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,

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

Miejsce obrad: „Aula Kula” bud A0, ul. Pigonia 1

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

09:00–09:30
Uroczyste otwarcie konferencji i wystąpienia zaproszonych gości
Otwarcie konferencji i powitanie gości - Rektor Uniwersytetu Rzeszowskiego
prof. dr hab. n. med. Adam Reich

Wystąpienia zaproszonych gości honorowych i przedstawicieli władz

I PANEL: <u>NIS2 zmienia zasady gry - nowa odpowiedzialność uczelni, administracji i biznesu - podmiotów kluczowych i ważnych</u>

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.

09:30–10:15

- „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.**

10:15–11:00

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

11:00–11:30

- 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**.

11:30–12:00 | Przerwa kawowa

II PANEL: <u>RODO + NIS2 + DORA + AI Act + zintegrowane zarządzanie bezpieczeństwem organizacji</u>

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

- **Prowadzący Panel - Andrzej Zieliński Zastępca Dyrektora w Departamencie Kontroli i Naruszeń w UODO.**
- paneliści: Radca prawny – partner zarządzający Kancelarii AXELO, Przedstawiciel Departamentu Prawnego MNiSW, Dyrektor Wydziału Bezpieczeństwa Podkarpackiego Urzędu Wojewódzkiego, Inspektor Ochrony Danych (IOD).

12:00–13:15

- 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 – prawnik, ekspertka w zakresie ochrony danych osobowych, bezpieczeństwa informacji, cyberbezpieczeństwa, compliance.**

III PANEL: <u>Ubezpieczenia od następstw incydentów jako element zarządzania ciągłością działania</u>

zakres tematyczny :
konstrukcja polis cybernetycznych dla podmiotów sektora publicznego, kryteria krok po kroku wymagane przez ubezpieczyciela, szacowanie strat po cyberataku.

13:15–14:15

- paneliści: **Radosław Ostrowski, Damian Chudzik, Katarzyna Worosz, Marek Żołdak** - przedstawiciele firm brokerskich, przedstawiciele firm ubezpieczeniowych, eksperci ds. likwidacji szkód cybernetycznych.

14:15–15:00 | Przerwa obiadowa

IV PANEL: <u>Cyberwojna, dezinformacja i bezpieczeństwo państwa</u>

zakres tematyczny :
ataki sponsorowane przez obce państwa; anatomia kampanii phishingowych i socjotechnicznych ukierunkowanych na kadrę akademicką.

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

15:00–15:45

- 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.**

15:45–16:30

- Prezentacja 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.**

16:30–16:45| Podsumowanie obrad.

DZIEŃ 2 – WARSZTATY - PRAKTYKA, INCYDENTY

Miejsce obrad: Aula „Kula”

V PANEL: <u>Cyberzagrożenia, incydenty, zarządzanie kryzysowe,</u>

9:00–09:45

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

VI PANEL: BLOK PRAKTYCZNY

zakres tematyczny :
jak wdrożyć wymagania NIS2 w organizacji publicznej krok po kroku. Zarządzanie kryzysowe, reputacja i komunikacja po incydencie

09:45–10:30

- paneliści: Pełnomocnik ds. cyberbezpieczeństwa UR, Kierownik Uniwersyteckiego Centrum Informatyzacji UR, Administrator Systemów Informatycznych UR, Koordynator 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

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

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.

13:15–14:15 | Przerwa obiadowa

14:15–15:30 | SESJA ZAMYKAJĄCA: <u>Cyberbezpieczeństwo - czego jeszcze nie widzimy na horyzoncie technologicznym?</u>

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