

SZKOLENIE STACJONARNE 13 czerwca 2025 r.

DOLNOŚLĄSKIE FORUM PRZEWODNICZĄCYCH RAD GMIN I POWIATÓW. CYBERBEZPIECZEŃSTWO I (AI) SZTUCZNA INTELIGENCJA W PRACY RADNEGO.

WAŻNE INFORMACJE O SZKOLENIU:

Zapraszamy na kolejne już w tym roku spotkanie w ramach Dolnośląskiego Forum Przewodniczących Rad Gmin i Powiatów, które poświęcone będzie niezwykle istotnemu tematowi – cyberbezpieczeństwu w kontekście nowych regulacji NIS-2 oraz uKSC. W dobie rosnącej liczby zagrożeń w cyberprzestrzeni oraz zmieniających się wymogów prawnych, szczególnie ważne jest, aby wszyscy pracownicy samorządowi skutecznie przygotowali się na nowe wyzwania.

Podczas szkolenia omówimy kluczowe obowiązki wynikające z regulacji NIS-2 oraz uKSC, w tym identyfikację ryzyk, procedury reagowania na incydenty i obowiązek raportowania. Uczestnicy poznają praktyczne wskazówki dotyczące wdrażania nowych przepisów, a także konsekwencje ich niewypełnienia. Nie zabraknie również przykładów studiów przypadków oraz wymiany doświadczeń.

CELE I KORZYŚCI:

- Zwiększysz świadomość i wiedzę o zagrożeniach cybernetycznych specyficznych dla JST,
- Poznasz praktyczne metody ochrony danych i systemów oraz reagowania na incydenty,
- Zrozumiesz wymogi prawne i obowiązki wynikające z NIS2 i uKSC,
- Rozwiniesz kompetencje radnych jako kluczowych aktorów w budowaniu kultury bezpieczeństwa,
- Nauczysz się rozpoznawać i przeciwdziałać atakom socjotechnicznym,
- Poznasz wpływ nowych technologii, w tym sztucznej inteligencji na cyberbezpieczeństwo.

W trakcie szkolenia będziemy rozważać:

- Czy dobrze rozumiem, jakie są najczęstsze cyberzagrożenia dla jednostek samorządu terytorialnego (JST), takie jak phishing, ransomware czy ataki na BIP i eSesję?
- Jaką rolę pełnię jako radny w kształtowaniu kultury bezpieczeństwa w gminie/powiecie?
- Czy wiem, dlaczego osoby publiczne, w tym radni, są szczególnie narażone na ataki cybernetyczne?
- Czy jestem świadomy odpowiedzialności za dostęp i poufność danych, z których korzystam jako użytkownik systemów JST?
- Jakie ryzyko niesie ze sobą praca zdalna i korzystanie z prywatnych urządzeń lub skrzynek mailowych w kontaktach z mieszkańcami?
- Czy potrafię stosować zasady bezpiecznej komunikacji, takie jak silne hasła, uwierzytelnianie wieloskładnikowe (MFA) i VPN?
- Czy znam kluczowe założenia dyrektywy NIS2 i jej wpływ na obowiązki JST, w tym sprawozdawczość i analizę ryzyka?
- Czy rozumiem wymagania ustawy o krajowym systemie cyberbezpieczeństwa (uKSC) dotyczące urzędów gmin i obowiązki zgłaszania incydentów?
- Czy potrafię rozpoznać próby socjotechniczne, takie jak phishingowe e-maile, SMS-y czy rozmowy telefoniczne?
- Jak reagować na podejrzane wiadomości i jakie są najczęstsze triki stosowane przez cyberprzestępców?
- Czy wiem, jak postępować w przypadku podejrzenia incydentu bezpieczeństwa?
- Jak sztuczna inteligencja jest wykorzystywana przez cyberprzestępców (np. deepfake, fałszywe e-maile) i jak może wspierać obronę (np. analiza logów)?
- Jakie informacje mogę bezpiecznie publikować jako osoba publiczna, a które mogą narazić mnie lub moją gminę na ryzyko?

- Czy potrafię zabezpieczyć swoją skrzynkę e-mail i telefon służbowy oraz prywatny?
- Jak zdobyta wiedza i umiejętności przełożą się na poprawę ciągłości działania i odporności mojej gminy na cyberzagrożenia?

PROGRAM:

1. Wprowadzenie:

- a. Powitanie uczestników, cel szkolenia.
- b. Wzrost liczby cyberataków na sektor publiczny – zagrożenia w kontekście JST.
- c. Rola radnych w kreowaniu kultury bezpieczeństwa w gminie.

2. Cyberzagrożenia w praktyce JST:

- a. Najczęstsze incydenty: phishing, ransomware, utrata danych, ataki na BIP i eSesję.
- b. Ataki celowane na osoby publiczne – dlaczego radny to atrakcyjny cel.
- c. Przykład realnego incydentu w polskiej gminie.

3. Rola radnych w ochronie informacji i systemów:

- a. Radny jako użytkownik systemu – odpowiedzialność za dostęp i poufność danych.
- b. Praca zdalna i korespondencja z mieszkańcami – ryzyko przy korzystaniu z prywatnych urządzeń i skrzynek mailowych.
- c. Bezpieczna komunikacja: zasady stosowania silnych haseł, MFA, VPN.

4. Podstawy prawne cyberbezpieczeństwa w administracji publicznej:

- a. Dyrektywa NIS2: kluczowe założenia i wpływ na JST.
- b. Obowiązki sprawozdawcze, szkolenia, analiza ryzyka, plan ciągłości działania.
- c. Nowe definicje podmiotów istotnych i ważnych – czy JST się kwalifikuje?
- d. Ustawa o krajowym systemie cyberbezpieczeństwa (uKSC).
- e. Wymagania wobec urzędów gmin, współpraca z CSIRT NASK.
- f. Obowiązek zgłaszania incydentów i wdrażania działań zaradczych.
- g. Rola radnych w nadzorze nad cyberbezpieczeństwem jednostek i podległych instytucji.

5. Test socjotechniczny – symulacja ataku:

- a. Symulowane e-maile, SMS-y i rozmowy telefoniczne z prośbą o dane lub kliknięcie linku
- b. Głosowanie: phishing czy nie?
- c. Jak rozpoznać manipulację? Omówienie najczęstszych trików.

6. Sztuczna inteligencja a cyberzagrożenia:

- a. Jak AI pomaga cyberprzestępcom: generowanie fałszywych e-maili, deepfake, voice cloning.
- b. AI w obronie: analiza logów, wykrywanie anomalii, chatboty ds. bezpieczeństwa.
- c. Czy radny może zaufać AI? Rola człowieka w weryfikacji informacji.

7. Bezpieczny radny – dobre praktyki:

- a. 10 kluczowych zasad bezpiecznego korzystania z urządzeń i internetu.
- b. Co można publikować jako osoba publiczna – zdjęcia, lokalizacja, screeny, dane kontaktowe.
- c. Jak zabezpieczyć skrzynkę e-mail i telefon służbowy/prywatny.
- d. Odpowiedzialność za dane osobowe i dostęp do informacji publicznej.

8. Podsumowanie i pytania.

ADRESACI:

członkowie Dolnośląskiego Forum Przewodniczących Rad Gmin i Powiatów, przewodniczący rad, radni, przewodniczący i członkowie komisji działających zgodnie z regulaminem pracy rady gminy (powiatu), osoby zajmujące się obsługą biur rad, osoby współpracujące z organem uchwałodawczym.

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

DOLNOŚLĄSKIE FORUM PRZEWODNICZĄCYCH RAD GMIN I POWIATÓW. CYBERBEZPIECZEŃSTWO I (AI) SZTUCZNA INTELIGENCJA W PRACY RADNEGO



Szkolenie będziemy realizowali **w formie stacjonarnej** w Biurze FRDL OKST, Wrocław
ul. Piłsudskiego 43, (III piętro.)



13 czerwca 2025 r.

Szkolenie w godzinach: 10:00-14:00



Cena: członkowie Forum w ramach składki, pozostałe osoby 510 PLN netto/os. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

CENA zawiera:

udział w profesjonalnym szkoleniu,
materiały szkoleniowe w wersji elektronicznej, możliwość konsultacji z trenerem podczas zajęć,
przerwy kawowe.

DANE DO KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego
Ośrodek Kształcenia Samorządu Terytorialnego im. Waleriana Pańki
ul. Moniuszki 7, 40-005 Katowice,
ul. Piłsudskiego 43, 50-032 Wrocław
tel. 71, 372 41 21, 722 152 180
milena.dudek@okst.pl; agnieszka.wronecka@okst.pl

DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

Nazwa i adres nabywcy
(dane do faktury)

Nazwa i adres odbiorcy

NIP

Telefon

1. Imię i nazwisko uczestnika,
stanowisko,
E-MAIL i TEL. DO KONTAKTU

2. Imię i nazwisko uczestnika,
stanowisko,
E-MAIL i TEL. DO KONTAKTU

Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe)

TAK ☐ NIE ☐

Członek FORUM Przewodniczących Rad

TAK ☐ NIE ☐

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora www.okst.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.okst.pl do 9 czerwca 2025 r.

UWAGA Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.

Podpis osoby upoważnionej _____