

SYLABUS ECCC

Obszar: **Kompetencje Cyfrowe – DigComp 2.2**

Moduł: **DC2.2 M4 Bezpieczeństwo**

Poziom: **Podstawowy (A2)** oraz samodzielnie i z odpowiednim wsparciem w razie potrzeb.

Moduł DC2.2 M4 Bezpieczeństwo poziom A2 obejmuje 2 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 A2):

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA			W	U	P
A2_CK1	(4.1) Zdobycie podstawowych umiejętności ochrony urządzeń i treści cyfrowych.	A2_EK1	Potrafi zidentyfikować proste sposoby ochrony swoich urządzeń i treści cyfrowych.		✓		
		A2_EK2	Potrafi rozróżnić proste ryzyka i zagrożenia w środowiskach cyfrowych.		✓		
		A2_EK3	Potrafi wybrać proste środki bezpieczeństwa i ochrony urządzeń i treści cyfrowych.		✓		
		A2_EK4	Potrafi zidentyfikować proste sposoby należytego uwzględniania wiarygodności i prywatności.		✓		
		A2_EK5	Zna zagrożenia, na jakie narażone jest urządzenie cyfrowe i potrafi się przed nimi zabezpieczyć.	✓			
		A2_EK6	Zna typy licencji oprogramowania.	✓			

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA			W	U	P
		A2_EK7	Wie, co to jest program antywirusowy i do czego służy	✓			
		A2_EK8	Potrafi zainstalować i skonfigurować program antywirusowy.		✓		
		A2_EK9	Potrafi skanować nośniki danych programem antywirusowym oraz podejmować decyzje w chwili wykrycia zagrożenia przez program antywirusowy		✓		
		A2_EK10	Wie, czym jest „mocne” hasło.	✓			
		A2_EK11	Zna zagrożenia wynikające z możliwości dostępu do urządzenia przez niepowołane osoby i potrafi zabezpieczyć urządzenie przed dostępem przez niepowołane osoby.	✓			
		Przykłady wg DigComp 2.2	Identyfikuje i stosuje różne sposoby ochrony urządzeń			✓	
			Stosuje właściwe „silne” hasła			✓	
A2_CK2	(4.2) Zdobycie podstawowych informacji na temat ochrony danych osobowych i prywatności w środowisku cyfrowym.	A2_EK12	Potrafi wybrać proste sposoby ochrony swoich danych osobowych i prywatności w środowiskach cyfrowych.		✓		
		A2_EK13	Potrafi zidentyfikować proste sposoby użytkowania i udostępniania informacji umożliwiające identyfikację osoby jednocześnie chroniąc siebie i innych przed zagrożeniami.		✓		
		A2_EK14	Potrafi zidentyfikować proste zasady polityki prywatności dotyczące sposobów przetwarzania danych osobowych w usługach cyfrowych.	✓			
		A2_EK15	Wie co to są krytyczne informacje osobowe, oraz ma świadomość, że nie wszystkie dane, swoje lub innych osób, można udostępniać w sieci.		✓		
		A2_EK16	Rozumie zagrożenia związane z próbą wyłudzenia danych osobowych podczas korzystania z Internetu.		✓		
		Przykłady wg DigComp 2.2	Chroni swoje dane osobowe i prywatność w sieci			✓	
			Nie udostępnia swoich danych w sieci	✓			
A2_CK3	(4.3) Przyswojenie wiedzy na temat ochrony zdrowia i dobrostanu wynikających z korzystania z technologii cyfrowych.	A2_EK17	Potrafi rozróżnić proste sposoby unikania ryzyka i zagrożenia zdrowia w odniesieniu do dobrostanu fizycznego i psychicznego podczas użytkowania technologii cyfrowych.		✓		
		A2_EK18	Potrafi wybrać proste sposoby ochrony siebie przed możliwymi zagrożeniami w środowiskach cyfrowych.		✓		
		A2_EK19	Potrafi zidentyfikować proste technologie cyfrowe sprzyjające dobrostanowi społecznemu i włączeniu		✓		

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
			społecznemu.			
		A2_EK20	Wie, czym jest cyberprzemoc i jak jej unikać.	✓		
		A2_EK21	Wie, że nowoczesne technologie cyfrowe mogą negatywnie wpływać na zdrowie fizyczne i psychiczne, jeżeli są używane niewłaściwie.			✓
		Przykłady wg DigComp 2.2	Unika ryzyka podczas pracy w Internecie		✓	
Chroni swoje zdrowie podczas pracy z urządzeniami TIK				✓		
A1_CK4	(4.4) Zdobycie podstawowych umiejętności związanych z ochroną środowiska wynikających z korzystania z technologii cyfrowych.	A2_EK22	Potrafi rozpoznać prosty wpływ na środowisko technologii cyfrowych i ich wykorzystywania.			✓
		A2_EK23	Jest świadomy wpływu technologii cyfrowych na środowisko naturalne oraz stara się go minimalizować poprzez właściwe stosowanie urządzeń cyfrowych.			✓
		A2_EK24	Wie jak i stara się oszczędzać energię elektryczną poprzez właściwe stosowanie urządzeń cyfrowych.			✓
		Przykłady wg DigComp 2.2	Chroni środowisko naturalne		✓	
			Oszczędza energię elektryczną		✓	

Umiejętności praktyczne, weryfikowane przez egzamin ECCC DC2.2 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.
- Programu antywirusowego pracującego w trybie "monitor", posiadającego funkcję heurystyka.
- Pakietu biurowego Libre Office.