

SYLABUS ECCC

Obszar: **Kompetencje Cyfrowe – DigComp 2.2**

Moduł: **DC2.2 M4 Bezpieczeństwo**

Poziom: **Zaawansowany (C5)** - oprócz wspierania innych.

Moduł **DC2.2 M4 Bezpieczeństwo** poziom C5 obejmuje 5 poziom kompetencji ramy DigComp 2.2 w Obszarze kompetencji 4: Bezpieczeństwo.

Podstawowe kompetencje są weryfikowane w następujących obszarach tematycznych:

1. Narzędzia służące ochronie.

Ochrona urządzeń i treści cyfrowych oraz rozumienie ryzyka i zagrożeń w środowisku cyfrowym. Wiedza dotycząca środków bezpieczeństwa i ochrony oraz należyte uwzględnienie wiarygodności i prywatności.

2. Ochrona danych osobowych i prywatności.

Ochrona danych osobowych i prywatności w środowisku cyfrowym. Rozumienie, jak używać i udostępniać dane osobowe zapewniając sobie i innym ochronę przed szkodą. Rozumienie, że w usługach cyfrowych stosowana jest „Polityka prywatności”, aby informować jak dane osobowe są wykorzystywane.

3. Ochrona zdrowia i dobrostanu.

Unikanie zagrożeń zdrowotnych i zagrożeń dla dobrostanu fizycznego oraz psychicznego podczas korzystania z technologii cyfrowych. Umiejętność chronienia siebie i innych przed ewentualnymi zagrożeniami w środowisku cyfrowym (np. wirtualnym nękanie). Świadomość znaczenia technologii cyfrowych dla dobrostanu społecznego i integracji społecznej.

4. Ochrona środowiska.

Świadomość wpływu na środowisko technologii cyfrowych i ich wykorzystywania.

Weryfikacja kompetencji jest realizowana w następujących grupach:

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

Zakres weryfikowany przez egzamin ECCC modułu DC2.2 M4 (poziom C5)

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA				
			W	U	P	
C5_CK1	Zdobycie zaawansowanych umiejętności ochrony urządzeń i treści cyfrowych.	C5_EK1	Ma świadomość konieczności ochrony urządzeń i treści cyfrowych.	✓		✓
		C5_EK2	Potrafi zastosować różne sposoby ochrony swoich urządzeń i treści cyfrowych.		✓	
		C5_EK3	Potrafi rozpoznać różnorodne ryzyka i zagrożenia w środowiskach cyfrowych (np. typy ataków).		✓	
		C5_EK4	Zna i potrafi zastosować środki bezpieczeństwa i ochrony.	✓	✓	
		C5_EK5	Potrafi zaangażować różne sposoby należytego uwzględniania wiarygodności i prywatności.		✓	✓

C5_CK1	Zdobycie zaawansowanych umiejętności ochrony urządzeń i treści cyfrowych.	Przykłady wg DigComp 2.2	Chroni konto na serwisie społecznościowym używając różnych metod, (np.: silne hasło, kontrola ostatnich logowań) i pokazać w jaki sposób to robić.		✓	✓	
			Potrafi wykryć ryzyka, takie jak otrzymywanie tweet'ów i wiadomości od followersów z fałszywych profili lub próby wyłudzenia informacji.	✓			
			Stosuje odpowiednie środki aby uniknąć próby wyłudzenia informacji (np.: kontrolować ustawienia prywatności).		✓	✓	
			Pomaga innym w wykrywaniu ryzyka i zagrożeń podczas użytkowania serwisu społecznościowego, cyfrowej platformy na ich komputerach (np.: kontrolowanie kto ma dostęp do plików).			✓	
			Chroni informacje i dane oraz treści na platformie cyfrowej swojej szkoły/firmy (np.: silne hasło, kontrola ostatnich logowań).		✓		
			Potrafi wykryć ryzyka i zagrożenia związane z udostępnianiem platformy cyfrowej oraz zastosować środki zapobiegawcze (np.: jak sprawdzać załączniki pod kątem obecności wirusów przed zainstalowaniem).	✓	✓		
			Postrzega zagrożenia związane z korzystaniem z publicznych sieci dostępowych, VPN.			✓	
			Zna typy ataków, których celem są urządzenia elektroniczne oraz znane sposoby dbania o ich bezpieczeństwo.	✓			
			Potrafi monitorować stan połączenia urządzenia cyfrowego z siecią i odpowiednio reagować na zagrożenie.		✓		
			Wie, czym jest szyfrowanie danych.	✓			
C5_CK2	Przyswojenie szerokiej wiedzy na temat ochrony danych osobowych i prywatności w środowisku cyfrowym, gromadzenia, wykorzystywania i udostępniania danych.	Przykłady wg DigComp 2.2	Kompresuje/szyfruje dane z wykorzystaniem złożonych hasel, w tym różne lokalizacje przechowywania danych.		✓		
			C5_EK6	Posiada dogłębną wiedzę na temat ochrony danych osobowych i prywatności w środowisku cyfrowym.	✓		
			C5_EK7	Potrafi zastosować różne sposoby ochrony swoich danych osobowych i prywatności w środowiskach cyfrowych.		✓	
			C5_EK8	Potrafi zastosować różne sposoby użytkowania i udostępniania informacji umożliwiających identyfikację osoby, jednocześnie chroniąc siebie i innych przez zagrożeniami.		✓	
			C5_EK9	Potrafi wyjaśnić zasady polityki prywatności dotyczące sposobów przetwarzania danych osobowych w usługach cyfrowych.		✓	
			Potrafi podnosić poziom ochrony swojej prywatności poprzez zmianę domyślnych ustawień prywatności online.		✓	✓	
			Potrafi adekwatnie do potrzeb modyfikować prawa dostępu dla udostępnionych danych.		✓	✓	

C5_CK3	Przyswojenie szerokiej wiedzy na temat ochrony zdrowia i dobrostanu wynikających z korzystania z technologii cyfrowych.	C5_EK10	Ma świadomość znaczenia technologii cyfrowych dla dobrostanu społecznego i integracji społecznej.	✓			
		C5_EK11	Zna i potrafi zaprezentować różne sposoby unikania ryzyka i zagrożenia zdrowia w odniesieniu do dobrostanu fizycznego i psychicznego podczas użytkowania technologii cyfrowych.	✓	✓		
		C5_EK12	Zna i potrafi zastosować różne sposoby ochrony siebie przed możliwymi zagrożeniami w środowiskach cyfrowych.	✓	✓		
		C5_EK13	Zna i potrafi zaprezentować różne technologie cyfrowe sprzyjające dobrostanowi społecznemu i włączeniu społecznemu.	✓	✓		
		Przykłady wg DigComp 2.2	Ma świadomość niekorzystnych dla zdrowia zagrożeń powodowanych uzależnieniem od technologii cyfrowych.				✓
Potrafi rozwiązywać problemy związane z uzależnieniem od technologii cyfrowych.	✓		✓				
Potrafi dostosować stanowisko pracy, aby spełniało podstawowe zasady ergonomii i higieny pracy.	✓		✓				
C5_CK4	Zdobycie zaawansowanych umiejętności związanych z ochroną środowiska wynikających z korzystania z technologii cyfrowych.	C5_EK14	Potrafi pokazać różnorodny wpływ na środowisko technologii cyfrowych i ich wykorzystywania.			✓	
		C5_EK15	Wie, jak zrównoważyć korzyści i skutki wynikające z korzystania z technologii cyfrowych.	✓			
		Przykłady wg DigComp 2.2	Ma wiedzę i potrafi dobierać energooszczędne urządzenia mając na względzie ochronę środowiska.	✓	✓		
			Ma świadomość jak ważne jest dbanie o środowisko naturalne.				✓

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/s.
- 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).