Program III Międzynarodowej Konferencji Naukowej
„Wielowymiarowość cyberbezpieczeństwa. Nowe wymiary przestępczości cyfrowej: prawo, technologia, społeczeństwo”
16-17 kwietnia 2026 r.

Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej
Ul. Jutrzenki 135
02-231 Warszawa

16 kwietnia 2026 r.

13.00 – 14.00 REJESTRACJA UCZESTNIKÓW

14.00 – POWITANIE PRZEZ DR JUSTYNĘ ŻYLIŃSKĄ, Rektor Uczelni

14:10 – WYKŁAD INAUGURACYJNY,
DR KRZYSZTOF GAWKOWSKI,
Wiceprezes Rady Ministrów, Minister Cyfryzacji

14.30 – 19.00 - PANEL PIERWSZY: SYSTEM ORGANIZACYJNO-PRAWNY WOBEC CYBERZAGROŻEŃ – WYZWANIA I ROZWIĄZANIA
PRZERWY KAWOWE: 15.30 – 15.45 oraz 17.30 – 17.45

Systemy prawno-organizacyjne nie nadążają za dynamicznym rozwojem technologii. Znaczna część przestępstw cyfrowych ma charakter transgraniczny, co rodzi trudności w zakresie ustalania jurysdykcji, harmonizacji regulacji prawnych oraz skutecznego ścigania sprawców. Jednocześnie rozwój cyfrowych dokumentów i elektronicznego obiegu informacji stwarza nowe pola działania dla cyberprzestępców, którzy coraz częściej atakują zarówno systemy informatyczne, jak i tradycyjne nośniki danych. Zjawisko to obejmuje m.in. fałszowanie dokumentów elektronicznych, kradzież tożsamości, manipulację danymi oraz podszywanie się pod uprawnione osoby w celu uzyskania dostępu do wrażliwych informacji.
W konsekwencji konieczne jest tworzenie i aktualizowanie regulacji – zarówno na poziomie krajowym, jak i międzynarodowym – które będą uwzględniać specyfikę cyberprzestrzeni, ochronę praw człowieka i prywatności, a także potrzebę ścisłej współpracy między państwami, organizacjami międzynarodowymi oraz sektorem prywatnym.

19.30 – UROCZYSTA KOLACJA

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

17 kwietnia 2026 r.

9.00 – 13:00 PANEL DRUGI: TECHNOLOGICZNY WYMIAR CYBERPRZESTĘPCZOŚCI

PRZERWA KAWOWA: 10.30 – 10.45

Nowoczesne technologie pełnią dziś podwójną rolę w obszarze cyberbezpieczeństwa – z jednej strony są wykorzystywane do popełniania przestępstw, z drugiej stanowią kluczowe narzędzia ich wykrywania i zwalczania.

W ramach panelu omówione zostaną kluczowe aspekty technologiczne cyberprzestępczości, w tym metody zabezpieczania systemów informatycznych, zastosowania kryptografii, rozwiązania typu zero trust oraz wykorzystanie sztucznej inteligencji i uczenia maszynowego do wykrywania zagrożeń.

Szczególna uwaga poświęcona zostanie ocenie skuteczności nowoczesnych narzędzi analitycznych i predykcyjnych oraz identyfikacja nowych i narastających ryzyk, takich jak deepfake, botnety, exploit kits czy dark web, które mogą prowadzić do manipulacji danymi, dezinformacji oraz naruszeń bezpieczeństwa cyfrowych dokumentów i systemów informatycznych.

13.00 – OBIAD

14.00 – 15.30 PANEL TRZECI: SPOŁECZNY WYMIAR CYBERBEZPIECZEŃSTWA. MOWA NIENAWIŚCI

PRZERWA KAWOWA: 15.30 – 15.45

Internet stał się przestrzenią zarówno otwartego dialogu, jak i narastającej mowy nienawiści, która ma poważne konsekwencje społeczne, psychologiczne i prawne. Podczas panelu omówiona zostanie skala tego zjawiska w sieci, dostępne mechanizmy prawne i technologiczne służące jego ograniczaniu oraz skuteczne sposoby przeciwdziałania. Szczególna uwaga zostanie poświęcona roli platform internetowych, mediów oraz odpowiedzialności użytkowników w tworzeniu bezpiecznej i odpowiedzialnej przestrzeni *online.* Dyskusja skupi się na praktycznych rozwiązaniach, dobrych praktykach i działaniach, które mogą pomóc ograniczyć hejt w sieci.

Panel osadzony będzie w szerszym kontekście cyberbezpieczeństwa, które nie jest tylko kwestią technologii i regulacji, ale przede wszystkim świadomości, edukacji oraz odpowiedzialności

użytkowników. Eksperci omówią wpływ cyberzagrożeń na społeczeństwo, w tym problem dezinformacji, ochrony prywatności oraz cyfrowego wykluczenia.

15.45 – 18:00 PANEL CZWARTY: WSPÓŁPRACA MIĘDZYNARODOWA W OBSZARZE CYBERBEZPIECZEŃSTWA -

W dobie dynamicznej globalnej cyfryzacji i rosnącej zależności od systemów informatycznych, cyberzagrożenia stają się coraz bardziej złożone i transgraniczne. Ataki na infrastrukturę krytyczną, kampanie dezinformacyjne, wycieki danych czy działalność cyberprzestępcza nie ograniczają się do granic państw, co wymusza nową jakość współpracy międzynarodowej. W konsekwencji państwa, organizacje i instytucje muszą zmierzyć się z wyzwaniami prawnymi, technicznymi oraz operacyjnymi, które wymagają skoordynowanych działań oraz spójnych ram regulacyjnych.

Panel poświęcony będzie międzynarodowej współpracy w obszarze cyberbezpieczeństwa, obowiązującym regulacjom oraz mechanizmom reagowania na transgraniczne incydenty cybernetyczne. Eksperci omówią kwestie suwerenności cyfrowej, odpowiedzialności państw i podmiotów prywatnych oraz skuteczności obecnych ram prawnych. Dyskusja skoncentruje się na praktycznych rozwiązaniach oraz kierunkach rozwoju polityki cyberbezpieczeństwa w wymiarze międzynarodowym.