Sudhara International
+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

ANALIZA RYZYK W SYSTEMIE ZARZĄDZANIA SZTUCZNĄ INTELIGENCJĄ AI NA ZGODNOŚĆ Z WYMAGANIEM NORMY ISO 42001

PROGRAM SZKOLENIA

🎯 Cel szkolenia

Celem szkolenia jest przygotowanie uczestników do identyfikowania, oceny i ograniczania ryzyk związanych z projektowaniem, wdrażaniem, użytkowaniem i nadzorowaniem systemów sztucznej inteligencji zgodnie z wymaganiami ISO/IEC 42001.

Szkolenie rozwija praktyczne rozumienie ryzyk charakterystycznych dla AI, takich jak błędy modeli, uprzedzenia, brak przejrzystości, naruszenia prywatności, drift modeli, ryzyka regulacyjne oraz zagrożenia operacyjne. Uczestnicy poznają sposoby budowania podejścia opartego na ryzyku w całym cyklu życia systemu AI, z uwzględnieniem wymagań zarządczych, technicznych, organizacyjnych i zgodnościowych:

- Zrozumienie unikalnych zagrożeń i podatności w systemach sztucznej inteligencji (halucynacje modeli, uprzedzenia, prywatność, ataki adversarialne, „model drift") oraz powiązanych ram regulacyjnych (NIST AI RMF, ISO/IEC 42001, EU AI Act).
- Nabycie umiejętności identyfikowania, oceniania i mitygowania ryzyk na każdym etapie cyklu życia AI, przy użyciu metodyk ISO/IEC 27005, ISO 31000 i technik z IEC 31010.
- Przygotowanie do dokumentowania i audytowania systemów AI oraz integracji zarządzania ryzykiem AI z systemami zarządzania bezpieczeństwem informacji.

Program szkolenia

PRE - TEST

1. **Wprowadzenie do zarządzania ryzykiem AI:**
   - Przegląd wytycznych NIST AI RMF (funkcje Govern, Map, Measure, Manage) i normy ISO/IEC 42001 (system zarządzania AI).
   - Omówienie klas ryzyka w projekcie AI Act (zakazane, wysokiego ryzyka, ograniczonego ryzyka, minimalnego ryzyka).
2. **Polityki i governance AI**:
   - Tworzenie polityk AI, wyznaczanie ról (właściciel modelu, risk owner, komisje etyczne), określenie apetytu na ryzyko.
   - Inwentaryzacja systemów AI (system cards, model cards), identyfikacja interesariuszy.
   - ***Ćwiczenie*: opracowanie karty systemu AI oraz listy interesariuszy.**
3. **Identyfikacja i analiza ryzyka:**
   - Ustalenie scenariuszy ryzyka dla danych wejściowych, algorytmów, modeli i środowiska operacyjnego;
   - Wykorzystanie technik IEC 31010 (analiza drzewa błędów, PESTLE, analizy przyczyn-skutków).
   - Oszacowanie prawdopodobieństwa i skutku, budowa macierzy ryzyka.
   - ***Ćwiczenie*: identyfikacja i ocena ryzyk dla przykładowego modelu uczenia maszynowego.**

4. **Ocena miar jakości:**
    - Opracowanie wskaźników beyond accuracy.
    - Miary sprawiedliwości (demographic parity, equalized odds), odporność (robustness), prywatność (differential privacy, privacy leakage), explainability, wykrywanie driftu; ustalanie progów akceptacji.
    - ***Ćwiczenie*: analiza zestawu wskaźników dla generatywnego modelu AI.**
5. **Zarządzanie i mitygacja ryzyka:**
    - Metody przeciwdziałania: kontroli jakości danych (data curation), redukcji biasu (re-sampling, re-weighting, fairness constraints), zabezpieczania pipeline'ów (kontrola wersji, CI/CD, monitorowanie), zarządzania prawami dostępu, podpisywania/watermarkowania generowanych treści, filtracji treści dla modeli generatywnych.
    - Plan działań naprawczych.
    - ***Ćwiczenie*: opracowanie planu mitygacji dla kluczowych ryzyk AI.**
6. **Zgodność, audit i ciągłe doskonalenie:**
    - Integracja zarządzania ryzykiem AI z ISO/IEC 42001, ISO/IEC 27001 i NIS 2.
    - Tworzenie procedur zgłaszania incydentów AI (hallucinacje, naruszenia prywatności), monitorowanie i aktualizacja modeli.
    - Przygotowanie do auditów wewnętrznych i zewnętrznych.

POST - TEST

👥 Grupa odbiorcza

Szkolenie jest skierowane do:

- menedżerów i koordynatorów odpowiedzialnych za wdrażanie i nadzorowanie systemów AI,
- specjalistów ds. compliance, governance, risk management i cyberbezpieczeństwa,
- właścicieli procesów biznesowych wykorzystujących rozwiązania AI,
- auditorów wewnętrznych i osób przygotowujących organizację do zgodności z ISO/IEC 42001,
- specjalistów IT, data science, machine learning i MLOps,
- osób odpowiedzialnych za jakość danych, prywatność i zgodność regulacyjną,
- kadry menedżerskiej podejmującej decyzje dotyczące akceptacji ryzyka AI,
- członków zespołów wdrażających rozwiązania sztucznej inteligencji w organizacji.

Szkolenie będzie szczególnie przydatne dla firm rozwijających, integrujących lub wykorzystujących systemy AI w procesach operacyjnych, produktowych, analitycznych i decyzyjnych.

✅ Korzyści po szkoleniu

Po szkoleniu uczestnicy:

- Rozumieją wymagania ISO/IEC 42001 w obszarze zarządzania ryzykiem AI.
- Potrafią identyfikować główne źródła ryzyk związanych z danymi, modelami, algorytmami i środowiskiem działania AI.
- Umieją oceniać wpływ ryzyk AI na organizację, użytkowników, klientów i interesariuszy.
- Potrafią tworzyć uporządkowaną dokumentację ryzyk oraz przypisywać odpowiedzialności właścicielom ryzyk.
- Rozumieją, jak definiować kryteria oceny, akceptacji i monitorowania ryzyk AI.
- Potrafią dobierać działania ograniczające ryzyko, zarówno techniczne, jak i organizacyjne.
- Wiedzą, jak powiązać zarządzanie ryzykiem AI z ładem organizacyjnym, bezpieczeństwem informacji i wymaganiami zgodności.
- Lepiej przygotowują organizację do auditów, przeglądów i nadzoru nad systemami AI.

Dodatkową korzyścią jest zwiększenie dojrzałości organizacji w zakresie odpowiedzialnego i bezpiecznego wykorzystania sztucznej inteligencji.

+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

Metodyka szkolenia

Szkolenie realizowane jest w formule praktyczno-warsztatowej, z naciskiem na zastosowanie wymagań normy ISO/IEC 42001 w realnych warunkach organizacyjnych.

Metodyka obejmuje:

- uporządkowane wprowadzenie do wymagań normy i powiązanych ram zarządzania ryzykiem AI,
- omówienie zagrożeń i scenariuszy ryzyka na przykładach rzeczywistych zastosowań AI,
- ćwiczenia praktyczne związane z identyfikacją ryzyk, oceną ich istotności oraz planowaniem działań mitygujących,
- analizę przypadków dotyczących modeli predykcyjnych i generatywnych,
- pracę z przykładami dokumentacji, kart systemów AI i podejść nadzorczych,
- dyskusję ekspercką nad typowymi błędami wdrożeniowymi i auditowymi,
- wymianę doświadczeń i odniesienie omawianych zagadnień do organizacji uczestników,
- pre i post testy weryfikującą wiedzę przed i po szkoleniu.

Podejście szkoleniowe koncentruje się nie tylko na wymaganiach formalnych, ale przede wszystkim na praktycznym zrozumieniu, jak skutecznie nadzorować ryzyka AI w organizacji.

Czas trwania szkolenia: 2 dni