

Slovenská obchodná a priemyselná komora, Žilinská regionálna komora
Vás pozýva na odborný **workshop**

SPRÁVA KYBERNETICKEJ BEZPEČNOSTI PRE **AI** PROJEKTY

ZOSÚLADENIE VÝVOJA UMELEJ INTELIGENCIE, RIADENIA RIZÍK
A PREVÁDZKY S NORMAMI ISO 42001 a 27001

9. december 2025 o 9.30 hod.

Žilinská RK SOPK, Háľkova 31, Žilina

Čo sa na workshope dozviete:

Vrcholoví manažéri a vedenie firmy: strategické smerovanie, súlad s predpismi (Compliance), rizikový apetít, **IT špecialisti a dátoví vedci:** technická implementácia, bezpečnosť životného cyklu, audit

Workshop poskytne praktický rámec pre identifikáciu a riadenie špecifických bezpečnostných hrozieb AI. Firmy získajú návod na bezpečné a súladné nasadenie AI, chrániac svoje dáta a modely pred útokmi.

PROGRAM:

od 9:30 do cca 14:00 hod. (prezencia účastníkov od 9:00, 11:30 - 11:45 Coffee break)

Modul 1: Strategické riadenie AI: Integrácia AIMS s ISMS

- Základ AIMS: Kľúčové požiadavky normy ISO/IEC 42001:2023 na zriadenie, implementáciu a neustále zlepšovanie Systému manažérstva AI (AIMS).
- Integrácia štandardov: Ako dosiahnuť bezproblémovú integráciu AIMS s existujúcimi štruktúrami ISO 27001 (ISMS) a ISO 27701 (PIMS) využitím spoločnej štruktúry (HLS).
- Kontext a rozsah (kap. 4): Definovanie roly organizácie (Poskytovateľ, Vývojár, Používateľ) a stanovenie rozsahu AIMS pre prispôsobenie bezpečnostných opatrení.
- Vodcovstvo a politika (kap. 5): Preukázanie záväzku vrcholového manažmentu (5.1) a návrh účinnej politiky AI (bezpečnosť, etika, zlepšovanie).

Modul 2: Identifikácia nových hrozieb AI a povinné hodnotenie rizík

- Rizikové prostredie AI: Identifikácia hrozieb špecifických pre AI (algoritmická zaujatosť, krádež modelu, manipulácia so vstupmi/výstupmi).
- Rámce riadenia rizík (ISO 23894): Aplikácia usmernení pre riadenie rizík AI, vrátane určenia tolerancie voči riziku.
- Povinné AIIA (ISO 42005): Proces posúdenia potenciálnych dôsledkov AI pre jednotlivcov, skupiny alebo spoločnosť.
- Modelovanie hrozieb pre AI: Techniky na dokumentovanie hrozieb počas životného cyklu AI (v súlade s OWASP, MITRE ATLAS).

Modul 3: Bezpečnosť už od návrhu (Security-by-Design): Implementácia technických opatrení

- Bezpečný životný cyklus AI (S-SDLC): Integrácia bezpečnostných princípov (ISO 27002) do každej fázy životného cyklu AI.
- Riadenie prístupu a údajov: Implementácia oddelených dátových prostredí a silného riadenia prístupu (ISO 27001 A.9) pre modely, dáta a API.
- Princíp najmenšieho privilégia: Aplikácia princípu "najmenšieho privilégia modelu" a validácia vstupných "promptov" (prevencia Prompt Injection).
- Pôvod a kvalita údajov: Povinný proces definovania kritérií pre prípravu údajov (ISO 42001 A.7.6) a zabezpečenie kvality a integrity tréningových dát.

Modul 4: Preukazovanie dôveryhodnosti: Monitorovanie, Red Teaming a audit

- Prevádzkové monitorovanie (kap. 9): Definovanie a dokumentovanie monitorovania systému a výkonu (napr. sledovanie "driftu" modelu a anomálneho správania).
- Zaznamenávanie a sledovateľnosť: Implementácia logovania udalostí primeraného riziku (ISO 42001 A.6.2.8) a ochrana auditných záznamov.
- AI Red Teaming a V&V: Využitie "Red Teaming" cvičení na posúdenie odolnosti modelov a používanie Verifikácie a Validácie (V&V) na udržanie robustnosti.
- Integrované riadenie incidentov: Vývoj postupov reakcie na incidenty špecifické pre AI (v súlade s ISO 27035).
- Pripravenosť na audit: Pochopenie procesu interného auditu (ISO 42001 kap. 9.2), požiadaviek na preskúmanie manažmentom a neustále zlepšovanie (kap. 10).

Lektor: Matúš SELECKÝ je skúsený konzultant a konateľ spoločnosti špecializujúcej sa na implementáciu AI riešení v oblasti spracovania dokumentov. Jeho odbornosť zahŕňa extrakciu, validáciu a efektívne spracovanie informácií z dokumentov, čím pomáha firmám zefektívniť procesy a zvýšiť konkurencieschopnosť. Lektor má bohaté skúsenosti s poskytovaním riešení pre medzinárodné spoločnosti pôsobiace v náročných odvetviach ako farmaceutický priemysel, zdravotníctvo a realitný sektor, najmä v USA, Írsku a Grécku.

Organizačný garant: Ing. Róbert Vydra, ŽRK SOPK, Háľkova 31, 010 01 ŽILINA
T: 041-7235 102, M: 0949727801, E: zahrza@za.scci.sk

Fakturácia: Anna Muziková, T: 041-72 35 101, E: ekonomza@za.scci.sk

Základný účastnícky poplatok:	98,40 €/osoba	(80,- €+23% DPH)
Člen SOPK, SPOK:	73,80 €/osoba	(60,- €+23% DPH)

Počas seminára je zabezpečené občerstvenie. Účastník obdrží študijné materiály (prezentáciu).

PRIHLÁŠKA

SPRÁVA KYBERNETICKEJ BEZPEČNOSTI PRE AI PROJEKTY ZOSÚLADENIE VÝVOJA UMELEJ INTELIGENCIE, RIADENIA RIZÍK A PREVÁDZKY S NORMAMI ISO 42001 A 27001

9. december 2025 od 9.30 hod., ŽRK SOPK, Háľkova 31, Žilina

Firma, inštitúcia					
Adresa					
IČO		DIČ		IČ DPH	
Tel./Mob.		E-mail			

Meno a priezvisko účastníkov	E-mail	Tel./Mob.

Potvrdzujeme účasť na seminári a úhradu účastníckeho poplatku vo výške € prevodom na účet SOPK Žilina v Tatra banke, a.s., IBAN: SK39 1100 0000 0026 2615 0448, VS: 091225.
IČO: 30842654, DIČ: 2020815236, IČ DPH: SK2020815236.

Túto prihlášku považujeme za záväznú a súhlasíme s podmienkami.

Dátum, meno a priezvisko kontaktnej osoby:

Registrácia Vašej účasti Vám bude potvrdená po doručení riadne vyplnenej prihlášky.

Prihlášku prosíme poslať čo najskôr pre včasnú rezerváciu miesta e-mailom na: zahrza@za.scci.sk
alebo formou **online prihlásenia na:**

<https://www.sopk.sk/za/event/sprava-kybernetickej-bezpecnosti-pre-ai-projekty-zosuladenie-vyvoja-ai-riadenia-rizik-a-prevadzky-s-normami-iso-42001-a-27001/>

Počet účastníkov na seminári je obmedzený. **Uzávierka prihlášok je 5.12.2025.**

V prípade vyššieho počtu prihlásených rozhoduje dátum odoslania prihlášky.

Účastnícky poplatok uhradte najneskôr 5.12.2025 na vyššie uvedený účet.

Po úhrade účastníckeho poplatku Vám faktúru odovzdáme na seminári pri prezencii, resp. pošleme mailom po uskutočnení seminára.

Doprava: Trolejbus č. 6 alebo 16 zo železničnej stanice, vystúpiť na 3. zastávke - Háľkova.

Vlastná doprava: z „Rondla“ smer „centrum“, po pravej strane 3. dvojdom bēžovej farby, vľajky pri budove.

Parkovanie je možné na Daxnerovej ul. na Malej Prahe - za semaformi 2. odb. vpravo (cena cca 0,80 €/hod.), platba SMS alebo platobnou kartou cez parkovací automat (ostatné uličky na Malej Prahe sú vyhradené len pre rezidentov), alebo v OC Aupark, cca 10 min. pešo (1,-€/hod., max. 6,-€/deň, platí sa v garáži pri odchode).

INFORMÁCIA O SPRACÚVANÍ A OCHRANE OSOBNÝCH ÚDAJOV

V zmysle Nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 z 27.4.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení, spracúva prevádzkovateľ, ktorým je Slovenská obchodná a priemyselná komora, so sídlom Grösslingova 4, 816 03 Bratislava, IČO: 30842654; Žilinská regionálna komora, Háľkova 31, 010 01 Žilina, osobné údaje uvedené v prihláške za účelom účasti na vyššie uvedenej akcii (seminár, webinár a pod.) - ďalej len ako „Akcia“ - po dobu stanovenú platným Registratúrnym poriadkom. Osobné údaje sú poskytnuté od tretej strany, ktorá dotknutú osobu na vyššie uvedenú Akciu prihlásila a je uvedená pod prihlasovacím údajom „Názov spoločnosti“. Osobné údaje sú poskytnuté v rozsahu: meno, priezvisko, telefonický kontakt, emailový kontakt a sú spracúvané na základe plnenia zmluvného vzťahu s treťou stranou (prihláška na Akciu) a za účelom zaslania pracovných materiálov a prístupového hesla na webinár. Ďalej Vás informujeme, že z daného podujatia budú za účelom zdokumentovania Akcie vyhotovené obrazové materiály (fotografie, kamerové záznamy), ktoré môžu byť využité na propagáciu aktivít prevádzkovateľa na jeho webovej stránke a profiloch na sociálnych sieťach. Získané osobné údaje nepodliehajú profilovaniu ani automatizovanému rozhodovaniu. Žilinská regionálna komora SOPK týmto prehlasuje, že nezamýšľa prenos osobných údajov do tretej krajiny ani medzinárodnej organizácie. Na základe písomnej žiadosti máte právo: žiadať o prístup k svojim osobným údajom, ich prípadnú opravu, obmedzenie spracúvania alebo ich vymazanie, namietať ich spracúvanie prípadne podať návrh na začatie konania dozornému orgánu (Úrad na ochranu osobných údajov SR). Podrobnejšie informácie o spracúvaní a ochrane osobných údajov ako aj právach dotknutých osôb v podmienkach prevádzkovateľa sú uvedené na stránke www.sopk.sk.