODUŁ 2 – Ryzyko i myślenie przyczynowo-skutkowe (audytowe)**

# 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](poswojsku.pl)**

**B. materiały wdrożeniowe na portalu Akademia Bezpieczeństwa GDDM [www.gddm.com.pl](www.gddm.com.pl)**

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

***AUTOR: Dariusz Gołębiowski***

***Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001***

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

# Informacje o prawach autorskich i moich utworach

W poradniku wykorzystano:

- własne materiały doradcze,
- 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

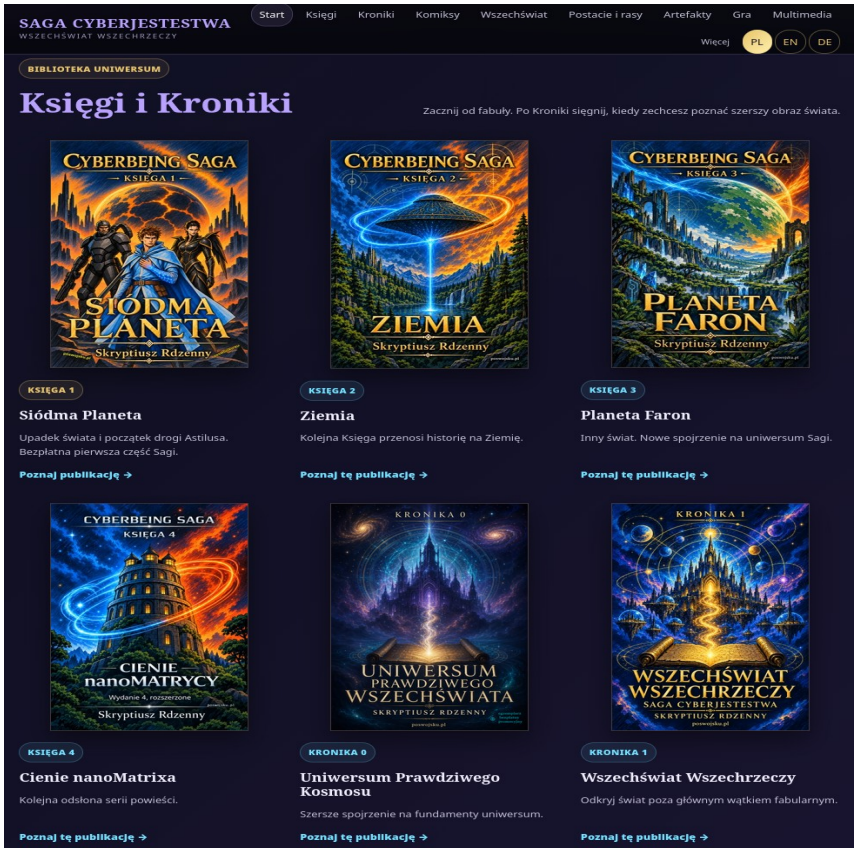
Księga 3 Planeta Faron

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

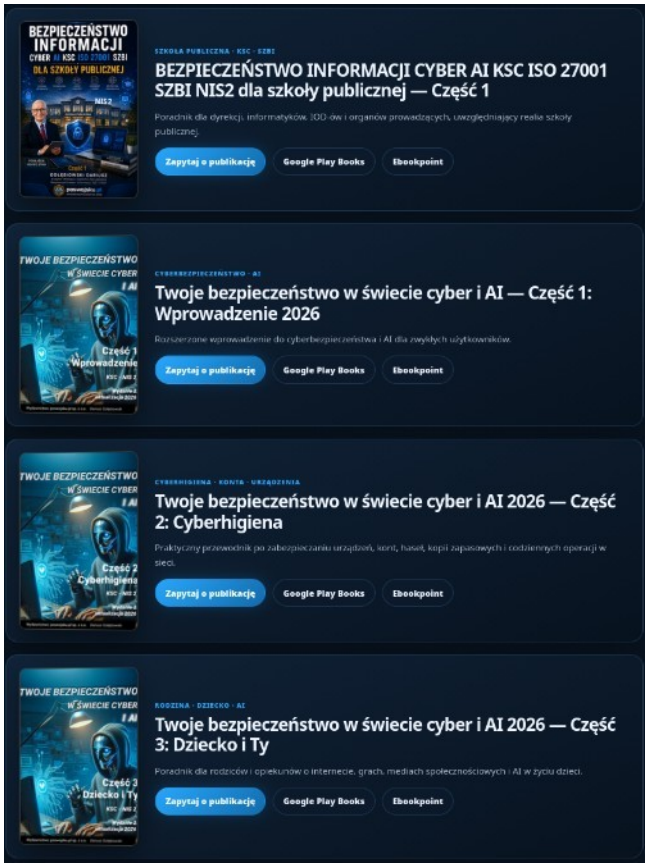
obowiązkowa, jeśli chcesz, żeby cyberhigiena była naturalną częścią Twojego życia.

**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 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.