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 6

Podsumowanie i dojrzałość

Dodatek: SZBI, incydent

AKADEMIA BEZPIECZEŃSTWA
poswojsku&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 oraz opracowaniem książki: BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001 NIS2 MODUŁ 6 Podsumowanie i dojrzałość. Dodatek SZBI.

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: 978-83-68360-57-8

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 NIS2 MODUŁ 6 Podsumowanie i dojrzałość. Dodatek SZBI.

Praktyczny przewodnik dla specjalistów bezpieczeństwa informacji oraz 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

WPROWADZENIE.....14

Lekcja 6.1 Bezpieczeństwo jako sposób myślenia - mindset, który zostaje.....17

Rola lekcji.....18

Cel lekcji 6.1.....19

Najczęstsze nieporozumienia.....20

Najważniejsza teza tej lekcji.....22

Czym jest mindset bezpieczeństwa w praktyce.....23

Czym mindset bezpieczeństwa NIE jest.....24

Bezpieczeństwo jako filtr decyzyjny.....25

Przykład – decyzja „na skróty”.....26

Mindset bezpieczeństwa a ludzie.....27

Jak utrwalić mindset po kursie.....28

Rola kierownictwa w utrzymaniu mindsetu.....29

Mindset bezpieczeństwa a NIS2/KSC.....30

Przykład – „bezpieczeństwo bez procedury”.....31

Ćwiczenie refleksyjne.....32
Puenta lekcji 6.1.....33
Co dalej.....33
Lekcja 6.2 Co dalej rozwijać w organizacji (a czego nie ruszać na siłę).....34
Rola lekcji.....35
Cel lekcja 6.2.....36
Najczęstszy błąd po szkoleniach.....37
Najważniejsza teza tej lekcji.....38
Rozwój bezpieczeństwa a dojrzałość organizacji.....39
Co warto rozwijać w pierwszej kolejności.....40
Czego NIE należy rozwijać „na siłę”.....41
Jak ocenić, czy coś warto rozwijać.....42
Bezpieczeństwo a zmiany w organizacji.....43
Wolne, ale systematyczne planowanie rozwoju.....44
Kierownictwo decyduje w wyborze kierunków działania.....45
NIS2/KSC a rozwój bezpieczeństwa.....46

Przykład – organizacja, która powiedziała firmom IT - „na razie nie”.....47
Ćwiczenie refleksyjne.....48
Puenta lekcji 6.2.....49
Co dalej.....49
Lekcja 6.3 Kiedy potrzebna audytorka, a kiedy informatyk oraz jak nie pomylić ról.....50
Rola lekcji.....51
Cel lekcji 6.3.....52
Najczęstszy błąd organizacyjny.....53
Najważniejsza teza tej lekcji.....54
Rola audytora – po co i kiedy.....55
Rola informatyka - po co i kiedy.....57
Dlaczego nie wolno mieszać ról: informatyk a audytor 59
Rola kierownictwa – często źle rozumiana.....60
Jak dobrać właściwe wsparcie personelu.....61
Przykład - źle dobrana pomoc.....62
Przykład – dobrze dobrana pomoc.....63

NIS2/KSC a role w organizacji.....64
Ćwiczenie refleksyjne.....65
Puenta lekcji 6.3.....66
Co dalej.....66
Lekcja 6.4 Co sprawdzać cyklicznie, żeby bezpieczeństwo nie „umarło”.....67
Rola lekcji.....68
Cel lekcji 6.4.....69
Dlaczego systemy bezpieczeństwa „umierają”.....70
Najważniejsza teza tej lekcji.....71
Utrzymanie SZBI - czym NIE jest cykliczne sprawdzanie.....72
Co warto sprawdzać systematycznie - minimum sensu.....73
Jak często sprawdzać?.....75
Kto powinien zajmować się sprawdzaniem?.....76
Jak robić to lekko i skutecznie.....77
Przykład – „system, który żyje”.....78
NIS2/KSC a cykliczne sprawdzanie.....79

Ćwiczenie praktyczne....80
Puenta lekcji 6.4....81
Co dalej....81
Lekcja 6.5 Jak reagować na incydenty i co z nimi robić dalej....82
Rola lekcji....83
Cel lekcji 6.5....84
Najczęstszy mit o incydentach....85
Najważniejsza teza tej lekcji....86
Czym jest incydent a czym nie jest....87
Klasyfikacja i zgłaszanie incydentów cyberbezpieczeństwa - KSC/NIS2....89
Incydent cyberbezpieczeństwa....89
Incydent poważny....89
Incydent niezakwalifikowany jako poważny....90
Zgłaszanie incydentów poważnych....90
Pierwsza reakcja – kluczowa faza....91
Oddzielenie dwóch etapów....92
Co robić po incydencie (najczęściej pomijane)....93

NIS2/KSC a reagowanie na incydenty.....94
Przykład – „incydent, który wzmocnił organizację”…95
Ćwiczenie praktyczne.....96
Puenta lekcji 6.5.....97
Co dalej.....97
Lekcja 6.6 Checklisty końcowe i narzędzia do dalszej pracy.....98
Rola lekcji.....99
Cel lekcji 6.6.....100
Najważniejsza zasada checklist.....101
CHECKLISTA 1: Czy nasze SZBI naprawdę żyje?….102
CHECKLISTA 2: Czy Twoja organizacja jest decyzyjnie gotowa na KSC/NIS2?.....103
CHECKLISTA 3: Czy wiemy, co robić przy incydencie? 105
CHECKLISTA 4: Czy role w bezpieczeństwie są jasne? 106
CHECKLISTA 5: „Czy rozwijamy bezpieczeństwo z głową?”.....107

Jak korzystać z Checklist w praktyce.....108
Checklisty a kultura organizacyjna.....109
PODSUMOWANIE.....110
DODATEK – Od Projektu do Procesu.....112
Dlaczego System Zarządzania Bezpieczeństwem Informacji musi być procesem, a nie jednorazowym wdrożeniem.....113
MODEL BŁĘDNY: Bezpieczeństwo jako Projekt (Pułapka „Zamku”).....114
MODEL WZORCOWY: Bezpieczeństwo jako Proces (Budowanie Odporności).....115
Mapa Drogowa SZBI – Plan Wdrożenia w Ujęciu Procesowym.....116
Dlaczego to jest kluczowe w kontekście KSC/uKSC? 122
Obsługa incydentu na poszczególnych stanowiskach – kto za co odpowiada.....123
Przykład incydentu.....123
Krok po kroku – kto i co robi?.....124

Pracownik, którego komputer jest źródłem incydentu – natychmiast.....124
Informatyk lub obsługa IT/CUW – niezwłocznie 124
Osoba odpowiedzialna za SZBI – pilnie.....125
Dyrektor podmiotu – niezwłocznie.....125
Osoba wyznaczona do zgłoszeń – niezwłocznie, maksymalnie 72 godziny.....126
IOD i administrator danych – równolegle.....127
Po opanowaniu zagrożenia.....128
Informacje o prawach autorskich i moich utworach. .129
ZAPROSZENIE.....130
Zostańmy w kontakcie!.....132
Ebooki poswojsku.pl.....133
Prawa autorskie i znaki towarowe.....137

WPROWADZENIE

Haker – osoba w kapturze siedząca w ciemnym pokoju. Dookoła monitory, a na nich jakieś dziwne napisy. Tak to sobie wyobrażasz? No to jesteś w wielkim błędzie. Teraz hakerka siedzi w eleganckim biurze, a jej ubiór wskazuje osobę na stanowisku kierowniczym. Tak - witaj w świecie, w którym słowo „cyberbezpieczeństwo", zlewa się ze słowem „biznes" i drugim równie ważnym – „AI". Sztuczna inteligencja, to podstawowe narzędzie pracy hakera, a jego praca, to po prostu biznes.

Jeśli trzymasz w ręku ekran z tym ebookiem, prawdopodobnie czujesz jedną z dwóch rzeczy:

albo ogromną ciekawość, jak okiełznać nadchodzące zmiany w przepisach (takich jak NIS2 czy uKSC),

albo lekki niepokój na myśl o tym, czy Twoja organizacja jest w ogóle przygotowana na to, co może przynieść jutrzejszy dzień.

Być może jeszcze nie rozumiesz, że Twoja organizacja zostanie zhakowana. Możesz się zabezpieczać, ale tak naprawdę trzeba pomyśleć przede wszystkim o:

- ciągłości działania,
- procedurach (w tym SZBI).

Chcę Ciebie uspokoić: ten ebook nie jest kolejnym podręcznikiem do „odhaczania" technicznych parametrów ani nudną instrukcją obsługi firewalla. To Twój przewodnik po świecie zarządzania ryzykiem.

Dlaczego właśnie ten ebook? Ponieważ wiem, że jako lider nie musisz stać się ekspertem od kodowania czy analizy pakietów danych. Musisz jednak zostać ekspertem od zrozumienia procesów. Moim celem jest przełożenie skomplikowanego języka prawników, programistów i innych techników - na język konkretnych decyzji biznesowych.

Kolejne moduły tej serii przeprowadzały Ciebie przez labirynt regulacji (NIS2, uKSC), standardów międzynarodowych (ISO 27001) oraz fundamentów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Zamiast straszyć Ciebie „atakami", pokazywałem, jak budować odporność. Zamiast zasypywać Ciebie terminologią, dawałem Tobie

narzędzia do podejmowania świadomych wyborów. W tym module, będę nawiązywał do poprzednich, a zatem będzie między innymi o tym:

Jak odróżnić realne zagrożenie od panicznej narracji.
Jak zarządzać zespołem, w którym każdy ma swoją rolę – od informatyka po audytora.
Jak budować kulturę bezpieczeństwa, która nie jest dla pracowników „dodatkowym obowiązkiem”, ale naturalnym sposobem pracy.
Jak planować rozwój organizacji tak, by była ona silna, zwarta i odporna na współczesne zagrożenia.

Przygotuj się na podróż od chaosu informacyjnego do spokoju wynikającego z wiedzy. Jeśli chcesz dowiedzieć się, jak sprawić, by bezpieczeństwo stało się fundamentem Twojego sukcesu, a nie kolejnym problemem do rozwiązania – jesteś w odpowiednim miejscu.

Zaczynajmy.

Autor poradnika: Dariusz Gołębiowski

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

Lekcja 6.1 Bezpieczeństwo jako sposób myślenia - mindset, który zostaje

MINDSET BEZPIECZEŃSTWA TO UMIEJĘTNOŚĆ SYSTEMATYCZNEGO ZADANIA SOBIE PYTANIA:

„CO MOŻE PÓJŚĆ NIE TAK – I CO ZROBIMY W TAKIEJ SYTUACJI?”

ZANIM DANY PROBLEM FAKTYCZNIE WYSTĄPI.

Rola lekcji

Ta lekcja nie uczy konkretnych narzędzi technicznych ani szczegółowych procedur operacyjnych. Jej celem jest zmiana paradygmatu postrzegania rzeczywistości. Uczy sposobu patrzenia na:

- procesy decyzyjne,
- ocenę ryzyka,
- zakres odpowiedzialności, który pozostaje w organizacji jako trwały element kultury organizacyjnej długo po zakończeniu szkolenia dla pracownic.

To moment przełomowy, w którym bezpieczeństwo

- przestaje być traktowane jako odrębny, techniczny „temat” lub projekt do odhaczenia na liście zadań,
- staje się naturalnym, stałym elementem codziennego myślenia i zarządzania wszystkimi aspektami działalności firmy.

Cel lekcji 6.1

Zakładam, że poniższa lekcja pomoże Czytelnikowi/Czytelniczce w:

- zrozumieniu, czym w praktyce jest mindset bezpieczeństwa i dlaczego jest on fundamentem skutecznego systemu zarządzania (SZBI),
- podejmowaniu właściwych decyzji biznesowych, uwzględniając potencjalne ryzyka i przygotowując na nie organizację,
- ustawieniu wewnętrznego kompasu wartości bezpieczeństwa, dzięki czemu zniknie potrzeba instrukcji dla każdej trudnej sytuacji,
- zrozumieniu fundamentalnej różnicy między „bezpieczeństwem na papierze” (wymogi formalne) a „bezpieczeństwem w głowie” (dojrzałość organizacyjna),
- utrzymaniu stałej czujności i odporności organizacji bez popadania w paranoję lub nadmierne blokowanie procesów biznesowych.

Najczęstsze nieporozumienia

Wiele osób oraz organizacji błędnie zakłada, że:

- „bezpieczeństwo to domena informatyka czy działu IT”, a to wyklucza odpowiedzialność zarządu i innych działów,
- „bezpieczeństwo to tylko procedury”, czyli zestaw dokumentów do podpisania (im grubszy segregator z procesami tym lepsza ocena ewentualnej kontroli),
- „bezpieczeństwo to zaawansowane systemy IT”, SIEM, firewall, antywirus, szyfrowanie, i … wszystko inne co nas chroni, a skoro jesteśmy chronieni, to przecież nie ma problemu.

Tymczasem - powyższe pojęcia, to jedynie potencjalne narzędzia oraz komponenty do ochrony organizacji. To jest tak samo - jak z systemem antywirusowym. Samo posiadanie antywirusa nas nie chroni. Dopiero - systematyczne, rozsądne skanowanie może dać pewien stopień ochrony. Ale nie 100%! Bo tyle nie uzyskamy nigdy jako działająca w teraźniejszości organizacja.

Ale możemy się znacząco zbliżyć do 100%, gdy zastosujemy odpowiednio dobrany dla danej organizacji mix zabezpieczeń. Skupieć musimy się m.in. na tych elementach:

- ludzie - szkolenia,
- procedury – odpowiednie dla faktycznej codziennej działaności organizacji,
- technologia – właściwie dobrane zabezpieczenia, wraz z personelem, który potrafi je obsłużyć.

Codzienne bezpieczeństwo nie polega jedynie na posiadaniu tych czy innych elementów, ale na sposobie, w jaki są one wykorzystywane. Prawdziwa ich wartość tkwi w:

- świadomym sposobie myślenia o procesach,
- pytaniach, które zadajemy przed uruchomieniem nowej usługi lub zmiany procedury,
- decyzjach, które podejmujemy w sytuacjach nieoczywistych i stresowych.

Najważniejsza teza tej lekcji

Wyjaśnienie:

mindset to z języka angielskiego - sposób myślenia

Mindset bezpieczeństwa to umiejętność systematycznego zadania sobie pytania:

„co może pójść nie tak – i co zrobimy w takiej sytuacji?”

zanim dany problem faktycznie wystąpi.

To podejście:

- nie służy spowalnianiu pracy czy wprowadzaniu biurokracji;
- służy budowaniu odporności organizacji i ochronie przed chaosem, który następuje, gdy coś idzie źle.

Czym jest mindset bezpieczeństwa w praktyce

Mindset bezpieczeństwa to codzienna praktyka oparta na kilku filarach:

- świadomość, że ryzyko jest stałym elementem każdego procesu biznesowego i nie można go całkowicie wyeliminować, a jedynie zarządzać nim.
- umiejętność dostrzegania sygnałów ostrzegawczych (anomalii) w codziennej pracy, zanim przerodzą się one w incydenty.
- gotowość do otwartej komunikacji o problemach i błędach bez obawy przed karami.
- całkowite odrzucenie iluzji „u nas to się nie wydarzy” lub „jesteśmy zbyt mali, by być celem ataku”.

To świadoma dojrzałość zarządzania, a nie strach przed atakiem.

Czym mindset bezpieczeństwa NIE jest

Ważne jest, aby potrafić oddzielić profesjonalny sposób myślenia (czyli mindset) w organizacji - od postaw destrukcyjnych. Czyli nie powinien on oznaczać:

- podejrzliwości wobec własnych pracowników czy klientów.
- blokowania jakichkolwiek działań biznesowych (paraliżu organizacji).
- życia w ciągłym stresie i lęku przed każdym kliknięciem.
- próby kontrolowania każdego, nawet najmniejszego ruchu każdej użytkowniczki w sposób inwazyjny.

Mindset bezpieczeństwa, to balans między:

bezpieczeństwem a użytecznością.

Podejście zrównoważone zapewnia efektywną pracę organizacji i jej bezpieczeństwo. Równocześnie ważnym jest - by nie popadać w paranoję.

Bezpieczeństwo jako filtr decyzyjny

Dojrzali Liderzy, rozumiejący we właściwy sposób omawiane zagadnienie, traktują bezpieczeństwo jako filtr, przez który przepuszczają każdą nową decyzję:

- przy planowaniu działań, w tym - zmian – zadają pytania:

  „jakie to ma ryzyko?”,

  „czy potrafimy je zaakceptować?”,

  „czy jesteśmy gotowi na konsekwencje?”.
- nie unikają trudnych decyzji, lecz podejmują je w oparciu o analizę faktów (w tym ryzyka),
- nie przenoszą odpowiedzialności za bezpieczeństwo na „specjalistów”, tylko biorą to „na klatę” - na siebie jako odpowiedzialni menedżerowie.

Taki sposób myślenia nie spowalnia procesów decyzyjnych organizacji. Wręcz przeciwnie – może on z biegiem czasu - podnosić ich jakość i chroni organizację przed kosztownymi błędami w przyszłości.

Przykład – decyzja „na skróty”

Rozważmy sytuację:

zespół chce wprowadzić szybkie rozwiązanie techniczne, które oszczędza jego czas, ale omija ustaloną procedurę uwierzytelniania czy może lepiej - kontroli dostępu.

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 NIS2 MODUŁ 6 Podsumowanie i dojrzałość. Dodatek SZBI.

Szczegóły oferty znajdziesz na stronie firmy Wydawnictwo Cyfrowe poswojsku.pl

Informacje o prawach autorskich i moich utworach

W poradniku wykorzystano:

- własne materiały doradcze,
- w poradniku wykorzystano wsparcie AI w analizie i zmianach 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. Dowiesz się, jak tworzyć silne hasła, chronić urządzenia, wykrywać próby oszustw i przygotować swoją rodzinę na zagrożenia cyfrowe. To pozycja obowiązkowa, jeśli

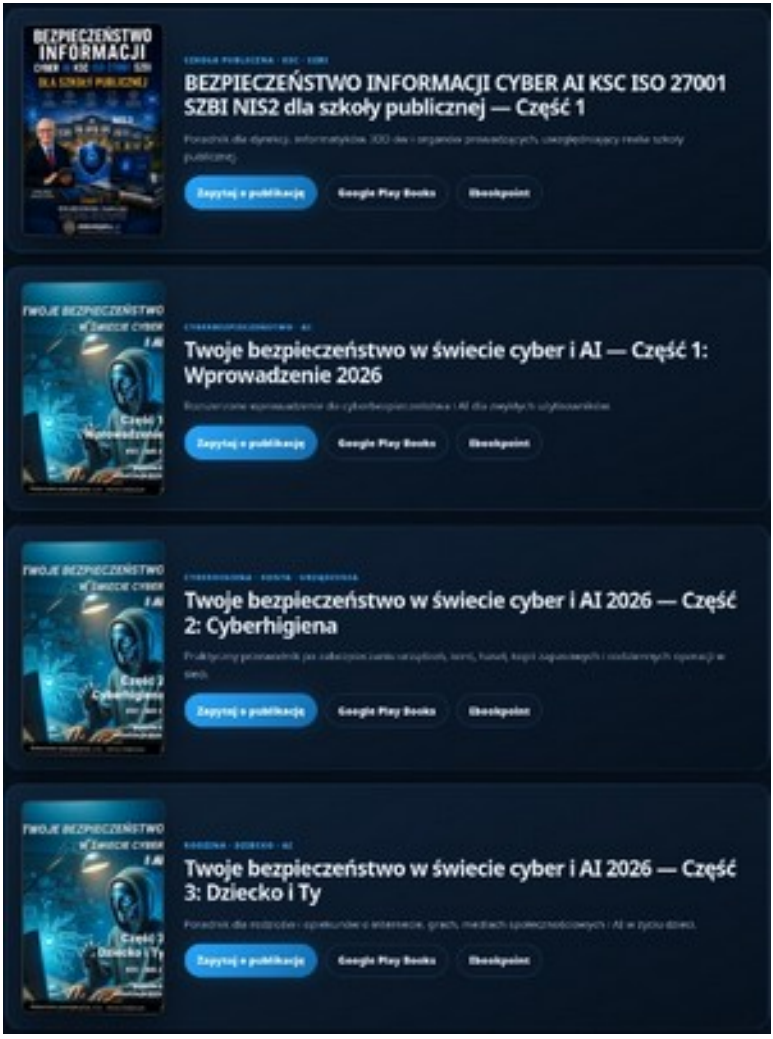
chcesz, żeby cyberhigiena była naturalną częścią Twojego życia.

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 2 PRAKTYCZNE POMYSŁY PRAWNE UWARUNKOWANIA dla edukatorów i edukatorek

Poradnik o wykorzystaniu AI w edukacji, z przykładami, ćwiczeniami, podstawami prawnymi.



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.