SYLABUS ECCC

Obszar: **Kompetencje Cyfrowe – DigComp 2.1**
Moduł: **DC2.1 M4 Bezpieczeństwo**
Poziom: **Zaawansowany (C5)** - oprócz wspierania innych.

Moduł DC2.1 M4 Bezpieczeństwo poziom C5 obejmuje 5 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.
   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 nękaniem). 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 C5)

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
C5_CK1	(4.1) Zdobycie zaawansowanych umiejętności ochrony urządzeń i treści cyfrowych.	DC2.1_1	Potrafi zastosować różne sposoby ochrony swoich urządzeń i treści cyfrowych.			
		DC2.1_2	Potrafi rozpoznać różnorodne ryzyka i zagrożenia w środowiskach cyfrowych (np. typy ataków).			
		DC2.1_3	Potrafi zastosować środki bezpieczeństwa i ochrony.			
		DC2.1_4	Potrafi zaangażować różne sposoby należytego uwzględniania wiarygodności i prywatności.			
		C5_EK1	Zna typy ataków, których celem są urządzenia elektroniczne oraz znane sposoby dbania o ich bezpieczeństwo.	✓		
		C5_EK2	Wie, czym jest szyfrowanie danych.	✓		

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
		C5_EK3	Potrafi monitorować stan połączenia urządzenia cyfrowego z siecią i odpowiednio reagować na zagrożenie.		✓	
		C5_EK4	Potrafi kompresować/szyfrować dane z wykorzystaniem złożonych haseł, w tym różne lokalizacje przechowywania danych.		✓	
		C5_EK5	Postrzega zagrożenia związane z korzystaniem z publicznych sieci dostępowych, VPN.			✓
		Przykłady wg DigComp 2.1	Chroni konto na serwisie społecznościowym używając różnych metod, (*np.: silne hasło, kontrola ostatnich logowań)* i potrafi pokazać w jaki sposób to robić.			✓
			Potrafi wykryć ryzyka, takie jak otrzymywanie tweet'ów i wiadomości od followersów z fałszywych profili lub próby wyłudzania informacji.		✓	
			Stosuje odpowiednie środki aby uniknąć próby wyłudzania 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 załadowaniem).*		✓	
C5_CK2	(4.2) Przyswojenie szerokiej wiedzy na temat ochrony danych osobowych i prywatności w środowisku cyfrowym.	DC2.1_5	Potrafi zastosować różne sposoby ochrony swoich danych osobowych i prywatności w środowiskach cyfrowych.			
		DC2.1_6	Potrafi zastosować różne sposoby użytkowania i udostępniania informacji umożliwiających identyfikację osoby, jednocześnie chroniąc siebie i innych przez zagrożeniami.			
		DC2.1_7	Potrafi wyjaśnić zasady polityki prywatności dotyczące sposobów przetwarzania danych osobowych w usługach cyfrowych.			
		C5_EK6	Posiada dogłębną wiedzę na temat ochrony danych osobowych i prywatności w środowisku cyfrowym.	✓		
		C5_EK7	Wie, że wiele usług interaktywnych wykorzystuje informacje o nim do filtrowania w komercyjnych Informacjach, w mniej lub bardziej wyraźny sposób.	✓		
		C5_EK8	Potrafi podnosić poziom ochrony swojej prywatności poprzez zmianę domyślnych ustawień prywatności online.		✓	
		C5_EK9	Potrafi adekwatnie do potrzeb modyfikować prawa dostępu dla udostępnionych danych.		✓	

CEL KSZTAŁCENIA		EFEKT KSZTAŁCENIA		W	U	P
		C5_EK10	Potrafi monitorować swoją tożsamość cyfrową i ślady cyfrowe.		✓	
C5_CK3	(4.3) Przyswojenie szerokiej wiedzy na temat ochrony zdrowia i dobrostanu wynikających z korzystania z technologii cyfrowych.	DC2.1_8	Potrafi zaprezentować różne sposoby unikania ryzyka I zagrożenia zdrowia w odniesieniu do dobrostanu fizycznego i psychicznego podczas użytkowania technologii cyfrowych.			
		DC2.1_9	Potrafi zastosować różne sposoby ochrony siebie przed możliwymi zagrożeniami w środowiskach cyfrowych.			
		DC2.1_10	Potrafi zaprezentować różne technologie cyfrowe sprzyjające dobrostanowi społecznemu I włączeniu społecznemu			
		C5_EK11	Zna skutki długotrwałego stosowania technologii.	✓		
		C5_EK12	Potrafi rozwiązywać problemy związane z uzależnieniem od technologii cyfrowych.		✓	
		C5_EK13	Potrafi dostosować stanowisko pracy, aby spełniało podstawowe zasady ergonomii i higieny pracy.		✓	
		C5_EK14	Ma świadomość niekorzystnych dla zdrowia zagrożeń powodowanych uzależnieniem od technologii cyfrowych.			✓
C5_CK4	(4.4) Zdobycie zaawansowanych umiejętności związanych z ochroną środowiska wynikających z korzystania z technologii cyfrowych.	DC2.1_11	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.	✓		
		C5_EK16	Ma wiedzę i potrafi dobierać energooszczędne urządzenia mając na względzie ochronę środowiska.	✓		
		C5_EK17	Potrafi korzystać z usług cyfrowych bez całkowitego uzależnienia od nich.		✓	

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).