

### Zadanie

*„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”  
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa  
Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625*

# Cyberzagrożenia a rozwój kompetencji cyfrowych

Prelegenci:

dr hab. Aleksandra Monarcha-Matlak, prof. US,  
dr Dominika Skoczylas  
Wydział Prawa i Administracji, Uniwersytet  
Szczeciński



**UKSW**  
UNIwersytet Kardynała  
STEFANA WYSZYŃSKIEGO  
W WARSZAWIE

**CLTC** Centrum Liderów  
Transformacji Cyfrowej



# Cyberzagrożenia a rozwój kompetencji cyfrowych

ROZWÓJ CYFRYZACJI I SIECI POŁĄCZEŃ  
= ZWIĘKSZENIE RYZYKA CYBERZAGROŻEŃ

**KONIECZNOŚĆ ROZWOJU KOMPETENCJI CYFROWYCH**

# Cyberzagrożenia a rozwój kompetencji cyfrowych

## CYBERZAGROŻENIE

- wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób\*

*\* (art. 2 pkt 8 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylecia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)*

# Cyberzagrożenia a rozwój kompetencji cyfrowych

## Aspekt podmiotowy:

- ochrona przed cyberzagrożeniami wszystkich członków społeczeństwa informacyjnego

## CEL: określenie:

- 1) zasad polityki cyberbezpieczeństwa w organizacji
- 2) zasad cyberhigieny i rozwoju umiejętności i kompetencji cyfrowych użytkowników sieci

# Cyberzagrożenia a rozwój kompetencji cyfrowych

## **Aspekt przedmiotowy:**

- zapewnienie bezpieczeństwa sieci, systemów teleinformatycznych, sprzętu, oprogramowania
- zwiększenie nakładów finansowych w zakresie wykorzystywania nowych technologii w procesach zarządzania w organizacji

# Cyberzagrożenia a rozwój kompetencji cyfrowych

## Rodzaje cyberzagrożeń:

- naruszenia w zakresie: przetwarzania danych osobowych, praw autorskich i praw pokrewnych, stabilnego działania systemów i sieci teleinformatycznych, przestępstwa komputerowe
- cyberprzemoc: szkodliwe/ nielegalne treści, naruszenie prywatności, cyberstalking, fomo, sieciorholizm itp.

# Cyberzagrożenia a rozwój kompetencji cyfrowych

## Rodzaje cyberzagrożeń:

- związane z brakiem kompetencji cyfrowych: nieświadomość użytkowników w zakresie istnienia potencjalnych cyberzagrożeń, nieumiejętne korzystanie z e-zasobów, podatność na cyberzagrożenia

# Cyberzagrożenia a rozwój kompetencji cyfrowych

## ATAKI NA ZASOBY SIECIOWE

**Phising**

**Sniffing**

**Spoffing**

**Denial of service**

**Hakerstwo**

**Spyware**

**Eksploit**

**Malware**

### **Źródła cyberzagrożeń:**

strony internetowe (platformy społecznościowe, instytucji publicznych i prywatnych)

### **Charakter cyberzagrożeń:**

nieprzewidywalny i nagły



# Cyberzagrożenia a rozwój kompetencji cyfrowych

## SKUTKI CYBERATAKÓW:

Ataki na sieci teleinformatyczne:

- upublicznienie danych uczelni lub pracowników/studentów
- nieuprawniona modyfikacja informacji (naruszenie zasady prawidłowego i rzetelnego i bezpiecznego przetwarzania danych osobowych)
- blokada świadczenia usług sieciowych (awarie, zakłócenia o długotrwałym bądź krótkotrwałym charakterze)

## NEGATYWNE SKUTKI: UCZELNIA/PRACOWNICY UCZELNI/STUDENCI

# Cyberzagrożenia a rozwój kompetencji cyfrowych

**Determinanty cyberbezpieczeństwa w szkołach wyższych:**

- 1. Aspekty prawne: kompleksowe rozwiązania z zakresu cyberbezpieczeństwa.**
- 2. Działania profilaktyczne: szkolenia, warsztaty w obszarze potencjalnych zagrożeń cyberbezpieczeństwa (świadomość cyberzagrożeń).**
- 3. Zgłaszanie nieprawidłowości, właściwa reakcja związana z klasyfikacją i obsługą incydentów (polityka cyberbezpieczeństwa).**

# Cyberzagrożenia a rozwój kompetencji cyfrowych

**Determinanty cyberbezpieczeństwa w szkołach wyższych:**

- 4. Rozwój kompetencji cyfrowych.**
- 5. Identyfikacja cyberzagrożenia - procedura i działania następcze.**
- 6. Współdziałanie naukowców i ekspertów w kwestii poprawy warunków cyberbezpieczeństwa w szkołach wyższych.**

# Cyberzagrożenia a rozwój kompetencji cyfrowych

## Kompetencje cyfrowe w zakresie:

- wykorzystywania technologii informacyjno-komunikacyjnych i obsługi narzędzi teleinformatycznych (sprzęt, oprogramowanie);
- znajomości procedur: identyfikacji, klasyfikacji i obsługi w przypadku wystąpienia zagrożenia;

# Cyberzagrożenia a rozwój kompetencji cyfrowych

## Kompetencje cyfrowe w zakresie:

- świadczenia usług edukacyjnych i stosowanie nowych form kształcenia na odległość (nauczanie zdalne, e-learning, nauczanie hybrydowe), a także umiejętnego korzystania z nich.