

SYLABUS ECCC

Obszar: **Kompetencje Cyfrowe – DigComp 2.1**

Moduł: **DC2.1 M4 Bezpieczeństwo**

Poziom: **Podstawowy (A1)** ze wsparciem.

Moduł **DC2.1 M4 Bezpieczeństwo** poziom A1 obejmuje 1 poziom kompetencji ramy DigComp 2.1 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 DC2.1 M4 (poziom A1):

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
A1_CK1	(4.1) Zdobycie podstawowych umiejętności ochrony urządzeń i treści cyfrowych.	DC2.1_1	Potrafi zidentyfikować proste sposoby ochrony swoich urządzeń i treści cyfrowych.			
		DC2.1_2	Potrafi rozróżnić proste ryzyka i zagrożenia w środowiskach cyfrowych.			
		DC2.1_3	Potrafi wybrać proste środki bezpieczeństwa i ochrony urządzeń i treści cyfrowych.			
		DC2.1_4	Potrafi zidentyfikować proste sposoby należytego uwzględniania wiarygodności i prywatności.			
		A1_EK1	Zna zagrożenia, na jakie narażone jest urządzenie cyfrowe i potrafi się przed nimi zabezpieczyć.	✓		
		A1_EK2	Zna zagrożenia wynikające z możliwości dostępu do urządzenia przez niepowołane osoby i potrafi zabezpieczyć urządzenie przed dostępem przez niepowołane osoby.	✓		

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA			W	U	P
		A1_EK3	Zna typy licencji oprogramowania.	✓			
		A1_EK4	Wie, co to jest program antywirusowy i do czego służy.	✓			
		A1_EK5	Wie, czym jest „mocne” hasło.	✓			
		A1_EK6	Potrafi zainstalować i skonfigurować program antywirusowy.		✓		
		A1_EK7	Potrafi skanować nośniki danych programem antywirusowym oraz podejmować decyzje w chwili wykrycia zagrożenia przez program antywirusowy.		✓		
A1_CK2	(4.2) Zdobycie podstawowych informacji na temat ochrony danych osobowych i prywatności w środowisku cyfrowym.	DC2.1_5	Potrafi wybrać proste sposoby ochrony swoich danych osobowych i prywatności w środowiskach cyfrowych.				
		DC2.1_6	Potrafi zidentyfikować proste sposoby użytkowania i udostępniania informacji umożliwiające identyfikację osoby jednocześnie chroniąc siebie i innych przed zagrożeniami.				
		DC2.1_7	Potrafi zidentyfikować proste zasady polityki prywatności dotyczące sposobów przetwarzania danych osobowych w usługach cyfrowych.				
		A1_EK8	Wie, co to są krytyczne informacje osobowe, oraz ma świadomość, że nie wszystkie dane, swoje lub innych osób, można udostępniać w sieci.	✓			
		A1_EK9	Wie, o odpowiednim zachowaniu się w domenie cyfrowej.	✓			
		A1_EK10	Zna zagrożenia związane z próbą wyłudzenia danych osobowych podczas korzystania z Internetu.		✓		
A1_CK3	(4.3) Przyswojenie wiedzy na temat ochrony zdrowia i dobrostanu wynikających z korzystania z technologii cyfrowych.	DC2.1_8	Potrafi rozróżnić proste sposoby unikania ryzyka i zagrożenia zdrowia w odniesieniu do dobrostanu fizycznego i psychicznego podczas użytkowania technologii cyfrowych.				
		DC2.1_9	Potrafi wybrać proste sposoby ochrony siebie przed możliwymi zagrożeniami w środowiskach cyfrowych.				
		DC2.1_10	Potrafi zidentyfikować proste technologie cyfrowe sprzyjające dobrostanowi społecznemu i włączeniu społecznemu.				
		A1_EK10	Wie, że nowoczesne technologie cyfrowe mogą negatywnie wpływać na zdrowie fizyczne i psychiczne, jeżeli są używane niewłaściwie.	✓			
		A1_EK11	Wie, czym jest cyberprzemoc i jak jej unikać.	✓			
A1_CK4	(4.4) Zdobycie podstawowych umiejętności związanych z ochroną środowiska wynikających z korzystania z technologii cyfrowych.	DC2.1_11	Potrafi rozpoznać prosty wpływ na środowisko technologii cyfrowych i ich wykorzystywania.				
		A1_EK13	Jest świadomy wpływu technologii cyfrowych na środowisko naturalne oraz stara się go minimalizować poprzez właściwe stosowanie urządzeń cyfrowych.			✓	
		A1_EK14	Ma świadomość problemów środowiskowych związanych z korzystaniem z technologii cyfrowych. Stara się oszczędzać energię elektryczną poprzez właściwe stosowanie urządzeń cyfrowych.			✓	

Umiejętności praktyczne, weryfikowane przez egzamin ECCC DC2.1 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.