

SYLABUS ECCC

Obszar: **Kompetencje Cyfrowe – DigComp 2.2**

Moduł: **DC2.2 M4 Bezpieczeństwo**

Poziom: **Średniozaawansowany (B3)** - samodzielnie i rozwiązując proste problemy.

Moduł **DC2.2 M4 Bezpieczeństwo** poziom B3 obejmuje 3 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.**
Unikania 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 B3)

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA			W	U	P
B3_CK1	(4.1) Przystwojenie wiedzy na temat ochrony urządzeń i treści cyfrowych.	B3_EK1	Potrafi zidentyfikować dobrze zdefiniowane i rutynowe sposoby ochrony swoich urządzeń i treści cyfrowych.		✓		
		B3_EK2	Potrafi rozróżnić dobrze zdefiniowane i rutynowe ryzyka i zagrożenia w środowiskach cyfrowych.	✓			
		B3_EK3	Potrafi wybrać dobrze zdefiniowane i rutynowe środki bezpieczeństwa i ochrony.		✓		
		B3_EK4	Potrafi zidentyfikować dobrze zdefiniowane i rutynowe sposoby należytego uwzględniania wiarygodności i prywatności.		✓		
		B3_EK5	Zna zagrożenia wynikające z otwierania niepewnych stron internetowych i otwierania załączników poczty elektronicznej od nieznanymi nadawców oraz korzystania z publicznych urządzeń.	✓			

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
		B3_EK6	Potrafi obsługiwać przeglądarkę w trybie prywatnym oraz zarządzać historią przeglądanych stron.		✓	
		B3_EK7	Potrafi znaleźć, instalować i konfigurować dodatki do przeglądarki zwiększające bezpieczeństwo.		✓	
		B3_EK8	Potrafi rozpoznawać potencjalnie niebezpieczne strony i wiadomości poczty elektronicznej.	✓		
		B3_EK9	Wie, czym są podpisy elektroniczne i certyfikaty potwierdzające tożsamość.	✓		
		B3_EK10	Wie, jak zabezpieczyć w podstawowy sposób swoje urządzenie cyfrowe (<i>komputer, laptop, urządzenie mobilne</i>).	✓		
		Przykłady wg DigComp 2.2	W Internecie pracuje z rozsądkiem i rozwagą.			✓
Pracując w sieci używa podpisu elektronicznego.			✓			
B3_CK2	(4.2) Nabycie wiedzy o ochronie danych osobowych i prywatności w środowisku cyfrowym.	B3_EK11	Potrafi wyjaśnić dobrze zdefiniowane i rutynowe sposoby ochrony swoich danych osobowych i prywatności w środowiskach cyfrowych.			✓
		B3_EK12	Potrafi wyjaśnić dobrze zdefiniowane i rutynowe sposoby użytkowania i udostępniania informacji umożliwiających identyfikację osoby jednocześnie chroniąc siebie i innych przed zagrożeniami.			✓
		B3_EK13	Potrafi wskazać dobrze zdefiniowane i rutynowe zasady polityki prywatności dotyczące sposobów przetwarzania danych osobowych w usługach cyfrowych.	✓		
		B3_EK14	Wie, jak działają sieci VPN oraz potrafi tworzyć połączenia między urządzeniami.	✓		
		B3_EK15	Potrafi sprawdzić autentyczność stron internetowych, np. instytucji finansowych.		✓	
		B3_EK16	Wie, jak uchronić się przed próbą wykradania danych.	✓		
		B3_EK17	Ma świadomość braku anonimowości w sieci Internet.			✓
		B3_EK18	Zna aspekty prawne związane z udostępnianiem i przetwarzaniem danych osobowych, w tym typy oświadczeń o udostępnianie danych osobowych	✓		
		B3_EK19	Świadomie udostępnia dane osobowe w sieci			✓
		Przykłady wg DigComp 2.2	Chroni swoje dane osobowe w Internecie.		✓	
Konfiguruje połączenia VPN pomiędzy stanowiskami.			✓			

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
B3_CK3	(4.3) Zdobycie umiejętności ochrony zdrowia i dobrostanu wynikających z korzystania z technologii cyfrowych.	B3_EK20	Potrafi wyjaśnić dobrze zidentyfikowane i rutynowe sposoby unikania ryzyka i zagrożenia zdrowia w odniesieniu do dobrostanu fizycznego i psychicznego podczas użytkowania technologii cyfrowych.	✓		
		B3_EK21	Potrafi wybrać dobrze zdefiniowane i rutynowe sposoby ochrony siebie przed możliwymi zagrożeniami w środowiskach cyfrowych.		✓	
		B3_EK22	Potrafi wskazać dobrze zdefiniowane i rutynowe technologie cyfrowe sprzyjające dobrostanowi społecznemu i włączeniu społecznemu.		✓	
		B3_EK23	Wie, jak chronić się i reagować na cyberprzemoc	✓		
		B3_EK24	Rozumie, czym jest uzależnienie od technologii cyfrowych i jak rozpoznawać objawy.			✓
		B3_EK25	Zna zagrożenia związane z korzystaniem z urządzeń cyfrowych, zasady ergonomii i higieny pracy	✓		
		Przykłady wg DigComp 2.2	Z rozsądkiem korzysta ze sprzętu komputerowego.		✓	
Zna zasady ochrony i reakcji na próby ataków cybernetycznych.	✓					
B3_CK4	(4.4) Zdobycie umiejętności związanych z ochroną środowiska wynikających z korzystania z technologii cyfrowych.	B3_EK26	Potrafi wskazać dobrze zdefiniowany i rutynowy wpływ technologii cyfrowych na środowisko.		✓	
		B3_EK27	Rozumie, jaki wpływ (pozytywny i negatywny) na środowisko naturalne mają urządzenia cyfrowe.			✓
		Przykłady wg DigComp 2.2	Chroni środowisko naturalne.		✓	
			Zużyty sprzęt oddaje do recyklingu.			✓

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, OpenVPN.
- 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.