Agenda Konferencji
17 - 18.09.2026 r.

„Zarządzanie Bezpieczeństwem Informacji w Sektorze Nauki i Szkolnictwa Wyższego oraz Administracji Publicznej. Wymagania NIS2 a Cyberodporność Podmiotów Kluczowych i Ważnych”.

Konferencja odbywa się w ramach „Podkarpackiego Forum Bezpieczeństwa 2026 - Kształtowanie bezpieczeństwa lokalnego - teoretyczne i praktyczne konteksty”

Organizator:

Uniwersytet Rzeszowski

Patronaty:
Honorowe:
- Ministerstwo Cyfryzacji
- Prezes Urzędu Ochrony Danych Osobowych
- Przewodniczący Sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
- Wojewoda Podkarpacki
- Konferencja Rektorów Akademickich Szkół Polskich (KRASP)

Medialny:
- Nowiny, Nowiny 24,

Komitet naukowy:
prof. dr hab. Janusz PASTERSKI
prof. dr hab. Sabina GRABOWSKA
prof. dr hab. n. med. Artur MAZUR
dr hab. Barbara PĘKALA, prof. UR
dr hab. Krzysztof ŻARNA, prof. UR
dr hab. Bogdan WIERZBIŃSKI, prof. UR
dr hab. Roman ULIASZ, prof. UR
dr hab. Grzegorz BONUSIAK, prof. UR
dr hab. Dorota SEMKÓW, prof. UR
dr hab. Jan BAZAN, prof. UR
dr inż. Przemysław PARDEL

Komitet organizacyjny:
dr Adam NAJDECKI
mgr SŁAWOMIR ADAMCZYK
mgr Krystian ANTOCHÓW
mgr Marek GROŃ
mgr Anna JANCZYCKA
mgr Przemysław MIKOŁAJCZYK

Termin:
17-18 września 2026 r.

Miejsce:
Uniwersytet Rzeszowski, budynek A0 (Aula Kula + 2 sale panelowe),

Format konferencji:

- 2 dniowa konferencja ogólnopolska, warsztaty i panele dyskusyjne,
- ok 200 - 250 uczestników,

PROGRAM KONFERENCJI

DZIEŃ 1 – STRATEGIA, REGULACJE PRAWNE, NORMY, PAŃSTWO

Miejsce obrad: „Aula Kula"

08:00–09:00
Rejestracja uczestników
otwarcie strefy wystawienniczej partnerów.

09:00–09:30
Uroczyste otwarcie konferencji i powitanie gości

- prof. dr hab. n. med. Adam Reich – JM Rektor Uniwersytetu Rzeszowskiego,
- Teresa Kubas-Hul – Wojewoda Podkarpacki
- Konrad Komornicki - Zastępca Prezesa UODO,
- Bartłomiej Pejo – Przewodniczący Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
- wystąpienia przedstawicieli zaproszonych gości.

I PANEL:

09:30–10:45
<u>NIS2 zmienia zasady gry - nowa odpowiedzialność uczelni, administracji i biznesu - podmiotów kluczowych i ważnych</u>

- „Norma PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 jako elementy spełnienia przez podmioty kluczowe i ważne wymagań Ustawy o krajowym systemie cyberbezpieczeństwa." – **Renata Podlewska – Pełnomocnik Dyrektora ds. Bezpieczeństwa Informacji, Inspektor Ochrony Danych - Regionalne Centrum Krwiodawstwa i Krwiolecznictwa w Poznaniu.**

10:45–11:30

- Strategia w budowaniu cyberodporności - czy polskie uczelnie są gotowe na rygor NIS2?– **Innocenta Dźwierzyńska, CEO Inamedu / Cyfrowi.ai - ekspert w obszarze transformacji cyfrowej, rozwoju biznesu i budowania cyberodporności organizacji.**

zakres tematyczny: Uczelnie jako infrastruktura krytyczna wiedzy i badań; Odpowiedzialność rektorów; Perspektywa budowania realnej cyberodporności uczelni nie tylko na poziomie technologii, procedur i zgodności regulacyjnej, ale przede wszystkim ludzi tworzących środowisko akademickie – pracowników naukowych i administracyjnych oraz studentów.

- Prezentacja na temat działań obejmujących kompleksowe wsparcie w zakresie cyberbezpieczeństwa skoncentrowane na praktycznych aspektach obrony przed cyberatakami i dezinformacją, adekwatne do grupy docelowej **– Piotr Moroch, Kierownik Centrum Poradnictwa Zawodowego, Wojewódzki Urząd Pracy w Rzeszowie**

11:30–12:00 |Przerwa kawowa + ekspozycje w strefie partnerów,

II PANEL:

12:00–13:15

RODO + NIS2 + DORA + AI Act - zintegrowane zarządzanie bezpieczeństwem organizacji

- **Prowadzący Panel - Andrzej Zieliński Zastępca Dyrektora w Departamencie Kontroli i Naruszeń w UODO.**

- Po drugiej stronie lustra - Teoria a praktyka AI Act, RODO i SZBI na uczelni: jak ocenić ryzyko systemu AI, zanim zrobi to regulator **– Beata Mroczek – ekspert ds. bezpieczeństwa informacji**

zakres tematyczny: nakładanie się systemów normatywnych; Nowe kompetencje i status prawny IOD w dobie sztucznej inteligencji; Architektura rygorów audytowych.

paneliści: Radca prawny – partner zarządzający Kancelarii AXELO, Przedstawiciel Departamentu Prawnego MNiSW, Dyrektor Wydziału Bezpieczeństwa Podkarpackiego Urzędu Wojewódzkiego, Inspektor Ochrony Danych (IOD).

zakres tematyczny : nakładanie się systemów normatywnych; Nowe kompetencje i status prawny IOD w dobie sztucznej inteligencji; architektura rygorów audytowych.

III PANEL:

13:15–14:15

Ubezpieczenia od następstw incydentów jako element zarządzania ciągłością działania

paneliści: Radosław OSTROWSKI, Damian CHUDZIK, Katarzyna WOROSZ, Marek ŻOŁDAK - przedstawiciele firm brokerskich, przedstawiciele firm ubezpieczeniowych, eksperci ds. likwidacji szkód cybernetycznych.

zakres tematyczny :

- konstrukcja polis cybernetycznych dla podmiotów sektora publicznego,
- kryteria due diligence wymagane przez ubezpieczyciel,
- szacowanie strat po cyberataku;

14:15–15:00 | Przerwa obiadowa

IV PANEL:

15:00–16:30

Cyberwojna, dezinformacja i bezpieczeństwo państwa

paneliści: przedstawiciel Agencji Bezpieczeństwa Wewnętrznego (ABW), Ekspert CSIRT GOV, RCB, **kom. Damian Szela - p.o. Naczelnik Wydziału Wywiadu Kryminalnego Zarządu w Rzeszowie przedstawiciel Centralnego Biura Zwalczania Cyberprzestępczości (CBZC)**, eksperci z Pracowni Kryminalistyki i Zakładu Bezpieczeństwa Wewnętrznego UR.

zakres tematyczny :

- Ataki sponsorowane przez obce państwa; Anatomia kampanii phishingowych i socjotechnicznych ukierunkowanych na kadrę akademicką,

  - Zwalczanie technologii deepfake i dezinformacji - budowanie obrony przed nowoczesnymi oszustwami opartymi na manipulacji psychologicznej i zaawansowanej sztucznej inteligencji **- kmdr por. dr inż. Adam Stojałowski - Kierownik Zakładu Systemów Informacyjnych, Akademia Marynarki Wojennej**

  - Dlaczego phishing pozostaje jednym z najskuteczniejszych wektorów ataku, w jaki sposób współczesne metody uwierzytelniania mogą ograniczać jego skuteczność oraz jak organizacje – w tym uczelnie – mogą budować zabezpieczenia, które nie opierają bezpieczeństwa wyłącznie na czujności użytkownika? - **Marcin Szary, CEO Secfense - ekspert w dziedzinie cyberbezpieczeństwa, tożsamości cyfrowej i kontroli dostępu** –

16:30–17:00| Podsumowanie dnia

DZIEŃ 2 – WARSZTATY - PRAKTYKA, INCYDENTY,

Miejsce obrad: Aula „Kula"

9:00–09:45

SESJA WPROWADZAJĄCA

Największe cyberzagrożenia dla Polski i sektora akademickiego w 2026 roku

prelegenci: Analitycy zagrożeń CERT Polska oraz NASK, Inspektorzy Ochrony Danych uczelni zrzeszonych w KRAUM.

- Największe cyberzagrożenia dla Polski i sektora akademickiego w 2026 roku **- Michał Dondajewski - starszy specjalista ds. rozwoju współpracy CSIRT, CERT Polska / CSIRT NASK**

09:45–10:30

BLOK PRAKTYCZNY

zakres tematyczny :

- Jak wdrożyć wymagania NIS2 w organizacji publicznej. Krok po kroku. Zarządzanie kryzysowe, reputacja i komunikacja po incydencie

prelegenci: Administrator Systemów Informatycznych (ASI UR), specjalista ds. SZBI, Konsultant Kancelarii Compliance, eksperci ds. komunikacji w sytuacjach kryzysowych, rzecznik prasowy.

11:15–11:45 | Przerwa kawowa

11:45–13:15 | SESJE WARSZTATOWE

Propozycje:

Warsztat 1: Audyt gotowości operacyjnej do wymagań NIS2 i KRI krok po kroku.
Scenariusz: Mapowanie aktywów, analiza luk i minimalizowanie ryzyka.

Warsztat 2: AI Act w praktyce akademickiej - bezpieczeństwo i legalność systemów sztucznej inteligencji.
Scenariusz: Klasyfikacja systemów wysokiego ryzyka i wymogi techniczne.

prowadzący: **dr hab. Roman Uliasz prof. UR, dr inż. Przemysław Pardel**

13:15–14:15 | Przerwa obiadowa

14:15–15:00

SESJA ZAMYKAJĄCA:

Cyberbezpieczeństwo - czego jeszcze nie widzimy na horyzoncie technologicznym?

prelegenci: Kierownik UCI UR, Pełnomocnik ds. Cyberbezpieczeństwa, ASI UR

15:00–15:30

Podsumowanie i zakończenie konferencji:

- Przedstawienie rekomendacji pokonferencyjnych w zakresie budowania cyberodporności uczelni wyższych i podmiotów ważnych,
- Wręczenie certyfikatów uczestnictwa.