

SCENARIUSZ LEKCJI WYCHOWAWCZYCH

autor: Adam Cyrański

To miała być tylko pomoc...

Cyberbezpieczeństwo, prywatność, zaufanie i cyberprzemoc

Wersja oparta na pracy uczniów, pytaniach badawczych i rutynach myślenia Project Zero

Założenie metodyczne

- Nauczyciel nie podaje gotowych rozwiązań jako pierwszy. Organizuje sytuacje, w których uczniowie obserwują, pytają, przyjmują różne perspektywy, szukają bezpiecznych rozwiązań i formułują własne zasady.
- Film lub storyboard jest pretekstem do dochodzenia: Co się stało? Kiedy przekroczono granicę? Jak można było temu zapobiec? Jak powinien zareagować świadek?
- Każda lekcja kończy się konkretnym produktem uczniowskim: mapą ryzyka, listą pytań, procedurą bezpieczeństwa albo kontraktem reagowania.

Adresaci	klasy 6–8 szkoły podstawowej lub klasa 1 szkoły ponadpodstawowej
Czas	2 lekcje wychowawcze po 45 minut
Materiały	storyboard/film, kartki A3, markery, karteczki samoprzylepne, karty ról, karty pracy
Rola nauczyciela	facylitator, moderator, organizator procesu, osoba dbająca o bezpieczeństwo rozmowy
Rola uczniów	badacze sytuacji, autorzy pytań, twórcy rozwiązań, uczestnicy dyskusji
Rutyny myślenia	Widzę – Myślę – Zastanawiam się; Wejść w buty / Step Inside; Różne punkty widzenia / Circle of Viewpoints; Kompas decyzyjny; Twierdzę – Uzasadniam – Pytam; Kiedyś myślałem – Teraz myślę

Uwaga o bezpieczeństwie rozmowy: temat może dotyczyć trudnych doświadczeń. Nie prosimy uczniów o ujawnianie własnych historii. Pracujemy na sytuacji fikcyjnej/filmowej. Jeśli uczeń sygnalizuje realny problem, nauczyciel uruchamia szkolne procedury wsparcia.

Oś pracy całego cyklu

Od zdarzenia do odpowiedzialnej decyzji

- Zauważam fakty: co rzeczywiście widzę w historii?
- Stawiam pytania: czego jeszcze nie wiem?
- Wchodzę w perspektywę różnych osób: ofiary, sprawcy, świadka, dorosłego, serwisanta.
- Szukam rozwiązań: co można zrobić przed, w trakcie i po zdarzeniu?
- Formułuję zasadę: jaką decyzję podejmę w podobnej sytuacji?

Zastosowane rutyny myślenia

Rutyna	Po co ją stosujemy?	Kiedy w lekcji?	Produkt uczniów
Widzę – Myślę – Zastanawiam się	oddzielenie faktów od interpretacji; uruchomienie pytań	początek pracy z kadrem lub sceną	tabela obserwacji i pytań
Wejść w buty / Step Inside	rozumienie motywacji, emocji i potrzeb różnych osób	analiza Tomkowi, Tomka, świadka, rodzica	notatka z perspektywy wybranej osoby
Różne punkty widzenia / Circle of Viewpoints	zobaczenie, że ta sama sytuacja wygląda inaczej z różnych miejsc	lekcja o zaufaniu i cyberprzemocy	krąg perspektyw + pytania z każdej roli
Kompas decyzyjny	ważenie korzyści, ryzyk, potrzebnej wiedzy i następnego kroku	decyzja: komu oddać sprzęt? co zrobić z cudzym materiałem?	plan działania
Twierdzę – Uzasadniam – Pytam	budowanie argumentu i dopisywanie pytań zamiast szybkich ocen	podsumowanie etapów pracy	argument + pytanie badawcze
Kiedyś myślałem – Teraz myślę	refleksja nad zmianą rozumienia prywatności i odpowiedzialności	bilet wyjścia	indywidualna refleksja

LEKCJA 1. Moje dane, moje hasła, moja chmura

Pytanie przewodnie: Co naprawdę oddaję drugiej osobie, gdy oddaję jej odblokowany telefon, komputer albo hasło?

Cele językiem ucznia

- Rozpoznam, jakie dane są zapisane w moim cyfrowym życiu.
- Postawię pytania o bezpieczeństwo urządzenia, hasła i chmury.
- Wypracuję bezpieczną procedurę działania w sytuacji awarii sprzętu.
- Wyjaśnię, dlaczego hasło i dostęp do chmury chronią nie tylko pliki, ale też relacje i prywatność.

Linia pracy uczniów

Etap 1. Wejście w problem (0–5 min)

Rutyna / metoda: Pytanie startowe

Co robią uczniowie: Indywidualnie zapisują odpowiedź: „Co Tomek naprawdę oddał koledze?” Następnie porównują odpowiedzi w parach.

Rola nauczyciela-facilitatora: Nie komentuje od razu poprawności. Zbiera różne odpowiedzi na tablicy i dopytuje: „Co jeszcze?” „Skąd to wiemy?”

Produkt / ślad myślenia: Chmura skojarzeń: komputer = dane + dostęp + zaufanie

Etap 2. Obserwacja kadru/sceny (5–12 min)

Rutyna / metoda: Widzę – Myślę – Zastanawiam się

Co robią uczniowie: Analizują kadr: Tomek przy komputerze / czarny ekran / SYSTEM FAILED.
Wypełniają trzy kolumny tabeli: fakty, interpretacje, pytania.

Rola nauczyciela-facilitatora: Pilnuje rozróżnienia: „Czy to jest fakt, czy przypuszczenie?” „Jakie pytanie warto zadać przed oceną sytuacji?”

Produkt / ślad myślenia: Tabela obserwacji i pytań

Etap 3. Mapa cyfrowego życia (12–20 min)

Rutyna / metoda: Mapa pojęciowa w grupach

Co robią uczniowie: Tworzą mapę: gdzie są moje dane?
telefon, chmura, komunikatory, poczta, zdjęcia, hasła, gry, dokumenty. Oznaczają kolorem miejsca największego ryzyka.

Rola nauczyciela-facilitatora: Zadaje pytania pogłębiające np: „Które z tych miejsc otwiera dostęp do kolejnych miejsc?” „Co może być ukryte w kopii zapasowej?”

Produkt / ślad myślenia: Mapa danych i ryzyka

Etap 4. Sytuacja decyzyjna (20–30 min)

Rutyna / metoda: Kompas decyzyjny

Co robią uczniowie: Badają propozycję: „Oddać komputer koledze, serwisowi, rodzicowi, nikomu?”

Wypełniają kompas: korzyści, obawy, czego trzeba się dowiedzieć, następny krok.

Rola nauczyciela-facilitatora: Nie podaje rozwiązań. Pomaga doprecyzować np: „Jakie warunki muszą być spełnione, żeby ta decyzja była bezpieczna?”

Produkt / ślad myślenia: Kompas decyzji

Etap 5. Projektowanie procedury (30–38 min)

Rutyna / metoda: Praca ekspercka w grupach

Co robią uczniowie: Tworzą procedurę: „Co robię, gdy sprzęt się zepsuje?”

Minimum 6 kroków. Każdy krok musi odpowiadać na konkretne ryzyko.

Rola nauczyciela-facilitatora: Pyta np.: „Jaki problem rozwiązuje ten krok?” „Co zrobisz z hasłami?” „Co z chmurą?” „Kto jest zaufanym dorosłym?”

Produkt / ślad myślenia: Procedura bezpieczeństwa

Etap 6. Argumentowanie (38–43 min)

Rutyna / metoda: Twierdzę – Uzasadniam – Pytam

Co robią uczniowie: Każda grupa formułuje jedno twierdzenie, jedno uzasadnienie i jedno pytanie, którego nadal nie rozstrzygnęła.

Rola nauczyciela-facilitatora: Moderuje krótką wymianę. Dbą, by pytania były traktowane jako wartościowy wynik pracy, nie jako brak wiedzy.

Produkt / ślad myślenia: Argumenty i pytania badawcze

Etap 7. Refleksja (43–45 min)

Rutyna / metoda: Kiedyś myślałem – Teraz myślę

Co robią uczniowie: Indywidualnie kończą zdanie: „Kiedyś myślałem, że hasło..., teraz myślę, że...”

Rola nauczyciela-facilitatora: Zbiera anonimowe karteczki lub prosi o kilka dobrowolnych wypowiedzi.

Produkt / ślad myślenia: Bilet wyjścia

Część dla nauczyciela: pytania facilitujące

Moment	Pytania nauczyciela	Możliwe tropy uczniów
Pytanie startowe	Co jest w komputerze poza sprzętem? Co znaczy „dostęp”? Czy plik w chmurze też może być zagrożony?	zdjęcia, hasła, wiadomości, historia rozmów, dostęp do kont, kopie zapasowe
Mapa ryzyka	Które konto otwiera dostęp do największej liczby rzeczy? Co się stanie, jeśli ktoś zna hasło do poczty?	poczta resetuje hasła; chmura zawiera zdjęcia; komunikator ujawnia relacje
Kompas	Co jest wygodne, ale ryzykowne? Czego musimy się dowiedzieć przed decyzją?	czy serwis ma uprawnienia; czy trzeba podawać hasło; czy można utworzyć konto gościa; czy dane są zaszyfrowane
Procedura	Który krok chroni prywatność? Który krok chroni dane przed utratą? Który krok chroni przed nadużyciem zaufania?	kopie zapasowe; blokada ekranu; 2FA; wylogowanie; dorosły; serwis; zmiana hasła po naprawie

Pojęcia do uporządkowania dopiero po pracy uczniów

- hasło jako klucz do danych, a nie tylko do aplikacji;
- uwierzytelnianie dwuskładnikowe jako dodatkowa warstwa ochrony;
- szyfrowanie jako zabezpieczenie danych przed odczytem bez klucza;
- chmura jako miejsce przechowywania danych, do którego dostęp zależy od bezpieczeństwa konta;
- kopia zapasowa jako ochrona przed utratą danych, ale również zasób wymagający ochrony.

LEKCJA 2. Zaufanie, granice i cyberprzemoc

Pytanie przewodnie: Kiedy ciekawość, żart albo „tylko przestanie dalej” staje się krzywdą?

Cele językiem ucznia

- Rozpoznam moment, w którym zostaje przekroczona granica zaufania.
- Przyjrę się sytuacji z różnych punktów widzenia: osoby skrzywdzonej, sprawcy, świadka i dorosłego.
- Postawię pytania, które pomagają zatrzymać ocenianie ofiary i skupić się na odpowiedzialności.
- Wypracuję klasowe sposoby reagowania na cyberprzemoc i naruszanie prywatności.

Linia pracy uczniów

Etap 1. Przypomnienie problemu (0–5 min)

Rutyna / metoda: Milczący zapis pytań

Co robią uczniowie: Zapisują 2 pytania do historii Tomkowi: jedno techniczne, jedno dotyczące relacji lub emocji.

Rola nauczyciela-facilitatora: Nie streszcza całej historii. Prosi o pytania, nie o szybkie oceny.

Produkt / ślad myślenia: Lista pytań uczniów

Etap 2. Szukanie granicy (5–13 min)

Rutyna / metoda: Linia zdarzeń

Co robią uczniowie: Grupy układają zdarzenia od „awaria” do „upokorzenie”. Zaznaczają moment, w którym ich zdaniem zaczęła się krzywda.

Rola nauczyciela-facilitatora: Pyta np.: „Dlaczego właśnie tutaj?” „Czy wcześniejszy moment też był ryzykowny?” „Co zmienia zgoda, a co jej brak?”

Produkt / ślad myślenia: Oś zdarzeń z punktem granicznym

Etap 3. Perspektywy osób (13–25 min)

Rutyna / metoda: Różne punkty widzenia / Circle of Viewpoints

Co robią uczniowie: Każda grupa losuje rolę: Tomek, Tomek, świadek, rodzic, nauczyciel, osoba z serwisu. Wypowiada się: „Myślę o tej sytuacji z punktu widzenia... Myślę... Pytanie, które mam, brzmi...”

Rola nauczyciela-facilitatora: Dbą, by uczniowie nie usprawiedliwiali krzywdy, ale rozumieli mechanizmy i odpowiedzialność. Dopisuje pytania do wspólnej mapy.

Produkt / ślad myślenia: Krąg perspektyw i pytań

Etap 4. Wejście w buty osoby skrzywdzonej i świadka (25–32 min)

Rutyna / metoda: Step Inside / Wejdź w buty

Co robią uczniowie: Wybierają jedną rolę i zapisują: Co ta osoba widzi/słyszy? Co może myśleć? O co może się bać? Czego potrzebuje?

Rola nauczyciela-facilitatora: Zabezpiecza rozmowę: „Nie opowiadamy prywatnych historii z klasy. Pracujemy na postaci z filmu.”

Produkt / ślad myślenia: Notatka empatyczna

Etap 5. Projektowanie reakcji (32–38 min)

Rutyna / metoda: Stacje zadaniowe

Co robią uczniowie: Przechodzą przez stacje: 1. Co robi ofiara? 2. Co robi świadek? 3. Co robi dorosły? 4. Co powinien zrobić sprawca, żeby zatrzymać krzywdę?

Rola nauczyciela-facilitatora: Pilnuje realizmu działań: „Co można zrobić od razu?” „Kto ma sprawczość?” „Jak zatrzymać dalsze rozsyłanie?”

Produkt / ślad myślenia: Tablica reakcji

Etap 6. Uzgodnienie zasad (38–43 min)

Rutyna / metoda: Kontrakt klasowy

Co robią uczniowie: Wybierają 5 zasad: czego nie robimy i co robimy, gdy ktoś jest krzywdzony. Zasady muszą być sformułowane działaniowo.

Rola nauczyciela-facilitatora: Pomaga przejść od hasel do konkretów: zamiast „szanujemy się” – „nie przesyłamy dalej screenów, które mogą upokorzyć”.

Produkt / ślad myślenia: Kontrakt reagowania

Etap 7. Refleksja końcowa (43–45 min)

Rutyna / metoda: Kiedyś myślałem – Teraz myślę

Co robią uczniowie: Kończą zdanie: „Kiedyś myślałem, że przestanie dalej..., teraz myślę, że...”

Rola nauczyciela-facilitatora: Zbiera bilety wyjścia jako informację o zmianie myślenia.

Produkt / ślad myślenia: Bilet wyjścia

Część dla nauczyciela: pytania facilitujące

Moment	Pytania nauczyciela	Możliwe tropy uczniów
Linia zdarzeń	Kiedy Tomek przestał pomagać? Czy samo zobaczenie pliku jest już problemem? Co zmienia intencja, a co skutek?	przeglądanie bez zgody; kopiowanie; drukowanie; pokazywanie; rozsyłanie; śmiech świadków
Różne punkty widzenia	Jakie pytanie zadałby Tomek? Jakie pytanie zadałby rodzic? Jakie pytanie zadałby nauczyciel? Jakie pytanie powinien zadać sobie świadek?	Kto ma dostęp? Jak zatrzymać rozpowszechnianie? Jak pomóc Kubie? Jakie są konsekwencje?
Step Inside	Czego Tomek może się bać? Co może widzieć świadek? Co może myśleć Tomek, zanim zrozumie skalę krzywdy?	wstyd, samotność, lęk przed szkołą, presja grupy, ciekawość, brak wyobraźni, poczucie winy
Stacje reakcji	Co można zrobić w pierwszych 10 minutach? Co w pierwszym dniu? Co musi zrobić szkoła?	nie przysyłać dalej; zgłosić dorosłemu; usunąć materiały; zabezpieczyć dowody; wesprzeć ofiarę; rozmowa z rodzicami

Granica, której pilnujemy w rozmowie

- Nie obwiniamy osoby skrzywdzonej za to, że miała prywatne dane.
- Nie normalizujemy zachowania sprawcy jako „żartu” lub „ciekawości”.
- Nie prosimy uczniów o przykłady z własnej klasy ani o ujawnianie prywatnych historii.
- Mówimy o odpowiedzialności, reagowaniu i możliwości szukania pomocy.

Karty pracy dla uczniów

Karta pracy 1. Widzę – Myślę – Zastanawiam się

WIDZĘ – fakty z kadru/sceny	MYŚLĘ – moje interpretacje	ZASTANAWIAM SIĘ – pytania

Karta pracy 2. Kompas decyzyjny

Decyzja do zbadania: Co zrobić, gdy zepsuje się komputer/telefon z prywatnymi danymi?

E – Co jest korzystne / pomocne?	W – Co jest ryzykowne / niepokojące?
N – Czego jeszcze musimy się dowiedzieć?	S – Jaki jest nasz bezpieczny następny krok?
Uzasadnienie decyzji grupy:	

Karta pracy 3. Różne punkty widzenia / Circle of Viewpoints

Wybierz perspektywę: Tomek / Tomek / świadek / rodzic / nauczyciel / osoba z serwisu.

Moja rola / perspektywa	
Myślę o tej sytuacji z punktu widzenia...	
Z tej perspektywy widzę problem tak...	
Pytanie, które mam z tej perspektywy, brzmi...	
Czego ta osoba potrzebuje?	
Jakie odpowiedzialne działanie może podjąć?	

Karta pracy 4. Wejdz w buty / Step Inside

Osoba, w której buty wchodzę	
Co ta osoba może widzieć lub słyszeć?	
Co może wiedzieć, myśleć albo błędnie zakładać?	
O co może się bać? Na czym może jej zależeć?	
Jakie wsparcie lub działanie byłoby dla niej potrzebne?	

Karta pracy 5. Stacje reagowania

Co może zrobić osoba skrzywdzona?	Co może zrobić świadek?	Co powinni zrobić dorośli?	Co powinien zrobić sprawca?

Karta pracy 6. Twierdzę – Uzasadniam – Pytam

UZASADNIAM to, ponieważ...	
PYTAM, bo nadal nie wiem...	
Mój następny bezpieczny krok to...	

Materiały pomocnicze dla nauczyciela

Przykładowe produkty końcowe uczniów

- Procedura: „Co robię, gdy zepsuje mi się komputer lub telefon?”
- Mapa ryzyka: „Gdzie są moje dane i kto może uzyskać do nich dostęp?”
- Krąg perspektyw: „Jak tę samą sytuację widzą różne osoby?”
- Kontrakt klasowy: „Jak reagujemy, gdy ktoś narusza cudzą prywatność?”
- Lista pytań do dalszej rozmowy: „Czego jeszcze musimy się dowiedzieć o chmurze, hasłach, cyberprzemocy?”

Propozycja klasowego kontraktu: nie wykorzystujemy cudzej prywatności przeciwko drugiej osobie

- Nie przeglądamy cudzych telefonów, komputerów, kont i folderów bez świadomej zgody.
- Nie robimy screenów prywatnych rozmów po to, by kogoś ośmieszyć lub wykorzystać przeciwko niemu.
- Nie przesyłamy dalej zdjęć, rozmów ani materiałów, które mogą kogoś upokorzyć.
- Gdy dostajemy taki materiał, zatrzymujemy łańcuch: nie komentujemy, nie rozsyłamy, zgłaszamy dorosłemu.
- Wspieramy osobę skrzywdzoną komunikatem: „To nie twoja wina. Pomogę ci zgłosić sprawę”.

Miejsca i osoby pomocy

- rodzic lub opiekun prawny;
- wychowawca, pedagog, psycholog szkolny, dyrektor;
- zaufany nauczyciel lub inny dorosły w szkole;
- telefon zaufania dla dzieci i młodzieży: 116 111;
- w sytuacji bezpośredniego zagrożenia życia lub zdrowia: 112.

Źródła inspiracji metodycznej

- Project Zero, Harvard Graduate School of Education: Thinking Routines – toolbox rutyn myślenia.
- Project Zero: See, Think, Wonder – rutyna uważnej obserwacji i stawiania pytań.
- Project Zero: Step Inside – rutyna wchodzenia w różne perspektywy.
- Project Zero: Circle of Viewpoints – rutyna eksplorowania punktów widzenia.
- Project Zero: Compass Points – rutyna badania propozycji i decyzji przez korzyści, ryzyka, potrzeby informacyjne i następny krok.