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

Cyberbezpieczeństwo a kompetencje cyfrowe

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

Ministerstwo Edukacji i Nauki

UKSW Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

CLTC Centrum Liderów Transformacji Cyfrowej

Cyberbezpieczeństwo a kompetencje cyfrowe

CYBERBEZPIECZEŃSTWO

- odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy*

**(art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa)*

Cyberbezpieczeństwo a kompetencje cyfrowe

CYBERBEZPIECZEŃSTWO

- działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami*

**(art. 2 pkt 1 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 uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)*

Cyberbezpieczeństwo a kompetencje cyfrowe

Warunki cyberbezpieczeństwa:	1. dostępność danych = cyberbezpieczeństwo danych	2 wiedza i umiejętności użytkowników; rozwój kompetencji cyfrowych
3. inwestycje w sektorze cyberbezpieczeństwa, wykorzystanie sztucznej inteligencji	4. wskazanie podmiotów zaangażowanych (określenie zadań i kompetencji)	5. legislacja (nowe technologie a warunki prawne)

Cyberbezpieczeństwo a kompetencje cyfrowe

Aspekty prawne

Wzrost kompetencji cyfrowych w zakresie struktury źródeł wiedzy o cyberbezpieczeństwie, w następujących zagadnieniach:

- zastosowanie środków komunikacji elektronicznej i technologii informacyjno-komunikacyjnych
- cyberprzestrzeń, cyberbezpieczeństwo, cyberzagrożenia
- informatyzacja
- cybernetyka i cyfryzacja

Cyberbezpieczeństwo a kompetencje cyfrowe

Aspekty prawne:

Wzrost kompetencji cyfrowych w zakresie struktury źródeł wiedzy o cyberbezpieczeństwie, w następujących zagadnieniach:

- świadczenie usług drogą elektroniczną
- ochrona danych osobowych
- e-administracja
- cyberhigiena

Cyberbezpieczeństwo a kompetencje cyfrowe

Struktura źródeł wiedzy o cyberbezpieczeństwie ma różnorodny i interdyscyplinarny charakter.

Kompetencje cyfrowe w zakresie cyberbezpieczeństwa powinny zatem uwzględniać zasięg (krajowy, unijny, międzynarodowy), **pochodzenie** (wewnętrzne bądź zewnętrzne) i rodzaj (dyrektywa, ustawa, rozporządzenie, strategii) **źródeł wiedzy.**

Cyberbezpieczeństwo a kompetencje cyfrowe

Kompetencje cyfrowe a struktura źródeł wiedzy o cyberbezpieczeństwie:

AKTY PRAWNE
(PRAWO KRAJOWE, PRAWO UE,
PRAWO MIĘDZYNARDOOWE)

ARTYKUŁY (CZASOPISMA)

ORZECZNICTWO

PUBLIKACJE ZWARTE
(MONOGRAFIE)

ŹRÓDŁA INTERNETOWE

MINISTERSTWO CYFRYZACJI

Cyberbezpieczeństwo a kompetencje cyfrowe

Znajomość struktury źródeł wiedzy o cyberbezpieczeństwie, tj.

1) powszechnie obowiązujących regulacji (prawa krajowego, prawa unijnego i prawa międzynarodowego);
2) fachowych i kompleksowych opracowań, pozwalających na analizę i interpretację aktualnych przepisów, opisujących terminologię związaną z cyberbezpieczeństwem, również w kontekście rozwoju kompetencji cyfrowych (problemy i wyzwania w zakresie cyberbezpieczeństwa, stanowiska doktryny);

Cyberbezpieczeństwo a kompetencje cyfrowe

Znajomość struktury źródeł wiedzy o cyberbezpieczeństwie, tj.

3) orzecznictwa;

4) rekomendacji, opinii, strategii działania określonych przez właściwe organy administracji publicznej i inne podmioty (spoza administracji publicznej).

Cyberbezpieczeństwo a kompetencje cyfrowe

Kompetencje cyfrowe powinny pozwolić na prawidłową klasyfikację źródeł wiedzy w aspekcie przedmiotu ochrony przed cyberzagrożeniami (informacji, usług, sieci i systemów teleinformatycznych).

WAŻNE: Cyberbezpieczeństwo i kompetencje cyfrowe: znajomość rozwiązań prawnych z zakresu:

prawa administracyjnego, prawa komunikacji elektronicznej, prawa nowych technologii, prawa cywilnego, prawa karnego, prawa gospodarczego publicznego