

SYLABUS ECCC

Obszar: Kompetencje Cyfrowe - DIGCOMP (Digital Competences)

Moduł: DC M4 Bezpieczeństwo

Poziom: Zaawansowany (C)

W module DC M4 Bezpieczeństwo podstawowe kompetencje są weryfikowane w następujących obszarach tematycznych:

1. **Narzędzia służące ochronie.**
Ochrona własnych urządzeń, świadomość zagrożeń i niebezpieczeństw online, znajomość ustawień bezpieczeństwa.
2. **Ochrona danych osobowych.**
Rozumienie warunków świadczenia usług, aktywna ochrona danych osobowych, szanowanie danych osobowych innych osób, ochrona przed oszustwami, zagrożeniami i przemocą online.
3. **Ochrona zdrowia fizycznego i psychicznego przed zagrożeniami wynikającymi z korzystania z technologii informacyjno-komunikacyjnych (TIK).**
Unikanie zagrożeń zdrowia wynikających z korzystania z TIK – w wymiarze zdrowia zarówno fizycznego, jak i psychicznego.
4. **Ochrona środowiska.**
Świadomość wpływu TIK na środowisko naturalne.

Weryfikacja kompetencji jest realizowana w następujących grupach:

1. Wiedza (W).
2. Umiejętności (U).
3. Postawa (P).

Zakres weryfikowany przez egzamin ECCC modułu DC M2 (poziom C)

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
C_CK1	(4.1) Zdobyć umiejętności zachowania się i dbania o bezpieczeństwo urządzeń.	C_EK1	Postrzega zagrożenia związane z korzystaniem z publicznych sieci dostępowych, VPN.			✓
		C_EK2	Zna typy ataków, których celem są urządzenia elektroniczne oraz znane sposoby dbania o ich bezpieczeństwo.	✓		
		C_EK3	Potrafi monitorować stan połączenia urządzenia cyfrowego z siecią i odpowiednio reagować na zagrożenie.		✓	
		C_EK4	Wie, czym jest szyfrowanie danych.	✓		
		C_EK5	Potrafi kompresować/szyfrować dane z wykorzystaniem złożonych haseł, w tym różne lokalizacje przechowywania danych.		✓	
C_CK2	(4.2) Przyswojenie szerokiej wiedzy na	C_EK6	Posiada dogłębną wiedzę z tematyki danych osobowych i prywatności w online.	✓		

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
	temat spraw związanych z prywatnością w sieci, gromadzenia, wykorzystywania i udostępniania danych.	C_EK7	Potrafi podnosić poziom ochrony swojej prywatności poprzez zmianę domyślnych ustawień prywatności online.		✓	
		C_EK8	Potrafi adekwatnie do potrzeb modyfikować prawa dostępu dla udostępnionych danych.		✓	
C_CK3	(4.3) Przyswojenie wiedzy na temat uzależnień od TIK i unikania zagrożeń dla zdrowia.	C_EK9	Wie, czym jest uzależnienie od TIK.	✓		
		C_EK10	Potrafi rozwiązywać problemy związane z uzależnieniem od TIK.		✓	
		C_EK11	Potrafi dostosować stanowisko pracy, aby spełniało podstawowe zasady ergonomii i higieny pracy.		✓	
C_CK4	(4.4) Zdobyć wiedzę na temat wpływu TIK na życie codzienne, środowisko naturalne.	C_EK12	Wie, jak obliczyć i obniżyć koszty użytkowania TIK.	✓		
		C_EK13	Ma wiedzę, jak dobrać urządzenia zużywające mniej energii, chroniące środowisko.	✓		

Oznaczenia podane w nawiasach przy celach kształcenia np.: (1.1) stanowią odniesienie do nazwy kompetencji podanej w Załączniku nr 2: *Standard wymagań dla kompetencji cyfrowych realizowanych w ramach projektów w PI 10(iii) wytycznych w zakresie realizacji przedsięwzięć z udziałem środków Europejskiego Funduszu Społecznego w obszarze edukacji na lata 2014-2020*, opublikowanych 2 czerwca 2015 roku przez Ministra Infrastruktury i Rozwoju (syg. MIIR 2014-2020/19(01)/06/2015).

Umiejętności praktyczne, weryfikowane przez egzamin ECCC DC M4, dotyczą:

- Stanowiska komputerowego klasy PC/laptop wyposażonego w interfejs sieciowy WiFi oraz z dostępem do Internetu o przepustowości minimum 2 Mb.
- Systemu operacyjnego Windows (wersja 7 lub nowszy - nadal wspierany przez producenta) lub Linux (jądro 3.x lub nowsze) z kontem z uprawnieniami administratora dostępnym dla studenta.
- Programów: Acrobat Reader, CCleaner, Eraser, Wireshark, SoftPerfect Network Scanner, GIMP, OpenVPN, 7z.
- Programu antywirusowego pracującego w trybie "monitor", posiadającego funkcję heurystyka.
- Pakietu biurowego Libre Office.
- Przeglądarki internetowej pozwalająca na pracę w trybie prywatnym i pozwalająca na instalację dodatków, takich jak: WOT, Adblock, Ghostery oraz obsługującej wtyczki: Flash, Java.
- Programu typu firewall (akceptowalny jest również domyślny systemowy).
- Programu szyfrujący katalogi i pliki (np. opartego o bibliotekę EncFS).