Fundusze Europejskie dla Wielkopolski | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | SAMORZĄD WOJEWÓDZTWA WIELKOPOLSKIEGO

PROGRAM

Cyberbezpieczeństwo w jednostkach samorządu terytorialnego

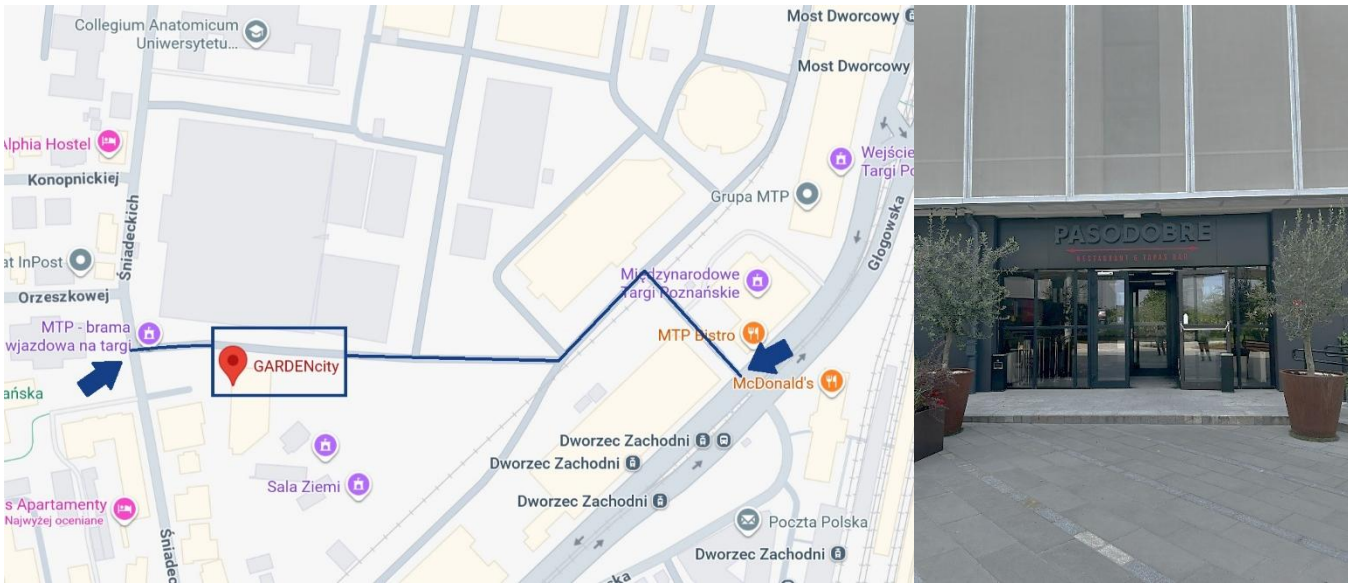
22.04.2026 r.

Lokalizacja:

GARDENcity (sala „Oregano and Wine", I piętro), ul. Śniadeckich 25, 60-734 Poznań

Wejście na teren Międzynarodowych Targów Poznańskich: bramą nr 9 od ulicy Głogowskiej lub od ulicy Śniadeckich 25

Wejście do budynku GARDENcity: od strony restauracji „Pasodobre"



Wydarzenie odbędzie się w budynku przystosowanym dla potrzeb osób z niepełnosprawnościami.

Najbliższy przystanek komunikacji miejskiej - przystanek tramwajowy „Dworzec Zachodni" (obsługujący linie: 5, 10, 11, 12, 17, 18). Schemat linii można znaleźć na stronie: https://www.ztm.poznan.pl/mapy-i-schematy-sieci/.

Parkowanie możliwe jest na parkingu PWK MTP lub na ulicach w pobliżu – nie zapewniamy miejsc parkingowych dla uczestników.

Rejestracja online na wydarzenie potrwa do 16 kwietnia br. (z możliwością wskazania specjalnych potrzeb): https://forms.gle/mA1BpTbTT6QKyKmc6

Ze względu na wielkość sali prosimy o uczestnictwo w szkoleniu do 2 osób reprezentujących daną jednostkę samorządu terytorialnego.

Cel szkolenia: wsparcie podmiotów z zakresu cyberbezpieczeństwa i praktycznego wykorzystania sztucznej inteligencji w codziennej pracy - zwiększenie świadomości na temat współczesnych cyberzagrożeń i wyposażenie pracowników w praktyczną wiedzę, jak korzystać z narzędzi AI w sposób bezpieczny, zgodny z prawem, zwiększający efektywność pracy i odporność organizacji.

Trener: Arkadiusz Stawczyk - audytor wiodący SZBI wg PN-EN ISO/IEC 27001:2023 oraz SZCD wg PN-EN IOS/IEC 22301:2020. Autor licznych polityk bezpieczeństwa, procedur i instrukcji związanych z cyberbezpieczeństwem i ochroną danych osobowych. W zakresie szkoleń specjalizuje się w tematyce cyberzagrożeń i budowania świadomości bezpieczeństwa informacji (KRI, NIS2/KSC, RODO).

PROGRAM	
8.30 – 9.00	**Rejestracja uczestników i kawa powitalna**
9.00 – 10.30	**1. Otoczenie prawne i obecne uwarunkowania:** • Otoczenie prawne w pigułce – rola pracownika w jednostkach samorządu terytorialnego w systemie cyberbezpieczeństwa zgodnie z wymaganiami KSC, RODO i dyrektywy NIS2 (ujęcie praktyczne: czego JST musi przestrzegać, jakie są minimalne standardy i odpowiedzialności). • Standardy i rekomendacje UE dotyczące odpowiedzialnego korzystania z AI – aktualne rekomendacje i standardy UE w obszarze odpowiedzialnego korzystania z AI, AI Act (praktyczne ujęcie dla JST: kategorie ryzyka, wymagania dotyczące transparentności, ograniczenia i obowiązki dotyczące przetwarzania danych, konsekwencje dla pracowników i procedur w urzędzie). • Aktualne trendy w cyberprzestępczości wymierzonej w samorządy – dlaczego urzędy są celem ataków? Najnowsze przypadki ataków na JST w Polsce (analiza typowych błędów i wniosków), jak cyberprzestępcy wykorzystują słabe ogniwa w strukturze organizacji? • Najczęstsze metody ataków stosowane wobec administracji: ransomware (mechanizm działania, najczęstsze wektory wejścia do systemu), phishing, smishing i inne. • Zmiany w ustawie o Krajowym Systemie Cyberbezpieczeństwa - najważniejsze założenia projektowanej nowelizacji KSC, nowe zobowiązania dla JST (m.in. systemy zgłoszeń, role i funkcje, obowiązki dokumentacyjne), wpływ zmian na codzienną praktykę urzędów. • Lokalne Centra Cyberbezpieczeństwa - analiza zagadnienia – podstawowa koncepcja LCC, modele współpracy JST w zwiększaniu odporności cybernetycznej, potencjalne korzyści i wyzwania.
10.30 – 10.45	**Przerwa**
10.45 – 12.30	**2. Bezpieczeństwo w codziennej pracy urzędnika:** • Zarządzanie tożsamością i dostępem – zasady tworzenia silnych, unikalnych haseł oraz stosowanie menedżerów haseł, rola i znaczenie uwierzytelniania dwuskładnikowego (2FA) w zabezpieczaniu, najczęstsze błędy użytkowników prowadzące do przejęcia kont. • Ochrona poczty elektronicznej – weryfikacja nadawców, rozpoznawanie podejrzanych domen i linków, bezpieczne otwieranie załączników. • Bezpieczne korzystanie ze sprzętu służbowego – aktualizacje, szyfrowanie dysków, automatyczna blokada ekranu, odpowiedzialne korzystanie z nośników danych. • Bezpieczeństwo pracy zdalnej i mobilnej – zagrożenia związane z publicznymi i niezaufanymi sieciami Wi-Fi, zasada „czystego biurka i czystego ekranu”, ochrona danych podczas pracy poza urzędem: transport dokumentów, zabezpieczanie urządzeń, ryzyko podglądania ekranu.
12.30 – 13.00	**Lunch**

13.00 – 14.30	**3. Sztuczna Inteligencja: Szanse i zagrożenia:** • AI jako narzędzie ataku – perspektywa cyberprzestępców – rozpoznawanie manipulacji opartych na AI oraz zaawansowane ataki socjotechniczne wspierane przez generatywne modele językowe), zagrożenia związane z vishingiem i innymi technikami, które wykorzystują realistyczne generowanie głosu przez AI, realne przykłady scenariuszy ataków na administrację publiczną. • Bezpieczne korzystanie z narzędzi AI w administracji – ochrona danych osobowych i informacji niejawnych, ryzyko wycieku danych wrażliwych i tajemnic służbowych podczas korzystania z publicznych czatbotów i publicznych punktów dostępu do Wi-Fi oraz sposobów minimalizacji ryzyka. • Halucynacje AI i zasady weryfikacji treści – wyjaśnienie zjawiska „halucynacji AI" – generowanie informacji nieprawdziwych, niepełnych lub nieistniejących, konsekwencje korzystania z nieweryfikowanych treści w pracy urzędniczej, zasady weryfikacji wyników generowanych przez AI (porównanie z wiarygodnymi źródłami, sprawdzanie dat, odwołań prawnych i faktów, analiza logiki i spójności wygenerowanej treści). **4. Moduł Warsztatowy:** • Analiza przykładowych incydentów i symulacje ataków – praca na rzeczywistych lub realistycznych przykładach wiadomości e-maili i SMS-ów; rozpoznawanie elementów wskazujących na próbę ataku, symulacje ataków phishingowych i smishingowych – omówienie sposobu działania, błędów popełnianych przez użytkowników i prawidłowych reakcji. • Obrona przed manipulacją i weryfikacja tożsamości – praktyczne metody weryfikacji tożsamości osoby kontaktującej się: zasady potwierdzania tożsamości dzwoniącego, rozpoznawanie prób podszywania się w komunikatorach i podczas rozmów telefonicznych, identyfikacja sygnałów ostrzegawczych stosowanych w atakach vishingowych, także tych generowanych przez AI. • Tworzenie procedur bezpieczeństwa – wypracowanie przez uczestników podstawowych procedur dotyczących zgłaszania incydentów bezpieczeństwa, postępowania z podejrzanymi wiadomościami i treściami, minimalizacji szkód po wykryciu incydentu, zasad bezpiecznej pracy z danymi i dokumentami. Budowanie „mini-checklist" dla urzędników - praktyczne narzędzia do wdrożenia po szkoleniu. • Konfiguracja prostych narzędzi AI wspomagających ochronę - ćwiczenia z konfiguracji i bezpiecznego użycia podstawowych narzędzi AI, które mogą wspierać bezpieczeństwo cyfrowe, automatyczna analiza treści e-mail pod kątem podejrzanych elementów, asystenci do sprawdzania zgodności treści, narzędzia wspomagające ocenę wiarygodności komunikatów. Praktyczne scenariusze wykorzystania AI w ograniczaniu ryzyka ludzkiego błędu.
14:30 – 15.00	**Sesja: Pytania i odpowiedzi.**

Wykonawca cyklu szkoleń:

Fundacja Rozwoju Demokracji Lokalnej
Ośrodek Regionalny w Zielonej Górze
al. Niepodległości 16/9, 65-048 Zielona Góra

Organizator:
Metropolia Poznań
ul. Kościelna 37, 60-537 Poznań
Osoba do kontaktu: Weronika Świst
tel. 533 228 481, e-mail: weronika.swist@metropoliapoznan.pl