

• Michał Grześlak • Dorota Janczak •

RAMOWE PROGRAMY SZKOLEŃ

dla nauczycieli odpowiedzialnych za nauczanie
w zakresie bezpieczeństwa informacyjnego
w szkołach na I, II i III etapie edukacyjnym



● Michał Grześlak ● Dorota Janczak ●

RAMOWE PROGRAMY SZKOLEŃ

**dla nauczycieli odpowiedzialnych za nauczanie
w zakresie bezpieczeństwa informacyjnego
w szkołach na I, II i III etapie edukacyjnym**

Ośrodek Rozwoju Edukacji

Warszawa 2018

Redaktor prowadzący
Waldemar Krawiec

Redakcja językowa i korekta
Karolina Strugińska

Redakcja techniczna i skład
Wojciech Romerowicz

Projekt okładki, layout
Wojciech Romerowicz

Elementy graficzne: © Astrovector/Fotolia.com

ISBN 978-83-66047-04-4

Ośrodek Rozwoju Edukacji
Wydział Rozwijania Kompetencji Kluczowych
Warszawa 2018
Wydanie I

Publikacja jest rozpowszechniana na zasadach licencji
Creative Commons 4.0 (CC BY-NC).
<https://creativecommons.org/licenses/by-nc/4.0/deed.pl>

Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
www.ore.edu.pl
tel. 22 345 37 00
fax 22 345 37 70
www.ore.edu.pl

Spis treści

Koncepcja i założenia ogólne szkolenia	6
---	----------

Ramowy program szkoleń

dla nauczycieli pierwszego etapu kształcenia (klas I–III SP)	
odpowiedzialnych za nauczanie w zakresie bezpieczeństwa	
informatycznego w szkołach.....	11

Część wstępna

Działania nauczyciela a bezpieczeństwo informatyczne	
w placówce oświatowej.....	17
Blok 1: Bezpieczeństwo informatyczne – podstawy.....	17
Blok 2: Dane osobowe.....	20
Blok 3: Prawo autorskie.....	22

Część główna

Bezpieczeństwo informatyczne ucznia	23
Blok 1: Mały uczeń przy komputerze	23
Blok 2: Bezpiecznie w sieci	25
Blok 3: Ochrona danych osobowych.....	27
Blok 4: Podstawy prawa autorskiego dla najmłodszych	28

Przykładowe scenariusze zajęć.....	31
Scenariusz zajęć nr 1	31
Scenariusz zajęć nr 2	34
Scenariusz zajęć nr 3	37
Scenariusz zajęć nr 4	40
Scenariusz zajęć nr 5	43

Ramowy program szkoleń

dla nauczycieli drugiego etapu kształcenia (klasy IV–VI SP)	
odpowiedzialnych za nauczanie w zakresie bezpieczeństwa	
informatycznego w szkołach.....	47

Część wstępna

Działania nauczyciela a bezpieczeństwo informatyczne	
w placówce oświatowej.....	51
Blok 1: Bezpieczeństwo informatyczne – podstawy.....	51
Blok 2: Prawo autorskie.....	54
Blok 3: Dane osobowe.....	55

Część główna

Bezpieczeństwo informacyjne ucznia	57
Blok 1: Korzystamy z mediów (cyfrowych).....	57
Blok 2: Oswajamy prawo autorskie	59
Blok 3: Mój wizerunek w sieci.....	60
Blok 4: Z głową w internecie.....	62
Blok 5: Aplikacje i urządzenia mobilne	64
Przykładowy rozkład treści.....	65
Przykładowe scenariusze zajęć.....	67
Scenariusz zajęć nr 1	67
Scenariusz zajęć nr 2	70
Scenariusz zajęć nr 3	73
Scenariusz zajęć nr 4	77
Scenariusz zajęć nr 5	81

Ramowy program szkoleń

dla nauczycieli drugiego etapu kształcenia (klasy VII–VIII SP)

odpowiedzialnych za nauczanie w zakresie bezpieczeństwa

informacyjnego w szkołach..... 85

Część wstępna

Działania nauczyciela a bezpieczeństwo informacyjne w placówce oświatowej.....	91
Blok 1: Bezpieczeństwo informacyjne – podstawy.....	91
Blok 2: Dane osobowe.....	94
Blok 3: Prawo autorskie.....	96

Część główna

Bezpieczeństwo informacyjne ucznia	97
Blok 1: Czym jest bezpieczeństwo informacyjne	97
Blok 2: Korzystamy z informacji.....	99
Blok 3: Ja jako autor	101
Blok 4: Moje dane	102
Blok 5: Bezpiecznie w sieci	104
Przykładowy rozkład treści.....	107
Przykładowe scenariusze zajęć.....	109
Scenariusz zajęć nr 1	109
Scenariusz zajęć nr 2	112
Scenariusz zajęć nr 3	115
Scenariusz zajęć nr 4	117
Scenariusz zajęć nr 5	120

Ramowy program szkoleń

dla nauczycieli trzeciego etapu kształcenia odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach ponadpodstawowych	123
---	-----

Część wstępna

Działania nauczyciela a bezpieczeństwo informacyjne w placówce oświatowej.....	127
Blok 1: Bezpieczeństwo informacyjne – podstawy.....	127
Blok 2: Dane osobowe.....	130
Blok 3: Prawo autorskie.....	132

Część główna

Bezpieczeństwo informacyjne ucznia	133
Blok 1: Czym jest bezpieczeństwo informacyjne	133
Blok 2: Korzystamy z informacji.....	135
Blok 3: Ja jako autor	137
Blok 4: Moje dane	138
Blok 5: Bezpiecznie w sieci	140

Przykładowy rozkład treści.....	143
--	------------

Przykładowe scenariusze zajęć.....	145
Scenariusz zajęć nr 1	145
Scenariusz zajęć nr 2	148
Scenariusz zajęć nr 3	150
Scenariusz zajęć nr 4	153
Scenariusz zajęć nr 5	155

O autorach	157
-------------------------	------------



Koncepcja i założenia ogólne szkolenia

Ramowe programy szkoleń dla nauczycieli odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach zostały opracowane zgodnie z nową podstawą programową kształcenia ogólnego¹. Zestaw programów szkoleń przedstawionych w tej publikacji, dotyczy przede wszystkim zagadnień z zakresu bezpieczeństwa informacyjnego na terenie placówek oświatowych oraz tych aspektów życia prywatnego, które mogą mieć znaczenie dla bezpieczeństwa informacyjnego uczniów.

Czym jest bezpieczeństwo informacyjne?

Autorzy programów, za Konstantym A. Wojtaszczykiem oraz Anną Materską-Sosnowską, interpretują bezpieczeństwo informacyjne nie tylko jako stan pewności i brak zagrożeń, lecz także jako zbiór działań, metod, procedur stosowanych przez uprawnione podmioty w celu zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem². Nie istnieje definicja bezpieczeństwa informacyjnego i bywa ono rozmaicie rozumiane przez różne podmioty, toteż autorzy wzięli pod uwagę także inne sformułowania, które dodatkowo wyjaśniają to pojęcie, tak aby zostało ono lepiej zrozumiane przez dzieci i młodzież podczas przygotowywania ich do życia w społeczeństwie informacyjnym. W swojej definicji Leszek F. Korzeniowski skupia się na bezpieczeństwie informacyjnym podmiotu (człowieka lub organizacji), które rozumie jako „(...) możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą”³. Natomiast Krzysztof Liderman dodaje: „(...) bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji”⁴. Z kolei Eugeniusz Nowak i Maciej Nowak podkreślają, iż bezpieczeństwo informacyjne to stan uwarunkowań wewnętrznych i zewnętrznych pozwalający państwu na rozwój społeczeństwa informacyjnego⁵.

¹ Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. z 2017 r., poz. 356).

² Wojtaszczyk K. A., Materska-Sosnowska A. (red.), (2009), *Bezpieczeństwo państwa. Wybrane problemy*, Warszawa: Oficyna Wydawnicza ASPRA-JR.

³ Korzeniowski L. F., (2012), *Podstawy nauk o bezpieczeństwie*, Warszawa: Difin, s. 147.

⁴ Liderman K., (2012), *Bezpieczeństwo informacyjne*, Warszawa: Wydawnictwo Naukowe PWN, s. 22.

⁵ Nowak E., Nowak M., (2011), *Zarys teorii bezpieczeństwa narodowego*, Warszawa: Difin, s. 103.



Termin „bezpieczeństwo” związany jest nierozdzielnie z pojęciem „zagrożenia”, toteż autorzy programów, skupiając się na kwestii zachowania bezpieczeństwa, poruszają także zagadnienia związane z prewencją i redukowaniem zagrożeń oraz ze skutkami naruszenia bezpieczeństwa. Szczególne miejsce zostało w programach poświęcone bezpieczeństwu dzieci i młodzieży w kontekście korzystania przez nie z technologii komunikacyjnych – ze względu na zagrożenia wynikające z użytkowania urządzeń elektronicznych i rozległych sieci komputerowych, ze szczególnym uwzględnieniem portali społecznościowych. Programy opracowano tak, aby kończący szkolenie nauczyciele potrafili przygotować uczniów do funkcjonowania w społeczeństwie informacyjnym, które stara się osiągać i utrzymywać bezpieczeństwo informacyjne, spełniając warunki m.in.: zapewnienia wysokiej jakości informacji oraz jej niezakłóconego przepływu, skutecznej ochrony danych osobowych, poszanowania i ochrony prawa obywateli do prywatności. Na te aspekty bezpieczeństwa kładzie się szczególny nacisk podczas przygotowania nauczycieli do prowadzenia zajęć.

Jak zapisano w podstawie programowej: „najważniejszym celem kształcenia w szkole podstawowej jest dbałość o integralny rozwój biologiczny, poznawczy, emocjonalny, społeczny i moralny ucznia”⁶. W cel ten wpisuje się także edukacja w zakresie bezpieczeństwa informacyjnego. Nawiązanie do tej tematyki znajdziemy w preambule do podstawy programowej szkoły podstawowej – można tam przeczytać, że „(...) szkoła ma stwarzać uczniom warunki do nabywania wiedzy i umiejętności potrzebnych do rozwiązywania problemów z wykorzystaniem metod i technik wywodzących się z informatyki, w tym logicznego i algorytmicznego myślenia, programowania, posługiwania się aplikacjami komputerowymi, wyszukiwania i wykorzystywania informacji z różnych źródeł, posługiwania się komputerem i podstawowymi urządzeniami cyfrowymi oraz stosowania tych umiejętności na zajęciach różnych przedmiotów – m.in do pracy z tekstem, wykonywania obliczeń, przetwarzania informacji i jej prezentacji w różnych postaciach. Szkoła ma również przygotowywać ich do dokonywania świadomych i odpowiedzialnych wyborów w trakcie korzystania z zasobów dostępnych w internecie, krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci”⁷.

⁶ Zał. nr 2 do Rozporządzenia Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. z 2017 r., poz. 356 ze zm.)

⁷ Ibidem.



Kwestia bezpieczeństwa informacyjnego w zapisach podstawy programowej dotyczących I etapu edukacyjnego (klasy I–III) pojawia się głównie w części poświęconej informatyce – w kontekście np. korzystania przez ucznia z udostępnianych mu stron i zasobów internetowych, wykorzystywania stwarzanej przez technologię możliwości komunikowania się podczas uczenia się, a także w odniesieniu do przestrzegania prawa i zasad bezpieczeństwa (rozdzielanie zachowań pożądanych i niepożądanych, przestrzeganie norm dotyczących korzystania z efektów pracy innych oraz reguł związanych z bezpieczeństwem w internecie). Pośrednio pojawia się ona także w zapisach dotyczących edukacji społecznej, przyrodniczej, plastycznej, technicznej, języka obcego i etyki. Edukacja na tym etapie ma charakter zintegrowany, łączący zagadnienia z zakresu różnych obszarów tematycznych, dlatego treści dotyczące bezpieczeństwa informacyjnego nie mogą być przekazywane wyłącznie podczas lekcji informatyki, powinny pojawić się także na zajęciach innych przedmiotów. Ze względu na specyfikę wieku wczesnoszkolnego tę tematykę omawiać należy w zakresie podstawowym, w formie dostosowanej do etapu rozwoju uczniów, w oparciu o elementy pedagogiki zabawy, gry czy też baśni.

Mając na uwadze spiralny układ treści nauczania, nauczyciele odpowiedzialni za kształcenie uczniów w wieku wczesnoszkolnym w zakresie bezpieczeństwa informacyjnego powinni znać zapisy podstawy programowej dotyczące tej tematyki także na kolejnych etapach edukacyjnych. Podobnie nauczyciele uczący starsze klasy powinni sobie uświadamiać, jakie zagadnienia z zakresu bezpieczeństwa informacyjnego uczniowie poznawali na wcześniejszych etapach edukacyjnych. Dlatego też zaplanowano zapoznanie uczestników szkoleń z zapisami podstaw programowych dotyczących kolejnych etapów kształcenia.

Na II (obejmującym klasy IV–VIII szkoły podstawowej) i III etapie edukacyjnym (obejmującym klasy szkół ponadpodstawowych) zajęcia dotyczące bezpieczeństwa informacyjnego realizuje się głównie na lekcjach informatyki, edukacji dla bezpieczeństwa oraz wiedzy o społeczeństwie, lecz elementy wiedzy z tego zakresu pojawiają się także w podstawach programowych innych przedmiotów.

Zapisy odnoszące się do bezpieczeństwa informacyjnego znajdujemy w celach kształcenia poszczególnych przedmiotów na wszystkich etapach edukacyjnych. Są to wskazania dotyczące posługiwania się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, tworzeniem informacji i komunikatów, a także wyszukiwania informacji i zasobów w internecie, oraz wszelkie zapisy na temat prywatności, poszanowania i ochrony praw oraz szeroko rozumianego bezpieczeństwa w cyberprzestrzeni. W związku z powyższym można stwierdzić, że skoro każdy



nauczyciel jest odpowiedzialny za przygotowanie uczniów do funkcjonowania w życiu codziennym, odpowiada również za przekazywanie uczniom wiedzy z zakresu bezpieczeństwa informacyjnego.

Uwzględniając cytowane powyżej zapisy, opracowano cztery ramowe programy szkoleń dostosowane swym zakresem do wieku, możliwości rozwojowych i doświadczeń uczniów, których będą nauczać uczestnicy każdej z grup szkoleniowych. Program każdego z kursów obejmuje 25 godzin lekcyjnych – realizowanych podczas co najmniej dwóch spotkań stacjonarnych oraz zajęć w formie zdalnej – i jest przeznaczony dla wychowawców oraz nauczycieli różnych przedmiotów, a w szczególności dla nauczycieli informatyki. Każdy z programów składa się z dwóch części. Część wstępna przeznaczona dla nauczycieli jako pracowników instytucji oświatowych porusza zagadnienia związane z obowiązującym prawem dotyczącym ochrony informacji. Natomiast część główna poświęcona jest pracy z uczniami skorelowanej z nową podstawą programową kształcenia ogólnego, z uwzględnieniem specyfiki nauczania i problematyki charakterystycznej dla poszczególnych etapów kształcenia.

Programy dotyczące nauczania klas starszych szkoły podstawowej w szczególności sposób uwzględniają problematykę młodzieżową oraz zachowania mające wpływ na powstawanie zagrożeń bezpieczeństwa informacyjnego. Program odnoszący się do trzeciego etapu edukacyjnego uwzględnia problematykę związaną z zainteresowaniami osób dorosłych oraz zachowania mające wpływ na ich bezpieczeństwo informacyjne w życiu prywatnym i zawodowym. Zaleca się, aby w czasie szkoleń łączyć problematykę bezpieczeństwa informacyjnego z doświadczeniem dzieci i młodzieży, a także samych nauczycieli – tak aby proponowane zajęcia odpowiadały na potrzeby poszczególnych grup szkoleniowych oraz zespołów klasowych, które będą kształcone jako docelowi adresaci. Wśród proponowanych rozwiązań znajdują się np. prowadzenie rozmów z dziećmi młodszymi czy przeprowadzenie wśród starszych uczniów anonimowej ankiety podsumowującej ich doświadczenia i problemy związane z omawianą tematyką.

W poszczególnych programach część treści została powtórzona w odniesieniu do konkretnych etapów kształcenia, z uwzględnieniem jej dostosowania do wieku uczniów – co ma związek z koncepcją nauczania zakładającą spiralny przyrost wiedzy.

Każdy z programów zawiera: informacje ogólne, wymagania wstępne stawiane uczestnikom, cele szkolenia, treści nauczania, przykładowy rozkład treści oraz zalecane formy i metody realizacji programu. Do każdego programu załączono po pięć przykładowych scenariuszy zajęć. Zaproponowane w programach formy i metody



pracy celowo zostały potraktowane swobodnie, aby umożliwić placówkom doskonalenia nauczycieli elastyczne przygotowanie szczegółowych programów szkoleń i ich dopasowanie do potrzeb lokalnego środowiska edukacyjnego.

Ramowy program szkoleń

dla nauczycieli pierwszego etapu kształcenia (klas I–III SP)
odpowiedzialnych za nauczanie w zakresie bezpieczeństwa
informacyjnego w szkołach



Informacje ogólne

Program szkolenia został opracowany w taki sposób, aby mogło ono służyć przygotowaniu nauczycieli do wprowadzania uczniów w problematykę wybranych aspektów bezpieczeństwa informacyjnego podczas zajęć edukacji wczesnoszkolnej związanych z różnymi obszarami tematycznymi.

Forma realizacji

Szkolenie ma charakter stacjonarny z możliwością realizacji w formie mieszanej (*blended learning*).

Czas trwania

25 godzin dydaktycznych

Liczebność grupy

Maksymalnie 14 osób

Uczestnicy

Szkolenie przeznaczone jest dla nauczycieli pierwszego etapu kształcenia (klas I–III SP) odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach.

Wymagania wstępne

Wymagana jest umiejętność posługiwania się komputerem i typowymi urządzeniami peryferyjnymi (klawiatura, monitor, mysz, drukarka) oraz pracy w środowisku Windows w zakresie: zarządzania folderami i plikami, uruchamiania programów, korzystania z podręcznych aplikacji Windows.



Przygotowanie do szkolenia obejmuje uczestnictwo w kursach online „Cyfrowe portfolio – bezpieczeństwo w komunikacji i w mediach” oraz „Cyfrowe portfolio – korzystanie z informacji” dostępnych na stronie: <https://e-kursy.ore.edu.pl/>. Zalecane jest ukończenie 1. modułu każdego z wymienionych kursów przed rozpoczęciem szkolenia oraz kontynuacja nauki na obu kursach online po jego ukończeniu.

Cele ogólne szkolenia

W części wstępnej:

- rozwijanie kompetencji merytorycznych poprzez zapoznanie nauczycieli z zagadnieniami dotyczącymi bezpieczeństwa informacyjnego w instytucjach oświatowych.

W części głównej:

- rozwijanie kompetencji medialnych i technicznych nauczycieli poprzez przygotowanie ich do wykorzystywania narzędzi technologii informacyjno-komunikacyjnych podczas organizowania zajęć związanych z bezpieczeństwem informacyjnym;
- przygotowanie nauczycieli klas I–III do włączania zagadnień dotyczących bezpieczeństwa informacyjnego w nauczanie uczniów w wieku wczesnoszkolnym.

Cele szczegółowe

W części wstępnej:

- poznanie przez nauczycieli typowych zagrożeń bezpieczeństwa informacyjnego w pracy i życiu prywatnym;
- przyswojenie podstawowych informacji związanych z prawami autorskimi i pokrewnymi w świetle działań placówki i nauczyciela;
- rozwijanie umiejętności ochrony danych osobowych uczniów, nauczycieli i innych pracowników placówki;
- poznanie przez nauczycieli sposobów organizowania działań profilaktycznych w placówce oświatowej;
- zapoznanie uczestników ze źródłami przydatnymi podczas organizowania działań mających na celu rozpowszechnianie wiedzy na temat bezpieczeństwa informacyjnego.



W części głównej:

- poznanie przez uczestników zasad bezpiecznej pracy z urządzeniami mobilnymi i komputerami koniecznych do wdrożenia w praktyce szkolnej;
- przyswojenie podstawowych informacji związanych z zastosowaniem w praktyce szkolnej praw autorskich i pokrewnych;
- dostrzeżenie zalet i wad internetu, jego najważniejszych zastosowań oraz określenie podstawowych zasad bezpiecznego korzystania z sieci;
- wykształcenie umiejętności reagowania na niebezpieczeństwa internetowe;
- przygotowanie do uzasadnienia konieczności ochrony danych osobowych;
- opanowanie umiejętności organizowania różnorodnych zajęć rozwijających nawyki i zachowania prowadzące do bezpiecznego korzystania z nowych technologii (w szczególności zabezpieczania danych oraz radzenia sobie z problemem obrażania w sieci);
- zapoznanie się z zapisami podstawy programowej dotyczącymi bezpieczeństwa informacyjnego w szkołach;
- przygotowanie do integrowania treści dotyczących bezpieczeństwa informacyjnego z wiedzą z różnych obszarów;
- zdobycie umiejętności wykorzystywania narzędzi technologii informacyjno-komunikacyjnych do organizowania zajęć związanych z bezpieczeństwem informacyjnym.

Treści kształcenia:

1. Bezpieczeństwo informacyjne w pracy i życiu prywatnym

- 1.1. Typowe zagrożenia bezpieczeństwa informacyjnego;
- 1.2. Źródła, z których nauczyciel może korzystać podczas organizowania działań mających na celu rozpowszechnianie wiedzy na temat bezpieczeństwa informacyjnego oraz budzenie świadomości istnienia zagrożeń;
- 1.3. Sposoby organizowania działań profilaktycznych w placówce oświatowej wśród pracowników i uczniów;
- 1.4. Przykłady przeznaczonych dla dzieci materiałów dotyczących bezpiecznego korzystania z komputera i internetu;
- 1.5. Bezpieczna praca z urządzeniami mobilnymi i komputerami;
- 1.6. Podstawa programowa a bezpieczeństwo informacyjne w szkołach;

2. Prawo autorskie w szkole i poza nią

- 2.1. Podstawowe informacje dotyczące praw autorskich i pokrewnych;
- 2.2. Pojęcie plagiatu w kontekście przygotowywania i publikowania autorских materiałów dydaktycznych;



- 2.3. Dozwolony użytek w edukacji;
- 2.4. Ochrona utworów z uwzględnieniem autorów nieletnich;
- 3. Ochrona danych osobowych**
 - 3.1. Konieczność ochrony danych osobowych;
 - 3.2. Ochrona danych osobowych uczniów i innych pracowników placówki;
 - 3.3. Ochrona wizerunku uczniów i nauczycieli;
 - 3.4. Zapoznanie z głównymi zmianami wdrażanymi w *Ogólnym Rozporządzeniu o Ochronie Danych Osobowych (RODO)*⁸, mającymi odniesienie do placówek edukacyjnych;
- 4. Internet i jego wykorzystanie**
 - 4.1. Najważniejsze zastosowania internetu;
 - 4.2. Zalety i wady internetu;
 - 4.3. Podstawowe zasady bezpiecznego korzystania z sieci;
 - 4.4. Reagowanie na niebezpieczeństwa internetowe (osoby i instytucje udzielające pomocy w razie problemów);
 - 4.5. Podstawowe sposoby zabezpieczania danych w internecie;
 - 4.6. Problem obrażania w sieci;
 - 4.7. Przykłady dobrych praktyk.

Rekomendowane formy i metody realizacji:

- wykład wzbogacony prezentacją (lub innymi materiałami multimedialnymi) oraz instruktaż służący zapoznaniu uczestników szkolenia z nowymi dla nich zagadnieniami;
- prezentacje każdego z uczestników przedstawiane całej grupie w celu upowszechnienia wypracowanych materiałów;
- praca indywidualna słuchacza;
- praca w grupach lub parach – wykonywanie ćwiczeń praktycznych i rozwiązywanie problemów;
- analiza tekstów dotyczących bezpieczeństwa informacyjnego;
- gry dydaktyczne – pozwalające zasugerować przykładowe metody pracy z uczniem;
- mapy myśli – służące wizualnemu opracowaniu omawianych zagadnień;
- dyskusje – pozwalające prowadzącemu i uczestnikom wymieniać się poglądami i doświadczeniami;
- rozmowy, testy, obserwacja działań uczestników szkolenia oraz analiza wypracowanych przez nich materiałów – jako metody sprawdzania zdobytej wiedzy.

⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.



Niezbędne oprogramowanie:

- system operacyjny Windows;
- przeglądarka internetowa – np. Firefox, Chrome;
- pakiet programów Microsoft Office;
- platforma e-learningowa (np. Moodle);
- darmowe aplikacje online używane podczas zajęć (np. Padlet, Autodraw).

Część wstępna

Działania nauczyciela a bezpieczeństwo informacyjne w placówce oświatowej



Czas trwania części: 7 godzin (w tym 2 godziny online)

Blok 1: Bezpieczeństwo informacyjne – podstawy

Cele operacyjne

Nauczyciel:

- potrafi definiować bezpieczeństwo informacyjne;
- zna zapisy podstawy programowej dotyczące bezpieczeństwa informacyjnego w szkole;
- umie rozpoznać podstawowe zagrożenia bezpieczeństwa informacyjnego i zna sposoby zapobiegania im;
- potrafi podejmować podstawowe działania profilaktyczne na rzecz bezpieczeństwa informacyjnego w szkole;
- zna zasady postępowania w przypadku wystąpienia zagrożeń bezpieczeństwa informacyjnego i potrafi zastosować je w praktyce;
- zna źródła, które może wykorzystać podczas organizowania działań mających na celu upowszechnianie wiedzy i pozwalających budować świadomość uczniów na temat istniejących zagrożeń;
- zna i potrafi stosować w praktyce podstawowe zasady bezpiecznej pracy z internetem.

Opis treści:

- rozumienie bezpieczeństwa informacyjnego;
- podstawa programowa a bezpieczeństwo informacyjne;
- podstawowe zagrożenia bezpieczeństwa informacyjnego;
- podstawowe działania na rzecz bezpieczeństwa informacyjnego w szkole i w życiu prywatnym;
- bezpieczna praca z internetem i zagrożenia z nim związane;
- sposoby zapobiegania poznanym zagrożeniom;
- systemowa interwencja i profilaktyka w środowisku szkolnym;
- zasady postępowania w przypadku wystąpienia zagrożeń bezpieczeństwa informacyjnego;
- źródła wiedzy na temat bezpieczeństwa informacyjnego.



Proponowane zasoby edukacyjne:

- Seria filmów edukacyjnych *Bezpieczeństwo dzieci i młodzieży online* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/bezpieczenstwo-dzieci-i-mlodziezy-online.html>;
- Blog „Dane osobowe”: *Kradzież tożsamości w Internecie* – <https://blog-daneosobowe.pl/kradziez-tozsamosci-w-internecie>;
- Praca zbiorowa, (2017), *Bezpieczne media. Poradnik dla rodziców*, Warszawa: Fundacja Dajemy Dzieciom Siłę (FDDS) i Fundacja Orange – https://www.edukacja.fdds.pl/fc63516e-e941-4d3c-827d-9febcbf076630/Extras/broszura_Dziecko-i-media-19-09-2017.pdf;
- Wojtasik Ł. (red.), (2013), *Jak reagować na cyberprzemoc. Poradnik dla szkół*, Warszawa: FDDS – https://www.edukacja.fdds.pl/fc63516e-e941-4d3c-827d-9febcbf076630/Extras/broszura_Dziecko-i-media-19-09-2017.pdf;
- Wójcik S. (oprac.), (2017), *Jak postępować w przypadku (cyber) przemocy? Systemowa interwencja i profilaktyka w szkole* (Wyciąg z materiałów klicksafe), Warszawa: FDDS – <https://www.saferinternet.pl/pliki/publikacje/Jak%20post%C4%99powa%C4%87%20w%20cyberprzemocy.pdf>;
- Czajka R., Lipszyc J., (2014), *Poradnik bezpieczeństwa mobilnego*, Warszawa: Fundacja Nowoczesna Polska – <https://edukacjamedialna.edu.pl/media/chunks/attachment/poradnik-bezpieczenstwa-mobilnego.pdf>;
- Rządowa strona „Bezpieczna Szkoła +”: *Promujemy bezpieczeństwo w sieci* – materiały i scenariusze zajęć – <https://bezpiecznaszkola.men.gov.pl/tematy/promujemy-bezpieczenstwo-w-sieci/informacje/>;
- Lizut J., Wrońska A. (red.), (2018), *Standard bezpieczeństwa online placówek oświatowych*, Warszawa: NASK – https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf;
- Strona „Cyfrowo Bezpieczni”: *Procedury bezpieczeństwa cyfrowego w szkołach* – pakiet dokumentów MEN – <https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Bezpieczeństwo informacji w sieci* – <https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci>;



- Praca zbiorowa, (2017), *Bezpieczna Szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, Warszawa: MEN – <http://bezpiecznaszkola.men.gov.pl/wp-content/uploads/2017/09/zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizyczne-go-i-cyfrowego-uczniow.pdf>;
- Zespół ekspertów NASK, (2017), *Jak zapewnić uczniom bezpieczeństwo w internecie – poradnik dla nauczycieli*, Warszawa: NASK – <https://akademia.nask.pl/pliki/1-jak-zapewnic-uczniom-bezpieczenstwo-w-internecie-poradnik-dla-nauczycieli.pdf>;
- Chocholska P. i in. (oprac.), (2017), *Jak reagować na problem nadmiernego korzystania z internetu przez dzieci i młodzież. Poradnik dla szkół*, Warszawa: FDDS – https://www.edukacja.fdds.pl/60d2a7cf-56e9-4281-a3d3-c9d4377ef098/Extras/ksiazka-jak_reagowac_na_problem_nadmiernego_korzystania_z_internetu-FDDS-12042017.pdf;
- Podstawa programowa dla poszczególnych typów szkół i etapów edukacyjnych wprowadzona w 2017 r. – <https://podstawaprogramowa.pl>.



Blok 2: Dane osobowe

Cele operacyjne

Nauczyciel:

- wie, czym są dane osobowe i w jaki sposób są chronione;
- zna zmiany w przepisach prawnych o ochronie danych osobowych wprowadzone w 2018 roku;
- zna praktyczne zastosowania zasad ochrony danych osobowych w życiu prywatnym i w szkole;
- potrafi chronić dane osobowe uczniów, nauczycieli i innych pracowników szkoły.

Opis treści:

- dane osobowe i powód ich ochrony;
- formy ochrony danych osobowych w Polsce i w Unii Europejskiej;
- *Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO)* – zmiany w ochronie danych osobowych wprowadzone w 2018 roku;
- obowiązujące przepisy prawa;
- zasady ochrony danych osobowych w życiu prywatnym i w szkole;
- ochrona danych osobowych uczniów, nauczycieli oraz innych pracowników szkół.

Proponowane zasoby edukacyjne:

- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Podstawy ochrony danych osobowych* – <https://cyfrowa-wyprawka.org/lekcja/podstawy-ochrony-danych-osobowych>;
- Strona Fundacji Panoptykon: cykl artykułów *RODO na tacy, czyli jak możemy skorzystać na nowych przepisach* – <https://panoptykon.org/rodo-na-tacy>;
- Strona The EU General Data Protection Regulation (GDPR) na temat RODO – <https://gdprexplained.eu/pl>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Wizerunek – jak chronić swoje prawa?* – <https://cyfrowa-wyprawka.org/lekcja/wizerunek-jak-chronic-swoje-prawa>;
- Serwis edukacyjny „DODO – dbamy o dane osobowe” – <http://dodo-bezpiecznie.blogspot.com/>;



- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak dzieci i młodzież chronią swoją prywatność?* – https://giodo.gov.pl/560/id_art/4699/j/pl;
- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak bezpiecznie zwiedzać cyfrowy świat?* – <https://giodo.gov.pl/pl/1520208/8510;>
- Wykład otwarty z cyklu „Lekcje z GODO” pt. *Elektroniczna dokumentacja szkolna i jej udostępnianie* – [https://www.youtube.com/watch?v=qwXla3bA1w8&feature=youtu.be.](https://www.youtube.com/watch?v=qwXla3bA1w8&feature=youtu.be)



Blok 3: Prawo autorskie

Cele operacyjne

Nauczyciel:

- wie, czym są prawa autorskie i prawa pokrewne;
- zna zasady korzystania z cudzych utworów;
- posiada praktyczną wiedzę na temat dozwolonego użytku edukacyjnego;
- potrafi chronić prawa autorskie, w tym także autorów nieletnich.

Opis treści:

- prawa autorskie i prawa pokrewne;
- obowiązujące przepisy prawne;
- dozwolony użytek edukacyjny;
- pojęcie plagiatu;
- prawa autorskie osoby nieletniej;
- prawa autorskie nauczyciela.

Proponowane zasoby edukacyjne:

- Czerniawski P., Lipszyc J., Wilkowski M., *Pierwsza pomoc w prawie autorskim: przewodnik*, Warszawa: Fundacja Nowoczesna Polska – <https://prawokultury.pl/publikacje/pierwsza-pomoc>;
- Poradnia na stronie „Prawokultury.pl”: *Pierwsza pomoc w prawie autorskim: zapytaj prawnika* – <https://prawokultury.pl/pierwsza-pomoc>;
- Strona „Prawokultury.pl”: *Krótki kurs własności intelektualnej. Materiały dla uczelni* – hasło: *Plagiat* – <https://prawokultury.pl/kurs/plagiat>;
- Siewicz K., (2016), *Prawo autorskie w edukacji: jak unikać naruszeń?*, Warszawa: Fundacja Nowoczesna Polska – <http://koed.org.pl/wp-content/uploads/2016/11/prawo-autorskie-w-edukacji-jak-unikac-naruszen-wersja-2016-1.pdf>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Prawo autorskie dla każdego* – <https://cyfrowa-wyprawka.org/lekcja/prawo-autorskie-dla-kazdego>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Jak etycznie publikować w sieci?* – <https://cyfrowa-wyprawka.org/lekcja/jak-etycznie-publikowac-w-sieci>.

Część główna

Bezpieczeństwo informacyjne ucznia



Czas trwania części: 18 godzin (w tym 3 godziny online)

Blok 1: Mały uczeń przy komputerze

Cele operacyjne

Nauczyciel:

- zna zasady bezpiecznej pracy z urządzeniami mobilnymi i komputerami oraz umie promować je wśród swoich uczniów;
- potrafi odnosić zagadnienia z różnych obszarów edukacyjnych do tematyki bezpieczeństwa informacyjnego;
- zna typowe zagrożenia bezpieczeństwa informacyjnego i potrafi wykorzystać tę wiedzę na zajęciach z uczniami w wieku wczesnoszkolnym;
- potrafi organizować działania promujące wiedzę z zakresu bezpieczeństwa informacyjnego wśród uczniów klas I–III;
- potrafi przekonać swoich uczniów o korzyściach płynących z wykorzystania różnorodnych mediów do nauki.

Opis treści:

- bezpieczna praca z urządzeniami mobilnymi i komputerami;
- uczenie się z pomocą mediów cyfrowych (i nie tylko);
- podstawa programowa a bezpieczeństwo informacyjne w szkołach;
- typowe zagrożenia bezpieczeństwa informacyjnego;
- źródła materiałów służących rozpowszechnianiu wiedzy na temat bezpieczeństwa informacyjnego wśród uczniów w wieku wczesnoszkolnym oraz budzeniu świadomości istnienia zagrożeń;
- przykłady materiałów przeznaczonych dla dzieci w wieku wczesnoszkolnym, dotyczących bezpiecznego korzystania z komputera i internetu oraz sposoby ich wykorzystywania na zajęciach w szkole.



Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Filmy z cyklu *Owce w sieci* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/owce-w-sieci.html>;
- Filmy z projektu edukacyjnego „Plik i Folder” – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/plik-i-folder.html>;
- Materiały edukacyjne z portalu „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/#sp1-3>;
- *Materiały instruktażowe dla uczniów szkół podstawowych, kl. I–III* z portalu „Cyfrowo bezpieczni” – <https://www.cyfrowobezpiecni.pl/strefa-ucznia/filmoteka/materialy-instruktażowe-dla-uczniow-szkol-podstawowych-kl1-3>;
- Portal „e-safety kit” – <http://www.esafetykit.net/index2.html>;
- Fundacja Dajemy Dzieciom Siłę, (2012), *Necio.pl – zabawa w internet. Zeszyt ćwiczeń*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/3ccaca09-feab-4c78-a384-268274e0cee1/Extras/broszura-necio-zeszyt-cwiczen-FDDS-12042017.pdf>;
- Film animowany *Mój przyjaciel Necio* – <https://www.edukacja.fdds.pl/3ccaca09-feab-4c78-a384-268274e0cee1/Extras/necio-bajka-small.mp4>;
- Piękoś A., (2012), *Necio.pl – zabawa w internet. Zestaw materiałów edukacyjnych dla dzieci w wieku 4–6 lat na temat bezpieczeństwa w sieci*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/3ccaca09-feab-4c78-a384-268274e0cee1/Extras/necio-scenariusz2017.pdf>.



Blok 2: Bezpiecznie w sieci

Cele operacyjne

Nauczyciel:

- umie planować i organizować zajęcia, wykorzystując treści przekazywane za pomocą różnych mediów (także internetu) do uczenia się;
- zna zalety i wady internetu oraz potrafi wykorzystać tę wiedzę na zajęciach z uczniami w wieku wczesnoszkolnym;
- potrafi zorganizować zajęcia pozwalające uczniom zapoznać się podstawowymi zasadami bezpiecznego korzystania z internetu (w tym szukania pomocy w sytuacjach problematycznych);
- potrafi zorganizować zajęcia pozwalające uczniom zapoznać się podstawowymi zasadami zabezpieczania danych w internecie.

Opis treści:

- najważniejsze zastosowania internetu;
- zalety i wady internetu;
- podstawowe zasady bezpiecznego korzystania z sieci;
- reagowanie na niebezpieczeństwa internetowe (osoby i instytucje udzielające pomocy w problematycznych sytuacjach);
- podstawowe sposoby zabezpieczania danych w internecie;
- problem obrażania w sieci;
- przykłady dobrych praktyk.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Materiały edukacyjne z portalu „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/#sp1-3>;
- Portal „e-safety kit” – <http://www.esafetykit.net/index2.html>;
- Strona „Bezpieczny Internet”: kurs *Edukacja w zakresie bezpieczeństwa w sieci* – <http://www.orange.pl/bezpiecznie-tu-i-tam.phtml>;
- Cykl filmów animowanych z portalu Sieciaki.pl *Zasady bezpiecznego korzystania z internetu* – https://www.edukacja.fdds.pl/?option=com_szkolenia&tekst=Sieciaki.pl+%E2%80%93+Zasady+bezpiecznego+korzystania+z+internetu.&-criteria=&blotem=&search=szukaj;



- Leszczyńska I., Ćwiek M. (oprac.), (2017), *Sieciaki.pl. Poznaj bezpieczny internet! Scenariusze zajęć edukacyjnych dla uczniów klas I–III oraz IV–VI szkoły podstawowej na temat bezpieczeństwa w sieci*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/9e0b89e2-561c-48af-b88f-639f63ba6120/Extras/Sieciaki-pl-Poznaj-bezpieczny-internet-zestaw-scenariuszy.pdf>;
- Magazyn dla uczniów *Sieciaki.pl. Poznaj bezpieczny internet!* – <http://edukacja.fdds.pl/66c0c787-d59d-4c06-9f87-4b4f05a625ed/Extras/Magazyn-Sieciaki-Poznaj-Bezpieczny-Internet.pdf>;
- NASK, *Przygody Plika i Foldera w sieci* – materiały dla nauczycieli i rodziców – https://www.saferinternet.pl/pliki/publikacje/nowa_ksiazeczka%20web.pdf;
- Best – Katalog Bezpiecznych Stron portalu „Sieciaki.pl” – <https://sieciaki.pl/best>;
- Piękoś A., (2017), *Zużka i Tunio poznają internet. Scenariusz zajęć na temat bezpieczeństwa w sieci dla uczniów klas II–IV szkół podstawowych*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/faf48471-5d99-4665-84c3-7472bb-d5e476/Extras/scenariusz-Zuzka-i-Tunio-FDDS-25042017.pdf>;
- *Owce w sieci. Podręcznik dla nauczycieli* – <https://www.edukacja.fdds.pl/77c20b1c-901f-4a43-9713-5ca705d1eb24/Extras/scenariusz-owce-w-sieci-FDDS-07042017.pdf>.



Blok 3: Ochrona danych osobowych

Cele operacyjne

Nauczyciel:

- potrafi planować i organizować zajęcia wspierające ucznia w dbaniu o ochronę własnych i cudzych danych osobowych;
- zna podstawowe sposoby zabezpieczania danych w internecie;
- potrafi kształtować w uczniach świadomość podstawowych zasad bezpiecznego korzystania z internetu w tym zabezpieczania danych.

Opis treści:

- ochrona danych osobowych uczniów i pracowników placówki;
- ochrona wizerunku uczniów i nauczycieli;
- podstawowe zasady bezpiecznego korzystania z sieci;
- podstawowe sposoby zabezpieczania danych w internecie.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Serwis edukacyjny „DODO – dbamy o dane osobowe” – <http://dodo-bezpiecznie.blogspot.com/>;
- Film *Chroń swoją prywatność* – https://www.edukacja.fdds.pl/411629a7-8510-424a-9bca-639c3774a7cb/Extras/film1_Chron_swoja_prywatnosc.mp4;
- Strona Generalnego Inspektora Ochrony Danych Osobowych – prace konkursowe – <https://giodo.gov.pl/pl/1520186/7645>;
- Strona „Cyfrowo bezpieczni”: *Materiały instruktażowe dla uczniów szkół podstawowych, kl. I–III* – <https://www.cyfrowobezpiecni.pl/strefa-ucznia/filmoteka/materiały-instruktażowe-dla-uczniow-szkol-podstawowych-kl1-3>.



Blok 4: Podstawy prawa autorskiego dla najmłodszych

Cele operacyjne

Nauczyciel:

- potrafi organizować zajęcia dotyczące różnych obszarów edukacyjnych, prezentujące w praktyce zasady korzystania z cudzych utworów.

Opis treści:

- ochrona utworów przygotowanych przez uczniów;
- podstawowe zasady dotyczące wykorzystania dozwolonego użytku edukacyjnego;
- pojęcie plagiatu.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Strona „Prawo Autorskie? OK” – <http://pa.ok.oeiizk.waw.pl>;
- Platforma edukacyjna Fundacji Dajemy Dzieciom Siłę: szkolenie 3... 2... 1... Internet! – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=9&fnd=&-grupa=0&offset=1&sort=1&szkolenie=1122&tekst=1122#opisszkolenia;
- Strona „Cyfrowo bezpieczni”: *Materiały instruktażowe dla uczniów szkół podstawowych, kl. IV–VI* – <https://www.cyfrowobezpieczni.pl/strefa-ucznia/filmoteka/materiały-instruktażowe-dla-uczniow-szkol-podstawowych-kl4-6>.

Przykładowy rozkład treści



Część wstępna (7 godzin)				
<i>Działania nauczyciela a bezpieczeństwo informacyjne w placówce oświatowej</i>				
Blok	Tytuł bloku	Ilość godzin		Treści kształcenia
		stacjonarnych	online	
1	<i>Nauczyciel i bezpieczeństwo informacyjne – podstawy</i>	3	1	1.1, 1.2, 1.3, 1.4, 1.6
2	<i>Prawo autorskie</i>	1	0,5	2.1, 2.2, 2.3, 2.4
3	<i>Dane osobowe</i>	1	0,5	3.1, 3.2, 3.3, 3.4
	Razem godzin	5	2	

Część główna (18 godzin)				
<i>Bezpieczeństwo informacyjne ucznia</i>				
Blok	Tytuł bloku	Ilość godzin		Treści kształcenia
		stacjonarnych	online	
1	<i>Mały uczeń przy komputerze</i>	5	1	1.1, 1.2, 1.4, 1.5, 1.6
2	<i>Bezpiecznie w sieci</i>	5	1	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7
3	<i>Ochrona danych osobowych</i>	3	0,5	3.1, 3.2, 3.3, 4.3, 4.5
4	<i>Podstawy prawa autorskiego dla najmłodszych</i>	2	0,5	2.1, 2.3, 2.3, 2.4
	Razem godzin	15	3	

Przykładowe scenariusze zajęć



Scenariusz zajęć nr 1

Część zajęć: Część wstępna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 1 – *Mały uczeń przy komputerze*

Temat zajęć: *Neciowe bajki i gry, które uczą*

Czas zajęć: 90 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić uczniom zasady pracy z urządzeniami mobilnymi i komputerami;
- łączyć zagadnienia z różnych obszarów edukacyjnych z tematyką bezpieczeństwa informacyjnego;
- przekonać swoich uczniów o korzyściach płynących z wykorzystywania różnorodnych mediów w trakcie nauki.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca indywidualna uczestników przy komputerze;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- aplikacja online – np. Padlet (lub analogiczna);
- edytor tekstu;
- platforma e-learningowa.



Zasoby do wykorzystania:

- Bajka edukacyjna *Mój przyjaciel Necio* – <https://youtu.be/lai4XRxyNgs>;
- Gry ze strony „Necio.pl – zabawa w internet” – <http://necio.pl/>.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej. Powstałe fragmenty opowieści zostaną ocenione przez współuczestników szkolenia zgodnie z kryteriami ustalonymi wspólnie przez prowadzącego i uczestników.

Przebieg zajęć:

1. Przedstawienie Necia
Uczestnicy oglądają animowany film opowiadający o Neciu – robocie wprowadzającym dzieci w świat internetu i nowych technologii <https://www.youtube.com/watch?v=lai4XRxyNgs&feature=youtu.be>, a następnie rozmawiają na temat możliwości wykorzystania bajek filmowych do zapoznawania uczniów z tematyką bezpieczeństwa informacyjnego.
2. Dokończenie historii Necia
Nauczyciele pracują w małych grupach. Mają za zadanie dopisać dalszą część opowieści, w której Necio będzie przedstawiał dzieciom zasady bezpiecznej pracy z urządzeniami mobilnymi i komputerami. Przed przystąpieniem do pracy wspólnie opracowują kryteria oceny (np. NaCoBeZu – „na co będę zwracał uwagę” – zaczerpnięte z oceny kształtującej).
3. Reguły bezpieczeństwa
Wszyscy uczestnicy biorą udział w burzy mózgów, wypisując w języku przystępnym dla uczniów podstawowe zasady pracy z wymienionymi urządzeniami na e-tablicy stworzonej np. na platformie Padlet. Wspólnie z prowadzącym omawiają zapisane zasady i segregują je, wyodrębniając kategorie.
4. Rozwijanie fabuły
Każda grupa pisze dalszy ciąg opowieści o Neciu w taki sposób, by wydarzenia przedstawiały zasady z jednej, wybranej przez grupę, kategorii.



5. Ocena opowieści dydaktycznych

Gotowe teksty zostają udostępnione pozostałym grupom i poddane ocenie (każda grupa ocenia inną opowieść) według wcześniej ustalonych kryteriów. Członkowie grup dokonują ewentualnej korekty swoich tekstów.

6. Gry dla dzieci w serwisie „Necio.pl”

Zadaniem każdego z uczestników szkolenia jest przetestowanie kilku gier z serwisu „Necio.pl” i zastanowienie się, w jaki sposób można wykorzystać ich potencjał edukacyjny przy organizowaniu zajęć dotyczących bezpiecznego korzystania z komputerów i internetu.

7. Wykorzystanie materiałów z serwisu „Necio.pl” – bank pomysłów

Nauczyciele pracują w tych samych grupach, w których tworzyli opowieści. Ich zadanie polega na stworzeniu propozycji wykorzystania napisanych bajek oraz wybranych gier z serwisu „Necio.pl” na zajęciach z uczniami. Pomysły są przedstawiane na forum całej grupy szkoleniowej. Uczestnicy i prowadzący komentują pomysły, przekazują informację zwrotną.

8. Podsumowanie zajęć

Nauczyciele zastanawiają się, które z metod i form pracy zaprezentowanych w czasie szkolenia mogą okazać się szczególnie przydatne w pracy z uczniami klas I–III. Prezentują własne spostrzeżenia, pomysły i inspiracje płynące z zajęć, rozmawiając na forum grupy szkoleniowej.



Scenariusz zajęć nr 2

Część zajęć: Część wstępna – Bezpieczeństwo informacyjne ucznia

Blok tematyczny: Blok 1 – Mały uczeń przy komputerze

Temat zajęć: Neciowe rady

Czas zajęć: 45 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- organizować działania promujące wiedzę z zakresu bezpieczeństwa informacyjnego wśród uczniów w wieku wczesnoszkolnym;
- łączyć zagadnienia z różnych obszarów edukacyjnych z tematyką bezpieczeństwa informacyjnego;
- wykorzystywać wiedzę o typowych zagrożeniach bezpieczeństwa informacyjnego w czasie zajęć z uczniami w wieku wczesnoszkolnym.

Metody nauczania:

- rozmowa;
- praca w parach;
- inscenizacja;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- szkolenia komputer z przeglądarką internetową dla każdego uczestnika;
- urządzenie z kamerą (np. laptop z kamerą internetową, tablet).

Zasoby do wykorzystania:

- Gra karciana „Bezpiecznie tu i tam”:
<http://www.orange.pl/ocp-http/PL/Binary2/2005906/4108095955.pdf>;



- Kartonowa postać Necia z 2. strony zeszytu ćwiczeń *Necio.pl* – zabawa w internet: <https://www.edukacja.fdds.pl/3ccaca09-feab-4c78-a384-268274e0cee1/Extras/broszura-necio-zeszyt-cwiczen-FDDS-12042017.pdf>.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Rozmowa

Uczestnicy szkolenia przedstawiają swoje pomysły i doświadczenia związane z tym, w jaki sposób przedstawiać uczniom korzyści i niebezpieczeństwa wynikające z wykorzystywania różnych mediów (w tym internetu) oraz jak sprawdzać wiedzę uczniów na ten temat?

2. Gra karciana „Bezpiecznie tu i tam”

Prowadzący przypomina uczestnikom szkolenia, że jednym ze sposobów uświadomienia uczniom wad i zalet mediów jest wykorzystanie gier edukacyjnych – np. z serwisu „Necio.pl”. Prezentuje nową grę edukacyjną „Bezpiecznie tu i tam” i zachęca uczestników do zagrania w nią. Uczestnicy łączą się w pary, testują grę, a na koniec wymieniają się opiniami na jej temat i pomysłami na jej wykorzystanie w czasie zajęć z uczniami. Omawiają zagadnienia przedstawiane w kartach. Zastanawiają się, w jaki sposób budować właściwe postawy uczniów?

3. Scenariusze z Neciem

Prowadzący przedstawia pomysł wykorzystania kart gry podczas kręcenia przez dzieci krótkich filmów dotyczących bezpieczeństwa informacyjnego. Tym razem rolę uczniów przyjmują uczestnicy szkolenia. Zadanie polega na wylosowaniu jednej z kart i przygotowaniu w parach krótkiej inscenizacji, w której wystąpi postać robota Necia prezentująca wylosowane na karcie zagadnienie w formie przystępnej dla dzieci.

4. Kręcenie filmików

Każda para otrzymuje tekturową postać robota Necia (w zależności od czasu i możliwości już przygotowaną lub w postaci szablonu do wycięcia i sklejenia), mocuje ją na ołówku w taki sposób, aby stała się ona kukiełką, która



będzie występowała w filmie. Uczestnicy nagrywają próbną wersję filmu, testując ustawienia (oświetlenie, odległość od mikrofonu, rodzaj planu itd.), a następnie przystępują do nagrywania właściwych filmików. Każde z nagrań powinno trwać nie dłużej niż minutę i składać się tylko z jednego ujęcia, tak aby niepotrzebna była już dodatkowa edycja wideo.

5. Prezentacja filmów lub scenek

Gotowe filmy są wyświetlane przy pomocy projektora na forum całej grupy szkoleniowej, a następnie omawiane przez prowadzącego i uczestników szkolenia. W przypadku niemożności wykorzystania urządzeń nagrywających zamiast filmów prezentowane są inscenizacje kukiełkowe na żywo.

6. Podsumowanie zajęć

Nauczyciele zastanawiają się, w jaki sposób zorganizować z uczniami zajęcia oparte na nagrywaniu filmów? Na co zwracać uwagę, aby cele zajęć zostały osiągnięte? Jak łączyć zagadnienia dotyczące bezpieczeństwa informacyjnego z zajęciami dotyczącymi różnych obszarów tematycznych?

Wskazówki, do pracy z małymi filmowcami:

- uczniowie powinni przeanalizować przykładowe filmy, aby lepiej zrozumieć język, jakim posługuje się film;
- należy dać uczniom czas na ćwiczenia praktyczne z kamerą;
- warto zainicjować burzę mózgów i dyskusję, zaangażować całą grupę;
- im starsi są uczniowie, tym mniejszy powinien być zakres pomocy nauczyciela;
- uczniowie zaczynają pracę od etapu planowania – faza ta decyduje o wynikach pracy nad projektem;
- scenariusz może zastąpić krótkie opowiadanie z zarysem historii, szczegóły rozplanujemy wówczas, tworząc scenorys;
- uczniowie powinni mieć jasno określone zadania do wykonania w projekcie – trzeba je przydzielać z namysłem, angażując wszystkich: każdy jest ważny bez względu na to, jaką rolę pełni;
- współpraca uczniów jest podstawą ich sukcesu – tworząc filmy, mogą oni nauczyć się pracy w zespole;
- uczniowie kończą pracę wtedy, gdy dokonają jej ewaluacji i wprowadzą ewentualne poprawki – należy zaplanować czas na ten etap;
- zagadnienia dotyczące bezpieczeństwa informacyjnego mogą być poruszane w czasie różnych lekcji i aktywności uczniów, także tych związanych z pracą nad filmem (np. zajęcia techniczne, muzyczne, lekcje języka polskiego czy przyrody).



Scenariusz zajęć nr 3

Część zajęć: Część wstępna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 2 – *Bezpiecznie w sieci*

Temat zajęć: *Podstawowe zasady bezpiecznego korzystania z internetu*

Czas zajęć: 45 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- planować i organizować zajęcia wykorzystujące treści pochodzące z różnych mediów (w tym internetowe) do nauki;
- zorganizować zajęcia pozwalające uczniom zapoznać się podstawowymi zasadami bezpiecznego korzystania z internetu;
- wykorzystać przykłady dobrych praktyk do planowania własnych zajęć.

Metody nauczania:

- rozmowa;
- instruktaż;
- praca w parach;
- praca z tekstem;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- program pozwalający na graficzne opracowanie rebusów – np. PowerPoint.

Zasoby do wykorzystania:

- Materiały ze strony: <https://sieciaki.pl/sieciomisja/zasady-bezpieczenstwa>;
- *Przygody Plika i Foldera w sieci* – materiały dla nauczycieli
https://www.saferinternet.pl/pliki/publikacje/nowa_ksiazeczka%20web.pdf.



Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Podanie tematu zajęć za pomocą rebusu
Prowadzący przedstawia temat zajęć: *Podstawowe zasady bezpiecznego korzystania z internetu* w formie rebusu do rozwiązania. Omawiając go, nauczyciele zastanawiają się, jakich zasad dotyczy? Na czym polega ich przestrzeganie? W jaki sposób nasi uczniowie powinni je wdrażać?
2. Przygotowanie rebusów
Prowadzący proponuje uczestnikom szkolenia opracowanie rebusów szyfrujących podstawowe zasady bezpieczeństwa w sieci (listę reguł można sformułować samodzielnie lub wykorzystać np. te dostępne na stronie <https://sieciaki.pl/sieciomisja/zasady-bezpieczenstwa>). Następnie prowadzący przedstawia zasady tworzenia rebusów i omawia wykorzystanie wybranych narzędzi do ich tworzenia (np. programu PowerPoint). Każdy z uczestników losuje jedną z reguł i wykonuje rebus, który ją ilustruje. Gotowe rebusy zostają udostępnione pozostałym uczestnikom.
3. Dyskusja
Uczestnicy szkolenia dyskutują w parach, w jaki sposób tworzenie rebusów przez uczniów może wspomagać zapamiętywanie przez nich innych zagadnień związanych z bezpieczeństwem informacyjnym. Dlaczego warto utrwalać wiedzę uczniów z pomocą rebusów? Na co zwracać uwagę w trakcie pracy? Uczestnicy dzielą się swoimi przemyśleniami z pozostałymi kursantami.
4. Ćwiczenia dla uczniów
Zadaniem uczestników kursu jest dobranie dla swoich uczniów ćwiczeń pozwalających zrozumieć i utrwalić omawiane zasady. Pracę w parach zaczynają od przejrzania przykładowych ćwiczeń zawartych w materiałach szkoleniowych dostępnych dla nauczycieli: (np. *Przygody Plika i Foldera w sieci* – https://www.saferinternet.pl/pliki/publikacje/nowa_ksiazeczka%20web.pdf).



5. Poszukiwanie inspiracji

Zadanie polega na znalezieniu w internecie takich ćwiczeń, które mogłyby zainspirować do stworzenia własnych lub które można byłoby wykorzystać do realizacji danego celu dydaktycznego (jest nim zrozumienie i utrwalenie omawianych zasad bezpiecznego korzystania z internetu). Wyszukane i zaadaptowane ćwiczenia są następnie prezentowane pozostałym uczestnikom, omawiane i poddawane krytycznej ocenie.

6. Podsumowanie zajęć

Uczestnicy omawiają problemy, które mogą się pojawić w czasie realizowania z uczniami zajęć na temat zasad bezpieczeństwa w internecie wykorzystujących proponowane metody pracy, oraz zbierają pomysły na ich rozwiązanie.



Scenariusz zajęć nr 4

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 2 – *Bezpiecznie w sieci*

Temat zajęć: *Scenariusze lekcji*

Czas zajęć: 45 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- zorganizować zajęcia pozwalające uczniom opanować podstawowe zasady bezpiecznego korzystania z internetu (w tym szukania pomocy w razie problemów);
- zorganizować zajęcia pozwalające uczniom poznać podstawowe zasady zabezpieczania danych w internecie;
- wykorzystywać przykłady dobrych praktyk.

Metody nauczania:

- rozmowa;
- praca z tekstem;
- praca grupowa;
- praca indywidualna uczestników przy komputerach;
- pokaz.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer podłączony do internetu dla każdego uczestnika szkolenia wyposażony w przeglądarkę internetową i pakiet programów Microsoft Office;
- platforma e-learningowa.



Zasoby do wykorzystania:

- Piękoś A., (2017), *Zużka i Tunio poznają internet. Scenariusz zajęć na temat bezpieczeństwa w sieci dla uczniów klas II–IV szkół podstawowych*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/faf48471-5d99-4665-84c3-7472bbd5e476/Extras/scenariusz-Zuzka-i-Tunio-FDDS-25042017.pdf>;
- *Owce w sieci. Podręcznik dla nauczycieli* – <https://www.edukacja.fdds.pl/77c20b1c-901f-4a43-9713-5ca705d1eb24/Extras/scenariusz-owce-w-sieci-FDDS-07042017.pdf>;
- Leszczyńska I., Ćwiek M. (oprac.), (2017), *Sieciaki.pl. Poznaj bezpieczny internet! Scenariusze zajęć edukacyjnych dla uczniów klas I–III oraz IV–VI szkoły podstawowej na temat bezpieczeństwa w sieci*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/9e0b89e2-561c-48af-b88f-639f63ba6120/Extras/Sieciaki-pl-Poznaj-bezpieczny-internet-zestaw-scenariuszy.pdf>.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Wprowadzenie
Prowadzący przedstawia temat zajęć: *Jak sobie radzić z cyberprzemocą?*
2. Przegląd i ocena materiałów
Uczestnicy szkolenia, pracując samodzielnie, przeglądają przydzielone przez prowadzącego zestawy scenariuszy dotyczące omawianej tematyki. Każdy uczestnik analizuje jeden zestaw.
3. Prowadzący prezentuje przykładowe dokumenty zawierające wzorcowe scenariusze:
 - Piękoś A., (2017), *Zużka i Tunio poznają internet. Scenariusz zajęć na temat bezpieczeństwa w sieci dla uczniów klas II–IV szkół podstawowych*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/faf48471-5d99-4665-84c3-7472bbd5e476/Extras/scenariusz-Zuzka-i-Tunio-FDDS-25042017.pdf>;
 - *Owce w sieci. Podręcznik dla nauczycieli* – <https://www.edukacja.fdds.pl/77c20b1c-901f-4a43-9713-5ca705d1eb24/Extras/scenariusz-owce-w-sieci-FDDS-07042017.pdf>;



- Leszczyńska I., Ćwiek M. (oprac.), (2017), *Sieciaki.pl. Poznaj bezpieczny internet! Scenariusze zajęć edukacyjnych dla uczniów klas I–III oraz IV–VI szkoły podstawowej na temat bezpieczeństwa w sieci*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/9e0b89e2-561c-48af-b88f-639f63ba6120/Extras/Sieciaki-pl-Poznaj-bezpieczny-internet-zestaw-scenariuszy.pdf>.
4. Zadaniem każdego z uczestników jest wskazanie scenariusza, który mógłby zostać bez trudu zrealizowany w pracy z jego uczniami. Do nazwy scenariusza nauczyciele dołączają komentarz wyjaśniający wybór i opis zmian, które należy wprowadzić, aby możliwe było wykorzystanie danego pomysłu w konkretnych realiach. Nauczyciele dzielą się swoimi pomysłami na adaptację scenariuszy na forum całej grupy, przedstawiają nowe koncepcje zainspirowane omawianymi scenariuszami, wymieniają się uwagami, wspierają.
 5. Pisanie własnych scenariuszy
Uczestnicy zostają podzieleni na grupy 3–4 osobowe zgodnie z poziomem klas, w których aktualnie uczą. Zadaniem każdej grupy jest napisanie ramowego scenariusza zajęć dla danego poziomu klasy. Konspekty muszą być dostosowane do wieku i możliwości uczniów, powinny integrować treści z różnych obszarów edukacyjnych oraz dotyczyć jednego zaproponowanych przez prowadzącego tematów np.: *Reagowanie na niebezpieczeństwa internetowe (osoby i instytucje udzielające pomocy w razie problemów)*, *Podstawowe sposoby zabezpieczania danych w internecie*, *Problem obrażania w sieci*.
 6. Prezentacja scenariuszy
Gotowe scenariusze są publikowane w e-portfolio szkolenia (repozytorium przydatnych materiałów – np. założonym na platformie e-learningowej) dostępnym dla wszystkich uczestników szkolenia i prezentowane na forum grupy szkoleniowej, a kursanci poddają je ocenie.
 7. Podsumowanie zajęć
Uczestnicy zajęć zastanawiają się, w jaki sposób można wykorzystać w pracy z uczniami doświadczenia zdobyte podczas opracowywania materiału. Omawiają problemy, które mogą się pojawić w czasie realizacji zajęć związanych z tą tematyką, oraz zbierają pomysły służące ich rozwiązaniu.



Scenariusz zajęć nr 5

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 4 – *Podstawy prawa autorskiego dla najmłodszych*

Temat zajęć: *Dlaczego chronimy prawa autorskie?*

Czas zajęć: 45 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- organizować zajęcia dotyczące różnych obszarów edukacyjnych, wykorzystujące w praktyce zasady korzystania z cudzych utworów.

Metody nauczania:

- rozmowa;
- instruktaż;
- praca w parach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- program do tworzenia prostych grafik np. aplikacja online AutoDraw.

Zasoby do wykorzystania:

Film *Rysunek Oli* – <https://www.youtube.com/watch?v=5MKRPkDqx-4>.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.



Przebieg zajęć:

1. Rozmowa o prawach autorskich

Prowadzący inicjuje rozmowę, zadając pytania: W jaki sposób przedstawiać uczniom temat prawa autorskiego? Jak wyjaśniać dlaczego chronimy prawa autora?

2. Prezentacja filmu

Prowadzący wyświetla film *Rysunek Oli* – <https://www.youtube.com/watch?v=5MKRPkDqx-4>, podkreślając, że służy on wykorzystaniu emocji uczniów do zrozumienia tematu. Uczestnicy zastanawiają się, jak uczyć, opierając się na emocjach? Wymieniają opinie i doświadczenia, formułują wskazówki.

3. Dozwolony użytek edukacyjny

Prowadzący przedstawia miniwykład mający na celu przypomnienie zasad dozwolonego użytku edukacyjnego. Nauczyciele w parach zastanawiają się, w jakich sytuacjach edukacyjnych powinni przekazywać wiedzę na temat prawa autorskiego. Dzielą się swoimi pomysłami na forum grupy i omawiają je.

4. Tworzenie materiałów

Prowadzący instruuje uczestników w zakresie opracowywania różnorodnych materiałów multimedialnych zgodnie z zasadami prawa autorskiego. Pokazuje, jak tworzyć plakaty z pomocą wybranego narzędzia – np. aplikacji online AutoDraw. Uczestnicy kursu, pracując w parach, przygotowują krótkie przewodniki w formie plakatów wizualizujących etapy postępowania w przypadku:

- tworzenia przez uczniów prezentacji multimedialnej na podstawie materiałów z internetu (adaptowanie cudzych zdjęć, tekstów, filmów);
- przygotowania krótkiego tekstu na podstawie materiałów z internetu (korzystanie z cudzych materiałów tekstowych i grafiki, cytowanie);
- montowania krótkiego filmiku (wykorzystanie cudzej muzyki, grafiki, ochrona wizerunku).

5. Prezentowanie gotowych prac

Po zaprezentowaniu przez uczestników wykonanych prac prowadzący zachęca do rozmowy, pytając, jak można wykorzystać w praktyce szkolnej stworzone przez nauczycieli plakaty? Dlaczego warto wdrażać uczniów od najmłodszych lat do zgodnego z prawem wykorzystywania cudzych utworów?



6. Podsumowanie zajęć

Uczestnicy zajęć przedstawiają, w jaki sposób można wykorzystać doświadczenia związane z opracowaniem materiału w pracy z uczniami. Omawiają problemy, które mogą się pojawić w czasie zajęć dotyczących tej tematyki, obmyślają sposoby ich rozwiązania.

Ramowy program szkoleń

dla nauczycieli drugiego etapu kształcenia (klasy IV–VI SP)
odpowiedzialnych za nauczanie w zakresie bezpieczeństwa
informacyjnego w szkołach



Informacje ogólne

Program szkolenia został opracowany w taki sposób, aby mogło ono służyć przygotowaniu nauczycieli szkół podstawowych nauczających w klasach IV–VI do wdrażania wybranych aspektów bezpieczeństwa informacyjnego podczas zajęć różnych przedmiotów, a szczególnie informatyki.

Forma realizacji

Szkolenie jest realizowane w formie mieszanej (*blended learning*).

Czas trwania

25 godzin dydaktycznych (w tym godzin 5 online)

Liczebność grupy

Maksymalnie 14 osób

Uczestnicy

Szkolenie przeznaczone jest dla nauczycieli drugiego etapu kształcenia (klasy IV–VI szkoły podstawowej) odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach.

Wymagania wstępne

Wymagana jest umiejętność posługiwania się komputerem i typowymi urządzeniami peryferyjnymi (klawiatura, monitor, mysz, drukarka) i pracy w środowisku Windows w zakresie zarządzania folderami i plikami, uruchamiania programów, korzystania z podręcznych aplikacji Windows.

Przygotowanie do szkolenia obejmuje uczestnictwo w kursach online „Bezpieczeństwo w komunikacji i w mediach” oraz „Korzystanie z informacji” dostępnych



na stronie <https://e-kursy.ore.edu.pl/>. Zalecane jest ukończenie 1. modułu każdego z wymienionych kursów przed rozpoczęciem szkolenia oraz kontynuacja nauki na obu kursach online po jego ukończeniu.

Cele ogólne szkolenia

W części wstępnej:

- rozwijanie kompetencji merytorycznych nauczycieli poprzez zapoznanie ich z zagadnieniami dotyczącymi bezpieczeństwa informacyjnego w instytucjach oświatowych.

W części głównej:

- rozwijanie kompetencji medialnych i technicznych nauczycieli poprzez przygotowanie ich do wykorzystywania narzędzi technologii informacyjno-komunikacyjnych przy organizowaniu zajęć związanych z bezpieczeństwem informacyjnym;
- przygotowanie nauczycieli klas I–III do włączania zagadnień dotyczących bezpieczeństwa informacyjnego w nauczanie uczniów w wieku wczesnoszkolnym.

Cele szczegółowe:

- dostrzeżenie przez nauczycieli typowych zagrożeń bezpieczeństwa informacyjnego w pracy i życiu prywatnym;
- rozwinięcie umiejętności krytycznej analizy informacji znalezionych w sieci;
- poznanie podstawowych regulacji z zakresu prawa autorskiego i praw pokrewnych w kontekście działań placówki i nauczyciela;
- wykształcenie umiejętności ochrony danych osobowych uczniów, nauczycieli i innych pracowników placówki;
- opanowanie podstawowych sposobów zabezpieczania danych w internecie;
- poznanie zasad bezpiecznej pracy z internetem oraz zagrożeń z nim związanych;
- określenie podstawowych rozwiązań w przypadku zetknięcia się z zagrożeniem w sieci;
- zapoznanie się z zapisami nowej postawy programowej dotyczącymi bezpieczeństwa informacyjnego w szkołach;
- przygotowanie do wykorzystywania narzędzi technologii informacyjno-komunikacyjnych podczas organizowania zajęć związanych z bezpieczeństwem informacyjnym.



Treści kształcenia:

1. **Bezpieczeństwo informacyjne w szkole i poza nią**
 - 1.1. Kierunki rozwoju mediów elektronicznych i zagrożenia z nimi związane;
 - 1.2. Typowe zagrożenia bezpieczeństwa informacyjnego;
 - 1.3. Podstawa programowa a bezpieczeństwo informacyjne w szkołach;
 - 1.4. Sposoby organizowania w placówce oświatowej działań profilaktycznych wśród pracowników i uczniów;
 - 1.5. Źródła, z których nauczyciel może korzystać organizując działania mające na celu rozpowszechnianie wiedzy na temat bezpieczeństwa informacyjnego oraz budzenie świadomości istnienia zagrożeń;
2. **Prawa autorskie i prawa pokrewne**
 - 2.1. Informacje podstawowe;
 - 2.2. Pojęcie plagiatu w kontekście przygotowywania i publikowania autorskich materiałów dydaktycznych;
 - 2.3. Dozwolony użytek w edukacji;
 - 2.4. Ochrona utworów z uwzględnieniem praw autorów nieletnich;
3. **Ochrona danych osobowych**
 - 3.1. Ochrona danych osobowych uczniów i innych pracowników placówki;
 - 3.2. Ochrona wizerunku uczniów i nauczycieli;
 - 3.3. Zapoznanie z głównymi zmianami wdrażanymi w RODO, mającymi odniesienie do placówek edukacyjnych;
 - 3.4. Podstawowe sposoby zabezpieczania danych w internecie;
4. **Bezpieczne korzystanie z internetu**
 - 4.1. Zalety i wady internetu – krytyczna analiza informacji znalezionych w sieci;
 - 4.2. Problem nadmiernego korzystania z mediów elektronicznych i internetu;
 - 4.3. Cyberprzemoc i zapobieganie jej;
 - 4.4. Problem obrażania w sieci;
 - 4.5. Rozwiązania polecane w przypadku zetknięcia się z zagrożeniem w sieci;
 - 4.6. Zasady bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych i sieci;
 - 4.7. Podstawowe sposoby zabezpieczania danych w internecie;
 - 4.8. Przykłady dobrych praktyk.

Formy i metody realizacji:

Przy zapoznawaniu uczestników szkolenia z określonymi w programie zagadnieniami czy problemami stosowana będzie forma wykładu wspartego prezentacją i/lub



materiałem multimedialnym oraz instruktaż. W czasie kursu każdy z uczestników będzie miał możliwość przedstawienia wypracowanych przez siebie materiałów całej grupie w formie różnego rodzaju prezentacji.

W celu ćwiczenia nowo nabytych umiejętności w czasie szkolenia dominującymi formami pracy będą praca indywidualna słuchacza oraz praca w grupach i/lub parach podczas wykonywania ćwiczeń i rozwiązywania problemów. Metodami stosowanymi w czasie kursu będą: analiza tekstów dotyczących problematyki szkolenia, gry dydaktyczne przeznaczone do wykorzystania w pracy z uczniem oraz mapa myśli ułatwiająca wizualne opracowanie poruszanych zagadnień.

Podczas szkolenia istotna będzie także dyskusja, pozwalająca uczestnikom i prowadzącemu wymieniać się poglądami oraz doświadczeniami. Omawiane będą zarówno problemy przedstawiane przez prowadzącego, jak i sugerowane przez słuchaczy. Główne metody sprawdzania zdobytej wiedzy i umiejętności to rozmowy, testy, obserwacja działań uczestników szkolenia oraz zespołowa analiza wypracowanych przez nich materiałów.

Niezbędne oprogramowanie:

- system operacyjny Windows;
- przeglądarka internetowa – np. Firefox, Chrome;
- pakiet programów Microsoft Office;
- platforma e-learningowa;
- darmowe aplikacje – np. Padlet, Kahoot!, MakebeliefsComix.

Część wstępna

Działania nauczyciela a bezpieczeństwo informacyjne w placówce oświatowej



Czas trwania części: 7 godzin (w tym 2 godziny online)

Blok 1: Bezpieczeństwo informacyjne – podstawy

Cele operacyjne

Nauczyciel:

- potrafi zdefiniować bezpieczeństwo informacyjne;
- zna zapisy podstawy programowej dotyczące bezpieczeństwa informacyjnego w szkole;
- rozpoznaje najczęściej występujące zagrożenia bezpieczeństwa informacyjnego i zna sposoby zapobiegania im;
- potrafi wdrożyć podstawowe działania profilaktyczne na rzecz bezpieczeństwa informacyjnego w szkole;
- przestrzega zasad postępowania w przypadku wystąpienia zagrożeń bezpieczeństwa informacyjnego;
- jest świadomy, jakie źródła może wykorzystać podczas działań mających na celu rozpowszechnianie wiedzy i pozwalających budować świadomość uczniów na temat istniejących zagrożeń;
- zna i potrafi stosować w praktyce podstawowe zasady bezpiecznej pracy z internetem;
- umie określić kierunki rozwoju mediów elektronicznych i zagrożenia z nimi związane.

Opis treści:

- rozumienie bezpieczeństwa informacyjnego;
- podstawa programowa a bezpieczeństwo informacyjne;
- najczęstsze zagrożenia bezpieczeństwa informacyjnego;
- podstawowe działania na rzecz bezpieczeństwa informacyjnego w szkole i w życiu prywatnym;
- bezpieczna praca z internetem i zagrożenia z nim związane;
- sposoby zapobiegania poznanyim zagrożeniom;
- systemowa interwencja i profilaktyka w szkołach;
- zasady postępowania w przypadku wystąpienia zagrożeń bezpieczeństwa informacyjnego;
- źródła wiedzy na temat bezpieczeństwa informacyjnego.



Proponowane zasoby edukacyjne:

- Wybrane fragmenty materiałów:
- Seria filmów edukacyjnych *Bezpieczeństwo dzieci i młodzieży online* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/bezpieczenstwo-dzieci-i-mlodziezy-online.html>;
- Blog „Dane osobowe”: *Kradzież tożsamości w Internecie* – <https://blog-daneosobowe.pl/kradziez-tozsamosci-w-internecie>;
- Praca zbiorowa, (2017), *Bezpieczne media. Poradnik dla rodziców*, Warszawa: FDDS i Fundacja Orange – https://www.edukacja.fdds.pl/fc63516e-e941-4d-3c-827d-9febcb076630/Extras/broszura_Dziecko-i-media-19-09-2017.pdf;
- Wojtasik Ł. (red.), (2017) *Jak reagować na cyberprzemoc. Poradnik dla szkół*, Warszawa: FDDS, wyd. II – https://www.edukacja.fdds.pl/cb0428e3-c0d8-47cb-8508-1b865100a1f9/Extras/ksiazka-jak_reagowac_na_cyberprzemoc-FDDS-12042017.pdf;
- Wójcik S. (oprac.), (2017), *Jak postępować w przypadku (cyber) przemocy? Systemowa interwencja i profilaktyka w szkole* (Wyciąg z materiałów klicksafe), Warszawa: FDDS – <https://www.saferinternet.pl/pliki/publikacje/Jak%20post%C4%99powa%C4%87%20w%20cyberprzemocy.pdf>;
- Czajka R., Lipszyc J., (2014), *Poradnik bezpieczeństwa mobilnego*, Warszawa: Fundacja Nowoczesna Polska – <https://edukacjamedialna.edu.pl/media/chunks/attachment/poradnik-bezpieczenstwa-mobilnego.pdf>;
- Rządowa strona „Bezpieczna Szkoła +”: *Promujemy bezpieczeństwo w sieci* – materiały i scenariusze zajęć – <https://bezpiecznaszkola.men.gov.pl/tematy/promujemy-bezpieczenstwo-w-sieci/informacje/>;
- Lizut J., Wrońska A. (red.), (2018), *Standard bezpieczeństwa online placówek oświatowych*, Warszawa: NASK – https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf;
- Strona „Cyfrowo Bezpieczni”: *Procedury bezpieczeństwa cyfrowego w szkołach* – pakiet dokumentów MEN – <https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Bezpieczeństwo informacji w sieci* – <https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci>;
- Praca zbiorowa, (2017), *Bezpieczna Szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, Warszawa: MEN – <http://bezpiecznaszkola.men.gov.pl/wp-content/uploads/2017/09/zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizycznego-i-cyfrowego-uczniow.pdf>;



- Zespół ekspertów NASK, (2017), *Jak zapewnić uczniom bezpieczeństwo w internecie – poradnik dla nauczycieli*, Warszawa: NASK – <https://akademia.nask.pl/pliki/1-jak-zapewnic-uczniom-bezpieczenstwo-w-internecie-poradnik-dla-nauczycieli.pdf>;
- Chocholska P. i in. (oprac.), (2017), *Jak reagować na problem nadmiernego korzystania z internetu przez dzieci i młodzież. Poradnik dla szkół*, Warszawa: FDDS – https://www.edukacja.fdds.pl/60d2a7cf-56e9-4281-a3d3-c9d4377ef098/Extras/ksiazka-jak_reagowac_na_problemy_nadmiernego_korzystania_z_internetu-FDDS-12042017.pdf;
- Podstawa programowa dla poszczególnych typów szkół i etapów edukacyjnych wprowadzona w 2017 r. – <https://podstawaprogramowa.pl>.



Blok 2: Prawo autorskie

Cele operacyjne

Nauczyciel:

- wie, czym są prawa autorskie i prawa pokrewne;
- zna zasady korzystania z cudzych utworów;
- korzysta z zasobów na zasadzie dozwolonego użytku edukacyjnego;
- potrafi chronić prawa autorskie, w tym także autorów nieletnich.

Opis treści:

- prawa autorskie i prawa pokrewne;
- obowiązujące przepisy prawne;
- dozwolony użytek edukacyjny;
- pojęcie plagiatu;
- prawa autorskie osoby nieletniej;
- prawa autorskie nauczyciela.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Czerniawski P., Lipszyc J., Wilkowski M., *Pierwsza pomoc w prawie autorskim: przewodnik*, Warszawa: Fundacja Nowoczesna Polska – <https://prawokultury.pl/publikacje/pierwsza-pomoc>;
- Poradnia na stronie „Prawokultury.pl”: *Pierwsza pomoc w prawie autorskim: zapytaj prawnika* – <https://prawokultury.pl/pierwsza-pomoc>;
- Siewicz K., (2016), *Prawo autorskie w edukacji: jak unikać naruszeń?*, Warszawa: Fundacja Nowoczesna Polska – <http://koed.org/wp-content/uploads/2016/11/prawo-autorskie-w-edukacji-jak-unikac-naruszen-wersja-2016-1.pdf>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Prawo autorskie dla każdego* – <https://cyfrowa-wyprawka.org/lekcja/prawo-autorskie-dla-kazdego>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Jak etycznie publikować w sieci?* – <https://cyfrowa-wyprawka.org/lekcja/jak-etycznie-publikowac-w-sieci>.



Blok 3: Dane osobowe

Cele operacyjne

Nauczyciel:

- wie, czym są dane osobowe i w jaki sposób są chronione;
- omawia zmiany w zakresie ochrony danych osobowych wprowadzone w 2018 roku;
- zna i stosuje zasady ochrony danych osobowych w życiu prywatnym i w szkole;
- potrafi chronić dane osobowe uczniów, nauczycieli i innych pracowników szkoły.

Opis treści:

- dane osobowe i powód ich ochrony;
- formy ochrony danych osobowych w Polsce i w Unii Europejskiej;
- *Ogólne Rozporządzenie o Ochronie Danych Osobowych 2016/679 (RODO)* – zmiany w zakresie ochrony danych osobowych wprowadzone w 2018 roku;
- obowiązujące przepisy prawa;
- zasady ochrony danych osobowych w życiu prywatnym i w szkole;
- ochrona danych osobowych uczniów, nauczycieli oraz innych pracowników szkół.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Podstawy ochrony danych osobowych* – <https://cyfrowa-wyprawka.org/lekcja/podstawy-ochrony-danych-osobowych>;
- Strona Fundacji Panoptykon: cykl artykułów *RODO na tacy, czyli jak możemy skorzystać na nowych przepisach* – <https://panoptykon.org/rodo-na-tacy>;
- Strona The EU General Data Protection Regulation (GDPR) na temat RODO – <https://gdprexplained.eu/pl>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Wizerunek – jak chronić swoje prawa?* – <https://cyfrowa-wyprawka.org/lekcja/wizerunek-jak-chronic-swoje-prawa>;
- Serwis edukacyjny „DODO – dbamy o dane osobowe” – <http://dodo-bezpiecznie.blogspot.com/>;
- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak dzieci i młodzież chronią swoją prywatność?* – https://giodo.gov.pl/560/id_art/4699/j/pl;
- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak bezpiecznie zwiedzać cyfrowy świat?* – <https://giodo.gov.pl/pl/1520208/8510>;



- Wykład otwarty z cyklu „Lekcje z GIODO” pt. *Elektroniczna dokumentacja szkolna i jej udostępnianie* –
<https://www.youtube.com/watch?v=qwXla3bA1w8&feature=youtu.be>.



Blok 1: Korzystamy z mediów (cyfrowych)

Cele operacyjne

Nauczyciel:

- potrafi przygotować uczniów do wyszukiwania w internecie i wykorzystywania profesjonalnie przygotowanych materiałów;
- wyjaśnia swoim uczniom korzyści płynące z wykorzystania różnorodnych mediów do nauki;
- zna zalety i wady internetu, wykorzystuje tę wiedzę na zajęciach z uczniami;
- potrafi zorganizować zajęcia przygotowujące uczniów do krytycznej oceny źródeł informacji;
- umie planować i organizować zajęcia wykorzystujące treści pochodzące z różnych mediów (w tym internetowe) do nauki.

Opis treści:

- używanie w szkole mediów cyfrowych (i nie tylko);
- zalety i wady mediów cyfrowych;
- wykorzystywanie treści internetowych do nauki;
- krytyczny odbiór informacji z różnych mediów.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Best – Katalog Bezpiecznych Stron portalu „Sieciaki.pl” – <https://sieciaki.pl/best>;
- Lekcja: *Sprawne szukanie informacji* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/sprawne-szukanie-informacji>;
- Lekcja: *Gdy wybierasz dobre źródło* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/gdy-wyberasz-dobre-zrodlo>;
- Lekcja: *Jedna informacja a źródeł mnóstwo!* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/jedna-informacja-a-zrodel-mnostwo>;
- Lekcja: *Czym się różni informacja od opinii?* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/czym-sie-rozni-informacja-od-opinii>;



- Lekcja: *Dobrze wykorzystaj czas poświęcony mediom* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/dobrze-wykorzystaj-czas-poswiecony-mediom>;
- Buchner A., *Jak rozróżniać informacje prawdziwe od fałszywych?*, Warszawa: Fundacja Orange – https://platforma.megamisja.pl/download/knowledge_base/scenario/8/Jak_rozrozniac_informacje_prawdziwe_od_falszywych.pdf.



Blok 2: Oswajamy prawo autorskie

Cele operacyjne

Nauczyciel:

- potrafi wyjaśnić uczniom podstawy ochrony ich praw jako autorów;
- umie przedstawić uczniom zasady korzystania z cudzych utworów.

Opis treści:

- ochrona utworów przygotowanych przez uczniów;
- podstawowe zasady dotyczące wykorzystania dozwolonego użytku edukacyjnego;
- pojęcie plagiatu.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Platforma edukacyjna Fundacji Dajemy Dzieciom Siłę: szkolenie 3... 2... 1... *Internet!* – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=9&fn-d=&grupa=0&offset=1&sort=1&szkolenie=1122&tekst=1122#opisszkolenia;
- Lekcja: *Prawo autorskie, czyli pokaż, co potrafisz* na stronie „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/prawo-autorskie-czyli-pokaz-co-potrafisz>;
- Lekcja: *Szanujmy twórców* na stronie „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/szanujmy-tworcow>;
- Lekcja: *Jak etycznie publikować w sieci?* na stronie „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/jak-etycznie-publikowac-w-sieci/>;
- Strona fotoprawo.pl: *Fakty i mity, czyli o prawach autorskich dla blogerów* – <https://fotoprawo.pl/index.php/2012/10/fakty-i-mity-czyli-o-prawach-autorskich-dla-bloggerow/>;
- Strona fotoprawo.pl: *Darmowe zdjęcia z sieci. Skąd brać? Jak korzystać?* – <https://fotoprawo.pl/index.php/2012/10/fakty-i-mity-czyli-o-prawach-autorskich-dla-bloggerow/>;
- Strona „Prawo Autorskie? OK” – <http://pa.ok.oeiizk.waw.pl>.



Blok 3: Mój wizerunek w sieci

Cele operacyjne

Nauczyciel:

- zna zasady ochrony wizerunku uczniów i nauczycieli oraz umie wykorzystywać tę wiedzę w szkole;
- potrafi planować i organizować zajęcia wspierające ucznia w zapewnianiu bezpieczeństwa własnym danym osobowym i dbaniu o swój wizerunek.

Opis treści:

- ochrona wizerunku uczniów i nauczycieli;
- problem publikacji zdjęć dzieci w internecie;
- ochrona prywatności w internecie;
- podstawowe sposoby zabezpieczania danych w internecie.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Lekcja: *Co się dzieje z moimi danymi?* na stronie „Edukacja medialna” – <http://edukacjamedialna.edu.pl/lekcje/co-sie-dzieje-z-moimi-danymi>;
- Filmy z cyklu *Owce w sieci* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/owce-w-sieci.html>;
- Dziemidowicz E., Wojtasik Ł., (2017), *Lekcja bezpieczeństwa – scenariusz zajęć*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=9&fnd=&grupa=0&offset=1&sort=1&szkolenie=1114&tekst=1114#opisszkolenia;
- *Zastanów się, zanim udostępnisz. Porady Facebooka i MediaSmarts* – https://www.edukacja.fdds.pl/4080c4da-0166-40df-9904-1ad38a6fc75f/Extras/ulotka-zastanow_sie_zanim_udostepnisz-FDDS-12042017.pdf;
- „Digital Youth. Magazyn o fenomenach internetu” nr 3 (05) 2017 – https://www.edukacja.fdds.pl/de4062e0-62db-4daf-b7ce-be4bfb32c2bd/Extras/broszura-digital-youth_3-2017.pdf;
- Lekcja: *Prawo do prywatności w sieci* na stronie „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/prawo-do-prywatnosci-w-sieci>;



- Lekcja: *Cyfrowy portret, czyli kilka słów o wizerunku w Internecie* na stronie „Edukacja medialna” – <http://edukacjamedialna.edu.pl/lekcje/cyfrowy-portret-czyli-kilka-slow-o-wizerunku-w-internecie/>;
- Platforma edukacyjna Fundacji Dajemy Dzieciom Siłę: szkolenie 3... 2... 1... *Internet!* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/321internet.html>;
- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak bezpiecznie zwiedzać cyfrowy świat?* – <https://giodo.gov.pl/pl/1520208/8510>.



Blok 4: Z głową w internecie

Cele operacyjne

Nauczyciel:

- kształtuje świadomość zagrożeń występujących w internecie;
- promuje wśród uczniów zasady bezpiecznego zachowania w sieci;
- wychowuje uczniów na problem nadmiernego korzystania z mediów, w tym internetu;
- potrafi wskazać uczniom podstawowe sposoby radzenia sobie z cyberprzemocą oraz innymi zagrożeniami w sieci, a także zapobiegania tym zjawiskom;
- wyszukuje i dobiera materiały dotyczące zagrożeń internetowych odpowiednie dla swoich uczniów.

Opis treści:

- zagrożenia internetowe;
- podstawowe problemy związane z korzystaniem z sieci;
- szkodliwe i niebezpieczne treści w internecie;
- nadmierne korzystanie z internetu przez dzieci;
- cyberprzemoc i sposoby zapobiegania jej;
- wsparcie dla uczniów doświadczających cyberprzemocy (w tym obrażenia w sieci);
- materiały edukacyjne dotyczące zagrożeń internetowych.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak bezpiecznie zwiedzać cyfrowy świat?* – <https://giodo.gov.pl/pl/1520208/8510>;
- Platforma edukacyjna Fundacji Dajemy Dzieciom Siłę: szkolenie 3... 2... 1... *Internet!* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/321internet.html>;
- Barlińska J. (oprac.), (2017), 3... 2... 1... *Internet! Scenariusz zajęć na temat bezpieczeństwa dzieci w internecie dla uczniów klas IV–VI szkół podstawowych*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/c7f40a29-f63c-455e-ac-17-1df53d0cf267/Extras/321internet-scenariusz-FDDS.pdf>;



- Leszczyńska I., Ćwiek M. (oprac.), (2017), *Sieciaki.pl. Poznaj bezpieczny internet! Scenariusze zajęć edukacyjnych dla uczniów klas I–III oraz IV–VI szkoły podstawowej na temat bezpieczeństwa w sieci*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/9e0b89e2-561c-48af-b88f-639f63ba6120/Extras/Sieciaki-pl-Poznaj-bezpieczny-internet-zestaw-scenariuszy.pdf>;
- Dziemidowicz E., Kępka M., (2017), *Internet bez hejtu. Scenariusz pikniku edukacyjnego*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&tekst=15447;
- Lekcja: *Bądźmy życzliwi w sieci!* na stronie „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/badzmy-zyczliwi-w-sieci>;
- Lekcja: *ABC bezpieczeństwa w sieci* na stronie „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/abc-bezpieczenstwa-w-sieci>;
- Sieciaki.pl: *Umowa internetowa* – wzór do wykorzystania – https://www.edukacja.fdds.pl/182a013b-6f93-4e75-8281-d4e730871b31/Extras/umowa_a4.png;
- „Rufus w opałach” – interaktywna decyzyjna gra video: informacje o grze na stronie akademia.nask.pl – <https://akademia.nask.pl/gr.html>;
- „Rufus w opałach” – interaktywna decyzyjna gra video: scenariusze zajęć <https://akademia.nask.pl/pobierz.php?i=115&hash=bd17>;
- „Odkrywcy Internetu” – gra planszowa: informacje o grze i materiały do pobrania – <http://wbp.poznan.ekursy.eu/course/view.php?id=27>.



Blok 5: Aplikacje i urządzenia mobilne

Cele operacyjne

Nauczyciel:

- zapoznaje uczniów z podstawami bezpiecznego użycia urządzeń mobilnych;
- przedstawia uczniom możliwe zagrożenia związane z użyciem technologii mobilnych;
- uwrażliwia uczniów na konieczność zabezpieczania danych.

Opis treści:

- podstawowe zasady bezpiecznego korzystania z urządzeń mobilnych;
- rozwój technologii mobilnych w kontekście bezpieczeństwa informacyjnego;
- problemy utraty danych i utraty anonimowości.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak bezpiecznie zwiedzać cyfrowy świat?* – <https://giodo.gov.pl/pl/1520208/8510>;
- Filmy z cyklu *Owce w sieci* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/owce-w-sieci.html>;
- *Owce w sieci. Podręcznik dla nauczycieli cz. 2* – https://www.saferinternet.pl/pliki/publikacje/booklet_cz2.pdf;
- Strona kampanii „Mama, tata, tablet” – <http://mamatatatablet.pl/>;
- Film *Homo tabletis* – <https://www.edukacja.fdds.pl/05333bc1-883a-4edc-b-058-51e560df0fb7/Extras/homo-tabletis-film.mp4>.

Przykładowy rozkład treści



Część wstępna (7 godzin)				
Działania nauczyciela a bezpieczeństwo informacyjne				
Blok	Tytuł bloku	Ilość godzin		Treści kształcenia
		stacjonarnych	online	
1	<i>Bezpieczeństwo informacyjne – podstawy</i>	3	1	1.1, 1.2, 1.3, 1.4, 1.5
2	<i>Prawo autorskie</i>	1	0,5	2.1, 2.2, 2.3, 2.4
3	<i>Dane osobowe</i>	1	0,5	3.1, 3.2, 3.3, 3.4
	Razem godzin	5	2	

Część główna (18 godzin)				
Bezpieczeństwo informacyjne ucznia				
Blok	Tytuł bloku	Ilość godzin		Treści kształcenia
		stacjonarnych	online	
1	<i>Korzystamy z mediów (cyfrowych)</i>	5	0,5	1.1, 1.5, 4.1, 4.2, 4.4, 4.6, 4.8
2	<i>Oswajamy prawo autorskie</i>	1	0,5	2.1, 2.2, 2.3, 2.4
3	<i>Mój wizerunek w sieci</i>	2	0,5	3.1, 3.2, 3.4
4	<i>Z głową w internecie</i>	5	1	4.2, 4.3, 4.4, 4.5, 4.8
5	<i>Aplikacje i urządzenia mobilne</i>	2	0,5	4.6, 4.7
	Razem godzin	15	3	

Przykładowe scenariusze zajęć



Scenariusz zajęć nr 1

Część zajęć: Część wstępna – *Działania nauczyciela a bezpieczeństwo informacyjne*

Blok tematyczny: Blok 2 – *Prawo autorskie*

Temat zajęć: *Podstawy prawa autorskiego*

Czas zajęć: 65 min (w tym 20-minutowa część poświęcona na pracę online)

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśniać, czym są prawa autorskie i prawa pokrewne;
- korzystać zgodnie z prawem z cudzych utworów;
- stosować w praktyce zasadę dozwolonego użytku edukacyjnego;
- chronić prawa autorskie, w tym także prawa autorów nieletnich.

Metody nauczania:

- rozmowa;
- dyskusja;
- wykład;
- praca indywidualna uczestników przy komputerach;
- instruktaż.

Środki dydaktyczne:

- komputer i projektor – dla prowadzącego;
- komputer z przeglądarką internetową i pakietem Microsoft Office – dla każdego uczestnika szkolenia;
- materiały przygotowane przez prowadzącego (przykłady plagiatów i tekstów oryginalnych).



Zasoby do wykorzystania:

- *Moja przygoda z prawem autorskim* – materiały szkoleniowe Ośrodka Edukacji Informatycznej i Zastosowań Komputerów – <http://pa.ok.oeiizk.waw.pl/course83377/course/course83377.html>;
- *Dozwolony użytek w edukacji* – infografika – https://centrumcyfrowe.pl/wp-content/uploads/2013/09/dozwolony_infografika_druk.pdf.

Fragmenty materiałów:

- Strona „Prawokultury.pl”: *Krótki kurs własności intelektualnej. Materiały dla uczelni* – hasło: *Plagiat* – <https://prawokultury.pl/kurs/plagiat>.

Materiały dodatkowe:

- Siewicz K., (2016), *Prawo autorskie w edukacji: jak unikać naruszeń?*, Warszawa: Fundacja Nowoczesna Polska – <http://koed.org.pl/wp-content/uploads/2016/11/prawo-autorskie-w-edukacji-jak-unikac-naruszen-wersja-2016-1.pdf>.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej. W czasie wykonywania ćwiczeń online natychmiast uzyskują automatyczną informację zwrotną.

Przebieg zajęć:

1. Wprowadzenie do tematu zajęć
Prowadzący zajęcia skłania uczestników do zastanowienia się, dlaczego i w jaki sposób należy uczyć o prawie autorskim? Prezentuje dostępny w internecie film pt. *Rysunek Oli* – <https://www.youtube.com/watch?v=5MKRPkDqx-4> stanowiący wstęp do dyskusji, dlaczego chronimy prawa autora?
2. Dozwolony użytek edukacyjny
Uczestnicy zapoznają się z infografiką *Dozwolony użytek w edukacji* – https://centrumcyfrowe.pl/wp-content/uploads/2013/09/dozwolony_infografika_druk.pdf. Omawiają poszczególne jej punkty na forum grupy. Prowadzący przedstawia im poradnię na stronie „Prawokultury.pl” *Pierwsza pomoc w prawie autorskim: zapytaj prawnika* – <https://prawokultury.pl/pierwsza-pomoc>, która umożliwia zadawanie specjalistom pytań z zakresu prawa autorskiego.



Uczestnicy szkolenia przeglądają odpowiedzi prawników na pytania, które dotychczas zostały zadane na stronie.

Uczestnicy w parach wybierają po jednym punkcie z infografiki. Mają za zadanie przygotować 1–2 pytania odnoszące się do treści wybranego punktu, by wspólnie stworzyć quiz złożony z pytań jednokrotnego wyboru (każde pytanie musi zawierać 2–4 odpowiedzi do wyboru, w tym jedną poprawną). Prowadzący szkolenie zbiera propozycje pytań, dokonuje ich weryfikacji. Wykorzystuje je do opracowania quizu, który będzie potrzebny w dalszej części szkolenia (patrz: scenariusz nr 4).

3. Wykrywanie plagiatu

Prowadzący wygłasza miniwykład połączony z instruktażem, zwracając uwagę słuchaczy na to, czym jest plagiat i jak można go wykryć. Uczestnicy otrzymują od prowadzącego krótkie teksty w wersji elektronicznej. Zadanie polega na sprawdzeniu, czy są to prace oryginalne. Uczestnicy, pracując indywidualnie, wykorzystują ogólnodostępne narzędzia, takie jak wyszukiwarki internetowe lub darmowe systemy antyplagiatowe. Następnie przedstawiają wyniki swej pracy i omawiają problemy, które się pojawiły, oraz wskazują możliwości ich rozwiązania.

4. Podsumowanie

Prowadzący podsumowuje omówione zagadnienia i wyjaśnia, na czym będzie polegała praca online.

5. Praca online

Uczestnicy szkolenia pracują samodzielnie, wykorzystując do samodzielnej nauki materiały szkoleniowe ze strony Ośrodka Edukacji Informatycznej i Zastosowań Komputerów – <http://pa.ok.oeiizk.waw.pl/course83377/course/course83377.html>. Poznają podstawowe pojęcia, uzupełniają i systematyzują wiedzę dotyczącą prawa autorskiego.



Scenariusz zajęć nr 2

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 1 – *Korzystamy z mediów (cyfrowych)*

Temat zajęć: *Wyszukiwanie treści w internecie*

Czas zajęć: 45 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- przygotować uczniów do wyszukiwania i wykorzystywania treści internetowych;
- wskazać korzyści płynące z wykorzystania różnorodnych mediów do nauki;
- przygotowywać uczniów do krytycznej oceny materiałów pochodzących z mediów – np. znalezionych w internecie;
- dostrzegać wady i zalety internetu i wykorzystywać tę wiedzę na zajęciach z uczniami.

Metody dydaktyczne:

- rozmowa;
- wykład;
- praca indywidualna uczestników przy komputerach;
- praca w grupach lub parach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową i pakietem Microsoft Office dla każdego uczestnika szkolenia;
- kartki, długopisy i pojemnik do zbierania kartek z pytaniami (ewentualnie kapelusz);
- materiały do ćwiczeń.



Zasoby do wykorzystania:

- Fragment tekstu *Gdy wybierasz dobre źródło* ze strony „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/gdy-wyberasz-dobre-zrodlo/#wiedza-w-pigulce> lub podobne materiały przygotowane przez prowadzącego.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Przedstawienie tematu zajęć

Prowadzący zapowiada tematykę zajęć i sprawdza wiedzę uczestników na temat wyszukiwania i weryfikowania informacji, uzupełnia ich wiadomości. Uczestnicy rozmawiają na temat zasad wyszukiwania informacji. Miniwykład przeprowadzony przez prowadzącego uzupełnia wiadomości, które pojawiły się w czasie rozmowy.

2. Wyszukiwanie informacji i ich weryfikacja:

Praca w parach:

- Wyszukiwanie ciekawostek i ocena ich wiarygodności
Uczestnicy poszukują w internecie ciekawostek dotyczących wybranego tematu z zakresu nauczanego przez siebie przedmiotu. Wymieniają się w parach zebranymi informacjami i oceniają nawzajem wiarygodność źródła oraz znalezionych informacji wg kryteriów podanych przez prowadzącego (np. wykorzystując materiał ze strony „Edukacja medialna” <https://edukacjamedialna.edu.pl/lekcje/gdy-wyberasz-dobre-zrodlo/#wiedza-w-pigulce>). Uczestnicy w parach wybierają jedną ciekawostkę, która pozytywnie przeszła krytyczną ocenę.
- Wyszukiwanie informacji na zadany temat
Każda para na podstawie znalezionych informacji przygotowuje przynajmniej jedno pytanie, na które inni uczestnicy szkolenia mają znaleźć odpowiedź. Pytania zostają zapisane na kartkach, a kartki wrzucone np. do kapelusza. Każdy zespół wypisuje słowa kluczowe, które pomogą udzielić odpowiedzi na postawione pytanie (będą one stanowić ewentualną pomoc dla innych uczestników w razie wystąpienia problemów ze znalezieniem informacji). Następnie każda para losuje pytanie



(w przypadku wylosowania przez parę samodzielnie opracowanego pytania, czynność zostaje powtórzona). Zadaniem nauczycieli jest znalezienie w internecie odpowiedzi na wylosowane pytanie – mogą oni skorzystać z słów kluczowych. Poszczególne pary przedstawiają wyniki swoich poszukiwań na forum i omawiają strategie wyszukiwania, pojawiające się problemy, sposoby weryfikacji źródeł itp.

3. Wyszukiwanie informacji w praktyce szkolnej – podsumowanie

Praca w grupach (2–4 osobowych):

- Zadania dla uczniów

Uczestnicy szkolenia zostają przyporządkowani do grup w zależności od nauczanego przedmiotu, poziomu nauczanych klas itp. Zadaniem każdej grupy jest opracowanie dla uczniów przynajmniej jednego ćwiczenia opartego na zdobytej dotychczas wiedzy, dotyczącego tematyki zajęć w powiązaniu z nauczaniem przedmiotem. Musi ono zawierać element wyszukiwania informacji związanej z opracowywanym w klasie tematem. Na zakończenie pracy grupy prezentują przygotowane zadania, uczestnicy komentują, wymieniają się opiniami itd.

4. Rozmowa podsumowująca

Prowadzący inicjuje rozmowę mającą na celu omówienie problemów, które mogą się pojawić w czasie zajęć wykorzystujących proponowane metody pracy z uczniami, oraz zebranie propozycji ich rozwiązania.



Scenariusz zajęć nr 3

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 3 – *Mój wizerunek w sieci*

Temat zajęć: *Chronię swoją prywatność w sieci*

Czas zajęć: 45 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wykorzystywać wiedzę na temat ochrony wizerunku uczniów i nauczycieli;
- planować i organizować zajęcia wspierające uczniów w dbaniu o własny wizerunek;
- dobierać odpowiednie materiały edukacyjne dla swoich uczniów;
- rozwijać umiejętności swoich uczniów dotyczące ochrony prywatności w sieci.

Metody nauczania:

- rozmowa;
- praca w grupie;
- burza mózgów;
- praca indywidualna uczestników przy komputerach;
- instruktaż.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową i pakietem Microsoft Office dla każdego uczestnika szkolenia;
- aplikacja online MakebeliefsComix;
- aplikacja Padlet (lub analogiczna).



Zasoby do wykorzystania:

- Filmy:
 - Zestaw 1
Bez kożuszka – https://www.youtube.com/watch?v=dGKt_WtrNXY;
Bekanie – https://www.youtube.com/watch?time_continue=13&v=yrAUoIHIErw.
 - Zestaw 2
3... 2... 1... Internet! Dane cz. 1 – <https://www.youtube.com/watch?v=zki95SBh7Sg>;
3... 2... 1... Internet! Dane cz. 2 – https://www.youtube.com/watch?v=3RMW8I-_byY;
3... 2... 1... Internet! Dane cz. 3 – <https://www.youtube.com/watch?v=el29Xcd0Nkw>.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Wprowadzenie
Prowadzący nawiązuje do tematu zajęć, inicjując krótką rozmowę nauczycieli na temat ich doświadczeń związanych z ochroną prywatności w sieci.
2. Wykorzystanie materiałów multimedialnych do przygotowania lekcji
Uczestnicy zostają podzieleni na grupy (podział w zależności od nauczanego przedmiotu lub poziomu nauczanej klasy). Każdy zespół losuje lub otrzymuje przydzielony zestaw materiałów multimedialnych. Pojedynczy zestaw może zostać przydzielony więcej niż jednej grupie.

Zestaw 1

Bez kożuszka – https://www.youtube.com/watch?v=dGKt_WtrNXY;

Bekanie – https://www.youtube.com/watch?time_continue=13&v=yrAUoIHIErw.

Zestaw 2

3... 2... 1... Internet! Dane cz. 1 –

<https://www.youtube.com/watch?v=zki95SBh7Sg>;



3... 2... 1... *Internet! Dane cz. 2* –

https://www.youtube.com/watch?v=3RMW8I-_byY;

3... 2... 1... *Internet! Dane cz. 3* –

<https://www.youtube.com/watch?v=el29Xcd0Nkw.>

3. Prezentacja pomysłów

Uczestnicy opracowują w grupach koncepcje wykorzystania wskazanych w zestawie materiałów na zajęciach z własnymi uczniami – zapisują pomysły w dokumencie tekstowym lub na kartkach, a następnie przedstawiają na forum całej grupy szkoleniowej, omawiają i komentują efekty swej pracy. Przedstawiciele grup przesyłają dokumenty z pomysłami do e-portfolio szkolenia (repozytorium przydatnych materiałów np. na platformie e-learningowej) dostępnego dla wszystkich uczestników szkolenia.

Przykładowy pomysł wykorzystania zestawu nr 2:

- Po projekcji filmu nr 1 uczniowie głosują, czy bohaterka filmu powinna opublikować swoje zdjęcia, czy też nie. Rozmawiają w parach, o tym jakie mogą być skutki każdego z wyborów. Dzieli się swoimi przemyśleniami na forum klasy.
- Po projekcji filmu nr 2 uczniowie biorą udział w rozmowie na temat konsekwencji opublikowania zdjęć – jakich jeszcze moglibyśmy się spodziewać?
- Po obejrzeniu filmu nr 3 uczniowie rozmawiają o rozwiązaniu przedstawionym w filmie. Zastanawiają się, z jakich powodów nasza prywatność w sieci może być zagrożona? W jaki sposób należy się przed tymi zagrożeniami chronić?
- Uczniowie opracowują zbiór rad pod hasłem: „Chroń swoją prywatność w sieci”.

4. Burza mózgów

Prowadzący inicjuje burzę mózgów na temat „Jak zagrożona jest prywatność uczniów w sieci?” – prosi uczestników o wypisanie na „cyfrowej tablicy” problemów dotyczących ochrony prywatności i wizerunku uczniów. Każdy z uczestników zgłasza minimum jeden pomysł. Prowadzący porządkuje hasła. Autorzy ustnie dodają wyjaśnienia.

5. Rozmowy w parach

Korzystając z wypisanych haseł, uczestnicy szkolenia pracujący w parach rozmawiają w celu sformułowania dobrych rad dla swoich uczniów. Następnie przedstawiają je na forum, np. zapisując w e-portfolio szkolenia, i dodają wyjaśnienia.



Przykładowy zestaw wskazówek może wyglądać następująco:

- Zastanów się dwa razy, zanim coś opublikujesz w internecie!
- Uważaj, jakie wiadomości na swój temat ujawniasz w sieci!
- Zabezpieczaj hasłem dostęp do telefonu!
- Nie udostępniaj innym swoich haseł!

6. Opracowanie komiksów

Prowadzący poleca uczestnikom przygotowanie komiksów przedstawiających i wyjaśniających treści opracowane w poprzednim zadaniu – w formie listy wskazówek. Zanim rozpoczną indywidualną pracę, zapozna je ich z zasadami tworzenia komiksów. Każdy z uczestników wybiera jedną z rad i przedstawia ją z pomocą komiksu składającego się z minimum 3 ramek komiksowych (komiksy są tworzone z pomocą serwisu online MakebeliefsComix).

7. Prezentacja prac

Gotowe komiksy są publikowane w e-portfolio szkolenia. Uczestnicy przeglądają prace. Zastanawiają się, w jaki sposób mogą wykorzystać tworzenie komiksów w pracy z uczniami podczas realizacji innego tematu związanego z bezpieczeństwem informacyjnym. Wymieniają się swoimi pomysłami w parach.

8. Podsumowanie zajęć

Uczestnicy analizują, na jakie trudności mogą natrafić podczas pracy z uczniami nad omówioną tematyką. Jak można im zapobiec lub zaradzić? – zastanawiają się, rozmawiając na forum grupy szkoleniowej.



Scenariusz zajęć nr 4

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 4 – *Z głową w internecie*

Temat zajęć: *Jak sobie radzić z cyberprzemocą?*

Czas zajęć: 45 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- kształtować świadomość uczniów w zakresie zagrożeń występujących w internecie;
- wyszukiwać i wybierać odpowiednie dla swoich uczniów materiały dotyczące zagrożeń internetowych.

Metody nauczania:

- rozmowa;
- dyskusja;
- wykład;
- praca indywidualna uczestników przy komputerach;
- instruktaż.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową i pakietem Microsoft Office dla każdego uczestnika szkolenia;
- ewentualnie: aplikacje online do prezentowania filmów lub dialogów.

Zasoby do wykorzystania:

Przykładowe scenariusze zajęć:

- Barlińska J. (oprac.), (2017), 3... 2... 1... *Internet! Scenariusz zajęć na temat bezpieczeństwa dzieci w internecie dla uczniów klas IV–VI szkół podstawowych*,



Warszawa: FDDS – <https://www.edukacja.fdds.pl/c7f40a29-f63c-455e-ac-17-1df53d0cf267/Extras/321internet-scenariusz-FDDS.pdf>;

- Leszczyńska I., Ćwiek M. (oprac.), (2017), *Sieciaki.pl. Poznaj bezpieczny internet! Scenariusze zajęć edukacyjnych dla uczniów klas I–III oraz IV–VI szkoły podstawowej na temat bezpieczeństwa w sieci*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/9e0b89e2-561c-48af-b88f-639f63ba6120/Extras/Sieciaki-pl-Poznaj-bezpieczny-internet-zestaw-scenariuszy.pdf>;
- Dziemidowicz E., Kępka M., (2017), *Internet bez hejtu. Scenariusz pikniku edukacyjnego*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/258277a5bad-5-4dba-b2bc-4e688dd67c1f/Extras/scenariusz-internet-bez-hejtu-scenariusz-pikniku-edukacyjnego-FDDS-07042017.pdf>.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Przedstawienie tematu zajęć
Prowadzący sygnalizuje tematykę zajęć: *Jak sobie radzić z cyberprzemocą?*
2. Przegląd i ocena materiałów
Uczestnicy szkolenia, pracując samodzielnie, przeglądają przydzielone przez prowadzącego zestawy scenariuszy zajęć dotyczących problemu cyberprzemocy.

Przykładowe dokumenty ze scenariuszami:

- Barlińska J. (oprac.), (2017), *3... 2... 1... Internet! Scenariusz zajęć na temat bezpieczeństwa dzieci w internecie dla uczniów klas IV–VI szkół podstawowych*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/c7f40a29-f63c-455e-ac17-1df53d0cf267/Extras/321internet-scenariusz-FDDS.pdf>;
- Leszczyńska I., Ćwiek M. (oprac.), (2017), *Sieciaki.pl. Poznaj bezpieczny internet! Scenariusze zajęć edukacyjnych dla uczniów klas I–III oraz IV–VI szkoły podstawowej na temat bezpieczeństwa w sieci*, Warszawa: <https://www.edukacja.fdds.pl/9e0b89e2-561c-48af-b88f-639f63ba6120/Extras/Sieciaki-pl-Poznaj-bezpieczny-internet-zestaw-scenariuszy.pdf>;



- Dziemidowicz E., Kępka M., (2017), *Internet bez hejtu. Scenariusz pikniku edukacyjnego*, Warszawa: FDDS – <https://www.edukacja.fdds.pl/258277a5-bad5-4dba-b2bc-4e688dd67c1f/Extras/scenariusz-internet-bez-hejtu-scenariusz-pikniku-edukacyjnego-FDDS-07042017.pdf>.

Zadaniem każdego uczestnika jest wybranie tego scenariusza, który możliwie najłatwiej potrafiłby zaadaptować w celu zrealizowania lekcji z własnymi uczniami. Do scenariusza dołączają komentarz wyjaśniający wybór i opis zmian, które należy wprowadzić, aby możliwe było zrealizowanie danego konspektu. Nauczyciele dzielą się swoimi spostrzeżeniami dotyczącymi adaptacji scenariuszy na forum całej grupy, przedstawiają pomysły zainspirowane omawianymi scenariuszami.

3. Jak zareagować na hejt? – dialog

Prowadzący łączy nauczycieli w pary. Zadaniem każdej pary jest napisanie krótkiego dialogu między fikcyjnymi osobami – przyjaciółmi z klasy, z których jeden udziela drugiemu dobrej rady. Dialog powinien prezentować jeden ze sposobów reagowania na hejt i wyjaśnienie, dlaczego taki sposób zachowania okazuje się skuteczny.

Przykładowe zasady zachowania w przypadku zetknięcia się z obrażaniem w sieci można znaleźć np. w scenariuszu pikniku edukacyjnego „Internet bez hejtu” (<https://www.edukacja.fdds.pl/258277a5-bad5-4dba-b2bc-4e688dd67c1f/Extras/scenariusz-internet-bez-hejtu-scenariusz-pikniku-edukacyjnego-FDDS-07042017.pdf>). Mogą brzmieć tak, jak przedstawione poniżej.

Zasady antyhejtowe:

- Nie odpowiadaj na hejterski komentarz pod wpływem chwili.
- Jeżeli bardzo się złościś, napisz odpowiedź, a potem weź głęboki oddech i ją skasuj.
- Nie odpowiadaj agresją na agresję.
- Nie lajkuj i nie udostępniaj hejterskich komentarzy.
- Jeżeli możesz, kasuj nienawistne komentarze.
- Zgłaszaj hejt, korzystając z opcji dostępnych w serwisach internetowych.
- Odróżniaj hejt od konstruktywnej krytyki.
- Gdy coś Ci się nie podoba, wyraż to kulturalnie.
- Nie rezygnuj z tego, co robisz, myślisz i mówisz, tylko ze względu na hejterów.



- Jeżeli nie możesz poradzić sobie z hejterem, zgłoś to znajomej zaufanej osobie lub zadzwoń na numer telefonu zaufania: 116 111.

Gotowe dialogi mogą następnie zostać zaprezentowane całej grupie szkoleniowej – w postaci:

- filmu imitującego czat internetowy;
- scenek wykorzystujących technikę dramy;
- plików tekstowych.

Prezentowane dialogi są oceniane przez uczestników szkolenia oraz prowadzącego.

4. Podsumowanie zajęć

Uczestnicy zajęć analizują, w jaki sposób można wykorzystać doświadczenia związane z opracowanym materiałem w pracy z uczniami. Omawiają problemy, które mogą się pojawić w czasie realizacji zajęć dotyczących tematyki hejtu, oraz zbierają propozycje ich rozwiązania.



Scenariusz zajęć nr 5

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 2 – *Oswajamy prawo autorskie*

Temat zajęć: *Wprowadzenie uczniów do problematyki prawa autorskiego*

Czas zajęć: 45 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić uczniom podstawy ochrony praw autorskich, w tym także praw uczniów – autorów;
- przedstawić uczniom zasady korzystania z cudzych utworów i ich praktyczne zastosowanie;
- opublikować w internecie opracowany przez siebie materiał zgodnie z prawem autorskim.

Metody nauczania:

- rozmowa;
- wykład;
- praca indywidualna uczestników przy komputerach;
- praca w parach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową i prostym oprogramowaniem do tworzenia plakatów (np. Canva, PowerPoint) dla każdego uczestnika;
- materiały do ćwiczeń.



Zasoby do wykorzystania:

- Materiały do lekcji odwróconej ze strony TED-Ed „Lessons worth sharing”: <https://ed.ted.com/on/FFI1BYX8>.

Formy oceny

W trakcie quizu oraz całych zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Przedstawienie tematu
Prowadzący wprowadza uczniów w problematykę prawa autorskiego. Rozpoczyna rozmowę na temat różnicy pomiędzy wykorzystywaniem cudzych utworów na terenie szkoły zgodnie z dozwolonym użyciem edukacyjnym a rozpowszechnianiem ich w internecie.
2. Quiz
Prowadzący sprawdza wiedzę uczestników w kontekście wymienionych wcześniej zagadnień poprzez wykorzystanie quizu online przygotowanego z pomocą serwisu Kahoot! (lub analogicznego) na podstawie pytań, które zostały opracowane przez uczestników szkolenia na jednych z poprzednich zajęć (część wstępna – blok 3). Pytania, które przysporzyły kłopotów uczestnikom szkolenia, zostają omówione.
3. Wyszukiwanie grafiki
Zadaniem nauczycieli będzie znalezienie grafiki, która może być swobodnie wykorzystywana w pracach uczniów i rozpowszechniana w internecie. Prowadzący przeprowadza miniwykład na temat licencji umożliwiających korzystanie z dostępnych materiałów oraz instruuje uczestników, w jaki sposób i gdzie mogą znaleźć grafiki opatrzone takimi licencjami. Nauczyciele pracują indywidualnie, wyszukując grafik posiadających określoną licencję na publikację wg ustalonych kryteriów – grafiki mogą dotyczyć np. zainteresowań uczestników szkolenia.
4. Przygotowanie i publikacja plakatów
Prowadzący nawiązuje do zajęć dotyczących ochrony danych osobowych. Przypomina uczestnikom reguły dotyczące ochrony danych i bezpiecznego



użytkowania internetu. Następnie uczestnicy, pracując w grupach, omawiają znaczenie każdego z haseł. Mogą one brzmieć tak, jak poniżej.

Zasady ochrony danych osobowych:

- Każda aktywność w sieci zostawia ślad.
- To, co robię w sieci, wpływa na mój wizerunek w realnym życiu.
- Zanim cokolwiek zamieszczę, zastanawiam się, czy w przyszłości nie będę tego żałował.
- Nie udostępniam danych i wizerunku innej osoby bez jej zgody.
- Nikt nie jest anonimowy w sieci.
- Dane zamieszczone w internecie pozostają tam na zawsze.
- Nie podaję swoich danych osobom poznanym w sieci.

Uczestnicy połączeni w pary losują hasło, którego treść mają za zadanie przedstawić w postaci plakatu. Planują jego zawartość i wyszukują grafiki posiadające odpowiednią licencję, uwzględniając to, że plakaty mają być docelowo opublikowane w internecie.

Gotowe plakaty są publikowane w e-portfolio szkolenia (np. na platformie e-learningowej). Uczestnicy szkolenia prezentują swoje prace na forum grupy. Omawiają przebieg pracy i ewentualne problemy, na które należy zwrócić uwagę, nadzorując realizowanie podobnego zadania przez uczniów. Zastanawiają się, jakie inne zagadnienia można przedstawiać lub utrzymywać, wykonując plakaty? W czasie rozmowy nauczyciele analizują, w jaki sposób zorganizować tego typu pracę uczniów na lekcji? Na co zwracać uwagę, aby cele zajęć zostały osiągnięte?

5. Podsumowanie

Każdy z uczestników dokonuje autorefleksji. Zapisuje i przesyła swe spostrzeżenia do prowadzącego. W refleksji mogą znaleźć się odpowiedzi na pytania:

- Czego się dziś nauczyłem?
- Co dziś sobie przypomniałem?
- Co mnie szczególnie zdziwiło?
- Nad czym muszę jeszcze popracować?

Ramowy program szkoleń

dla nauczycieli drugiego etapu kształcenia (klasy VII–VIII SP)
odpowiedzialnych za nauczanie w zakresie bezpieczeństwa
informacyjnego w szkołach



Informacje ogólne

Program szkolenia został opracowany w taki sposób, aby mogło ono służyć przygotowaniu nauczycieli szkół podstawowych nauczających w klasach VII–VIII do wdrażania wybranych aspektów bezpieczeństwa informacyjnego podczas zajęć różnych przedmiotów, a szczególnie informatyki. W programie uwzględniono problematykę młodzieżową oraz zachowania, które mogą powodować zagrożenia bezpieczeństwa informacyjnego.

Forma realizacji

Szkolenie jest realizowane w formie mieszanej (*blended learning*).

Czas trwania

25 godzin dydaktycznych (w tym 5 godzin online)

Liczebność grupy

Maksymalnie 14 osób

Uczestnicy

Szkolenie przeznaczone jest dla nauczycieli drugiego etapu kształcenia (klas VII–VIII szkoły podstawowej) odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach.

Wymagania wstępne

Wymagana jest umiejętność posługiwania się komputerem i typowymi urządzeniami peryferyjnymi (klawiatura, monitor, mysz, drukarka) oraz pracy w środowisku Windows w zakresie: zarządzania folderami i plikami, uruchamiania programów, korzystania z podręcznych aplikacji Windows.



Przygotowanie do szkolenia obejmuje uczestnictwo w kursach online „Bezpieczeństwo w komunikacji i w mediach” oraz „Korzystanie z informacji” dostępnych na stronie <https://e-kursy.ore.edu.pl/>. Zalecane jest ukończenie 1. modułu każdego z wymienionych kursów przed rozpoczęciem szkolenia oraz kontynuacja nauki na obu kursach online po jego ukończeniu.

Cele ogólne szkolenia

W części wstępnej:

- rozwijanie kompetencji merytorycznych nauczycieli przez zapoznanie ich z zagadnieniami dotyczącymi bezpieczeństwa informacyjnego w instytucjach oświatowych.

W części głównej:

- rozwijanie kompetencji medialnych i technicznych nauczycieli poprzez przygotowanie ich do wykorzystywania narzędzi technologii informacyjno-komunikacyjnych w celu organizowania zajęć związanych z bezpieczeństwem informacyjnym;
- przygotowanie nauczycieli klas VII–VIII do omawiania zagadnień dotyczących bezpieczeństwa informacyjnego podczas zajęć nauczanych przez nich przedmiotów.

Cele szczegółowe:

- wskazanie korelacji pomiędzy treściami związanymi z bezpieczeństwem informacyjnym a podstawą programową poszczególnych przedmiotów;
- upowszechnienie podstawowych informacji na temat praw autorskich i pokrewnych w kontekście działań placówek oświatowych i nauczycieli;
- rozwijanie umiejętności ochrony danych osobowych uczniów, nauczycieli i innych pracowników;
- zapoznanie uczestników z treścią RODO i jego zapisami dotyczącymi edukacji;
- rozpoznawanie przez nauczycieli typowych zagrożeń bezpieczeństwa informacyjnego w pracy i życiu prywatnym;
- przygotowanie nauczycieli do organizacji działań profilaktycznych w placówce wśród uczniów i innych nauczycieli;
- poznanie sposobów rozwijania u uczniów umiejętności poddawania informacji znalezionych w sieci krytycznej analizie;



- uświadomienie nauczycielom skutków hejtu i cyberprzemocy;
- zapoznanie uczestników z możliwymi konsekwencjami publikacji własnego lub cudzego wizerunku w sieci;
- określenie podstawowych sposobów reagowania na niebezpieczeństwa internetowe;
- opracowanie sposobów rozwijania wśród uczniów umiejętności budowania z innymi użytkownikami sieci relacji opartych na szacunku;
- ukazanie problematyki związanej z obrażaniem w sieci;
- wskazanie okoliczności i sposobów, które należy wykorzystywać, by podczas pracy z uczniami mówić o prawie autorskim i prawach pokrewnych;
- zapoznanie z kierunkami rozwoju mediów elektronicznych i wskazanie zagrożeń z tym związanych;
- uwrażliwienie na problem nadmiernego korzystania z mediów elektronicznych i internetu;
- sformułowanie zasad bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych oraz internetu;
- poznanie przez nauczycieli podstawowych sposobów zabezpieczania danych w internecie.

Treści kształcenia:

1. Bezpieczeństwo informacyjne w szkole i poza nią

- 1.1. Korelacja treści związanych z bezpieczeństwem informacyjnym i podstawą programową przedmiotu nauczanego przez danego nauczyciela;
- 1.2. Typowe zagrożenia bezpieczeństwa informacyjnego;
- 1.3. Organizacja działań profilaktycznych wśród uczniów i pracowników placówki oświatowej;
- 1.4. Rozwijanie umiejętności krytycznej analizy informacji znalezionych w sieci;
- 1.5. Kierunki rozwoju mediów elektronicznych i zagrożenia z nimi związane;
- 1.6. Zasady bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych i sieci;

2. Prawa autorskie i prawa pokrewne

- 2.1. Przepisy prawa autorskiego i praw pokrewnych;
- 2.2. Pojęcie plagiatu w kontekście przygotowywania i publikowania autorskich materiałów dydaktycznych;
- 2.3. Dozwolony użytek w edukacji;
- 2.4. Ochrona utworów z uwzględnieniem praw autorów nieletnich;
- 2.5. Prace uczniów a prawo autorskie;



3. Ochrona danych osobowych

- 3.1. Dane osobowe uczniów i pracowników placówki edukacyjnej oraz ich ochrona;
- 3.1. Wizerunek ucznia oraz nauczyciela i jego ochrona;
- 3.1. Prawa uczniów i obowiązki placówki edukacyjnej w świetle zapisów RODO;
- 3.1. Podstawowe sposoby zabezpieczania danych w internecie;

4. Bezpieczne korzystanie z internetu

- 4.1. Konsekwencje hejtu i cyberprzemocy;
- 4.2. Publikacja wizerunku w sieci i jej możliwe skutki;
- 4.3. Sposoby reagowania na niebezpieczeństwa internetowe, możliwość uzyskania pomocy;
- 4.4. Budowanie z innymi użytkownikami sieci relacji opartych na wzajemnym szacunku;
- 4.5. Obrażanie w sieci;
- 4.6. Problem nadmiernego korzystania z mediów elektronicznych i internetu.

Rekomendowane formy i metody realizacji:

- wykład wzbogacony prezentacją multimedialną (lub innymi materiałami multimedialnymi) służący zaznajomieniu uczestników z nowymi dla nich zagadnieniami;
- praca indywidualna słuchaczy podczas realizacji rozmaitych ćwiczeń związanych z omawianą problematyką;
- praca w grupach i dzielenie się uczestników wypracowanymi wnioskami oraz materiałami – np. w formie prezentacji;
- gry dydaktyczne – pozwalające zasugerować przykładowe metody pracy z uczniami;
- analiza tekstów związanych z problematyką szkolenia;
- mapy myśli, ułatwiające wizualne opracowanie poruszanych zagadnień;
- dyskusje pozwalające prowadzącemu i uczestnikom wymieniać się poglądami i doświadczeniami;
- rozmowy, interaktywne quizy, obserwacja działań uczestników, wspólna analiza wypracowanych przez nich materiałów – jako metody weryfikacji i oceny zdobytej wiedzy.

Niezbędne oprogramowanie:

- system operacyjny Windows;
- przeglądarka internetowa, np. Firefox, Chrome;



- pakiet programów Microsoft Office lub LibreOffice;
- poczta elektroniczna;
- platforma społecznościowa np. Facebook;
- platforma e-learningowa;
- darmowe aplikacje używane podczas zajęć – np. Padlet, Kahoot!, MakebeliefsComix LearningApps.

Część wstępna

Działania nauczyciela a bezpieczeństwo informacyjne w placówce oświatowej



Czas trwania części: 7 godzin (w tym 2 godziny online)

Blok 1: Bezpieczeństwo informacyjne – podstawy

Cele operacyjne

Nauczyciel:

- potrafi definiować bezpieczeństwo informacyjne;
- zna podstawę programową pod względem zapisów dotyczących bezpieczeństwa informacyjnego w szkole;
- umie rozpoznać podstawowe zagrożenia bezpieczeństwa informacyjnego i zna sposoby zapobiegania im;
- potrafi podejmować podstawowe działania profilaktyczne na rzecz bezpieczeństwa informacyjnego w szkole;
- zna zasady postępowania w przypadku wystąpienia zagrożeń bezpieczeństwa informacyjnego i potrafi zastosować je w praktyce;
- zna źródła, które może wykorzystać, organizując działania służące rozpowszechnianiu wiedzy i pozwalające budować świadomość istniejących zagrożeń;
- zna i potrafi stosować w praktyce podstawowe zasady bezpiecznej pracy z internetem.

Opis treści:

- rozumienie bezpieczeństwa informacyjnego;
- podstawa programowa a bezpieczeństwo informacyjne;
- podstawowe zagrożenia bezpieczeństwa informacyjnego;
- podstawowe działania na rzecz bezpieczeństwa informacyjnego w szkole i w życiu prywatnym;
- bezpieczna praca z internetem i zagrożenia z nim związane;
- sposoby zapobiegania poznanym zagrożeniom;
- systemowa interwencja i profilaktyka w szkół;
- zasady postępowania w przypadku wystąpienia zagrożeń bezpieczeństwa informacyjnego;
- źródła wiedzy na temat bezpieczeństwa informacyjnego.



Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Seria filmów edukacyjnych *Bezpieczeństwo dzieci i młodzieży online* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/bezpieczenstwo-dzieci-i-mlodziezy-online.html>;
- Blog „Dane osobowe”: *Kradzież tożsamości w Internecie* – <https://blog-daneosobowe.pl/kradziez-tozsamosci-w-internecie>;
- Praca zbiorowa, (2017), *Bezpieczne media. Poradnik dla rodziców*, Warszawa: FDDS, Fundacja Orange – https://www.edukacja.fdds.pl/fc63516e-e941-4d-3c-827d-9febcb076630/Extras/broszura_Dziecko-i-media-19-09-2017.pdf;
- Wojtasik Ł. (red.), (2013), *Jak reagować na cyberprzemoc. Poradnik dla szkół*, Warszawa: FDDS – https://www.edukacja.fdds.pl/cb0428e3-c0d8-47cb-8508-1b865100a1f9/Extras/ksiazka-jak_reagowac_na_cyberprzemoc-FDDS-12042017.pdf;
- Wójcik S. (oprac.), (2017), *Jak postępować w przypadku (cyber) przemocy? Systemowa interwencja i profilaktyka w szkole* (Wyciąg z materiałów klicksafe), Warszawa: FDDS – <https://www.saferinternet.pl/pliki/publikacje/Jak%20post%C4%99powa%C4%87%20w%20cyberprzemocy.pdf>;
- Czajka R., Lipszyc J., (2014), *Poradnik bezpieczeństwa mobilnego*, Warszawa: Fundacja Nowoczesna Polska – <https://edukacjamedialna.edu.pl/media/chunks/attachment/poradnik-bezpieczenstwa-mobilnego.pdf>;
- Rządowa strona „Bezpieczna Szkoła +”: *Promujemy bezpieczeństwo w sieci* – materiały i scenariusze zajęć – <https://bezpiecznaszkola.men.gov.pl/tematy/promujemy-bezpieczenstwo-w-sieci/informacje/>;
- Lizut J., Wrońska A. (red.), (2018), *Standard bezpieczeństwa online placówek oświatowych*, Warszawa: NASK – https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf;
- Strona „Cyfrowo Bezpieczni”: *Procedury bezpieczeństwa cyfrowego w szkołach* – pakiet dokumentów MEN – <https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach>;
- Strona Fundacji Panoptikon „Cyfrowa Wyprawka”: *Bezpieczeństwo informacji w sieci* – <https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci>;
- Praca zbiorowa, (2017), *Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, Warszawa: MEN – <http://bezpiecznaszkola.men.gov.pl/wp-content/uploads/2017/09/zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizycznego-i-cyfrowego-uczniow.pdf>;



- Zespół ekspertów NASK, (2017), *Jak zapewnić uczniom bezpieczeństwo w internecie – poradnik dla nauczycieli*, Warszawa: NASK – <https://akademia.nask.pl/pliki/1-jak-zapewnic-uczniom-bezpieczenstwo-w-internecie-poradnik-dla-nauczycieli.pdf>;
- Chocholska P. i in. (oprac.), (2017), *Jak reagować na problem nadmiernego korzystania z internetu przez dzieci i młodzież. Poradnik dla szkół*, Warszawa: FDDS – https://www.edukacja.fdds.pl/60d2a7cf-56e9-4281-a3d3-c9d4377ef098/Extras/ksiazka-jak_reagowac_na_problem_nadmiernego_korzystania_z_internetu-FDDS-12042017.pdf;
- Podstawa programowa dla poszczególnych szkół i etapów edukacyjnych wprowadzona w 2017 r. – <https://podstawaprogramowa.pl>.



Blok 2: Dane osobowe

Cele operacyjne

Nauczyciel:

- wie, czym są dane osobowe i w jaki sposób są chronione;
- zna zmiany w przepisach prawnych o ochronie danych osobowych wprowadzone w 2018 roku;
- stosuje w praktyce zasady ochrony danych osobowych w życiu prywatnym i w szkole;
- potrafi chronić dane osobowe uczniów, nauczycieli i innych pracowników szkoły.

Opis treści:

- dane osobowe i przyczyny ich ochrony;
- formy ochrony danych osobowych w Polsce i w Unii Europejskiej – *Ogólne Rozporządzenie o Ochronie Danych Osobowych 2016/679 (RODO)* – zmiany w ochronie danych osobowych z 2018 roku;
- obowiązujące przepisy prawne;
- zasady ochrony danych osobowych w życiu prywatnym i w szkole;
- ochrona danych osobowych uczniów, nauczycieli oraz innych pracowników szkół;

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: Podstawy ochrony danych osobowych – <https://cyfrowa-wyprawka.org/lekcja/podstawy-ochrony-danych-osobowych>;
- Strona Fundacji Panoptykon: cykl artykułów *RODO na tacy, czyli jak możemy skorzystać na nowych przepisach* – <https://panoptykon.org/rodo-na-tacy>;
- Strona The EU General Data Protection Regulation (GDPR) na temat RODO – <https://gdprexplained.eu/pl>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: Wizerunek – jak chronić swoje prawa? – <https://cyfrowa-wyprawka.org/lekcja/wizerunek-jak-chronic-swoje-prawa>;
- Serwis edukacyjny „DODO – dbamy o dane osobowe” – <http://dodo-bezpiecznie.blogspot.com/>;



- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak dzieci i młodzież chronią swoją prywatność?* – https://giodo.gov.pl/560/id_art/4699/j/pl;
- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak bezpiecznie zwiedzać cyfrowy świat?* – <https://giodo.gov.pl/pl/1520208/8510>;
- Wykład otwarty z cyklu „Lekcje z GIODO” pt. *Elektroniczna dokumentacja szkolna i jej udostępnianie* – <https://www.youtube.com/watch?v=qwXla3bA1w8&feature=youtu.be>.



Blok 3: Prawo autorskie

Cele operacyjne

Nauczyciel:

- wie, czym są prawa autorskie i prawa pokrewne;
- zna zasady korzystania z cudzych utworów;
- zna praktyczne zastosowania dozwolonego użytku edukacyjnego;
- potrafi chronić prawa autorskie, w tym także autorów nieletnich.

Opis treści:

- prawa autorskie i prawa pokrewne;
- obowiązujące przepisy prawne;
- dozwolony użytek edukacyjny;
- pojęcie plagiatu;
- prawa autorskie osoby nieletniej;
- prawa autorskie nauczyciela.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Czerniawski P., Lipszyc J., Wilkowski M., *Pierwsza pomoc w prawie autorskim: przewodnik*, Warszawa: Fundacja Nowoczesna Polska – <https://prawokultury.pl/publikacje/pierwsza-pomoc>;
- Poradnia na stronie „Prawokultury.pl”: *Pierwsza pomoc w prawie autorskim: zapytaj prawnika* – <https://prawokultury.pl/pierwsza-pomoc>;
- Strona „Prawokultury.pl”: *Krótki kurs własności intelektualnej. Materiały dla uczelni* – hasło: *Plagiat* – <https://prawokultury.pl/kurs/plagiat>;
- Siewicz K., (2016), *Prawo autorskie w edukacji: jak unikać naruszeń?*, Warszawa: Fundacja Nowoczesna Polska – <http://koed.org.pl/wp-content/uploads/2016/11/prawo-autorskie-w-edukacji-jak-unikac-naruszen-wersja-2016-1.pdf>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Prawo autorskie dla każdego* – <https://cyfrowa-wyprawka.org/lekcja/prawo-autorskie-dla-kazdego>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Jak etycznie publikować w sieci?* – <https://cyfrowa-wyprawka.org/lekcja/jak-etycznie-publikowac-w-sieci>.

Część główna

Bezpieczeństwo informacyjne ucznia



Czas trwania części: 18 godzin (w tym 3 godziny online)

Blok 1: Czym jest bezpieczeństwo informacyjne

Cele operacyjne

Nauczyciel:

- wie, na czym polega bezpieczeństwo informacyjne;
- umie zapoznać uczniów z typowymi zagrożeniami bezpieczeństwa informacyjnego;
- potrafi z pomocą internetu określić podstawowe kierunki rozwoju mediów elektronicznych;
- potrafi przedstawić swoim uczniom podstawowe kierunki rozwoju mediów elektronicznych i wskazać zagrożenia z nimi związane;
- zna zasady bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych i sieci;
- potrafi zorganizować zajęcia dotyczące zasad bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych i sieci.

Opis treści:

- kierunki rozwoju mediów elektronicznych;
- bezpieczeństwo informacyjne – definicja;
- zasady bezpiecznego korzystania z urządzeń mobilnych, sieci i mediów elektronicznych;
- użycie w szkole mediów cyfrowych (i nie tylko);
- zalety i wady mediów cyfrowych;
- wykorzystanie treści internetowych do nauki;
- krytyczny odbiór informacji z różnych mediów.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Kubiak M., Topolewski S. (red.), (2016), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach – https://repozytorium.uph.edu.pl/bitstream/handle/11331/1205/Bezpieczenstwo_informacyjne_w_21_wieku.pdf?sequence=1?_TF;



- Filmy o kierunkach rozwoju mediów elektronicznych:
 - *A Day Made of Glass 2: Same Day. Expanded Corning Vision* (2012) – <https://youtu.be/jZkHpNnXLB0>;
 - *Epaper-Newspaper* (2009) – <https://youtu.be/0B28SHBmMNI>;
 - *Productivity Future Vision* (2011) – <https://youtu.be/a6cNdhOKwi0>;
- Wojtasik Ł., Maryl-Wójcik M., Topolewska K. (oprac.), (2017) *Dzień z życia – scenariusz zajęć*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=1&fnd=&grupa=0&offset=2&sort=1&szkolenie=1121#opisszkolenia;
- Henryk Batuta – hasło w Wikipedii – https://pl.wikipedia.org/wiki/Henryk_Batuta;
- *Dziecko uzależnione od komputera? Podpowiadamy, jak pomóc i gdzie szukać wsparcia!* – wywiad z Kariną Stasiak specjalistą terapii uzależnień – <http://www.uzaleznieniabehawioralne.pl/siecioholizm/dziecko-uzalezni-one-odkomputera-podpowiadamy-jak-pomoc-i-gdzie-szukac-wsparcia/>;
- Wrzesień-Gandolfo A. (red.), (2014), *Bezpieczeństwo dzieci online. Kompendium wiedzy*, Warszawa: NASK, FDDS – https://www.edukacja.fdds.pl/dd5bcf-09-cf2d-4340-9eb3-2c437ef66245/Extras/ksiazkaBezpieczenstwo_dzieci_online_Kompendium_dla_rodzicow_i_profesjonalistow-FDDS-12042017.pdf.



Blok 2: Korzystamy z informacji

Cele operacyjne

Nauczyciel:

- potrafi przygotować uczniów do wyszukiwania i wykorzystywania treści w internecie;
- umie zorganizować zajęcia przygotowujące uczniów do krytycznej oceny źródeł informacji;
- jest w stanie planować i organizować zajęcia wykorzystujące treści pochodzące z różnych mediów (w tym internetowe) do nauki;
- umie wytłumaczyć uczniom zasady korzystania z cudzych utworów;
- potrafi wyjaśnić zasady dozwolonego użytku w edukacji.

Opis treści:

- sposoby wyszukiwania rzetelnych informacji w internecie;
- krytyczna ocena wyszukiwanych treści;
- możliwości wykorzystywania cudzych prac;
- dozwolony użytek edukacyjny.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Lekcja: *Sprawne szukanie informacji* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/sprawne-szukanie-informacji>;
- Lekcja: *Gdy wybierasz dobre źródło* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/gdy-wybierasz-dobre-zrodlo>;
- Lekcja: *Jedna informacja a źródeł mnóstwo!* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/jedna-informacja-a-zrodel-mnostwo>;
- Lekcja: *Czym się różni informacja od opinii?* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/czym-sie-rozni-informacja-od-opinii>;
- Buchner A., *Jak rozróżniać informacje prawdziwe od fałszywych?*, Warszawa: Fundacja Orange – https://platforma.megamisja.pl/download/knowledge_base/scenario/8/Jak_rozrozniac_informacje_prawdziwe_od_falszywych.pdf;
- Lekcja: *Szanujmy twórców* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/szanujmy-tworcow>;



- Strona fotoprawo.pl: *Darmowe zdjęcia z sieci. Skąd brać? Jak korzystać?* – <https://fotoprawo.pl/index.php/2012/10/fakty-i-mity-czyli-o-prawach-autorskich-dla-blogerow/>;
- Lekcja: *Dozwolony użytek edukacyjny* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/dozwolony-uzytek-edukacyjny/>;
- Lekcja: *Otwarte zasoby – otwarte umysły* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/otwarte-zasoby-otwarte-umysly/>.



Blok 3: Ja jako autor

Cele operacyjne

Nauczyciel:

- zna podstawowe przepisy prawa autorskiego i praw pokrewnych;
- potrafi wyjaśnić uczniom zasady ochrony praw przysługujących im jako autorom;
- wie, gdzie znaleźć informacje na temat praw autorów nieletnich;
- jest świadom, na jakie użycie utworów pozwalają licencje Creative Commons.

Opis treści:

- ochrona utworów przygotowanych przez uczniów;
- praca ucznia na stronie internetowej szkoły;
- metody unikania plagiatu;
- wolne licencje Creative Commons.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Artykuł *Poznaj licencje Creative Commons* – <https://creativecommons.pl/poznaj-licencje-creative-commons/>;
- *Prawa autorskie ucznia* – porady ekspertów wydawnictwa OPERON – <http://oswiataiprawo.pl/porady/prawa-autorskie-ucznia/>;
- Lekcja: *Prawa wyłączne – twórcy i użytkownicy* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/prawa-wylaczne-tworcy-i-uzytkownicy/>;
- Lekcja: *Osobiste prawa autora* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/osobiste-prawa-autora/>;
- Strona fotoprawo.pl: *Fakty i mity, czyli o prawach autorskich dla blogerów* – <https://fotoprawo.pl/index.php/2012/10/fakty-i-mity-czyli-o-prawach-autorskich-dla-blogerow/>;
- *Prawo Autorskie? OK!* – kurs Ośrodka Edukacji Informatycznej i Zastosowań Komputerów – <http://pa.ok.oeiizk.waw.pl>;
- Lekcja: *Jak etycznie publikować w sieci?* na stronie „Edukacja medialna” – <https://edukacjamedialna.edu.pl/lekcje/jak-etycznie-publikowac-w-sieci/>.



Blok 4: Moje dane

Cele operacyjne

Nauczyciel:

- zna zasady ochrony wizerunku uczniów i nauczycieli i umie wykorzystywać tę wiedzę w szkole;
- potrafi planować i organizować zajęcia wspierające uczniów w dbaniu własny wizerunek;
- uwrażliwia uczniów na problem zabezpieczania danych;
- wie, jak zabezpieczać dane umieszczane w internecie;
- zna treść *Ogólnego Rozporządzenia o Ochronie Danych Osobowych 2016/679 (RODO)*;
- potrafi zapoznać uczniów z zapisami RODO, które ich bezpośrednio dotyczą.

Opis treści:

- ochrona wizerunku uczniów i nauczycieli;
- ochrona prywatności w internecie;
- podstawowe sposoby zabezpieczania danych w internecie;
- zapisy RODO dotyczące uczniów;
- umiejętność dbania o własne dane;
- problemy związane z publikacją zdjęć w internecie.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Lekcja: *Dane osobowe i ochrona tożsamości* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/dane-osobowe-i-ochrona-tozsamosci/>;
- Lekcja: *Kim jestem w internecie?* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/kim-jestem-w-internecie/>;
- Strona Fundacji Panoptykon: cykl artykułów RODO na tacy. Odcinek V: *Lekcje samoobrony, czyli jak skorzystać z praw, które daje RODO?* – <https://panoptykon.org/rodo-na-tacy-V>;
- Zmiany w ochronie danych osobowych dzieci – <https://samorząd.infor.pl/sektor/organizacja/rodo-2018/767926,Zmiany-w-ochronie-danych-osobowych-dzieci-po-25-maja-2018-r.html>;



- Stępniewski R., (2018), *RODO i nowe prawa osób, których dane dotyczą*, Warszawa: Rzetelna Grupa – <https://www.politykabezpieczenstwa.pl/pl/a/rodo-i-nowe-prawa-osob-ktorych-dane-dotyczy>;
- Lekcja: *Jak wzmocnić swoją prywatność?* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/jak-wzmocnic-swoja-prywatnosc/>;
- *Kurs Cyfrowego Obywatelstwa i Bezpieczeństwa* Fundacji Szkoła z Klasą – <https://obywatelstwocyfrowe.szkolazklasa.org.pl/>;
- Staśkiewicz J., (2017), *Prosty i szybki sposób na bezpieczne przestanie poufnych danych* – artykuł na blogu „OpenSecurity.pl” – <https://opensecurity.pl/prosty-i-szybki-sposob-na-bezpieczne-przeslanie-poufnych-danych/>;
- FDDS, (2016), *Seksting – scenariusz zajęć dla uczniów szkół ponadpodstawowych*, Warszawa: FDDS; https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=1&fnd=&grupa=0&offset=1&sort=1&szkolenie=15246&tekst=-seksing&criteria=&blotem=#opisszkolenia;
- Lekcja: *Cyfrowy portret, czyli kilka słów o wizerunku w Internecie* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/cyfrowy-portret-czyli-kilka-slow-o-wizerunku-w-internecie/>;
- Golański A., (2018), *Używasz Facebooka? Sprawdź, czy 15 pytań wystarczy, by zgadnąć, kim jesteś* – artykuł na stronie „dobreprogramy.pl” – <https://www.dobreprogramy.pl/Uzywasz-Facebooka-Sprawdz-czy-15-pytan-wystarczy-by-zgadnac-kim-jestes,News,87214.html>.



Blok 5: Bezpiecznie w sieci

Cele operacyjne

Nauczyciel:

- potrafi kształtować świadomość uczniów w zakresie zagrożeń występujących w internecie;
- umie uświadamiać uczniów na temat możliwych zagrożeń związanych z używaniem i nadużywaniem technologii;
- promuje wśród uczniów zasady bezpiecznego zachowania w sieci;
- uwrażliwia uczniów na problem nadmiernego korzystania z mediów, w tym internetu;
- potrafi wskazać uczniom podstawowe sposoby radzenia sobie z hejtem i cyberprzemocą, a także zapobiegania tym zjawiskom;
- zwraca uwagę uczniów na problem publikacji wizerunku w internecie i jego konsekwencje;
- potrafi wskazać uczniom miejsca, w których mogą uzyskać pomoc w przypadku zaistnienia zagrożenia sieciowego.

Opis treści:

- zagrożenia internetowe;
- podstawowe problemy związane z korzystaniem z sieci;
- szkodliwe i niebezpieczne treści w internecie;
- problem utraty danych i anonimowości;
- nadmierne korzystanie przez młodzież z mediów elektronicznych i internetu;
- budowanie relacji w oparciu o wzajemny szacunek;
- cyberprzemoc i sposoby zapobiegania jej;
- wsparcie uczniów doświadczających cyberprzemocy (w tym hejtu i obrażania w sieci).

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Film *Jonasa magiczna sztuczka ze znikaniem* – kampania Policji w Lozannie służąca poprawie bezpieczeństwa pieszych – https://www.youtube.com/watch?v=TP6L41rjK_I;



- Film *Nadużywanie internetu przez dzieci i młodzież* opublikowany przez FDDS – <https://youtu.be/3CZXHJWsung>;
- Film *E-uzależnienia* wyprodukowany przez Telewizję Kopernik – <https://youtu.be/t4t-DKy8B1c>;
- Film *Uważaj, co udostępniasz. Social media stalker* na kanale „Z Dobrym Słowem” – <https://youtu.be/CLRBYhd7e4Q>;
- Lekcja: *Netykieta, czyli o kulturze w internecie* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/netykieta-czyli-o-kulturze-w-internecie/>;
- Dziemidowicz E., Wojtasik Ł., (2017), *Lekcja bezpieczeństwa – scenariusz zajęć*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=9&fnd=&grupa=0&offset=1&sort=1&szkolenie=1114&tekst=1114#opisszkolenia;
- „Digital Youth. Magazyn o fenomenach internetu” nr 3 (05) 2017 – https://www.edukacja.fdds.pl/de4062e0-62db-4daf-b7ce-be4bfb32c2bd/Extras/broszura-digital-youth_3-2017.pdf;
- *Skrywany płacz, wzrost agresji, chroniczny smutek – oto sygnały świadczące o tym, że twoje dziecko może być ofiarą przemocy w internecie* – artykuł na portalu Onet.pl – https://www.onet.pl/?utm_source=kobieta_viasg&utm_medium=nitro&utm_campaign=allonet_nitro_new&srcc=ucs&pid=af119100-47d8-418e-b08b-e0b66b0a1b9f&sid=63eeb4cc-4788-4ae3-a160-ddd0a01f6209&utm_v=2;
- Dziemidowicz E., Kępka M., (2017), *Internet bez hejtu. Scenariusz pikniku edukacyjnego*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&tekst=15447;
- Lekcja: *Słowa, które ranią* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/slowa-ktore-rania/>;
- „Rufus w opałach” – interaktywna decyzyjna gra video: informacje o grze na stronie akademia.nask.pl – <https://akademia.nask.pl/gru.html>;
- „Rufus w opałach”. Interaktywna decyzyjna gra video – scenariusze zajęć – <https://akademia.nask.pl/pobierz.php?i=115&hash=bd17>;
- „Odkrywcy Internetu” – gra planszowa: informacje o grze i materiały do pobrania – <http://wbp.poznan.ekursy.eu/course/view.php?id=27>;
- Lekcja: *Prawo do prywatności w sieci* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/prawo-do-prywatnosci-w-sieci>;
- *Kim są patostreamerzy i co to w ogóle jest?* – artykuł na blogu „ZUCH.media” – <http://zuch.media/kim-sa-patostreamerzy/>;
- *Gdzie szukać pomocy?* – wskazówki na stronie [cyfrowobezpieczni.pl](http://www.cyfrowobezpieczni.pl) – <https://www.cyfrowobezpieczni.pl/gdzie-szukac-pomocy>.

Przykładowy rozkład treści



Część wstępna (7 godzin)				
Działania nauczyciela a bezpieczeństwo informacyjne				
Blok	Tytuł bloku	Ilość godzin		Treści kształcenia
		stacjonarnych	online	
1	<i>Bezpieczeństwo informacyjne – podstawy</i>	3	1	1.1, 1.2, 1.3, 1.4, 1.5
2	<i>Prawo autorskie</i>	1	0,5	2.1, 2.2, 2.3, 2.4
3	<i>Dane osobowe</i>	1	0,5	3.1, 3.2, 3.3, 3.4
	Razem godzin	5	2	

Część główna (18 godzin)				
Bezpieczeństwo informacyjne ucznia				
Blok	Tytuł bloku	Ilość godzin		Treści kształcenia
		stacjonarnych	online	
1	<i>Czym jest bezpieczeństwo informacyjne</i>	3	0,5	1.2, 1.5, 1.6
2	<i>Korzystamy z informacji</i>	3	0,5	1.4, 2.3, 2.4
3	<i>Ja jako autor</i>	3	0,5	2.1, 2.2, 2.5
4	<i>Moje dane</i>	3	1	3.1, 3.2, 3.3, 3.4, 4.2
5	<i>Bezpiecznie w sieci</i>	3	0,5	4.1, 4.2, 4.3, 4.4, 4.5, 4.6
	Razem godzin	15	3	

Przykładowe scenariusze zajęć



Scenariusz zajęć nr 1

Część zajęć: Część wstępna – *Działania nauczyciela a bezpieczeństwo informacyjne*

Blok tematyczny: Blok 1 – *Bezpieczeństwo informacyjne – podstawy*

Temat zajęć: *Bezpieczeństwo informacyjne a podstawa programowa przedmiotu, którego nauczam*

Czas zajęć: 35 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić uczniom, na czym polega bezpieczeństwo informacyjne;
- znaleźć w podstawie programowej nauczanego przez siebie przedmiotu zapisy dotyczące bezpieczeństwa informacyjnego;
- łączyć na zajęciach zagadnienia z różnych obszarów edukacyjnych z tematyką bezpieczeństwa informacyjnego.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca indywidualna uczestników przy komputerach;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- aplikacja online – np. Padlet (lub analogiczna);
- edytor tekstu;
- platforma e-learningowa.



Zasoby do wykorzystania:

- Film *A Day Made of Glass 2: Same Day. Expanded Corning Vision* (2012) – <https://youtu.be/jZkHpNnXLB0>;
- Kubiak M., Topolewski S. (red.), (2016), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach – https://repozytorium.uph.edu.pl/bitstream/handle/11331/1205/Bezpieczenstwo_informacyjne_w_21_wieku.pdf?sequence=1\U;
- Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnościami intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. z 2017 r., poz. 356) – <http://www.dziennikustaw.gov.pl/DU/2017/356>.

Formy oceny:

Uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Projekcja filmu
Uczestnicy oglądają film *A Day Made of Glass 2: Same Day. Expanded Corning Vision* (2012). Po projekcji prowadzący zaczyna rozmowę na temat kierunku rozwoju mediów elektronicznych. Zwraca uwagę, że film przedstawia wizję przyszłości wykreowaną w 2012 roku. Pyta uczestników, czy zauważyli w przedstawionej rzeczywistości jakieś elementy, które dziś już są dostępne.
2. Dyskusja
Prowadzący inicjuje burzę mózgów, pytając uczestników, czy dostrzegają jakieś zagrożenia związane z dynamicznym rozwojem technologii. Zwraca uwagę na aspekty związane z przechowywaniem informacji i dostępem do nich.
3. Praca z tekstem
Prowadzący dzieli uczestników na kilka zespołów (w zależności od nauczanego przez nich przedmiotu) i zaprasza do pracy z tekstem *Bezpieczeństwo informacyjne w XXI wieku*. Prosi każdą z grup o przygotowanie kilku slajdów



prezentacji wyjaśniających, na czym polega bezpieczeństwo informacyjne. Moderuje pracę uczestników w taki sposób, aby zostały wykorzystane różne podejścia do zagadnienia bezpieczeństwa informacyjnego.

4. Odniesienie do podstaw programowych

Kolejnym krokiem w pracy zespołów jest umieszczenie w stworzonych prezentacjach slajdów zawierających odwołania do podstaw programowych przedmiotów nauczanych przez członków danej grupy. Należy wskazać te zapisy, które dotyczą kwestii bezpieczeństwa informacyjnego.

5. Prezentacja prac

Po zakończeniu pracy zespoły udostępniają i wzajemnie oceniają swoje prezentacje, omawiają w szczególności miejsca korelacji podstawy programowej różnych przedmiotów z treściami dotyczącymi bezpieczeństwa informacyjnego. Następuje krótka dyskusja dotycząca bezpieczeństwa informacyjnego w szkole i życiu prywatnym. Prowadzący zapisuje wnioski nauczycieli dotyczące tego tematu.

6. Podsumowanie

Na zakończenie zajęć prowadzący zbiera wnioski i dokonuje zwięzłej oceny pracy nauczycieli. Opracowane materiały zostają umieszczone w miejscu dostępnym dla uczestników szkolenia – np. w notesie OneNote danej grupy szkoleniowej w chmurze lub na platformie e-learningowej.



Scenariusz zajęć nr 2

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 1 – *Bezpieczeństwo informacyjne – podstawy*

Temat zajęć: *Fałszywe informacje w sieci*

Czas zajęć: 30 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić uczniom, na czym polega bezpieczeństwo informacyjne;
- znaleźć w podstawie programowej nauczanego przez siebie przedmiotu zapisy dotyczące bezpieczeństwa informacyjnego;
- łączyć na zajęciach zagadnienia z różnych obszarów edukacyjnych z tematyką bezpieczeństwa informacyjnego;
- przedstawić uczniom przykłady stron internetowych zawierających niezrelatywne informacje.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca indywidualna uczestników przy komputerach;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- aplikacja notes OneNote Online, Padlet (lub analogiczna);
- edytor tekstu;
- platforma e-learningowa.



Zasoby do wykorzystania:

- *Henryk Batuta* – hasło w *Wikipedii* – https://pl.wikipedia.org/wiki/Henryk_Batuta;
- Mapy Google – <https://www.google.pl/maps>;

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Praca z wirtualną mapą i tekstem z *Wikipedii*
Prowadzący prosi, aby uczestnicy szkolenia skorzystali z komputerów i otworzyli aplikację Mapy Google. Na ekranie projektora wyświetla starą fotografię przedstawiającą fasadę domu przy ulicy Henryka Batuty 1. w Warszawie. Pyta uczestników, czy dostrzegają na tym zdjęciu coś podejrzanego. Jeśli pojawią się głosy, że tabliczki z nazwami ulic wyglądają w rzeczywistości inaczej – objaśnia, że zdjęcie zostało wykonane przed wprowadzeniem obecnej identyfikacji wizualnej w Warszawie. Następnie prosi, aby uczestnicy na mapie Google odszukali ulicę Batuty i określili, w której części Warszawy ona się znajduje. Po wykonaniu przez nich ćwiczenia prowadzący wyjaśnia, że właśnie w tej chwili ich bezpieczeństwo informacyjne zostało zagrożone. Prowadzący prosi o wyszukanie w *Wikipedii* informacji o *Henryku Batucie* – uczestnicy przekonują się, że jest to postać fikcyjna.
2. Definicja bezpieczeństwa informacyjnego
Prowadzący przytacza definicję bezpieczeństwa informacyjnego stworzoną przez L. Korzeniowskiego, który skupia się na bezpieczeństwie informacyjnym podmiotu (człowieka lub organizacji), które rozumie jako „(...) możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą”. Następnie rozpoczyna dyskusję na temat jakości informacji dostępnych w internecie.
3. Weryfikowanie informacji
Prowadzący prosi uczestników szkolenia o wskazanie sposobów weryfikowania informacji znalezionych w internecie. Propozycje zostają zapisane na tablicy lub w innym miejscu, na bieżąco trwa dyskusja na temat jakości przedstawianych pomysłów.



4. Podsumowanie

Na zakończenie prowadzący podsumowuje zajęcia, podaje sposoby weryfikowania informacji i chwali uczestników za wykonanie dobrej pracy.



Scenariusz zajęć nr 3

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 5 – *Bezpiecznie w sieci*

Temat zajęć: *Złe decyzje Rufusa*

Czas zajęć: 60 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić uczniom, na czym polegają niebezpieczne zachowania w internecie;
- uczulić uczniów na problem nadmiernego korzystania z sieci;
- wskazać zagrożenia związane z utratą anonimowości;
- przedstawić uczniom sposoby zapobiegania cyberprzemocy.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca indywidualna uczestników przy komputerach;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- aplikacja notes OneNote Online, Padlet (lub analogiczna);
- gra decyzyjna „Rufus w opałach” zainstalowana na komputerze prowadzącego;
- platforma e-learningowa.

Zasoby do wykorzystania:

- Decyzyjna gra video „Rufus w opałach”.



Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Zapoznanie z grą

Prowadzący prosi, aby uczestnicy szkolenia ustawili swoje krzesła i usiedli przed ekranem. Następnie na ekranie projektora uruchamia grę decyzyjną „Rufus w opałach”. Prosi uczestników, aby ustalili, w jaki sposób będą podejmowali decyzje dotyczące postępowania bohatera gry w określonych sytuacjach. Prowadzący przeprowadza grę do końca zgodnie z sugestiami uczestników.

2. Dyskusja na temat gry

Prowadzący wyjaśnia, że w zależności od decyzji podjętych w trakcie gry możliwe są różne jej zakończenia i zachęca, aby uczestnicy zapoznali się po zajęciach z innymi wariantami. Prosi uczestników, by podzielili się wrażeniami i ocenili „Rufusa w opałach” jako narzędzie dydaktyczne – następuje krótka rozmowa dotycząca wad i zalet przedstawionej gry.

3. Scenariusze zajęć

Uczestnicy zostają podzieleni na kilkusobowe zespoły. Prowadzący prosi ich o stworzenie scenariuszy zajęć, które mogliby przeprowadzić ze swoimi uczniami, w oparciu o wykorzystanie poznanej gry.

4. Podsumowanie

Na zakończenie zajęć uczestnicy przedstawiają swoje pomysły i wzajemnie je oceniają. Wytworzone przez nauczycieli scenariusze zostają umieszczone w notesie OneNote w chmurze lub na platformie e-learningowej.



Scenariusz zajęć nr 4

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 5 – *Bezpiecznie w sieci*

Temat zajęć: *Nadużywanie technologii*

Czas zajęć: 60 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić uczniom, na czym polega bezpieczeństwo informacyjne;
- podać przykłady konsekwencji wynikających z nadużywania technologii w życiu codziennym;
- zwrócić uwagę uczniów na zagrożenia związane z użytkowaniem technologii informacyjnych;
- wskazać miejsca, w których można uzyskać pomoc w razie utraty bezpieczeństwa.

Metody nauczania:

- rozmowa;
- burza mózgów
- praca indywidualna uczestników przy komputerach;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- aplikacja OneNote Online, Padlet (lub analogiczna);
- edytor tekstu;
- platforma e-learningowa.



Zasoby do wykorzystania:

- Film *Jonasa magiczna sztuczka ze znikaniem* – kampania Policji w Lozannie służąca poprawie bezpieczeństwa pieszych – https://www.youtube.com/watch?v=TP6L41rjK_I.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Bezpieczeństwo pieszych
Prowadzący zaczyna zajęcia od wyświetlenia spotu: *Jonasa magiczna sztuczka ze znikaniem* stworzonego na zamówienie policji z Lozanny na potrzeby kampanii służącej poprawie bezpieczeństwa pieszych. Po obejrzeniu filmu prowadzący zaprasza uczestników do rozmowy na temat zagrożeń związanych z używaniem i nadużywaniem technologii. W jej trakcie powinny zostać omówione niebezpieczeństwa, które można zakwalifikować do grup takich jak: zagrożenia fizyczne, psychiczne, moralne, społeczne, intelektualne.
2. Rodzaje zagrożeń – praca w grupach
Prowadzący dzieli uczestników na pięć grup i prosi, aby każda z nich opracowała przewodnik po wskazanej grupie zagrożeń. Gotowy przewodnik powinien: zawierać krótką charakterystykę zagrożeń z danej grupy, wskazywać kilka czynników prowadzących do wystąpienia tego typu sytuacji, omawiać działania profilaktyczne i możliwe sposoby reagowania na wystąpienie tego rodzaju niebezpieczeństw, a także podpowiadać, gdzie należy szukać pomocy, jeśli zetkniemy się z zagrożeniami z tej grupy. Po zakończeniu pracy następuje prezentacja efektów działań poszczególnych zespołów i ocena przydatności wytworzonych materiałów do wykorzystania podczas zajęć w szkole.
3. Quiz
Prowadzący demonstruje uczestnikom działanie platformy Kahoot! W formie quizu składającego się z kilku pytań dotyczących zagrożeń internetowych sprawdza ich wiedzę. Następnie zaprasza zespoły do komputerów i prosi o przygotowanie podobnego quizu z wykorzystaniem opracowanych materiałów.



4. Podsumowanie

Na zakończenie zajęć każdy zespół przeprowadza przygotowany przez siebie quiz wśród pozostałych uczestników i następuje ocena zdobytych wiadomości.



Scenariusz zajęć nr 5

Część zajęć: Część główna – Bezpieczeństwo informacyjne ucznia

Blok tematyczny: Blok 4 – Moje dane

Temat zajęć: Zabezpieczanie danych przed innymi

Czas zajęć: 40 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wytłumaczyć uczniom, dlaczego należy zabezpieczać swoje dane, przekazując je za pomocą internetu;
- podać kilka najbardziej popularnych sposobów zabezpieczenia danych;
- wyjaśnić, w jaki sposób zabezpieczyć pliki przechowywane na komputerze i wysyłane mailowo.

Metody nauczania:

- rozmowa;
- praca indywidualna uczestników przy komputerach.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową i zainstalowanym programem 7zip dla każdego uczestnika szkolenia;
- aplikacja OneNote Online, Padlet (lub analogiczna);
- edytor tekstu;
- platforma e-learningowa.

Zasoby do wykorzystania:

- aplikacja do archiwizacji plików 7zip do pobrania ze strony: <https://7-zip.org.pl/>;
- instrukcja obsługi programu 7zip na stronie magazynu „Komputer Świat” – <http://www.komputerswiat.pl/poradniki/programy/7-zip/2015/09/najlepsze-porady-do-7-zip.aspx>.



Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Przygotowanie

Przed zajęciami prowadzący umieszcza w chmurze zabezpieczony hasłem plik z jakimiś „bardzo ważnymi” informacjami – np. instrukcją obsługi programu 7zip – i generuje link do jego pobrania, który rozsyła do wszystkich uczestników.

2. Praca z programem 7zip

Po rozpoczęciu zajęć prowadzący prosi uczestników o pobranie wskazanego pliku na pulpity ich komputerów, a także odczytanie przesłanej wiadomości. Gdy uczestnicy zaczynają zgłaszać problemy z otwarciem pliku spowodowane koniecznością wpisania nieznanego im hasła, prowadzący rozpoczyna dyskusję dotyczącą zabezpieczania ważnych plików umieszczanych w sieci lub przesyłanych za pomocą internetu. Uczestnicy zastanawiają się, jakie treści powinny być zabezpieczane i dlaczego. Prowadzący prosi, by nauczyciele określili sposób, w jaki należy przekazywać hasło do pliku, aby zabezpieczenie okazało się skuteczne.

3. Zabezpieczanie hasłem w teorii i praktyce

Prowadzący dyktuje hasło do odczytania pliku. Uczestnicy zapoznają się z instrukcją tworzenia archiwów zabezpieczonych hasłem. Prowadzący prosi uczestników o stworzenie pliku tekstowego z bardzo ważną poradą dotyczącą bezpieczeństwa informacyjnego, a następnie o zabezpieczenie pliku hasłem i przekazanie uczestnikowi siedzącemu obok. Uczestnicy przekazują sobie hasła do plików i odczytują otrzymane informacje.

4. Podsumowanie ćwiczenia

Prowadzący zwraca uwagę, że wszyscy powinni zabezpieczać pliki w przedstawiony na zajęciach sposób, jeśli przesyłają w nich dane osobowe swoje lub innych osób np. do banków, organizatorów wycieczek lub urzędów.

Ramowy program szkoleń

dla nauczycieli trzeciego etapu kształcenia odpowiedzialnych
za nauczanie w zakresie bezpieczeństwa informacyjnego
w szkołach ponadpodstawowych



Informacje ogólne

Program szkolenia został opracowany w taki sposób, aby mogło ono przygotować nauczycieli szkół ponadpodstawowych do wdrażania wybranych aspektów bezpieczeństwa informacyjnego podczas zajęć różnych przedmiotów, szczególnie informatyki. W programie uwzględniono doświadczenia osób dorosłych oraz zachowania, które mogą mieć wpływ na występowanie zagrożeń w zakresie bezpieczeństwa informacyjnego w życiu prywatnym i zawodowym.

Forma realizacji

Szkolenie jest realizowane w formie mieszanej (*blended learning*).

Czas trwania

25 godzin dydaktycznych (w tym 5 godzin online)

Liczebność grupy

Maksymalnie 14 osób

Uczestnicy

Szkolenie przeznaczone jest dla nauczycieli trzeciego etapu kształcenia (szkoły ponadpodstawowej) odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego.

Wymagania wstępne

Wymagana jest umiejętność posługiwania się komputerem i typowymi urządzeniami peryferyjnymi (klawiatura, monitor, mysz, drukarka) oraz pracy w środowisku Windows w zakresie: zarządzania folderami i plikami, uruchamiania programów, korzystania z podręcznych aplikacji Windows. Przygotowanie do szkolenia obejmuje uczestnictwo w kursach online „Bezpieczeństwo w komunikacji i w mediach” oraz



„Korzystanie z informacji” dostępnych na stronie <https://e-kursy.ore.edu.pl/>. Zalecane jest ukończenie 1. modułu każdego z wymienionych kursów przed rozpoczęciem szkolenia oraz kontynuacja nauki na obu kursach online po jego ukończeniu.

Cele ogólne szkolenia

W części wstępnej:

- rozwijanie kompetencji merytorycznych poprzez zapoznanie nauczycieli z zagadnieniami dotyczącymi bezpieczeństwa informacyjnego w instytucjach oświatowych.

W części głównej:

- rozwijanie kompetencji medialnych i technicznych nauczycieli poprzez przygotowanie ich do wykorzystania narzędzi technologii informacyjno-komunikacyjnych w celu organizowania zajęć związanych z bezpieczeństwem informacyjnym;
- przygotowanie nauczycieli do omawiania zagadnień dotyczących bezpieczeństwa informacyjnego na zajęciach nauczanych przez nich przedmiotów.

Cele szczegółowe:

- zapoznanie nauczycieli z kierunkami rozwoju mediów elektronicznych i wskazywanie zagrożeń z nimi związanych;
- uświadomienie typowych zagrożeń bezpieczeństwa informacyjnego w pracy i życiu prywatnym;
- ukazanie korelacji treści związanych z bezpieczeństwem informacyjnym z podstawą programową poszczególnych przedmiotów;
- poznanie przez nauczycieli zasad bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych i sieci;
- wskazanie uczestnikom zasad bezpiecznej pracy w chmurze;
- przygotowanie nauczycieli do organizowania działań profilaktycznych w placówce;
- poszerzenie wiedzy uczestników na temat prawa autorskiego i praw pokrewnych;
- rozwijanie umiejętności ochrony danych osobowych uczniów, nauczycieli i innych pracowników placówki;
- zapoznanie uczestników z treścią RODO i jego zapisami dotyczącymi edukacji;
- poznanie podstawowych sposobów zabezpieczania danych w internecie;



- przyswojenie przez uczestników zasad dbania o własny wizerunek w sieci;
- uświadomienie nauczycielom możliwych konsekwencji opublikowania własnego lub cudzego wizerunku w sieci;
- zwrócenie uwagi uczestników na problem utraty tożsamości i możliwość kompromitacji w sieci;
- wyczulenie uczestników na oszustwa internetowe i ich konsekwencje;
- zapoznanie nauczycieli z problemem sekstingu i uwodzenia w sieci;
- uświadomienie uczestnikom konsekwencji cyberprzemocy;
- zapoznanie nauczycieli z problemem nadmiernego korzystania z mediów elektronicznych i internetu;
- wykształcenie podstawowych sposobów reagowania na niebezpieczeństwa internetowe;
- wskazanie nauczycielom miejsc, w których można uzyskać pomoc w przypadku zaistnienia cyberprzemocy.

Treści kształcenia

1. Bezpieczeństwo informacyjne w szkole i poza nią

- 1.1. Kierunki rozwoju mediów elektronicznych i zagrożenia z nimi związane;
- 1.2. Typowe zagrożenia bezpieczeństwa informacyjnego;
- 1.3. Korelacja treści dotyczących bezpieczeństwa informacyjnego z podstawą programową poszczególnych przedmiotów;
- 1.4. Zasady bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych i sieci;
- 1.5. Właściwości chmury i sposoby bezpiecznego korzystania z niej;
- 1.6. Organizacja działań profilaktycznych wśród uczniów i pracowników placówki oświatowej.

2. Prawa autorskie i prawa pokrewne

- 2.1. Przepisy prawa autorskiego i praw pokrewnych;
- 2.2. Pojęcie plagiatu w kontekście przygotowywania i publikowania autorskich materiałów dydaktycznych;
- 2.3. Dozwolony użytek w edukacji;
- 2.4. Publikacja materiałów w sieci a prawo autorskie.

3. Ochrona danych osobowych

- 3.1. Dane osobowe uczniów i pracowników placówki edukacyjnej oraz ich ochrona;
- 3.2. Treść RODO – prawa uczniów i obowiązki placówki edukacyjnej;
- 3.3. Podstawowe sposoby zabezpieczania danych w internecie;
- 3.4. Wizerunek ucznia i nauczyciela oraz jego ochrona.



4. Bezpieczne korzystanie z internetu

- 4.1. Konsekwencje hejtu i cyberprzemocy;
- 4.2. Publikacja wizerunku w sieci i jej konsekwencje;
- 4.3. Utrata tożsamości i kompromitacja w sieci;
- 4.4. Oszustwa internetowe;
- 4.5. Seksting i uwodzenie w sieci;
- 4.6. Problem nadmiernego korzystania z mediów elektronicznych i internetu;
- 4.7. Sposoby reagowania na niebezpieczeństwa internetowe i poszukiwanie pomocy.

Rekomendowane formy i metody realizacji:

- wykład wzbogacony prezentacją multimedialną (lub innymi materiałami multimedialnymi) – służący zaznajomieniu uczestników z nowymi dla nich zagadnieniami;
- praca indywidualna słuchaczy podczas wykonywania rozmaitych ćwiczeń związanych z przedstawianą problematyką;
- praca w grupach i dzielenie się uczestników wypracowanymi wnioskami oraz materiałami – np. w formie prezentacji;
- gry dydaktyczne – pozwalające zasugerować przykładowe metody pracy z uczniami;
- analiza tekstów związanych z tematyką szkolenia;
- mapy myśli – ułatwiające wizualne opracowanie omawianych zagadnień;
- dyskusje – pozwalające na wymianę poglądów i doświadczeń pomiędzy słuchaczami oraz prowadzącym (problemy przedstawiane przez prowadzącego oraz słuchaczy);
- rozmowy, interaktywne quizy, obserwacja działań uczestników szkolenia, wspólna analiza wypracowanych materiałów – jako formy weryfikacji i oceny zdobywanej wiedzy.

Niezbędne oprogramowanie:

- system operacyjny Windows;
- przeglądarka internetowa – np. Firefox, Chrome;
- pakiet biurowy Microsoft Office lub LibreOffice;
- poczta elektroniczna;
- platforma społecznościowa np. Facebook;
- platforma e-learningowa;
- darmowe aplikacje używane podczas zajęć (np. Padlet, Kahoot!, MakebeliefsComix, LearningApps).

Część wstępna

Działania nauczyciela a bezpieczeństwo informacyjne w placówce oświatowej



Czas trwania części: 7 godzin (w tym 2 godziny online)

Blok 1: Bezpieczeństwo informacyjne – podstawy

Cele operacyjne

Nauczyciel:

- potrafi definiować bezpieczeństwo informacyjne;
- zna zapisy podstawy programowej dotyczące bezpieczeństwa informacyjnego w szkole;
- umie rozpoznać podstawowe zagrożenia bezpieczeństwa informacyjnego i zna sposoby zapobiegania im;
- potrafi prowadzić podstawowe działania profilaktyczne na rzecz bezpieczeństwa informacyjnego w szkole;
- zna zasady postępowania w przypadku zagrożenia bezpieczeństwa informacyjnego i potrafi zastosować je w praktyce;
- wskazuje źródła, które może wykorzystać podczas organizowania działań mających na celu rozpowszechnianie wiedzy i pozwalających wzmacniać wśród uczniów świadomość istniejących zagrożeń;
- zna i stosuje w praktyce podstawowe zasady bezpiecznej pracy z internetem.

Opis treści:

- definicja bezpieczeństwa informacyjnego;
- podstawa programowa a bezpieczeństwo informacyjne;
- podstawowe zagrożenia bezpieczeństwa informacyjnego;
- podstawowe działania na rzecz bezpieczeństwa informacyjnego w szkole i w życiu prywatnym;
- bezpieczna praca z internetem i zagrożenia z nim związane;
- sposoby zapobiegania poznanyim zagrożeniom;
- systemowa interwencja i profilaktyka w szkół;
- zasady postępowania w przypadku wystąpienia zagrożeń bezpieczeństwa informacyjnego;
- źródła wiedzy na temat bezpieczeństwa informacyjnego.



Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Seria filmów edukacyjnych *Bezpieczeństwo dzieci i młodzieży online* – <https://www.saferinternet.pl/materialy-edukacyjne/materialy-multimedialne/bezpieczenstwo-dzieci-i-mlodziezy-online.html>;
- Blog „Dane osobowe”: *Kradzież tożsamości w Internecie* – <https://blog-daneosobowe.pl/kradziez-tozsamosci-w-internecie>;
- Praca zbiorowa, (2017), *Bezpieczne media. Poradnik dla rodziców*, Warszawa: FDDS, Fundacja Orange – https://www.edukacja.fdds.pl/fc63516e-e941-4d3c-827d-9febcbf076630/Extras/broszura_Dziecko-i-media-19-09-2017.pdf;
- Wojtasik Ł. (red.), (2013), *Jak reagować na cyberprzemoc. Poradnik dla szkół*, Warszawa: FDDS – https://www.edukacja.fdds.pl/cb0428e3-c0d8-47cb-8508-1b865100a1f9/Extras/ksiazka-jak_reagowac_na_cyberprzemoc-FDDS-12042017.pdf;
- Wójcik S. (oprac.), (2017), *Jak postępować w przypadku (cyber) przemocy? Systemowa interwencja i profilaktyka w szkole* (Wyciąg z materiałów klicksafe), Warszawa: FDDS – <https://www.saferinternet.pl/pliki/publikacje/Jak%20post%C4%99powa%C4%87%20w%20cyberprzemocy.pdf>;
- Czajka R., Lipszyc J., (2014), *Poradnik bezpieczeństwa mobilnego*, Warszawa: Fundacja Nowoczesna Polska – <https://edukacjamedialna.edu.pl/media/chunks/attachment/poradnik-bezpieczenstwa-mobilnego.pdf>;
- Rządowa strona „Bezpieczna Szkoła +”: *Promujemy bezpieczeństwo w sieci* – materiały i scenariusze zajęć – <https://bezpiecznaszkola.men.gov.pl/tematy/promujemy-bezpieczenstwo-w-sieci/informacje/>;
- Lizut J. Wrońska A. (red.), (2018), *Standard bezpieczeństwa online placówek oświatowych*, Warszawa: NASK – https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf;
- Strona „Cyfrowo Bezpieczni”: *Procedury bezpieczeństwa cyfrowego w szkołach* – pakiet dokumentów MEN – <https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Bezpieczeństwo informacji w sieci* – <https://cyfrowa-wyprawka.org/lekcja/bezpieczenstwo-informacji-w-sieci>;



- Praca zbiorowa, (2017), *Bezpieczna Szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, Warszawa: MEN – <http://bezpiecznaszkola.men.gov.pl/wp-content/uploads/2017/09/zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizyczne-go-i-cyfrowego-uczniow.pdf>;
- Zespół ekspertów NASK, (2017), *Jak zapewnić uczniom bezpieczeństwo w internecie – poradnik dla nauczycieli*, Warszawa: NASK – <https://akademia.nask.pl/pliki/1-jak-zapewnic-uczniom-bezpieczenstwo-w-internecie-poradnik-dla-nauczycieli.pdf>;
- Chocholska P. i in. (oprac.), (2017), *Jak reagować na problem nadmiernego korzystania z internetu przez dzieci i młodzież. Poradnik dla szkół*, Warszawa: FDDS – https://www.edukacja.fdds.pl/60d2a7cf-56e9-4281-a3d3-c9d4377ef098/Extras/ksiazka-jak_reagowac_na_problem_nadmiernego_korzystania_z_internetu-FDDS-12042017.pdf;
- Podstawa programowa dla poszczególnych szkół i etapów edukacyjnych wprowadzona w 2017 r. – <https://podstawaprogramowa.pl>.



Blok 2: Dane osobowe

Cele operacyjne

Nauczyciel:

- wie, czym są dane osobowe i jakiej ochronie podlegają;
- zna zmiany w przepisach prawnych o ochronie danych osobowych wprowadzone w 2018 roku;
- umie praktycznie stosować zasady ochrony danych osobowych w życiu prywatnym i w szkole;
- potrafi chronić dane osobowe uczniów, nauczycieli i innych pracowników szkoły.

Opis treści:

- dane osobowe i powód ich ochrony;
- formy ochrony danych osobowych w Polsce i w Unii Europejskiej;
- *Ogólne Rozporządzenie o Ochronie Danych Osobowych 2016/679 (RODO)* – zmiany w zakresie ochrony danych osobowych wprowadzone w 2018 roku;
- ochrona danych osobowych – obowiązujące prawo;
- zasady ochrony danych osobowych w życiu prywatnym i w szkole;
- ochrona danych osobowych uczniów, nauczycieli oraz innych pracowników szkół.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Podstawy ochrony danych osobowych* – <https://cyfrowa-wyprawka.org/lekcja/podstawy-ochrony-danych-osobowych>;
- Strona Fundacji Panoptykon: cykl artykułów *RODO na tacy, czyli jak możemy skorzystać na nowych przepisach* – <https://panoptykon.org/rodo-na-tacy>;
- Strona The EU General Data Protection Regulation (GDPR) na temat RODO – <https://gdprexplained.eu/pl>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Wizerunek – jak chronić swoje prawa?* – <https://cyfrowa-wyprawka.org/lekcja/wizerunek-jak-chronic-swoje-prawa>;
- Serwis edukacyjny „DODO – dbamy o dane osobowe” – <http://dodo-bezpiecznie.blogspot.com/>;



- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak dzieci i młodzież chronią swoją prywatność?* – https://giodo.gov.pl/560/id_art/4699/j/pl;
- Strona Generalnego Inspektora Ochrony Danych Osobowych: *Jak bezpiecznie zwiedzać cyfrowy świat?* – <https://giodo.gov.pl/pl/1520208/8510>;
- Wykład otwarty z cyklu „Lekcje z GIODO” pt. *Elektroniczna dokumentacja szkolna i jej udostępnianie* – <https://www.youtube.com/watch?v=qwXla3bA1w8&feature=youtu.be>.



Blok 3: Prawo autorskie

Cele operacyjne

Nauczyciel:

- wie, czym są prawa autorskie i prawa pokrewne;
- zna zasady korzystania z cudzych utworów;
- posiada praktyczną wiedzę na temat dozwolonego użytku edukacyjnego;
- potrafi chronić prawa autorskie, w tym także prawa autorów nieletnich.

Opis treści:

- prawa autorskie i prawa pokrewne;
- obowiązujące prawo;
- dozwolony użytek edukacyjny;
- pojęcie plagiatu;
- prawa autorskie osoby nieletniej;
- prawa autorskie nauczyciela.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Czerniawski P., Lipszyc J., Wilkowski M., *Pierwsza pomoc w prawie autorskim: przewodnik*, Warszawa: Fundacja Nowoczesna Polska – <https://prawokultury.pl/publikacje/pierwsza-pomoc>;
- Poradnia na stronie „Prawokultury.pl”: *Pierwsza pomoc w prawie autorskim: zapytaj prawnika* – <https://prawokultury.pl/pierwsza-pomoc>;
- Strona „Prawokultury.pl”: *Krótki kurs własności intelektualnej. Materiały dla uczelni* – hasło: *Plagiat* – <https://prawokultury.pl/kurs/plagiat>;
- Siewicz K., (2016), *Prawo autorskie w edukacji: jak unikać naruszeń?*, Warszawa: Fundacja Nowoczesna Polska – <http://koed.org.pl/wp-content/uploads/2016/11/prawo-autorskie-w-edukacji-jak-unikac-naruszen-wersja-2016-1.pdf>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Prawo autorskie dla każdego* – <https://cyfrowa-wyprawka.org/lekcja/prawo-autorskie-dla-kazdego>;
- Strona Fundacji Panoptykon „Cyfrowa Wyprawka”: *Jak etycznie publikować w sieci?* – <https://cyfrowa-wyprawka.org/lekcja/jak-etycznie-publikowac-w-sieci>.



Czas trwania części: 18 godzin (w tym 3 online)

Blok 1: Czym jest bezpieczeństwo informacyjne

Cele operacyjne

Nauczyciel:

- wie, na czym polega bezpieczeństwo informacyjne;
- potrafi przestrzec uczniów przed typowymi zagrożeniami bezpieczeństwa informacyjnego;
- potrafi z pomocą internetu określić podstawowe kierunki rozwoju mediów elektronicznych;
- potrafi przedstawić swoim uczniom podstawowe kierunki rozwoju mediów elektronicznych i wskazać zagrożenia z nimi związane;
- zna zasady bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych i sieci;
- wie, czym jest chmura, i korzysta z niej;
- potrafi podać kilka przykładów usług wykonywanych w chmurze;
- wie, jakie środki ostrożności należy zachować, korzystając z chmury;
- potrafi zorganizować zajęcia dotyczące zasad bezpiecznego korzystania z urządzeń mobilnych, mediów elektronicznych i sieci.

Opis treści:

- kierunki rozwoju mediów elektronicznych – możliwe zagrożenia;
- bezpieczeństwo informacyjne;
- bezpieczne korzystanie z urządzeń mobilnych, sieci i mediów elektronicznych;
- usługi w chmurze;
- zalety i wady mediów cyfrowych;
- zastosowanie chmury do nauki i rozrywki;
- zagrożenia związane z korzystaniem z usług w chmurze;
- krytyczny odbiór informacji pochodzących z różnych mediów.



Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Kubiak M., Topolewski S. (red.), (2016), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach – https://repozytorium.uph.edu.pl/bitstream/handle/11331/1205/Bezpieczenstwo_informacyjne_w_21_wieku.pdf?sequence=12\U\;
- Filmy o kierunkach rozwoju mediów elektronicznych:
 - *A Day Made of Glass 2: Same Day. Expanded Corning Vision* (2012) – <https://youtu.be/jZkHpNnXLBO>;
 - *Epaper-Newspaper* (2009) – <https://youtu.be/OB28SHBmMNI>;
 - *Productivity Future Vision* (2011) – <https://youtu.be/a6cNdhOKwi0>;
- Wojtasik Ł., Maryl-Wójcik M., Topolewska K. (oprac.), (2017), *Dzień z życia – scenariusz zajęć*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=1&fnd=&grupa=0&offset=2&sort=1&szkolenie=1121#opisszkolenia;
- Lekcja: *Oblicza wolności słowa* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/oblicza-wolnosci-slowa/>;
- Lekcja: *Wśród ekranów i interfejsów* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/wsrod-ekranow-i-interfejsow/>;
- Lekcja: *Medialny savoir-vivre* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/medialny-savoir-vivre/>;
- Lekcja: *Efektywna komunikacja w sieci* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/efektywna-komunikacja-w-sieci/>;
- Film *Office 365 – Zaczynamy!* prezentujący chmurę Microsoft dla edukacji – <https://youtu.be/v8yAw0z9CJg>;
- Kursy dla nauczycieli z zakresu obsługi narzędzi Microsoft wykorzystujących chmurę – <https://education.microsoft.com/courses-and-resources/courses>;
- Film *Uważaj, co udostępniasz. Social media stalker* na kanale „Z Dobrym Słowem” – <https://youtu.be/CLRBYhd7e4Q>;
- Wrzesień-Gandolfo A. (red.), (2014), *Bezpieczeństwo dzieci online. Kompendium wiedzy*, Warszawa: NASK, FDDS – https://www.edukacja.fdds.pl/dd5bcf09-cf2d-4340-9eb3-2c437ef66245/Extras/ksiazkaBezpieczenstwo_dzieci_online_Kompendium_dla_rodzicow_i_profesjonalistow-FDDS-12042017.pdf.



Blok 2: Korzystamy z informacji

Cele operacyjne

Nauczyciel:

- potrafi przygotować uczniów do wyszukiwania i wykorzystywania treści z internetu;
- potrafi zorganizować zajęcia przygotowujące uczniów do krytycznej oceny źródeł informacji;
- umie planować i organizować zajęcia wykorzystujące treści pochodzące z różnych mediów (w tym internetowe) do nauki;
- umie przedstawić uczniom zasady korzystania z cudzych utworów;
- potrafi wyjaśnić swoim uczniom zasady dozwolonego użytku w edukacji.

Opis treści:

- sposoby wyszukiwania w internecie rzetelnych informacji;
- krytyczna ocena wyszukanych treści;
- zasady korzystania z cudzych prac;
- pojęcie dozwolonego użytku edukacyjnego.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Lekcja: *Sprawne szukanie informacji* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/sprawne-szukanie-informacji>;
- Lekcja: *Gdy wybierasz dobre źródło* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/gdy-wybierasz-dobre-zrodlo>;
- Lekcja: *Jedna informacja – a źródeł mnóstwo!* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/jedna-informacja-a-zrodel-mnostwo>;
- Lekcja: *Czym się różni informacja od opinii?* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/czym-sie-rozni-informacja-od-opinii>;
- Buchner A., *Jak rozróżniać informacje prawdziwe od fałszywych?*, Warszawa: Fundacja Orange – https://platforma.megamisja.pl/download/knowledge_base/scenario/8/Jak_rozrozniać_informacje_prawdziwe_od_fałszywych.pdf;
- Lekcja: *Szanujmy twórców* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/szanujmy-tworcow>;



- Strona fotoprawo.pl: *Darmowe zdjęcia z sieci. Skąd brać? Jak korzystać?* – <https://fotoprawo.pl/index.php/2012/10/fakty-i-mity-czyli-o-prawach-autorskich-dla-blogerow/>;
- Lekcja: *Dozwolony użytek edukacyjny* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/dozwolony-uzytek-edukacyjny/>;
- Lekcja: *Otwarte zasoby – otwarte umysły* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/otwarte-zasoby-otwarte-umysly/>.



Blok 3: Ja jako autor

Cele operacyjne

Nauczyciel:

- zna podstawowe przepisy prawa autorskiego i praw pokrewnych;
- potrafi wyjaśnić uczniom zasady ochrony ich praw jako autorów;
- wie, gdzie można znaleźć informacje na temat praw autorów nieletnich;
- potrafi używać licencji Creative Commons.

Opis treści:

- ochrona utworów przygotowanych przez uczniów;
- redagowanie przez ucznia strony internetowej szkoły;
- pojęcie plagiatu;
- wolne licencje Creative Commons.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Artykuł: *Poznaj licencje Creative Commons* – <https://creativecommons.pl/poznaj-licencje-creative-commons/>;
- *Prawa autorskie ucznia* – porady ekspertów wydawnictwa OPERON – <http://oswiataiprawo.pl/porady/prawa-autorskie-ucznia/>;
- Lekcja: *Prawa wyłączne – twórcy i użytkownicy* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/prawa-wylaczne-tworcy-i-uzytkownicy/>;
- Lekcja: *Prawo autorskie* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/prawo-autorskie/>;
- Lekcja: *Osobiste prawa autora* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/osobiste-prawa-autora/>;
- Strona fotoprawo.pl: *Fakty i mity, czyli o prawach autorskich dla blogerów* – <https://fotoprawo.pl/index.php/2012/10/fakty-i-mity-czyli-o-prawach-autorskich-dla-blogerow/>;
- *Prawo Autorskie? OK!* – kurs Ośrodka Edukacji Informatycznej i Zastosowań Komputerów – <http://pa.ok.oeiizk.waw.pl/>;
- Lekcja: *Jak etycznie publikować w sieci?* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/jak-etycznie-publikowac-w-sieci/>.



Blok 4: Moje dane

Cele operacyjne

Nauczyciel:

- zna zasady ochrony wizerunku uczniów i nauczycieli oraz umie wykorzystywać tę wiedzę w szkole;
- potrafi planować i organizować zajęcia wspierające uczniów w dbaniu o własny wizerunek;
- uwrażliwia uczniów na problem zabezpieczania danych;
- wie, jak zabezpieczać dane umieszczane w internecie;
- zna treść *Ogólnego Rozporządzenia o Ochronie Danych Osobowych 2016/679 (RODO)*;
- potrafi zapoznać uczniów z zapisami RODO, które bezpośrednio ich dotyczą.

Opis treści:

- ochrona wizerunku uczniów i nauczycieli;
- ochrona prywatności w internecie;
- podstawowe sposoby zabezpieczania danych w internecie;
- zapisy RODO dotyczące uczniów;
- umiejętność dbania o własne dane;
- publikacja fotografii w internecie.

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Lekcja: *Wizerunek osób publicznych* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/wizerunek-osob-publicznych/>;
- Lekcja: *Dane osobowe i ochrona tożsamości* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/dane-osobowe-i-ochrona-tozsamosci/>;
- Lekcja: *Ochrona danych osobowych* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/ochrona-danych-osobowych/>;
- Lekcja: *Kim jestem w internecie?* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/kim-jestem-w-internecie/>;
- Strona Fundacji Panoptikon: cykl artykułów *RODO na tacy*. Odcinek V: *Lekcje samoobrony, czyli jak skorzystać z praw, które daje RODO?* – <https://panoptikon.org/rodo-na-tacy-V>;



- Pawłowska-Ptaszyńska M., *Zmiany w ochronie danych osobowych dzieci po 25 maja 2018 r.* – <https://samorząd.infor.pl/sektor/organizacja/rodo-2018/767926,Zmiany-w-ochronie-danych-osobowych-dzieci-po-25-maja-2018-r.html>;
- Stępniewski R., (2018), *RODO i nowe prawa osób, których dane dotyczą*, Warszawa: Rzetelna Grupa – <https://www.politykabezpieczenstwa.pl/pl/a/rodo-i-nowe-prawa-osob-ktorych-dane-dotyczy>;
- Lekcja: *Jak wzmocnić swoją prywatność?* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/jak-wzmocnic-swoja-prywatnosc/>;
- *Kurs Cyfrowego Obywatelstwa i Bezpieczeństwa* Fundacji Szkoła z Klasą – <https://obywatelstwocyfrowe.szkołazklasa.org.pl/>;
- Staśkiewicz J., (2017), *Prosty i szybki sposób na bezpieczne przesłanie poufnych danych* – artykuł na blogu „OpenSecurity.pl” – <https://opensecurity.pl/prosty-i-szybki-sposob-na-bezpieczne-przeslanie-poufnych-danych/>;
- FDDS, (2016), *Seksting – scenariusz zajęć dla uczniów szkół ponadpodstawowych*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=1&fnd=&grupa=0&offset=1&sort=1&szkolenie=15246&tekst=seksting&criteria=&blo-tem=#opisszkolenia;
- Lekcja: *Cyfrowy portret, czyli kilka słów o wizerunku w Internecie* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/cyfrowy-portret-czyli-kilka-slow-o-wizerunku-w-internecie>;
- Golański A., (2018), *Używasz Facebooka? Sprawdź, czy 15 pytań wystarczy, by zgadnąć, kim jesteś* artykuł na stronie „dobreprogramy.pl” – <https://www.dobreprogramy.pl/Uzywasz-Facebooka-Sprawdz-czy-15-pytan-wystarczy-by-zgadnac-kim-jestes,News,87214.html>.



Blok 5: Bezpiecznie w sieci

Cele operacyjne

Nauczyciel:

- potrafi kształtować świadomość uczniów w zakresie zagrożeń występujących w internecie;
- umie uświadamiać uczniów na temat możliwych zagrożeń związanych z używaniem i nadużywaniem technologii;
- promuje wśród uczniów zasady bezpiecznego zachowania w sieci;
- uwrażliwia uczniów na problem nadmiernego korzystania z mediów, w tym internetu;
- potrafi wskazać uczniom podstawowe sposoby radzenia sobie z hejtem i cyberprzemocą, a także zapobiegania tym zjawiskom;
- zwraca uwagę uczniów na problem publikacji wizerunku i jego konsekwencje;
- potrafi wskazać uczniom miejsca, w których mogą uzyskać pomoc w przypadku zaistnienia zagrożenia sieciowego.

Opis treści:

- zagrożenia internetowe;
- podstawowe problemy związane z korzystaniem z sieci;
- szkodliwe i niebezpieczne treści w internecie;
- problem utraty danych i anonimowości;
- zjawisko nadmiernego korzystania przez młodzież z mediów elektronicznych i internetu;
- budowanie relacji w oparciu o wzajemny szacunek;
- cyberprzemoc i sposoby zapobiegania jej;
- utrata tożsamości i kompromitacja w sieci;
- oszustwa internetowe;
- seksting i uwodzenie w sieci;
- wsparcie dla uczniów doświadczających cyberprzemocy (w tym hejtu i obrażania w sieci).

Proponowane zasoby edukacyjne:

Wybrane fragmenty materiałów:

- Film *Jonasa magiczna sztuczka ze znikaniem* – kampania Policji w Lozannie służąca poprawie bezpieczeństwa pieszych – https://www.youtube.com/watch?v=TP6L41rjK_I;



- Film *Nadużywanie internetu przez dzieci i młodzież* opublikowany przez FDDS – <https://youtu.be/3CZXHJWsung>;
- Film *E-uzależnienia* wyprodukowany przez Telewizję Kopernik – <https://youtu.be/t4t-DKy8B1c>;
- Film *Uważaj, co udostępniasz. Social media stalker* na kanale „Z Dobrym Słowem” – <https://youtu.be/CLRBYhd7e4Q>;
- Lekcja: *Incognito w internecie* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/incognito-w-internecie/>;
- Lekcja: *Uzależnienia technologiczne* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/uzaleznienia-technologiczne/>;
- FDDS, (2016), *Seksting. Scenariusz zajęć dla uczniów szkół ponadpodstawowych*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=1&fnd=&grupa=0&offset=1&sort=1&szkolenie=15246&tekst=seksing&criteria=&blo-tem=#opisszkolenia;
- Lekcja: *Sexting i sextortion* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/sexting-i-sextortion/>;
- Cisek R., (2017), *Kradzież tożsamości – odpowiedzialność prawna (cywilna i kar-na)* – artykuł w serwisie „NoweMEDIA.org.pl” – <http://www.nowemedia.org.pl/joomla/index.php/wiadomosci/item/884-kradziez-tozsamosci%E2%80%93odpowiedzialnosc-prawna-cywilna-karna>;
- Lekcja: *Bankowość elektroniczna* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/bankowosc-elektroniczna/>;
- Lekcja: *Netykieta, czyli o kulturze w internecie* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/netykieta-czyli-o-kulturze-w-internecie/>;
- Dziemidowicz E., Wojtasik Ł., (2017), *Lekcja bezpieczeństwa – scena-riusz zajęć*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=9&fnd=&grupa=0&offset=1&sort=1&szkole-nie=1114&tekst=1114#opisszkolenia;
- „Digital Youth. Magazyn o fenomenach internetu” nr 3 (05) 2017 – https://www.edukacja.fdds.pl/de4062e0-62db-4daf-b7ce-be4bfb32c2bd/Extras/broszura-digital-youth_3-2017.pdf;
- Dziemidowicz E., Kępka M., (2017), *Internet bez hejtu. Scenariusz pikniku edu-kacyjnego*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&tekst=15447;
- Lekcja: *Słowa, które ranią* na stronie „Edukacja Medialna” – <http://edukacjamedialna.edu.pl/lekcje/slowa-ktore-rania/>;



- „Odkrywcy Internetu” – gra planszowa: informacje o grze i materiały do pobrania – <http://wbp.poznan.ekursy.eu/course/view.php?id=27>;
- Lekcja: *Prawo do prywatności w sieci* na stronie „Edukacja Medialna” – <https://edukacjamedialna.edu.pl/lekcje/prawo-do-prywatnosci-w-sieci>;
- *Kim są patostreamerzy i co to w ogóle jest?* – artykuł na blogu „ZUCH.media” – <http://zuch.media/kim-sa-patostreamerzy/>;
- *Gdzie szukać pomocy?* – wskazówki na stronie cyfrowobezpiecni.pl – <https://www.cyfrowobezpiecni.pl/gdzie-szukac-pomocy>.

Przykładowy rozkład treści



Część wstępna (7 godzin)				
Działania nauczyciela a bezpieczeństwo informacyjne				
Blok	Tytuł bloku	Ilość godzin		Treści kształcenia
		stacjonarnych	online	
1	<i>Bezpieczeństwo informacyjne – podstawy</i>	3	1	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
2	<i>Prawo autorskie</i>	1	0,5	2.1, 2.2, 2.3, 2.4
3	<i>Dane osobowe</i>	1	0,5	3.1, 3.2, 3.3, 3.4
	Razem godzin	5	2	

Część główna (18 godzin)				
Bezpieczeństwo informacyjne ucznia				
Blok	Tytuł bloku	Ilość godzin		Treści kształcenia
		stacjonarnych	online	
1	<i>Czym jest bezpieczeństwo informacyjne</i>	3	0,5	1.1, 1.2, 1.4, 1.5
2	<i>Korzystamy z informacji</i>	2	0,5	1.5, 2.2, 2.3
3	<i>Ja jako autor</i>	2	0,5	2.1, 2.2, 2.4
4	<i>Moje dane</i>	3	0,5	3.1, 3.2, 3.3, 3.4, 4.2
5	<i>Bezpiecznie w sieci</i>	5	1	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7
	Razem godzin	15	3	

Przykładowe scenariusze zajęć



Scenariusz zajęć nr 1

Część zajęć: Część wstępna – *Działania nauczyciela a bezpieczeństwo informacyjne*

Blok tematyczny: Blok 1 – *Bezpieczeństwo informacyjne – podstawy*

Temat zajęć: *Bezpieczeństwo informacyjne a podstawa programowa przedmiotu, którego nauczam*

Czas zajęć: 35 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić uczniom, na czym polega bezpieczeństwo informacyjne;
- znaleźć w podstawie programowej nauczanego przez siebie przedmiotu odwołania do bezpieczeństwa informacyjnego;
- łączyć na zajęciach zagadnienia z różnych obszarów edukacyjnych z tematyką bezpieczeństwa informacyjnego.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca indywidualna uczestników przy komputerach;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- aplikacja online – np. Padlet (lub analogiczna);
- edytor tekstu;
- platforma e-learningowa.



Zasoby do wykorzystania:

- Film: *A Day Made of Glass 2: Same Day. Expanded Corning Vision* (2012) – <https://youtu.be/jZkHpNnXLB0>;
- Kubiak M., Topolewski S. (red.), (2016), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach – https://repozytorium.uph.edu.pl/bitstream/handle/11331/1205/Bezpieczenstwo_informacyjne_w_21_wieku.pdf?sequence=1;
- Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnościami intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. z 2017 r., poz. 356) – <http://www.dziennikustaw.gov.pl/DU/2017/356>.

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Projekcja filmu
Uczestnicy oglądają film *A Day Made of Glass 2: Same Day. Expanded Corning Vision* (2012). Po projekcji prowadzący zaczyna rozmowę na temat kierunku rozwoju mediów elektronicznych. Zwraca uwagę, że film przedstawia wizję przyszłości wykreowaną w 2012 roku. Pyta uczestników, czy zauważyli w przedstawionej rzeczywistości jakieś elementy, które już dziś są dostępne.
2. Dyskusja
Prowadzący inicjuje burzę mózgów, pytając uczestników, czy dostrzegają jakieś zagrożenia związane z dynamicznym rozwojem technologii. Zwraca uwagę na zagrożenia związane z przechowywaniem informacji i dostępem do nich.
3. Praca z tekstem
Prowadzący dzieli uczestników na kilka zespołów (w zależności od nauczanego przez nich przedmiotu) i zaprasza do pracy z tekstem *Bezpieczeństwo informacyjne w XXI wieku*. Prosi każdą z grup o przygotowanie kilku slajdów



prezentacji wyjaśniających, na czym polega bezpieczeństwo informacyjne. Moderuje pracę uczestników w taki sposób, aby zostały wykorzystane różne podejścia do zagadnienia bezpieczeństwa informacyjnego.

4. Odniesienie do podstaw programowych

Kolejnym krokiem w pracy zespołów jest dodanie do stworzonej prezentacji slajdów zawierających odwołania do podstaw programowych przedmiotów nauczanych przez członków danej grupy. Należy wskazać te zapisy, które dotyczą kwestii bezpieczeństwa informacyjnego.

5. Prezentacja prac

Po zakończeniu pracy zespoły udostępniają i wzajemnie oceniają swoje prezentacje, omawiają w szczególności miejsca korelacji podstawy programowej różnych przedmiotów z treściami dotyczącymi bezpieczeństwa informacyjnego. Następuje krótka dyskusja dotycząca bezpieczeństwa informacyjnego w szkole i życiu prywatnym. Prowadzący zapisuje wnioski nauczycieli dotyczące tego tematu.

6. Na zakończenie zajęć prowadzący zbiera wnioski i dokonuje zwięzłej oceny pracy uczestników. Opracowane materiały zostają umieszczone w miejscu dostępnym dla uczestników szkolenia – np. w notesie OneNote danej grupy szkoleniowej w chmurze lub na platformie e-learningowej.



Scenariusz zajęć nr 2

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 4 – *Moje dane*

Temat zajęć: *Ochrona wizerunku w mediach społecznościowych i nie tylko*

Czas zajęć: 35 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić uczniom, co składa się na wizerunek danej osoby i dlaczego należy go chronić;
- wskazać konsekwencje kompromitacji w sieci i pogorszenia wizerunku;
- ukazać przykłady utraty dobrego imienia.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- aplikacja online – np. Padlet (lub analogiczna);
- edytor tekstu;
- platforma e-learningowa.

Zasoby do wykorzystania:

- Film *Uważaj, co udostępniasz. Social media stalker* na kanale „Z Dobrym Słowem” – <https://youtu.be/CLRBYhd7e4Q>.



Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Projekcja filmu

Uczestnicy oglądają materiał *Uważaj, co udostępniasz. Social media stalker* dostępny na kanale „Z Dobrym Słowem”. Po obejrzeniu filmu prowadzący zaczyna rozmowę na temat związany z treścią materiału czyli pogorszeniem wizerunku, które może skutkować kompromitacją danej osoby w sieci. Pyta uczestników, czy zetknęli się z przypadkami utraty wizerunku w swoim otoczeniu. Jeśli tak, prosi ich o przedstawienie wydarzeń, które do tego doprowadziły, zwracając przy tym uwagę, aby osoba opowiadająca dokonała anonimizacji bohaterów. Uczestnicy analizują możliwe konsekwencje. Ich spostrzeżenia zostają zapisane na tablicy lub w notesie danej grupy szkoleniowej w chmurze.

2. Ochrona wizerunku – praca w grupach

Prowadzący prosi, aby uczestnicy podzielili się na grupy i spróbowali wspólnie wypracować wskazówki dotyczące prewencji zagrożeń i ochrony wizerunku oraz zapisali je w wirtualnej notatce. Po zakończeniu pracy zespoły prezentują sformułowane przez siebie zalecenia, dokonując wzajemnej oceny ich trafności.

3. Podsumowanie

Wszystkie opracowane materiały zostają umieszczone w miejscu dostępnym dla uczestników szkolenia np. w notesie OneNote w chmurze lub na platformie e-learningowej.



Scenariusz zajęć nr 3

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 5 – *Bezpiecznie w sieci*

Temat zajęć: *Ochrona wizerunku w mediach społecznościowych i nie tylko*

Czas zajęć: 45 min (+ 40 min pracy online uczestników przed zajęciami)

Cele:

Nauczyciel po udziale w zajęciach umie:

- poprowadzić zajęcia na trudny temat;
- wyjaśnić uczniom, czym jest wizerunek danej osoby i dlaczego należy go chronić;
- scharakteryzować zjawisko sekstingu;
- uświadomić uczniom konsekwencje sekstingu;
- wskazać instytucje udzielające wsparcia w przypadku.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- platforma e-learningowa.

Zasoby do wykorzystania:

- Film *Na zawsze* (2015) – materiał edukacyjny Fundacji Dzieci Niczyje – <https://youtu.be/XH6MEbuvihE>;
- Film *Historia Julki* (2015) – materiał edukacyjny Fundacji Dzieci Niczyje – <https://youtu.be/sWwM36pA0yw>;



- Film *Historia Mateusza* (2015) – materiał edukacyjny Fundacji Dzieci Niczyje – <https://youtu.be/GmaVd1icRSg>;
- FDDS, (2016), *Seksting. Scenariusz zajęć dla uczniów szkół ponadpodstawowych*, Warszawa: FDDS – https://www.edukacja.fdds.pl/?option=com_szkolenia&optsr=1&fnd=&grupa=0&offset=1&sort=1&szkolenie=15246&tekst=seksing&criteria=&blo-tem=#opisszkolenia;

Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Przygotowanie do zajęć
Uczestnicy przed spotkaniem otrzymują polecenie obejrzenia filmu *Na zawsze*.
2. Rozmowa o filmie
Po rozpoczęciu zajęć prowadzący rozpoczyna rozmowę na temat filmu. Prezentuje uczestnikom dodatkowe materiały w postaci filmów – przedstawiających wydarzenia z punktu widzenia bohaterów: Julki i Mateusza – oraz scenariusza zajęć do przeprowadzenia z uczniami.
3. Organizacja zajęć realizujących trudną tematykę
Prowadzący rozmawia z uczestnikami na temat prowadzenia zajęć dotyczących tematyki, która może okazać się dla młodzieży trudna i drażliwa. Uczestnicy dzielą się doświadczeniami z tego zakresu i wspólnie ustalają strategię przygotowania się do prowadzenia i realizacji problematycznych zajęć. Analizują scenariusz przygotowany przez autorów filmu i zastanawiają się nad możliwością jego zrealizowania.
4. Praca w grupach
Uczestnicy dzielą się na 5 zespołów i przygotowują krótkie wystąpienia na temat sekstingu na podstawie materiałów zaprezentowanych przez prowadzącego. Następuje prezentacja wyników pracy grup.



5. Podsumowanie

Uczestnicy rozmawiają o tym, co w czasie pracy było dla nich trudne i jak sobie z tym poradzili. Prowadzący wspólnie z uczestnikami ocenia wystąpienia poszczególnych zespołów.



Scenariusz zajęć nr 4

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 3 – *Bezpiecznie w sieci*

Temat zajęć: *Publikujemy w sieci materiały na licencji CC*

Czas zajęć: 30 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- poprowadzić zajęcia na temat podstaw prawa autorskiego;
- wyjaśnić uczniom, czym są licencje Creative Commons;
- wskazać miejsca, w których można znaleźć zasady dotyczące wykorzystania wolnych licencji.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca indywidualna przy komputerze;
- praca w grupach;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- platforma e-learningowa.

Zasoby do wykorzystania:

- Artykuł *Poznaj licencje Creative Commons* – <https://creativecommons.pl/poznaj-licencje-creative-commons/>.



Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Wolne licencje – wprowadzenie

Prowadzący wyświetla na ekranie duży symbol licencji CC: Uznanie autorstwa – Użycie niekomercyjne – Na tych samych warunkach 4.0. Następnie pyta uczestników, czy wiedzą, co oznacza ten symbol? Wyjaśnia, że jest to oznaczenie wolnych licencji – skrót ich angielskiej nazwy Creative Commons. Prowadzący prosi, aby uczestnicy weszli na stronę internetową opisującą poszczególne licencje i określili, co oznacza przedstawiony symbol.

2. Typy licencji – praca w grupach

Uczestnicy zostają poproszeni o dobranie się w kilkusobowe grupy. Zadaniem każdej z nich jest opracowanie krótkiej prezentacji na temat zasad udzielania konkretnej licencji wskazanej przez prowadzącego. Zespoły prezentują opracowane informacje, dzięki czemu scharakteryzowane zostają wszystkie typy wolnych licencji CC. Prowadzący wraz z uczestnikami ocenia wystąpienia poszczególnych zespołów.

3. Dyskusja

Uczestnicy i prowadzący zastanawiają się, czy prace uczniów powinny być udostępniane w oparciu o licencje CC, a jeśli tak – które licencje należy wybrać, aby umożliwiały nauczycielom wykorzystywanie materiałów w przyszłości.

4. Podsumowanie

Wnioski i refleksje uczestników zostają zapisane w notesie OneNote.



Scenariusz zajęć nr 5

Część zajęć: Część główna – *Bezpieczeństwo informacyjne ucznia*

Blok tematyczny: Blok 1 – *Czym jest bezpieczeństwo informacyjne*

Temat zajęć: *Praca w chmurze*

Czas zajęć: 30 min

Cele:

Nauczyciel po udziale w zajęciach umie:

- wyjaśnić, czym jest chmura;
- przedstawić wady i zalety pracy w chmurze;
- poprowadzić zajęcia z wykorzystaniem chmury.

Metody nauczania:

- rozmowa;
- burza mózgów;
- praca przy komputerze;
- prezentacja.

Środki dydaktyczne:

- komputer i projektor dla prowadzącego;
- komputer z przeglądarką internetową dla każdego uczestnika szkolenia;
- usługa w chmurze – np. z darmowego pakietu Microsoft Office 365 lub Google;
- platforma e-learningowa.

Zasoby do wykorzystania:

- miejsce w chmurze na dokumenty z możliwością udostępniania plików do edycji np. OneDrive lub Google Drive;
- Film *Microsoft Datacenter Tour* – wirtualna wycieczka po centrum obliczeniowym (chmurze) – https://youtu.be/zXsoygN_v7A;



Formy oceny:

W trakcie zajęć uczestnicy otrzymują od siebie nawzajem oraz od prowadzącego szkolenie informację zwrotną w postaci krótkiej oceny słownej.

Przebieg zajęć:

1. Ćwiczenie wprowadzające

Prowadzący pokazuje uczestnikom kartkę z pustą tabelą do uzupełnienia. W tabeli znajdują się pola konieczne do uzupełnienia przez każdego z uczestników informacjami takimi jak: imię i nazwisko każdego z uczestników; nazwa szkoły, w której pracuje; nauczany przez niego przedmiot. Prowadzący zadaje pytanie: ile czasu potrzeba na uzupełnienie stosownych rubryk przez jednego uczestnika? A ile czasu zajmuje uzupełnienie całej tabeli? Następnie każe uczestnikom rozważyć, czy dałoby się uzyskać lepszy wynik dla całej tabeli. Czy jest możliwy do osiągnięcia czas wypełnienia całej tabeli porównywalny z czasem wypełniania rubryk przeznaczonych dla jednej osoby? Prosi uczestników, aby chwilę podyskutowali na ten temat.

2. Praca w chmurze – teoria i praktyka

Prowadzący pyta uczestników, czy wiedzą, czym jest wirtualna chmura i w jaki sposób działa. W celu uzupełnienia ich odpowiedzi wyświetla i jednocześnie omawia film prezentujący wirtualną wycieczkę po chmurze. Następnie przypomina uczestnikom ich numery z listy obecności i udostępnia im do edycji zaprezentowaną wcześniej tabelę w wersji cyfrowej. Informuje ich, aby edytowali w tabeli wyłącznie wiersze opatrzone własnym numerem z listy. Wszyscy uczestnicy jednocześnie uzupełniają tabelę. Prowadzący wskazuje zalety takiej formy pracy i każe uczestnikom zastanowić się, czy dostrzegają jakieś minusy tego rozwiązania. Podkreśla, że kłopotów nastroić mogą takie same prawa do edycji dokumentu dla wszystkich użytkowników. Gdyby w tej sytuacji nie przyporządkowano każdemu konkretnego miejsca na dokonanie wpisu, uczestnicy przeszkadzaliby sobie wzajemnie, opóźniając wykonanie pracy.

3. Podsumowanie

Prowadzący prezentuje wypełnioną tabelę i wyłącza możliwość jej edytowania. Uczestnicy rozmawiają o zaletach wykorzystania chmury podczas pracy zespołowej, zastanawiają się nad bezpieczeństwem przechowywania plików w chmurze w kontekście zachowania bezpieczeństwa informacyjnego. Prowadzący wspólnie z uczestnikami podsumowuje i ocenia zajęcia.



O autorach

Dorota Janczak

Ekspert w zakresie wykorzystania nowych technologii w edukacji; doktorantka Wydziału Pedagogicznego Uniwersytetu Warszawskiego; członkini grupy SuperbelfrzyRP. Pracując w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie na stanowisku kierownika Pracowni Dydaktyki Cyfrowej, zajmuje się kształceniem ustawicznym nauczycieli oraz pracowników organów nadzorujących i prowadzących szkoły w zakresie wykorzystania technologii informacyjnej i komunikacyjnej. Na co dzień korzysta z nowoczesnych narzędzi i metod pracy oraz promuje ich stosowanie w pracy nauczycieli. Prowadzi zajęcia dydaktyczne na wielu specjalistycznych kursach. Jest autorem szkoleń dotyczących użycia TIK w pracy z uczniami, a także pomysłodawcą i koordynatorem projektów edukacyjnych, także międzynarodowych, oraz trenerem *Intel Classmate Learning Series for 1:1 e-learning in the classroom*. Współorganizowała konkurs Microsoft „WebQuest w Webuzzie”, zdobyła tytuł *Microsoft Innovative Educator Expert* – corocznie przyznawany liderom wykorzystującym nowe technologie do wprowadzania zmian w edukacji. Wspierając nauczycieli w ich doskonaleniu zawodowym, współpracuje z wieloma instytucjami i organizacjami, np. Narodowym Instytutem Audiowizualnym czy Uniwersytetem Warszawskim. Posiada certyfikat metodyka zdalnego nauczania przyznany przez Stowarzyszenie E-learningu Akademickiego, potwierdzający kompetencje w zakresie tworzenia treści oraz prowadzenia zajęć dydaktycznych z wykorzystaniem technik i metod kształcenia na odległość. Jest autorką licznych publikacji – np. serii artykułów dla miesięczników „Wychowanie w Przedszkolu” i „Dyrektor Szkoły” oraz kwartalników „Meritum” i „W cyfrowej szkole”. Zajmuje się także prawem autorskim w edukacji, dzieląc się swoją wiedzą w tym zakresie poprzez wystąpienia, artykuły oraz prowadzenie serwisu <http://pa.ok.oeiizk.waw.pl/> zawierającego między innymi materiały szkoleniowe dla nauczycieli i uczniów.

Michał Grześlak

Nauczyciel dyplomowany, konsultant w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie. Prowadzi szkolenia, warsztaty oraz konsultacje dla administratorów szkolnych pracowni komputerowych, nauczycieli oraz kadry kierowniczej, pełni także funkcję Administratora Systemów Informatycznych. Szkoli z zakresu podstaw programowania nauczycieli w ramach realizacji projektu „Warszawa Programuje”. Bierze udział jako wykładowca w projekcie UODO i OEIiZK „Twoje dane – twoja sprawa”. W swojej codziennej pracy wykorzystuje produkty



firmy Microsoft, takie jak Office 365 czy rozwiązania serwerowe. W 2017 r. znalazł się na liście 100 osób wyróżnionych przez Szerokie Porozumienie na Rzecz Umiejętności Cyfrowych za działalność na rzecz rozwijania umiejętności cyfrowych w Polsce. Posiada tytuł *Microsoft Innovative Educator Master Trainer*. Jest współautorem scenariuszy szkoleń dla trenerów z zakresu wykorzystania usługi Office 365 w szkołach, prowadzi szkolenia i warsztaty dla przedstawicieli sektora edukacyjnego z całej Polski na temat tej usługi oraz nowych technologii w edukacji. Uczestniczył w specjalistycznych konferencjach cyklicznie organizowanych przez OEliZK pn. „Bezpieczeństwo informacyjne w szkole i placówce oświatowej” jako prowadzący i prelegent. Publikował artykuły w kwartalniku edukacyjnym „Meritum”. Od wielu lat współorganizuje Ogólnopolski Zjazd Opiekunów Szkolnych Pracowni Internetowych w Mrozach (aktualnie konferencję edukacyjną „Majowe Mrozy” w Warszawie). Prowadził zajęcia w ramach Akademii Profesjonalnego Nauczyciela, jest instruktorem Akademii Cisco oraz trenerem projektu „Intel-Teach to the Future”. Od 1997 r. pracuje jako nauczyciel zajęć komputerowych oraz informatyki w Zespole Szkół w Izabelinie, gdzie stworzył sieć komputerową. Uczył informatyki także w XXVII Liceum Ogólnokształcącym im. T. Czackiego w Warszawie. Był egzaminatorem Europejskiego Certyfikatu Umiejętności Komputerowych (ECDL). Współpracował w ramach realizacji projektu „Nowoczesna Klasa”. Prowadził prelekcje i warsztaty dotyczące bezpieczeństwa i ochrony danych osobowych podczas konferencji „Nowoczesne Technologie Informacyjne w Służbie Cyfrowej Szkoły i Administracji Publicznej w Radomiu”, a także podczas „Konferencji Administratorów Szkolnych Sieci Komputerowych” w Nowym Tomyślu. Uczestniczył w szkoleniach trenerów i nauczycieli w projekcie „Mistrzowie Kodowania”. Współtworzył dwumiesięcznik oświatowy „Uczę Nowocześnie”, a także współorganizował konkurs oraz forum „Innowacyjnych Nauczycieli” Microsoft.

