Załącznik nr 1 do Uchwały Wojewódzkiego Zespołu Koordynacji nr 1/2026 z dnia 17 lutego 2026r.

Rekomendacja w ramach Wojewódzkiego Zespołu Koordynacji (WZK)

SYSTEMOWE WZMOCNIENIE KOMPETENCJI TECHNOLOGICZNYCH I ODPORNOŚCI CYFROWEJ DZIECI I MŁODZIEŻY – CYBERBEZPIECZEŃSTWO i AI

KARTA WDROŻENIOWA **–** WZK/2026/KPO/03

Pole	Treść (wypełniona)
Numer rekomendacji	WZK/2026/KPO/03
Źródło rekomendacji	WZK – rekomendacja strategiczna
Tytuł rekomendacji	Systemowe wzmocnienie kompetencji technologicznych i odporności cyfrowej dzieci i młodzieży – Cyberbezpieczenstwo i AI
Opis rekomendacji	Wobec rosnącej skali cyberataków oraz zwiększającego się wpływu sztucznej inteligencji na życie młodych ludzi konieczne jest systemowe zwiększenie kompetencji uczniów i nauczycieli w obszarach cyberbezpieczeństwa, technologii cyfrowych oraz AI. Program zakłada wprowadzenie do szkół zajęć z zakresu cyberbezpieczeństwa i sztucznej inteligencji w formie elastycznych zajęć — dopasowanych do wieku, etapu edukacji i wyposażenia szkoły — obejmujących zarówno podstawy bezpieczeństwa cyfrowego, jak i bardziej zaawansowane treści dla szkół o profilach informatycznych (np. analiza zagrożeń, etyczny hacking, język Python w cyberbezpieczeństwie). W zakresie AI zajęcia obejmą: programowanie AI, przetwarzanie języka naturalnego, uczenie maszynowe, głębokie uczenie, tworzenie zapytań, trening AI, a także aspekty związane z bezpiecznym tworzeniem i korzystaniem z AI. Priorytetem jest także nauka bezpiecznego i odpowiedzialnego korzystania z narzędzi AI. Rekomendacja uwzględnia również rozwój **odporności technologicznej** — łączącej kompetencje cyfrowe, emocjonalne, społeczne i poznawcze — tak aby młodzi ludzie potrafili bezpiecznie i świadomie funkcjonować w środowisku informacyjnym, unikać manipulacji i radzić sobie z przeciążeniem technologicznym.
Cel wdrożenia	Zwiększenie praktycznej świadomości młodzieży i nauczycieli w zakresie cyberbezpieczeństwa oraz odpowiedzialnego wykorzystania AI, a także rozwój odporności technologicznej wzmacniającej bezpieczeństwo cyfrowe i przygotowanie do przyszłego rynku pracy.
Uzasadnienie	Rosnąca liczba cyberataków oraz agresywne kampanie dezinformacyjne wymagają systemowego przygotowania uczniów i

Załącznik nr 1 do Uchwały Wojewódzkiego Zespołu Koordynacji nr 1/2026 z dnia 17 lutego 2026r.

Pole	Treść (wypełniona)
	nauczycieli do bezpiecznego funkcjonowania w świecie cyfrowym. Jednocześnie gwałtowny rozwój sztucznej inteligencji tworzy ogromne zapotrzebowanie na kompetencje z zakresu technologii informacyjnych i analitycznych. Wczesne wprowadzenie młodzieży w tematykę AI i cyberbezpieczeństwa pozwoli im świadomie korzystać z technologii, kształtować krytyczne myślenie, a w przypadku uczniów z kierunków informatycznych — zdobywać kompetencje specjalistyczne. Odporność technologiczna łączy kompetencje: • poznawcze (krytyczne myślenie, analiza informacji), • emocjonalne (radzenie sobie ze stresem, presją cyfrową), • społeczne (współpraca, komunikacja), • techniczne (AI, cyberbezpieczeństwo, narzędzia cyfrowe). Tak szerokie ujęcie pozwoli skuteczniej przeciwdziałać zagrożeniom i wspierać rozwój młodych ludzi.
Oczekiwane efekty	**Efekty dla uczniów i nauczycieli:** • nabycie praktycznych kompetencji w zakresie cyberbezpieczeństwa i AI, • zwiększenie świadomego, bezpiecznego i krytycznego korzystania z technologii, • rozwój odporności technologicznej (cyfrowej, emocjonalnej, społecznej i poznawczej), • lepsze przygotowanie młodzieży do zawodów IT/AI. **Efekty systemowe:** • podniesienie odporności regionu na cyberzagrożenia, • modernizacja zasobów technologicznych szkół, • rozwój ekosystemu współpracy szkół z uczelniami i branżą, • regularna aktualizacja treści programowych (co 12 miesięcy), • powstanie ścieżek praktyk, konkursów, stypendiów i projektów uczniowskich. **Długofalowy impact:** • wzrost kompetencji ICT/AI w regionie, • zwiększenie bezpieczeństwa cyfrowego szkół, • wzmacnianie świadomości młodych ludzi w kontekście zagrożeń technologicznych i geopolitycznych.
Rekomendowane działania	**1. Zbudowanie wojewódzkiego modelu „odporności technologicznej” w oparciu o <u>Dwa filary</u>:** **FILAR I: Sprawczość technologiczna i bezpieczeństwo cyfrowe** Cel filaru: Wyposażenie uczniów i nauczycieli w praktyczne kompetencje rozumienia, tworzenia i bezpiecznego wykorzystywania technologii cyfrowych i AI. Podkomponenty: • **cyberbezpieczeństwo techniczne**

Załącznik nr 1 do Uchwały Wojewódzkiego Zespołu Koordynacji nr 1/2026 z dnia 17 lutego 2026r.

Pole	Treść (wypełniona)
	(podstawy ochrony systemów, sieci, danych, reagowanie na incydenty), • **świadomość działania technologii i AI** (jak działają algorytmy, modele AI, sieci, chmura), • **programowanie i tworzenie rozwiązań cyfrowych** (kodowanie, praca z danymi, sieci, IoT, AI), • **krytyczne myślenie wobec technologii i algorytmów** (dezinformacja, deepfake, manipulacje), • **etyka i odpowiedzialność technologiczna** (prawo, RODO, odpowiedzialne użycie AI). **FILAR II: Odporność psychiczna i społeczna w środowisku cyfrowym** Cel filaru: Wzmocnienie zdolności młodych ludzi do zachowania równowagi psychicznej, koncentracji i relacji społecznych w świecie intensywnej technologii. Podkomponenty: • **higiena cyfrowa i zarządzanie uwagą** (czas ekranowy, przeciążenie informacyjne), • **odporność emocjonalna na presję cyfrową** (stres, lęk, porównania społeczne, FOMO), • **kompetencje społeczne i relacje offline** (współpraca, komunikacja, empatia), • **świadomość mechanizmów socjotechniki i manipulacji** (wpływ emocjonalny informacji, panika, polaryzacja), • **refleksja i samoregulacja** (uważność, odpowiedzialne decyzje). Elementy wspólne, umożliwiające skuteczne wdrażanie obu filarów na poziomie województwa. 1. **Przygotowanie nauczycieli** – szkolenia kompetencyjne (cyber, AI, psychospołeczne, kreatywność) – materiały dydaktyczne – sieci wsparcia i laboratoria metodyczne 2. **Zajęcia w szkołach (program dydaktyczny)** – moduły elastyczne – projekty interdyscyplinarne – scenariusze działań dla różnych etapów edukacji 3. **Infrastruktura i sprzęt** – dostęp do urządzeń i Internetu – narzędzia AI zgodne z zasadami bezpieczeństwa i etyki – oprogramowanie edukacyjne 4. **Współpraca z uczelniami i partnerami społecznymi** – ekspertów od AI, psychologów, pedagogów, badaczy – wspólne projekty i badania

Załącznik nr 1 do Uchwały Wojewódzkiego Zespołu Koordynacji nr 1/2026 z dnia 17 lutego 2026r.

Pole	Treść (wypełniona)
	– mentoring i wsparcie dla szkół
Poziom wdrażania	**Regionalny.** Możliwy do wdrożenia w ramach obecnych kompetencji, ale wymaga koordynacji i finansowania.
Realizatorzy i partnerzy	Lider: Politechnika Partnerzy: • **Samorząd Województwa** – koordynacja, finansowanie, organizacja partnerstw. • **Podkarpacki Zespół Placówek Wojewódzkich w Rzeszowie -** treści merytoryczne, szkolenia, mentoring • **Kuratorium** – włączanie elementów do nadzoru pedagogicznego i programów nauczania. • **Uczelnie** – treści merytoryczne, szkolenia, mentoring. • **Firmy z branży IT/AI** – sprzęt, konkursy, projekty, praktyczne know-how. • **Szkoły i nauczyciele** – realizacja na co dzień. • **Młodzieżowe Rady / organizacje uczniowskie** – projektowanie inicjatyw dla młodych. • **Rodzice** – elementy edukacji cyfrowej również dla nich. *Wskazany katalog realizatorów i partnerów ma charakter otwarty i może być rozszerzany w zależności od potrzeb wdrożeniowych oraz dostępnych instrumentów finansowania.*
Źródła finansowania	Środki unijne, Fundusze celowe MEN/MNiSW, środki własne JST/szkół, inne
Harmonogram	**A. Etap 1 – Przygotowanie (3–5 miesięcy)** 1. UMWP + WZK powołują zespół ds. odporności technologicznej. 2. Opracowanie programu 2 filarów — w wersji minimum i rozszerzonej. 3. Stworzenie „Koszyka działań", z którego powiaty i szkoły wybierają moduły zależnie od zasobów. 4. Utworzenie katalogu partnerów (uczelnie, cyber firmy, AI laboratoria, NGO). **B. Etap 2 – Pilotaż (6 miesięcy)** 1. Po jednej szkole z każdego powiatu testuje 2 filary. 2. Diagnoza sprzętowa (gdzie trzeba minimalnych zakupów). 3. Szkolenia dla nauczycieli — praktyczne, nie teoretyczne. 4. Stworzenie platformy wymiany materiałów. **C. Etap 3 – Skalowanie (rok szkolny 1–2)** 1. Szkoły wdrażają tylko wybrane moduły **—** w zależności od realnych warunków. 2. Uczelnie prowadzą cykl praktycznych warsztatów i konsultacji. 3. Powiaty połączą działania szkół z poradnictwem zawodowym i PUP. **D. Etap 4 – Utrwalenie (po 24 miesiącach**) 1. Certyfikacja szkół wdrażających odporność technologiczną. 2. Stała współpraca szkół z biznesem. 3. Aktualizacja programu co 2 lata (AI i cyber szybko się

Załącznik nr 1 do Uchwały Wojewódzkiego Zespołu Koordynacji nr 1/2026 z dnia 17 lutego 2026r.

Pole	Treść (wypełniona)
	zmieniają).
Wskaźniki realizacji	• liczba szkół objętych wsparciem, • liczba nauczycieli, którzy ukończyli kursy / studia, • liczba uczniów, którzy uczestniczyli w zajęciach, • liczba nowych pracowni cyber/AI, • liczba zrealizowanych projektów uczniowskich.
Uwagi dodatkowe	Co jest kluczowe w budowaniu odporności młodych? • realizm zamiast straszenia, • sprawczość zamiast bezradności, • kompetencje miękkie + cyfrowe, • radzenie sobie w złożoności, • praca z emocjami i stresem, • zrozumienie zagrożeń bez epatowania przemocą, • budowanie zaufania i wspólnoty, • edukacja o świecie globalnym i lokalnym, • wzmacnianie odporności: poznawczej, emocjonalnej, cyfrowej, społecznej, technologicznej.

METODOLOGIA WDRAŻANIA

SYSTEMU BUDOWANIA ODPORNOŚCI TECHNOLOGICZNEJ MŁODYCH W PODKARPACKIEM

W ostatnich latach świat technologii zmienia się tak szybko, że szkoły często mają trudności, by za nim nadążyć. Dzieci i młodzież żyją w czasach, gdy cyfrowe technologie, media społecznościowe i sztuczna inteligencja wnikają w niemal każdy aspekt życia. Szkoły nie zawsze nadążają z odpowiednim przygotowaniem do świadomego i bezpiecznego funkcjonowania w takim środowisku. Dlatego potrzebujemy systemu, który pomoże młodym

nie tylko korzystać z technologii, ale też rozumieć je, krytycznie oceniać i wykorzystywać twórczo oraz odpowiedzialnie.

Budowanie odporności technologicznej to właśnie całościowe podejście do nauki — nie tylko programowania czy obsługi sprzętu, lecz także rozwijania świadomości cyberbezpieczeństwa, umiejętności radzenia sobie z presją cyfrową oraz kreatywnego i odpowiedzialnego wykorzystywania AI. Szkoły powinny stać się miejscem, gdzie młodzi ludzie uczą się nie być biernymi odbiorcami technologii, ale świadomymi użytkownikami i twórcami.

Realizacja takiego systemu musi być elastyczna i dostosowana do różnych możliwości szkół – od tych podstawowych, które nie mają dużych zasobów, po te z nowoczesnymi pracowniami, partnerstwami naukowymi i technicznym zapleczem. Dzięki temu każda szkoła może wdrożyć model na swoim poziomie, korzystając z gotowych modułów edukacyjnych, które nie tylko uczą o technologii, lecz także zachęcają do pracy zespołowej, refleksji czy ćwiczeń poza ekranem.

1. Niezwykle istotnym elementem jest wsparcie nauczycieli — nie jako samych ekspertów technologicznych, lecz jako przewodników, którzy potrafią pomóc uczniom rozwijać kompetencje cyfrowe i psychospołeczne. Szkolenia muszą być praktyczne, prowadzone przez specjalistów z różnych dziedzin, tak by nauczyciele czuli się pewnie i mogli efektywnie przekazywać wiedzę.
2. Zajęcia zaś nie powinny być nowym, izolowanym przedmiotem. Lepiej, gdyby tematy z zakresu bezpieczeństwa cyfrowego, AI czy krytycznego myślenia włączano w istniejące lekcje — informatyki, historii, języka polskiego czy wychowania do życia w społeczeństwie. To pozwala młodym uczyć się technologii „w kontekście życia" i lepiej rozumieć jej wpływ na codzienność oraz świat. Dodatkowo projekty interdyscyplinarne, hackathony czy „Dni Odporności Cyfrowej" wprowadzają praktykę i interakcję, zwiększając zaangażowanie i motywację.
3. Infrastruktura techniczna to kolejny ważny element – nie musi to być od razu pełne wyposażenie, ale przynajmniej stabilny dostęp do internetu i podstawowe urządzenia. Dla szkół z mniej rozwiniętym zapleczem program przewiduje rozwiązania niemal „na wynajem" – mobilne pracownie AI czy wypożyczalnie robotów edukacyjnych, które pozwolą na korzystanie z nowoczesnych narzędzi w różnych miejscach. Dla tych, które mają ograniczony dostęp do sprzętu, przewidziane są także wersje analogowe zajęć, jak gry planszowe czy symulacje, które uczą zasad cyberbezpieczeństwa i kreatywności bez ekranów.
4. Współpraca z uczelniami i sektorem technologicznym sprawia, że młodzież ma kontakt z prawdziwymi ekspertami, projektami i nowinkami technologicznymi. Mentoring przez studentów, wykłady, wizyty w laboratoriach czy konkursy tworzą most między teorią a praktyką, a także inspirują do dalszego rozwoju i kariery w branży. To podnosi atrakcyjność edukacji oraz realnie wpływa na aspiracje młodych ludzi.

Technologie rozwijają się błyskawicznie, więc program wymaga regularnej rewizji i certyfikacji szkół, które wdrażają odporność technologiczną. Takie działania zapewnią, że edukacja pozostanie świeża, atrakcyjna i skuteczna. Dlatego potrzebne jest podejście, które **łączy trzy perspektywy**:

1. **Techniczną** – korzystanie z narzędzi, cyberbezpieczeństwo, rozumienie AI.

2. **Społeczną i emocjonalną** – krytyczne myślenie, odporność psychiczna, radzenie sobie z presją cyfrową.
3. **Kreatywną i rozwojową** – umiejętność tworzenia, eksperymentowania, wykorzystania technologii jako narzędzia rozwoju, a nie tylko rozrywki.

Tylko takie podejście pozwoli młodym ludziom nie być biernymi odbiorcami technologii, lecz jej świadomymi użytkownikami i twórcami.

Budowa modelu „Odporności technologicznej" opartego na dwóch filarach
Model stanowi ramę programową umożliwiającą wdrażanie działań w szkołach o różnych zasobach. Rekomendowany model odporności technologicznej opiera się na dwóch filarach:

(1) *Rozwój kompetencji cyfrowych i cyberbezpieczeństwa*– którego celem jest zmniejszenie ryzyka incydentów cybernetycznych i dezinformacji

(2) *Utrzymaniu równowagi psychicznej i społecznej w świecie cyfrowym* – którego celem jest ograniczenie skutków przeciążenia informacyjnego, paniki społecznej i podatności na manipulację

Pierwszy filar dotyczy bezpieczeństwa: uczy uczniów i nauczycieli, jak rozumieć technologie, chronić dane, rozpoznawać manipulacje i bezpiecznie korzystać z AI.

Drugi filar dotyczy odporności ludzi: jak ograniczać stres cyfrowy, zachować koncentrację, relacje społeczne i równowagę między technologią a życiem offline.

Dopiero połączenie obu filarów daje realną odporność systemu edukacji – techniczną i społeczną – co jest kluczowe z punktu widzenia bezpieczeństwa regionu To podejście prewencyjne, a nie reaktywne

1. Opracowanie wojewódzkiej wersji modelu. Proponowane Działania:

1.1. Przygotowanie opisów kompetencji, celów i wskaźników dla każdego filaru, oraz stworzenie dwóch wariantów realizacji:

- **wersja podstawowa** – możliwa do wdrożenia w każdej szkole, bez specjalnych zasobów,
- **wersja rozszerzona** – dla szkół dysponujących pracowniami IT, robotyką i partnerstwami akademickimi.

1.2. Utworzenie „Koszyka działań" . Zestaw materiałów umożliwiających wdrażanie modelu:

- 5–10 mikro-modułów (45–90 min) w każdym filarze,
- propozycje projektów semestralnych i rocznych,
- wersje **low-tech** i **high-tech**,
- komplet materiałów: scenariusze zajęć, karty pracy, checklisty.

1.3. Zapewnienie równowagi między technologią a życiem offline. Każdy moduł uwzględnia:

- pracę zespołową i interakcję bezpośrednią,
- trening uważności, refleksji i regulacji emocji,

- ćwiczenia poza ekranem wzmacniające koncentrację i kompetencje społeczne.

2. Przygotowanie nauczycieli - Zasadniczym elementem modelu jest wsparcie nauczycieli jako przewodników po świecie technologii – nie w roli ekspertów technicznych, lecz moderatorów uczniowskiego rozwoju kompetencji. Proponowane Działania:

2.1. Moduły szkoleniowe (2–4 godz.)
Zakres:
- bezpieczna praca z AI,
- podstawy cyberhigieny,
- proste narzędzia rozwijania odporności poznawczej,
- praca z uczniami nad stresem cyfrowym.

Forma:
- warsztaty online i stacjonarne,
- prowadzenie przez praktyków IT, psychologów, specjalistów AI.

2.2. Studia podyplomowe
Kierunek: *Odporność technologiczna i edukacja dla bezpieczeństwa cyfrowego*, obejmujący:

- AI w edukacji,
- cyberbezpieczeństwo,
- uważność i dobrostan cyfrowy,
- tutoring projektów technologicznych.

2.3. Biblioteka scenariuszy
- minimum 100 scenariuszy dostosowanych do dwóch filarów,
- wersje dla szkół low-tech, high-tech
- oznaczenie poziomu trudności i wymogów sprzętowych,
- materiały zgodne z RODO i zasadami pracy z AI.

2.4. Stałe wsparcie ekspertów
- comiesięczne dyżury online,
- konsultacje projektów szkolnych,
- krótkie materiały wideo („Pogotowie cyber i AI") możliwe do wykorzystania na lekcji.

3. Realizacja zajęć w szkołach – podejście elastyczne. Model nie tworzy nowego przedmiotu. Zakłada wdrażanie modułów w ramach już istniejących lekcji i aktywności, co sprzyja praktycznemu uczeniu technologii „w kontekście życia".

4. Sprzęt – podejście pragmatyczne. Inwestycje sprzętowe mają wspierać rozwój kompetencji, ale nie stanowią głównego celu programu. Priorytetem jest dostępność podstawowych narzędzi i możliwość pracy projektowej. Proponowane Działania:

4.1. Modernizacja infrastruktury
- priorytet dla szkół z realnymi brakami,

- kluczowe: stabilny internet, podstawowe komputery, sieć,
- minimum: jedna sala wyposażona w 10 stanowisk do pracy zespołowej.

4.2. Roboty edukacyjne

- wybór tanich, skalowalnych rozwiązań,
- wypożyczalnie działające na poziomie powiatów.

4.3. Mobilne pracownie AI

- zestawy np. 10 laptopów w walizce,
- wypożyczanie na 4–6 tygodni.

4.4. Wersje analogowe dla szkół bez sprzętu

- gry planszowe o cyberbezpieczeństwie,
- symulacje papierowe,
- praca na scenariuszach i case'ach.

4.5. Inne

- Licencje na platformy związane z cyberbezpieczeństwem (np. TryHackMe, HackTheBox),
- Laboratoria Internetu Rzeczy, Sieci LAN/Wi-Fi
- Laboratoria AI

5. Współpraca z uczelniami i sektorem technologicznym: Partnerstwa z sektorem naukowym i biznesem umożliwiają kontakt z realnymi zastosowaniami technologii, wzmacniają motywację i rozwijają aspiracje edukacyjne uczniów. Proponowane Działania:

5.1. Mentoring

- opieka studentów kierunków IT nad zespołami uczniów,
- wsparcie w realizacji projektów AI i cyber.

5.2. Wykłady i seminaria

Tematy m.in.:

- zasady działania AI,
- zagrożenia cybernetyczne w regionie,
- ścieżki kariery w zawodach przyszłości.

5.3. Wizyty studyjne

- laboratoria AI,
- centra danych,
- jednostki CERT,
- firmy technologiczne.

5.4. Konkursy i wspólne działania

- „Narzędzie dla lokalnej społeczności" – challenge projektowy,
- konkurs na najlepszy projekt AI w edukacji,
- turniej „Cyberbezpieczna szkoła".

5.5. Programy partnerskie

- pakiety edukacyjne od firm,
- staże obserwacyjne,
- cykl „AI w praktyce".

Efekt systemowy to model tworzy spójny ekosystem, który:

- wzmacnia odporność poznawczą i emocjonalną,
- rozwija krytyczne myślenie i świadomość cyfrową,
- umożliwia bezpieczne i twórcze wykorzystanie technologii,
- wspiera równowagę między środowiskiem cyfrowym a offline,
- przygotowuje do pracy i życia w zmieniającym się świecie technologii,
- buduje trwałą współpracę między szkołami, biznesem i uczelniami.