PROGRAM
VI Zjazdu Pracowników Pionów Ochrony Informacji Niejawnych
oraz XVIII Forum Kierowników Jednostek Organizacyjnych i Pełnomocników ds. Ochrony Informacji Niejawnych
Bukowina Tatrzańska, 26–28 października 2026 r.

DZIEŃ I – 26.10.2026
BEZPIECZEŃSTWO PAŃSTWA I NOWA MAPA ZAGROŻEŃ DLA INFORMACJI CHRONIONYCH

13.00 – 14.00 - Obiad

14.00 – 14.10 - Otwarcie VI Zjazdu
Powitanie uczestników, gości honorowych, prelegentów i partnerów wydarzenia.
Wprowadzenie do tematyki VI Zjazdu.

14.10 – 14.40
Ochrona danych osobowych w państwie przyfrontowym w jednostkach organizacyjnych przetwarzających informacje niejawne
Zakres tematyczny wystąpienia:
- ochrona danych osobowych w warunkach podwyższonego ryzyka,
- relacja między ochroną danych osobowych a ochroną informacji niejawnych,
- odpowiedzialność jednostki organizacyjnej,
- ryzyka związane z cyfryzacją, obiegiem dokumentów i komunikacją,
- praktyczne znaczenie właściwych procedur i świadomości pracowników.

Prelegent: Monika Krasińska – Dyrektor Departamentu Prawa i Nowych Technologii UODO

14.40 – 15.45 - SESJA OTWARCIA
Czy jesteśmy przygotowani na kryzys, którego jeszcze nie nazwano?
Charakter sesji: panel strategiczny dotyczący bezpieczeństwa państwa, odporności instytucji oraz sytuacji Polski jako państwa funkcjonującego w warunkach narastających zagrożeń.
Zakres sesji:
- aktualne uwarunkowania bezpieczeństwa Polski i Europy,
- działania poniżej progu wojny i presja na instytucje państwa,
- odporność państwa, administracji, przedsiębiorstw i społeczeństwa,
- rola informacji w sytuacji narastającego zagrożenia,
- znaczenie ochrony informacji prawnie chronionych dla bezpieczeństwa narodowego.

Moderator: prof. dr hab. Dariusz Szostek, sędzia Trybunału Konstytucyjnego
Uczestnicy:
- prof. dr hab. inż. Aleksander Nawrat - Pracownik naukowy Politechniki Śląskiej, Prezes Zarządu MATIC S. A.
- prof. dr hab. Jan Kozak – Dyrektor Instytutu Sztucznej Inteligencji i Cyberbezpieczeństwa w Katowicach
- prof. dr hab. Robert Socha - Pracownik naukowy Akademii WSB
- Michał Kanownik – Prezes Zarządu Cyfrowa Polska
- dr Tamara Rud - Ekspert ds. cyberbezpieczeństwa w specjalizacji cyber wywiad

15.45 – 16.00 - Przerwa

16.00 – 17.00 - SESJA

Nowa mapa zagrożeń dla ochrony informacji niejawnych w jednostkach organizacyjnych.

Charakter sesji: panel praktyczno-ekspercki dotyczący zagrożeń bezpośrednio związanych z ochroną informacji niejawnych w administracji publicznej, samorządzie, służbach, podmiotach gospodarczych i jednostkach realizujących zadania na rzecz bezpieczeństwa państwa.

Zakres sesji:

- zagrożenia szpiegowskie wobec jednostek organizacyjnych,
- zagrożenia wewnętrzne i osobowe,
- nieuprawniony dostęp do informacji,
- słabe punkty organizacji, procedur i nadzoru,
- ochrona informacji w relacjach z wykonawcami, podwykonawcami i partnerami zewnętrznymi,
- najważniejsze wyzwania dla kierowników jednostek i pełnomocników ochrony.

Moderator: gen. bryg. Paweł Pruszyński - b. Zastępca szefa Agencji Bezpieczeństwa Wewnętrznego
Uczestnicy:

- płk Tomasz Borkowski - b. Funkcjonariusz służb specjalnych (ABW, UOP)
- płk Dariusz Siwek - b. Dyrektor Delegatury Agencji Bezpieczeństwa Wewnętrznego w Opolu
- płk dr inż. Dobrosław Mąka - specjalista w zakresie analizy zagrożeń i zarządzania ryzykiem, wykładowca przedmiotów z dziedziny bezpieczeństwa narodowego
- ppłk Grzegorz Zbiróg - b. Naczelnik Wydziału Ochrony Informacji Niejawnych Delegatury ABW w Lublinie. Specjalizuje się w budowie kancelarii tajnych oraz uzyskiwaniu dla przedsiębiorstw świadectw bezpieczeństwa przemysłowego
- prof. dr hab. inż. Aleksander Nawrat

Efekt sesji: wskazanie kluczowych zagrożeń dla systemu ochrony informacji niejawnych w jednostkach organizacyjnych.

17.00 – 18.00 - SESJA

Szpiegostwo XXI wieku — człowiek, technologia czy algorytm?

Charakter sesji: panel poświęcony współczesnym metodom pozyskiwania informacji, ze szczególnym akcentem na człowieka, rozpoznanie osobowe, socjotechnikę, OSINT oraz zagrożenia wynikające z codziennego korzystania z technologii.

Zakres sesji:

- współczesne formy działalności wywiadowczej,
- HUMINT, OSINT i rozpoznanie środowiskowe,
- socjotechnika, manipulacja, presja i budowanie relacji operacyjnej,
- smartfon, komunikatory i media społecznościowe jako źródła informacji,
- pracownik jako pierwsza linia bezpieczeństwa,
- jak rozpoznawać symptomy zainteresowania informacją chronioną.

Moderator: prof. dr hab. Jan Kozak - Dyrektor Instytutu Sztucznej Inteligencji i
Uczestnicy:

- prof. dr hab. Dariusz Szostek
- dr Tamara Rud
- dr Anna Nastuła – Prawnik, ekspert Ochrony Danych Osobowych
- dr inż. Jan Derkacz - pracownik naukowo-dydaktyczny AGH w Krakowie
- Michał Kanownik - Prezes Zarządu Związku Cyfrowa Polska

Efekt sesji: praktyczne wskazanie, jak współczesne działania rozpoznawcze mogą dotykać zwykłych pracowników jednostek organizacyjnych.

18.00 – 18.15 - Przerwa

18.15 – 18.40
Spotkanie autorskie / rozmowa specjalna
Literatura szpiegowska a realne zagrożenia wywiadowcze.
Rozmowa z autorem książek o tematyce szpiegowskiej o tym, gdzie kończy się fikcja literacka, a zaczyna realna wiedza o mechanizmach działania służb, agentury, dezinformacji i presji na człowieka.

Gość specjalny: ppłk Robert Michniewicz – oficer wywiadu, autor książek o tematyce szpiegowskiej
Rozmowę prowadzi: dr Anna Nastuła

18.40 – 19.30 - WYSTĄPIENIA SPECJALNE
1. gen. Mieczysław Bieniek - były Zastępca Dowódcy Strategicznego NATO Po lipcowym szczycie NATO — bezpieczeństwo Polski i Europy
2. Przedstawiciel Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni Walki w cyberprzestrzeni — przeciwdziałanie i zwalczanie cyberataków
3. Przedstawiciel Centralnego Biura Zwalczania Cyberprzestępczości Wykrywanie cybersprawców. Praktyczne możliwości współpracy z Zarządem Terenowym CBZC

20.00 - Uroczysta kolacja

DZIEŃ II – 27.10.2026
INFORMACJA JAKO POLE WALKI
Praktyka, błędy, incydenty, technologia i odpowiedzialność

07.30 – 09.00 - Śniadanie

09.00 – 10.00 - DEBATA
Dezinformacja, cyberatak, wyciek informacji — jak reaguje odpowiedzialna jednostka organizacyjna?
Charakter debaty: praktyczny panel dotyczący pierwszych decyzji, zarządzania incydentem, komunikacji kryzysowej i odpowiedzialności organizacyjnej.
Zakres debaty:

- cyberatak, incydent bezpieczeństwa i wyciek informacji — pierwsze decyzje kierownictwa,
- fałszywe narracje, operacje wpływu, deepfake, boty i trolle jako element presji na instytucje,
- wywoływanie paniki, strachu i chaosu informacyjnego,
- rola kierownika jednostki, pełnomocnika ochrony, pionu ochrony, IT i komunikacji,
- procedury reagowania, dokumentowanie incydentu i komunikacja wewnętrzna,
- współpraca z właściwymi organami i służbami,
- praktyczne wnioski dla jednostek organizacyjnych.

Moderator: Michał Kanownik
Uczestnicy:

- prof. dr hab. inż. Aleksander Nawrat
- prof. dr hab. Dariusz Szostek
- prof. dr hab. Robert Socha
- prof. dr hab. Jan Kozak
- płk dr hab. inż. Dobrosław Mąka

10.00 – 11.00 - PANEL PRAKTYCZNY

Zanim powiesz, wyślesz, klikniesz — pomyśl. Bezpieczeństwo informacyjne na co dzień.

Charakter panelu: praktyczna sesja o codziennych nawykach, błędach pracowników i prostych standardach bezpieczeństwa, które decydują o realnej ochronie informacji.

Główne zagadnienia:

- rozmowy, maile, załączniki, wydruki, skany, notatki i dokumenty robocze,
- niezablokowany ekran, dokumenty pozostawione na biurku, niekontrolowany dostęp do pomieszczeń,
- „odpowiedz wszystkim", niewłaściwy adresat, prywatne kanały komunikacji,
- zdjęcia z biura, relacje z wydarzeń, media społecznościowe i niezamierzone ujawnianie informacji,
- bezpieczeństwo spotkań, prezentacji, list uczestników i materiałów roboczych,
- odpowiedzialność pracowników i przełożonych za przestrzeganie prostych zasad,
- Rok Świadomości i Bezpieczeństwa Informacyjnego jako impuls do edukacji i porządkowania standardów.

Moderator: Elżbieta Bińczyk - Pełnomocnik Zarządu ds. Ochrony Informacji Niejawnych

Uczestnicy:

- dr Tamara Rud
- dr Anna Nastuła
- mjr Alicja Kazusek - b. Oficer Agencji Bezpieczeństwa Wewnętrznego
- kpt. Beata Jachymska - b. Naczelnik Departamentu OIN Agencji Bezpieczeństwa Wewnętrznego
- kpt. Grzegorz Stefan - b. funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego

Efekt panelu: katalog najczęstszych codziennych zachowań ryzykownych oraz prostych zasad, które powinny być wdrażane w każdej jednostce organizacyjnej.

11.00 – 11.15 - Przerwa

11.15 – 12.00 - SESJA

Systemowe błędy w ochronie informacji niejawnych — praktyka, kontrola, audyt i odpowiedzialność.

Charakter sesji: panel ekspercki poświęcony błędom organizacyjnym i proceduralnym, odróżniony od wcześniejszego panelu o codziennych nawykach pracowników.

Zakres sesji:

- błędy kierowników jednostek organizacyjnych,
- błędy pełnomocników ochrony i pionów ochrony,
- błędy w kancelariach tajnych i obiegu dokumentów,
- nieaktualna lub formalna dokumentacja bezpieczeństwa,
- problemy z nadzorem nad wykonawcami i osobami dopuszczonymi do informacji,
- błędy ujawniane podczas kontroli i audytów,
- jak budować system realny, a nie tylko formalny.

Moderator: płk Dariusz Siwek – były Dyrektor Delegatury ABW

Uczestnicy:

- ppłk Grzegorz Zbiróg
- mjr Alicja Kazusek – b. Oficer Agencji Bezpieczeństwa Wewnętrznego
- mjr Michał Cyndel -
- kpt. Beata Jachymska – były Naczelnik Wydziału Departamentu OIN ABW
- kpt. Grzegorz Stefan – były oficer ABW
- dr Anna Nastuła

Efekt sesji: wskazanie najważniejszych błędów systemowych oraz praktycznych działań naprawczych.

12.00 – 13.15 - DEBATA TECHNOLOGICZNA

Jak nowoczesne technologie mogą wspierać ochronę informacji niejawnych?

AI w pracy pełnomocnika ochrony — wsparcie, ryzyko czy złudzenie bezpieczeństwa?
Charakter debaty: główna debata technologiczna VI Zjazdu, koncentrująca w jednym miejscu temat sztucznej inteligencji, automatyzacji i nowych narzędzi wspierających bezpieczeństwo informacji.
Zakres debaty:

- sztuczna inteligencja jako narzędzie wspierające analizę ryzyka,
- automatyzacja procesów i dokumentowania czynności,
- monitoring zagrożeń i wykrywanie anomalii,
- wykrywanie dezinformacji i manipulacji informacyjnej,
- bezpieczeństwo dokumentów i obiegu informacji,
- czy AI może wspierać pełnomocnika ochrony,
- jakie zadania można automatyzować,
- gdzie kończy się wsparcie technologiczne, a zaczyna ryzyko,
- czy technologia może osłabić odpowiedzialność człowieka,
- jak bezpiecznie korzystać z AI w obszarze informacji prawnie chronionych.

Moderator: prof. dr hab. inż. Aleksander Nawrat
Uczestnicy:

- gen. bryg. Paweł Pruszyński
- dr Tamara Rud
- płk dr inż. Dobrosław Mąka
- Michał Kanownik

13.15 – 13.30 - Przerwa

13.30 – 15.00 - DEBATA

OTWARTA DEBATA PRAKTYKÓW

Praktyczne problemy ochrony informacji niejawnych w jednostkach organizacyjnych w stanie zagrożenia bezpieczeństwa państwa Charakter debaty: otwarta dyskusja praktyków z udziałem uczestników sali. Celem jest zebranie realnych problemów, postulatów i propozycji zmian wynikających z codziennej pracy pionów ochrony informacji niejawnych.
Zakres debaty:

- szczególne obowiązki kierowników jednostek organizacyjnych i pełnomocników ochrony,
- postępowania przetargowe z dostępem do informacji niejawnych,
- wykonawcy, podwykonawcy i nadzór nad realizacją zadań,
- dokumentacja bezpieczeństwa i jej praktyczne stosowanie,
- trudności w stosowaniu ustawy i przepisów wykonawczych,
- najczęstsze problemy praktyczne pionów ochrony,
- propozycje zmian legislacyjnych i organizacyjnych,
- rekomendacje dla administracji publicznej i jednostek organizacyjnych,
- wnioski do dalszych prac KSOIN i SWBN.

Moderator: ppłk Grzegorz Zbiróg
Uczestnicy:

- mjr Alicja Kazusek
- mjr Michał Cyndel
- kpt. Beata Jachymska
- kpt. Grzegorz Stefan
- Elżbieta Bińczyk

- uczestnicy VI Zjazdu

Efekt debaty: roboczy katalog problemów środowiska oraz propozycje rekomendacji końcowych VI Zjazdu.

15.00 – 16.00 – Obiad

16.00 – 19.00 - Czas wolny, konsultacje, korzystanie z atrakcji ośrodka

19.00 – Kolacja góralska

DZIEŃ III - 28.10.2026

OCHRONA INFORMACJI 2030

Przyszłość, odpowiedzialność i rekomendacje środowiska

07.30 – 09.00 - Śniadanie

09.00 – 09.40

Ochrona informacji niejawnych 2030 — kierunki zmian, nowe zagrożenia i odpowiedzialność człowieka.

Charakter wystąpienia: syntetyczne spojrzenie na przyszłość systemu ochrony informacji niejawnych, bez powtarzania szczegółowej debaty technologicznej z Dnia II.

Zakres wystąpienia:

- przyszłość systemu ochrony informacji niejawnych,
- nowe modele zagrożeń wobec informacji chronionych,
- zmiany organizacyjne, proceduralne i technologiczne,
- cyfryzacja procesów a odpowiedzialność człowieka,
- kompetencje przyszłości pełnomocnika ochrony,
- znaczenie edukacji, świadomości i kultury bezpieczeństwa.

Prelegent: płk Tomasz Borkowski

09.40 – 10.20

Modelowe funkcjonowanie jednostki organizacyjnej w stanie podwyższonego zagrożenia bezpieczeństwa państwa.

Charakter wystąpienia: praktyczne podsumowanie, jak jednostka organizacyjna powinna funkcjonować w sytuacji narastającego zagrożenia, presji informacyjnej, cyberataków, zagrożeń osobowych i organizacyjnych.

Zakres wystąpienia:

- odpowiedzialność kierownika jednostki organizacyjnej,
- rola pełnomocnika ochrony i pionu ochrony informacji,
- przygotowanie jednostki na sytuacje kryzysowe,
- bezpieczeństwo informacji jako element ciągłości działania,
- współpraca wewnętrzna: kierownictwo, pion ochrony, IT, administracja, komunikacja,
- praktyczne obowiązki w warunkach podwyższonego zagrożenia.

Prelegent: Michał Kanownik – Prezes Zarządu Cyfrowa Polska

10.20 – 10.40 - SESJA KOŃCOWA

Rekomendacje VI Zjazdu

Przedstawienie najważniejszych wniosków z obrad oraz roboczych rekomendacji środowiska kierowników jednostek organizacyjnych, pełnomocników ochrony i pracowników pionów ochrony informacji niejawnych.
Zakres sesji:

- najważniejsze zagrożenia zidentyfikowane podczas VI Zjazdu,
- praktyczne problemy wymagające dalszych prac,
- postulaty zmian legislacyjnych i organizacyjnych,
- potrzeby edukacyjne i szkoleniowe,
- kierunki dalszej aktywności KSOIN i SWBN.

Prowadzenie: Tadeusz Koczkowski

10.40 – 11.00 - Zakończenie VI Zjazdu
Podsumowanie obrad. Podziękowanie uczestnikom, prelegentom, partnerom i gościom. Zapowiedź dalszych działań KSOIN i SWBN.

Prowadzenie: Tadeusz Koczkowski