



AUTORSKI PROGRAM
SZKOLENIA KOMPETENCJI CYFROWYCH
DLA PRACOWNIKÓW GMINNYCH SAMORZĄDOWYCH INSTYTUCJI KULTURY

SCENARIUSZ NR 1: „DZIENNIKARSTWO ONLINE – PRZYGOTOWANIE UCZESTNIKÓW ZAJĘĆ DO PROFESJONALNEJ REALIZACJI ZADAŃ TWÓRCÓW ZASOBÓW INFORMACYJNYCH PUBLIKOWANYCH W INTERNECIE”

*Program powstał na potrzeby projektu realizowanego w ramach
Działania 3.2 Innowacyjne rozwiązania na rzecz aktywizacji cyfrowej Program Operacyjny
Polska Cyfrowa 2014-2020*

Autorzy programu:

Elżbieta Fim – Szkoła Podstawowa im. Stefana Wyszyńskiego w Nasutowie

Barbara Gnysińska – Szkoła Podstawowa im. Zofii Trzczińskiej – Kamińskiej w Leścach

WPROWADZENIE

Dynamiczny rozwój technologii komputerowej oraz ciągle wzrastające znaczenie Internetu w życiu codziennym spowodowały konieczność systematycznego rozwoju kompetencji cyfrowych niemal wszystkich osób. Rozwój kompetencji cyfrowych musi następować zarówno w zakresie korzystania z technologii cyfrowych, jaki i posługiwania się nimi we wszystkich sferach życia zawodowego i prywatnego.

Nabycie tych umiejętności pozwala na:

- lepszą i sprawniejszą komunikację między społeczeństwem,
- korzystanie z e-usług administracji publicznej (załatwianie on-line spraw urzędowych - o dogodnej dla siebie porze, bez konieczności wychodzenia i odwiedzania urzędów),
- umiejętne publikowanie i zamieszczanie informacji na różnych portalach społecznościowych, stronach internetowych, blogach i innych multimediami,
- nowe style promocji i prezentacji,
- nowe style spędzania czasu wolnego lub jego organizacji,
- korzystanie ze wsparcia zamieszczonego w zasobach Internetu.

W dzisiejszych czasach Internet przeobraził się w autonomiczne medium. W parze z tym procesem wykształcało się pojęcie dziennikarza internetowego¹. Według Leszka Olszańskiego, obecnie coraz trudniej deprecjonować tę gałąź dziennikarstwa, szczególnie

¹ **Dziennikarstwo internetowe** - przygotowywanie przekazu dotyczącego wydarzeń i faktów, zgodnego ze specyfiką Internetu, i jego rozpowszechnianie za pośrednictwem Internetu (a zwłaszcza portali, wortalu, blogów, newsletterów, kanałów RSS itp.) do szerokiego grona odbiorców. [[Marek Jeleśniański, Definicja dziennikarstwa internetowego - iredaktor.pl](#)]

od momentu, gdy za publikacje online zaczęto przyznawać nagrody Pulitzera². Przekaz internetowy, który można by uznać za dziennikarski, powinien:

- mieć charakter informacyjny,
- być gatunkowo zbliżony do komunikatów medialnych,
- być przygotowany z zamiarem publikacji przede wszystkim w Internecie,
- oraz przez określony czas być dostępny w Internecie.

Samorządowe instytucje kultury w dobie cyfryzacji stanęły przed bardzo trudnym zadaniem, a mianowicie stworzenie oferty kulturalno-edukacyjnej zgodnej z oczekiwaniami współczesnego odbiorcy wychowanego w świecie informacyjnym.

Obecnie ponad 500 usług można załatwić drogą elektroniczną, dlatego kompetencje cyfrowe³ stały się celem samym w sobie i konieczne dla każdego obywatela w dobie postępu komunikacyjno-informacyjnego. Poza tym stosowanie nowych technologii kształtuje podstawowe kompetencje kluczowe oraz pozytywne postawy społeczne wśród użytkowników ze względu na obowiązującą netykietę oraz rozbudza świadomość na temat praw autorskich, cyberprzemocy, zjawisk fake news oraz hate.

1. KATALOG KOMPETENCJI CYFROWYCH.

Proponowany program ma na celu sprostać oczekiwaniom współczesnego społeczeństwa i przygotować pracowników samorządowych instytucji kultury do stworzenia oferty zgodnej oraz podejmowania działań przygotowujących dzieci, młodzież i dorosłych do życia w sieci technologii cyfrowej i informacyjnej. Aby móc korzystać z dobrodziejstw cyfryzacji należy się do tego przygotować i opanować wiele kompetencji z „Katalogu

² Cyberdziennikarstwo [w:] Łoża. Listopad 2006. Numer 13 (2) 2006.

³ **Kompetencje informatyczne (cyfrowe)**, to jeden z najważniejszych obszarów 8 kompetencji kluczowych w procesie uczenia się przez całe życie, które są niezbędne do pełnego uczestnictwa w życiu coraz bardziej scyfryzowanego społeczeństwa. W tym ujęciu kompetencje cyfrowe można zdefiniować jako swobodne i krytyczne korzystanie z technologii informacyjno-komunikacyjnych, aby osiągać cele związane pracą, zatrudnieniem, nauką, wypoczynkiem i uczestnictwem w życiu społecznym. Kompetencje cyfrowe należą do umiejętności przekrojowych, czyli występują i są wręcz niezbędne w nabywaniu kompetencji w pozostałych obszarach (np. umiejętnościach nauki języków, umiejętności uczenia się czy świadomości kulturowej). <http://vccsystem.eu/system-certifikacji/kompetencje-cyfrowe/>

cyfrowych usług polskiej administracji", które opracowało Ministerstwo Cyfryzacji. Katalog dostępny jest na stronie www.gov.pl, który zawiera m.in. zestawienie wszystkich usług elektronicznych, z jakich Polacy mogą obecnie korzystać na najpopularniejszych portalach rządowych - <https://mc.gov.pl/aktualnosci/katalog-cyfrowych-uslug-polskiej-administracji-aktualizacja>. Tematyka programu szkolenia w zakresie zdobywania kompetencji cyfrowych w ramach projektu oparty jest na kompetencjach zamieszczonych we wcześniej wspomnianym katalogu.

Poniższa tabela prezentuje zestaw kompetencji cyfrowych w 5 kategoriach, które uwzględniają treści proponowanego programu.

Tabela nr 1. Zestaw kompetencji cyfrowych w 5 kategoriach

Kategoria	Rodzaj kompetencji
UMIEJĘTNOŚCI INFORMACYJNE	<ol style="list-style-type: none">1. Przeglądanie, szukanie i filtrowanie informacji2. Ocena informacji3. Przechowywanie i wyszukiwanie informacji
UMIEJĘTNOŚCI KOMUNIKACYJNE	<ol style="list-style-type: none">1. Komunikacja z wykorzystaniem narzędzi cyfrowych i aplikacji2. Dzielenie się informacjami i zasobami3. Aktywność obywatelska online4. Współpraca z wykorzystaniem narzędzi cyfrowych5. Netykieta6. Zarządzanie tożsamością cyfrową
TWORZENIE TREŚCI	<ol style="list-style-type: none">1. Tworzenie treści2. Integracja i przetwarzanie treści.3. Przestrzeganie prawa autorskiego i licencji4. Programowanie
BEZPIECZEŃSTWO	<ol style="list-style-type: none">1. Narzędzia służące ochronie2. Ochrona danych osobowych3. Ochrona zdrowia fizycznego i psychicznego przed zagrożeniami wynikającymi z korzystania z technologii informacyjno-komunikacyjnych

	4. Ochrona środowiska
ROZWIĄZYWANIE PROBLEMÓW	<ol style="list-style-type: none">1. Rozwiązywanie problemów technicznych2. Rozpoznawanie potrzeb i narzędzi niezbędnych do rozwiązywania problemów3. Innowacyjność i twórcze wykorzystywanie technologii4. Rozpoznawanie braków w zakresie kompetencji cyfrowych

Powodzenie realizacji zadań w zakresie korzystania z nowoczesnych technologii oraz zasobów sieci zależy będzie od gotowości i przygotowania pracowników gminnych samorządowych instytucji kultury. Proponowany program szkolenia kompetencji cyfrowych adresowany jest do wszystkich pracowników GOK-ów, chcących swobodnie poruszać się po zasobach Internetu oraz poszukujących nowych metod i form na organizację warsztatów z wykorzystaniem stron internetowych i blogów oraz wiele innych. Poza tym ma stanowić **wsparcie dla rozwoju w zakresie kompetencji cyfrowych** i ich wykorzystywania w życiu codziennym. Program realizowany będzie w następującym zakresie:

1. [Prowadzenie rozmów przez Internet \(np. wideorozmowy, rozmowy grupowe\).](#)
2. [Korzystanie z usług GOOGLE](#)
3. [Prowadzenie konta na kanale YouTube.](#)
4. [Prowadzenie transmisji internetowych w serwisach społecznościowych](#)
5. [Rodzaje licencji \(licencje otwarte, komercyjne\) na których mogą być udostępnione treści i oprogramowanie.](#)
6. [Bezpieczeństwo i prawa autorskie](#)
7. Tworzenie własnego BLOGA
8. Tworzenie własnej strony internetowej
9. [Ochrona komputera i innych urządzeń przed złośliwym oprogramowaniem.](#)

2. ZAŁOŻENIA PROGRAMU:

1. **Rodzaj zajęć** – zajęcia warsztatowe
2. **Grupa docelowa:**
 - **I ETAP szkolenia** - pracownicy gminnych samorządowych ośrodków kultury

- **II ETAP szkolenia** – dzieci i młodzież uczestniczące w warsztatach z dziennikarstwa online
3. **Liczebność grupy** –max. 12 osób.
 4. **Liczba godzin** – 30 godzin zajęć grupowych (zorganizowanie 15 spotkań w cyklu 2 - godzinnym).
 5. **Wsparcie** – w celu lepszej i sprawniejszej komunikacji oraz merytorycznego i metodycznego wsparcia realizacja projektu będzie dodatkowo wzmocniona o wyszukane propozycje materiałów, tutoriali i filmików instruktażowych zamieszczonych w zasobach Internetu. Poza tym pierwszy etap projektu będzie obejmować działania mające na celu podniesienie kompetencji pracowników GOK w takim stopniu, aby mogli oni docelowo samodzielnie lub w asyście trenera przeprowadzić szkolenia dla dzieci i młodzieży. Po zakończeniu szkolenia, każdy pracownik GOK, który zrealizuje pełen kurs nauczania, otrzyma wsparcie co najmniej w postaci mentoringu (doradztwa) zorientowanego na odkrywanie i rozwijanie jego potencjału, a także bezpłatną aktualizację materiałów dydaktycznych.

Wydzielone krótkie partie materiału zapewniają indywidualizację pracy z beneficjentami oraz możliwość modyfikacji zadań w zakresie kolejności realizowanych treści. Natomiast różnorodność ćwiczeń pozwoli uniknąć stanu zniechęcenia.

Bezpośredni kontakt z mentorem-szkoleniowcem stworzy warunki na nabycie doświadczenia pod okiem fachowca w zakresie podstawowych kompetencji TIK, do których m.in. należą: wykorzystanie komputera lub tabletu, aplikacji lub programów oraz biegłość poruszania się w sieci.

Dobre zrozumienie tematyki szkoleń oraz systemu działania w sieci spełni założone cele i zaowocuje świadomym i celowym wykorzystaniem kompetencji cyfrowych w zakresie podstawowych kompetencji kluczowych (m.in.: korzystanie z darmowych aplikacji GOOGLE, korzystania z portali społecznościowych jako funkcjonowanie w grupie, czy prowadzenia strony internetowej oraz korzystania z portali edukacyjnych w ramach samorealizacji i rozwoju potencjału osobistego).

6. Środowisko:

- **sala komputerowa lub sala multimedialna wyposażona przynajmniej w ekran i projektor** – 1 komputer albo tablet dla każdego uczestnika szkolenia

- **materiały dydaktyczne** - dla każdego uczestnika
- **dostęp do Internetu**, dowolna przeglądarka internetowa,

3. CEL OGÓLNY:

Rozwój kompetencji cyfrowych, w tym zwiększenie stopnia oraz poprawa umiejętności korzystania z Internetu w tym e-usług publicznych,

3.1. CEL DŁUGOOKRESOWY:

1. stworzenie trwałej struktury dostępu do wiedzy w zakresie prowadzenia i animowania aktywności cyfrowej oraz podwyższania kompetencji cyfrowych na poziomie gminnych instytucji kultury;
2. wzrost aktywności cyfrowej społeczności lokalnej, która będzie mogła liczniej i częściej uczestniczyć w oferowanych zajęciach i wydarzeniach organizowanych przez gminne samorządowe jednostki kultury.

3.2. CEL KRÓTKOOKRESOWY:

1. zwiększenie kompetencji cyfrowych pracowników gminnych samorządowych instytucji kultury
2. rozwijanie kompetencji cyfrowych dzieci i młodzieży w wieku 10 - 18 lat poprzez organizację zajęć szkoleniowych w w/w instytucjach

3.3. CELE SZCZEGÓŁOWE:

1. rozwój kompetencji cyfrowych umożliwiających stworzenie popytu na Internet oraz technologie informacyjno-komunikacyjne wśród obywateli Polski,
2. stworzenie trwałych mechanizmów podnoszenia kompetencji cyfrowych na poziomie lokalnym w gminach

4. METODOLOGIA:

Szkolenie opiera się na metodologii uczenia dorosłych. Uczenie przez doświadczenie i eksperymentowanie oznacza, że szkolenie ma charakter głównie warsztatowy. Wykład i pokaz są w niewielkim stopniu wykorzystywane jedynie jako wsparcie i mają na celu ukierunkowanie uczestnika szkolenia na samodzielne eksperymentowanie i poszukiwanie rozwiązań.

Metody pracy:

1. **Obserwacja** (pokaz)
2. **Dyskusja** (wymiana poglądów i pomysłów)
3. Metoda „**Praktycznego działania**”
4. Metoda **kierowania korzystaniem z materiałów źródłowych i narzędzi TIK**
5. Metoda **projektów** (zadań)
6. Metoda **podająca** (instrukcje do zadań)
7. Metody **aktywizujące**

5. FORMY PRACY:

1. **Zajęcia warsztatowe**
2. **Indywidualna**
3. **Grupowa (zespołowa)**

6. ZAKRES TREŚCI NAUCZANIA:

6.1.1. Charakterystyka

Proponowany program szkolenia przeznaczony jest dla wszystkich osób, które zainteresowane są działalnością dziennikarską w sieci, również w ramach różnych portali społecznościowych. Prezentowany materiał szkoleniowy poświęcony jest przygotowaniu odpowiedzialnego i przewidującego konsekwencje swoich działań użytkownika Internetu. Założenia programowe mają stanowić wsparcie w rozwijaniu zainteresowań, także dziennikarskich i kompetencji językowych. Dzięki tym materiałom każdy uczestnik szkolenia pozna filozofię i sposób funkcjonowania sieci społecznościowych oraz wykorzystania ich w działalności na rzecz swojej społeczności lokalnej lub prywatnie. Zrozumie jak ochronić swoją prywatność w sieci, czym są prawa autorskie, własność intelektualna, a także pozna jakie konsekwencje kradzież treści. Nabędzie umiejętności pozwalające na bezpieczne poruszanie się w świecie wirtualnym, w tym m.in jak nawiązywać i kontynuować swoje znajomości, kształtować swój wizerunek lub najbliższego środowiska, wykorzystywać i dzielić się swą twórczością.

W dalszej części dot. tworzenia blogów i różnego rodzaju stron internetowych, proponowane materiały adresowane są osób mających zamiar prowadzić własną stronę internetową lub blog. Prezentowany moduł szkoleniowy poświęcony jest przygotowaniu kreatywnego bloggera, który dzięki swoim dzieciom będzie mógł działać na swoją rzecz jak i najbliższego środowiska. Dzięki tym materiałom każdy użytkownik pozna wartościowe i pochodzące z legalnych źródeł treści, dzięki którym będzie mógł atrakcyjnie tworzyć swoją stronę lub bloga, nabędzie podstawowe umiejętności pozwalające mu stworzyć, zarządzać, opracowywać i dodawać do nich treści (słowne, graficzne, muzyczne, filmowe). Zrozumie jak zapewnić bezpieczeństwo sobie w sieci i swoim dzieciom. Poza tym pozna gdzie szukać darmowego wsparcia w Internecie oraz na czym polega praca dziennikarza internetowego.

Ważnym aspektem szkolenia będzie poznanie praktycznych podstaw prawa autorskiego, niezbędnego do korzystania z zasobów sieci i zdobycie umiejętności wyszukiwania legalnych źródeł tj.: film, muzyka, książki i inne. Uczestnicy szkolenia zapoznają się z zasadami działania grup dyskusyjnych, poznają tajniki pracy dziennikarza.

ŚRODOWISKO PRACY: laptop dla każdego uczestnika (zestaw komputerowy) lub tablet z dostępem do Internetu oraz zainstalowaną przeglądarką internetową, ekran, projektor multimedialny, głośniki, kamerki internetowe w przypadku stanowisk stacjonarnych.

MATERIAŁY POMOCNICZE W RAMACH WSPARCIA: instrukcje słowne, elementy wykładu lub teorii, filmy instruktażowe (tutorial).

6.1.2. ZAKRES TREŚCI PROGRAMOWYCH ORAZ UWAGI O REALIZACJI

Informacje wstępne: Zajęcia prowadzone głównie na zasadzie zajęć praktycznych na urządzeniach cyfrowych poparte wykładem i instruktażem słownym Trenera. Podstawą równomiernej pracy wszystkich uczestników szkolenia jest prowadzenie warsztatów z wykorzystaniem pokazu/projeksi wykonywanych ćwiczeń i zadań.

1. Korzystanie z usług GOOGLE



CELE I KOMPETENCJE CYFROWE

- Nabycie wiedzy na temat sposobów i metod wyszukiwania informacji w sieci.
- Kształtowanie umiejętności pozyskiwania informacji w sieci.
- Nabycie umiejętności obsługi komputera i korzystania z przeglądarki internetowej w trybie zaawansowanym.
- Kształtowanie sprawności w przeglądaniu najpopularniejszych stron i serwisów związanych z dziennikarstwem oraz promocją..
- Nabycie umiejętności korzystania z narzędzi portali edukacyjnych.
- Poznanie usług serwisu społecznościowego GOOGLE



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Działanie konta Google. Konto Google zapewnia nam dostęp do większości naszych usług (np. Google Ads, Gmaila i YouTube) za pomocą tej samej nazwy użytkownika i hasła. Jeśli korzystasz już z jakiejś usługi Google, np. Gmaila, oznacza to, że masz konto Google.



UWAGA !!! *Gdy zakładamy konto Google, zostaniemy poproszeni o podanie pewnych danych osobowych. Podając dokładne informacje, pomagasz chronić swoje konto i dopasowywać usługi GOOGLE.*

Konto Google daje nam dostęp do wielu usług Google. Dzięki niemu możesz np.:

- wysyłać i odbierać e-maile poprzez Gmaila,
- znajdować nowe, ciekawe filmy na YouTube,
- pobierać aplikacje z Google Play.



UWAGA !!! *Konto Google (osobiste) zapewnia dostęp do produktów i usług Google, takich jak Gmail, Dysk Google, Kalendarz i Zdjęcia. Można utworzyć konto bez Gmaila przy użyciu dowolnego adresu e-mail, na przykład adresu firmowego lub adresu w innej usłudze poczty internetowej, takiej jak Yahoo!® lub Microsoft®Outlook®. Zarejestrowanie się w Gmailu powoduje automatyczne utworzenie konta Google z adresem w domenie @gmail.com.*

Możliwości i zalety poczty Google Gmail

Elektroniczną skrzynkę pocztową posiada dziś niemal każdy. Z pewnością jednak nie wszyscy są w pełni zadowoleni z jej funkcjonalności, designu czy przejrzystości interfejsu. Ciekawą propozycją jest poczta Gmail, należąca do Google. Do najważniejszych zalet Gmail należą m.in.: brak uciążliwych reklam, prosta obsługa, szyfrowanie połączenia, skuteczny filtr antyspamowy, wbudowany komunikator z wideo-rozmowami Google Talk oraz całe mnóstwo możliwości personalizacji wyglądu naszej skrzynki.

Gmail na chwilę obecną oddaje do naszej dyspozycji ponad 15 GB przestrzeni dyskowej, do przechowywania naszych wiadomości. Dzięki tak dużej pojemności skrzynki możemy po prostu archiwizować, bez konieczności usuwania wiadomości. Gdyby pojemność 15 GB okazała się dla nas zbyt mała, istnieje możliwość płatnego powiększenia

swojego konta, nawet do 1000GB. Dodatkowo strona internetowa z aplikacją Gmail bardzo szybko się ładuje umożliwiając nam natychmiastowy dostęp do maila.

Gmail etykiety wiadomości. Bardzo praktycznym rozwiązaniem w kwestii segregowania naszych wiadomości jest wprowadzony przez Google system etykiet. Zakłada on, że każdy z naszych listów może zostać oznaczony specjalną etykietą o dowolnej nazwie, jak np. Zaproszenia, Redakcja czy Osobiste. Każdej wiadomości możemy nadać nieskończenie wiele etykiet, dzięki czemu wiadomość tę odnajdziemy później pod tymi właśnie kategoriami z lewej strony interfejsu.

Filtry wiadomości. Zachowanie porządku w skrzynce pocztowej to niełatwe zadanie. Gmail oferuje swoim użytkownikom praktyczne filtry, pozwalające na porządkowanie wiadomości w sposób automatyczny. W praktyce oznacza to, że możemy automatycznie przypisywać wiadomościom od konkretnych osób wybrane przez nas etykiety. Jest to szczególnie przydatne jeśli wyjątkowo często mailujemy z konkretną osobą, lub regularnie otrzymujemy wiadomości z jednego adresu mailowego.

Filtr antyspamowy. Google prowadzi zdecydowaną politykę antyspamową. Jeśli jednak zdarzy nam się odebrać niepożądaną wiadomość, wystarczy skorzystać z opcji „Zgłoś spam”. Maile z tego adresu już do nas nie trafią.

Inne konta pocztowe, połącz wszystkie skrzynki z gmail. Google umożliwia nam podpięcie do Gmaila dodatkowych, zewnętrznych kont pocztowych. Dzięki temu nasze wiadomości z adresu służbowego i prywatnego mogą być pobierane i wysyłane z jednego miejsca. Wystarczy podać swój adres e-mail, hasło i serwer POP. Gmail pozwala nam również na stworzenie wielu różnych sygnatur – innej dla każdego wykorzystywanego adresu.

Bezpieczeństwo. Bardzo dużą zaletą poczty Gmail jest również szyfrowanie połączenia. Opcja „Always use https” sprawia, że korzystając z naszej poczty już zawsze będziemy używać bezpiecznego, zaszyfrowanego protokołu.

Bardzo dobre wsparcie dla urządzeń mobilnych.

Z poczty Gmail możemy korzystać wykorzystując inne urządzenia mobilne. Bez problemu sprawdzimy skrzynkę odbiorczą, skorzystamy z kalendarza i innych funkcji w telefonie komórkowym lub tablecie z Androidem. Dostępny tam widżet Gmail pozwoli nam przeglądać odebrane wiadomości i pisać nowe e-maile bezpośrednio na głównym ekranie urządzenia.

Dostępność w trybie offline. Możemy odczytywać archiwalne wiadomości bez dostępu do Internetu. W tym celu konieczne jest wcześniejsze pobranie wiadomości wraz z załącznikami na dysk.



UWAGA !!! Wszystkie możliwości, jakie oferuje swoim użytkownikom **GOOGLE GMAIL** są całkowicie bezpłatne. Jediną wadą poczty może być stosunkowo niewielki rozmiar załączników, wynoszący maksymalnie 25 MB. Większe załączniki możemy udostępniać za pomocą także darmowej usługi Google Drive.

Usługi konta Google: Gmail, Google Analytics, Google Webmaster Tools, Google Talk, Picasa , Web Albums, Czytnik Google, Google Apps, Dysk Google, Kalendarz Google, Blogger, Google Sites, Notatnik Google, Google Checkout, Orkut, Google Video, YouTube, Google AdWords, Google AdSense, Google+, Google in Your Language

Podstawowe usługi **GOOGLE**⁴

1. **Tłumacz Google** - Bezpłatna usługa **Google** szybko przetłumaczy słowa, wyrażenia i strony internetowe z polskiego na ponad 100 innych języków i odwrotnie.
2. **Google Play** – internetowy sklep Google z aplikacjami, grami, muzyką, książkami, magazynami, filmami i programami TV. Treści ze sklepu są przeznaczone do korzystania za pomocą urządzeń działających pod kontrolą systemu operacyjnego Android, ale z niektórych można także korzystać na laptopie czy komputerze stacjonarnym.
3. **Wiadomości Google**, ang. Google News – internetowy agregator wiadomości z serwisów informacyjnych.
4. **Mapy Google, Google Maps** – serwis internetowy umożliwiający wyszukiwanie obiektów, oglądanie map, zdjęć lotniczych powierzchni Ziemi, 360° panoramiczne widoki z poziomu ulic (Street view), natężenie ruchu ulicznego w czasie rzeczywistym oraz planowanie tras podróży samochodem, transportem publicznym, rowerem, pieszo, samolotem, czy promem. Został stworzony w 2005 roku przez Google.

⁴ pl.wikipedia.org

Jest darmowy dla niekomercyjnych użytkowników. W 2018 uruchomiono opcję Mapy Google "Dla Ciebie"⁵.

5. **Książki Google**, ang. Google Books – wyszukiwarka książek wykorzystująca technologię OCR. Wyszukiwanie obejmuje książki znajdujące się w największych księgarniach i bibliotekach na świecie.
6. **Google Duo** – komunikator internetowy wyprodukowany przez amerykańskie przedsiębiorstwo Google. Do korzystania z komunikatora wymagany jest numer telefonu. Komunikator służy do przeprowadzania wideorozmów. Funkcja Puk, puk umożliwia wyświetlanie obrazu z kamery rozmówcy przed odebraniem połączenia.
7. **Google Keep** – Usługa umożliwia tworzenie notatek tekstowych, dźwiękowych i ze zdjęciem. Użytkownik Google Keep może utworzyć notatkę z przypomnieniem opartym na lokalizacji oraz ustawić przypomnienie czasowe.
8. **Google Classroom** to bezpłatna usługa dla szkół, organizacji non-profit oraz użytkowników korzystających z osobistego konta Google. Ułatwia ona uczniom i osobom prowadzącym zajęcia komunikację w szkole i poza nią. Classroom oszczędza czas i papier, a także pomaga w tworzeniu zajęć, rozsyłaniu zadań, komunikowaniu się i organizowaniu pracy.

Praca w chmurze na Dysku Google

Dysk Google umożliwia tworzenie dokumentów tekstowych, arkuszy kalkulacyjnych, prezentacji, obrazów i innych z każdego komputera, który ma dostęp do Internetu. Pozwala także na pracę wielu osób na tym samym dokumencie – również w tym samym czasie.

W zależności od naszych potrzeb, możemy:

- utworzyć nowy folder, w którym będziemy przechowywać dokumenty;
- przesać na swój Dysk Google plik, do którego będziemy mieli dostęp z każdego komputera przyłączonego do Sieci,
- utworzyć nowy dokument tekstowy;
- utworzyć arkusz kalkulacyjny,
- utworzyć prezentację multimedialną,

⁵ [Mapy Google "Dla Ciebie" - uruchom już dziś i nie czekaj na Google! - Android.com.pl](#), Android.com.pl - Największe Polskie Centrum Google Android, 14 lipca 2018 [dostęp 2019-02-19] (pol.).

- wybrać inną aplikację z listy



TUTORIALE, SAMOUCZKI, FILMY INSTRUKTAŻOWE,

- <https://www.youtube.com/watch?v=q4UXANoxXeU&feature=youtu.be> Jak założyć konto Google + Gmail.
- <https://www.youtube.com/watch?v=OdFtCeM5Slw> CppTesty - Konto Gmail cz. 1 – podstawy pracy w chmurze
- <https://www.youtube.com/watch?v=uulba8soP8o> Google Drive - praca w chmurze
- <https://www.youtube.com/watch?v=8-UYreKI9Ao> Jak korzystać z "chmury" ? (GOOGLE DYSK) - poradnik, krok po kroku



__PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

Wyszukiwanie informacji na temat pracy dziennikarza.

- Wprowadzenie pojęcia: dziennikarstwo online, dziennikarz internetowy, portale internetowe, strona www,

ĆWICZENIE – Opracowanie listy wybranych kompetencji dziennikarza – czas 10 min

1. Podziel uczestników na grupy 3-osobowe.
 2. Rozdaj kartony, mazaki.
 3. Poproś aby opracowali dowolną techniką listę wybranych kompetencji osób które wykonują zawód dziennikarza
 4. Poproś liderów każdej grupie, aby zaprezentowali wyniki pracy zespołu.
- Gdzie szukać
 1. Serwisy branżowe
 2. Fora dziennikarskie
https://www.goldenline.pl/grupy/Media_i_dziennikarstwo/dziennikarstwo/rady-dla-poczatkujacych-dziennikarzy,132908/.
 3. Dziennikarski savoir vivre https://www.goldenline.pl/grupy/Media_i_dziennikarstwo/dziennikarstwo/dziennikarski-savoir-vivre,785166/
 4. Blogi i serwisy dla profesjonalistów w branży dziennikarstwa

ĆWICZENIE– Zakładanie konta GOOGLE



Obejrzyj filmy instruktażowe nt. zakładania konta GOOGLE

- https://www.youtube.com/watch?v=rlc0XBr_1Js Jak założyć konto na gmail, jak założyć konto Google
- <https://www.youtube.com/watch?v=Jrl2HuaqXJ0Q> Jak utworzyć konto Google
- <https://www.youtube.com/watch?v=hkzpRto3NxA> Jak założyć konto Google

Załącz konto osobiste zgodnie z instrukcją z filmu oraz zapoznaj się z dostępnymi usługami.

ĆWICZENIE – Google Drive

Wyszukaj 3 dowolne serwisy branżowe. Wybierz dowolny artykuł i skopiuj jego adres URL do Worda. Zapisz plik na swoim dysku GOOGLE DRIVE lub zapisz na dysku i wyślij na swoją pocztę elektroniczną.

ĆWICZENIE– projektowanie artykułu – zaplanowanie zadań, podział ról – czas 30 min

- Podziel uczestników na grupy 3-osobowe.
- Rozdaj kartony, mazaki.
- Poproś aby zaplanowali swój projekt pracy zespołu redakcyjnego z podziałem na zadania
- Poproś liderów każdej grupy, aby zaprezentowali wyniki pracy zespołu.

ĆWICZENIE– udostępnianie dokumentów

- Udostępnij listę cech dziennikarza innym uczestnikom szkolenia wykorzystując funkcję UDOSTĘPNIJ. Nadaj im wszystkie uprawnienia (możliwe opcje to: edytowanie, komentowanie czy tylko wyświetlanie)
- Wspólnie dopiszcie jeszcze w dokumencie Dziennikarski savoir vivre

DYSKUSJA I POKAZ: inne aplikacje/usługi konta GOOGLE

- Przegląd aplikacji GOOGLE

ĆWICZENIE– Praca z kalendarzem GOOGLE

- Utwórz nowy kalendarz pod dowolną nazwą, np. NASZA GAZETA
- Udostępnij kalendarz swojemu sąsiadowi
- Wspólnie z sąsiadem zaplanuj w kalendarzu zadania dla zespołu redakcyjnego. (uzupełnijcie oba kalendarze – Twój i sąsiada)

2. Prowadzenie rozmów przez Internet (np. wideorozmowy, rozmowy grupowe).



CELE I KOMPETENCJE CYFROWE

- Opanowanie umiejętności w zakresie korzystania z komunikatorów, prowadzenia wideokonferencji, rozmów na czacie zarówno na komputerze jak i z użyciem urządzenia mobilnego.
- Nabycie umiejętności nawiązania rozmowy online z innymi użytkownikami.
- Nabycie umiejętności i wiedzy na temat darmowych komunikatorów WhatsApp na Androidzie.
- Umiejętność nawiązywania wideo rozmowy oraz czatu.
- Nabycie umiejętności korzystania z forów wymiany informacji oraz poznanie zasad korzystania z tej usługi.
- Opanowanie umiejętności konfigurowania konta.
- Nabycie umiejętności nawiązania rozmowy online z innymi użytkownikami portali społecznościowych.
- Nabycie wiedzy i umiejętności w zakresie korzystania z komunikatora Facebook Messenger.
- Poznanie zasad netykiety w Internecie.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Czat oraz darmowe wideorozmowy w Facebook Messengerze

Portal społecznościowy Facebook w 2015 roku zaoferował swoim użytkownikom nową funkcję w aplikacji mobilnej Messenger służącej do obsługi chatu. Dzięki czemu użytkownicy największego portalu społecznościowego na świecie za pomocą swoich smartfonów i tabletów mogą prowadzić między sobą wideorozmowy.

Messenger⁶ to aplikacja Facebooka służąca do komunikacji pomiędzy użytkownikami portalu.

⁶ **Facebook Messenger** - komunikator internetowy stworzony przez Facebooka. Służy do wysyłania wiadomości, zdjęć, filmów, naklejek i innych plików, a także pozwala reagować na wiadomości znajomych (tz. reakcje) oraz wchodzić w interakcje z botami. Usługa pozwala również na połączenia głosowe (także grupowe) oraz na wideorozmowy. Aplikacja ma możliwość szyfrowania wiadomości oraz grania w minigry.

Przykładowe komunikatory:

- **Telegram,**
- **Skype,**
- **Hangout,** (komunikator znajdujący się w usługach konta GOOGLE)

DYSKUSJA, POKAZ


- E-konsultacje – jak z nich korzystać?
- Gdzie szukać pomocy?
- Przykłady wykorzystania w praktyce:
 - Konsultacje ze specjalistami medycznymi GRUPA LUXMED,
 - rozmowa tekstowa (czat) podczas pomocy online przy rezerwacji biletu lotniczego, w biurze turystycznym i innych
- Korzystanie ze Sklepu Play na urządzeniach mobilnych.
- Prowadzenie wideorozmowy na wybranym komunikatorze
- Wymiana doświadczeń
- Wnioski na temat, który komunikator jest przystępniejszy w obsłudze

DYSKUSJA, POKAZ - Wprowadzenie pojęcia: Streaming - Media strumieniowe

- Dźwięk, obraz oraz dodatkowe dane opisowe, to najczęściej przesyłane dane w postaci mediów strumieniowych:
- dźwięk - radio internetowe,
- obraz - telewizja internetowa,
- dodatkowe dane opisowe - napisy do filmu albo nazwy piosenek

DYSKUSJA, POKAZ - Korzystanie z komunikatora internetowego Hangout

- *Hangout. Korzystanie z Hangoutna na koncie Google.* www.hagouts.google.com
- Rozmowy między uczestnikami
- Konfiguracja połączenia
- Zapraszanie innych do rozmowy lub czatu
- Dodawanie kontaktów.

 **UWAGA!!!** Wszystkie ćwiczenia należy wykonywać z wykorzystaniem projektora multimedialnego dla psychicznego komfortu uczestników szkolenia. Pozwoli to na weryfikację realizacji zadania przez samych uczestników.

 **ISTOTNE FAKTY:**

- Do Hangouta można zaprosić maksymalnie 10 osób
- Nadawanie na żywo musi odbywać się na tym samym koncju, na którym mamy założony G+. Jeśli organizujemy Hangout na koncju firmowym, które nie jest połączone z YouTube – należy założyć konto osobowe na G+, które byłoby połączone z YouTube (z tego samego adresu e-mail) i nadać mu uprawnienia administratora naszej strony firmowej.
- W Hangout nadawanym na żywo (oraz publicznym) nie mogą brać udziału osoby, które nie ukończyły 18 roku życia. Tu decyduje data urodzenia wpisana przez użytkownika z G+.
- W czasie nadawania na żywo na YT, istnieje opcja dodawania komentarzy w czasie rzeczywistym. Osoby, które nie mogły wziąć udziału w Hangout, spokojnie zatem mogą zadać pytanie poprzez komentarz.
- Naturalnie trzeba posiadać kamerkę internetową oraz mikrofon.
- W trakcie trwania Google Hangout, jego założyciel może w każdym momencie wyprosić innych użytkowników, wyłączyć im mikrofon lub też nadawanie obrazu. Twórca wideorozmowy może również decydować kto pojawia się na ekranie głównym - wystarczy kliknąć w obraz nadawany przez uczestnika. Aplikacja sama też rozpoznaje kto w danym momencie mówi i automatycznie pojawia się na ekranie głównym.

Google Hangouts udostępnia również harmonogram najciekawszych wideorozmów, tak aby móc zapisać je do swojego kalendarza

Prowadzenie komunikacji z odbiorcami zgodnie z zasadą netykiety.

Netykieta to zbiór zasad przyzwoitego zachowania w Internecie.

Na poziomie komunikacji elektronicznej zarówno na blogach, stronach internetowych, jak i poczcie elektronicznej powinno się przestrzegać określonych zasad. Są to:

- zakaz stosowania wulgaryzmów,

- zakaz wysyłania SPAMU,
- duże załączniki w e-mailu pakujemy programem do kompresji, żeby nie zapychał odbiorcy skrzynki,
- nie cytujemy całych wiadomości,
- wiadomości powinny mieć temat,
- listy e-mailowe piszemy w formacie tekstowym, a nie HTML-u
- unikamy błędów w tekście listu, używamy narzędzi do sprawdzania pisowni,
- nie piszemy tekstów dużymi literami,
- na forach dyskusyjnych należy pisać konkretnie i na temat
- szanujemy prywatność innych – nie piszemy np. na blogu o prywatnych sprawach znajomych,
- nie wolno kopiować, plagiatować i wklejać cudzych tekstów bez podawania przypisu czy źródła.

Trolling - negatywne zjawisko, głównie występujące na [forach internetowych](#) polegające na celowym wszczynaniu kłótni przez niektórych użytkowników.

Trolle prowokują kłótnie poprzez obrażanie, wyśmiewanie i poniżanie innych użytkowników.



PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

Prowadzenie rozmów przez Internet (np. wideorozmowy, rozmowy grupowe).

DYSKUSJA, POKAZ, ĆWICZENIA: Czat oraz darmowe wideorozmowy w Facebook Messengerze

- Aplikacje do komunikacji: **Skype, Telegram, Facebook Messenger, Hangout**
- Jak wykorzystać do rozmów ze znajomymi lub osobami z którymi chcemy przeprowadzić wywiad?
- Przykłady wykorzystania komunikatorów do prowadzenia rozmów służbowych
- Zalety korzystania z komunikatorów

Korzystanie z komunikatora internetowego Skype

ĆWICZENIE: [Korzystanie z komunikatora internetowego Skype](#)

- Prowadzenie wideo rozmowy i czatu z wykorzystaniem Skype. Instalacja Skype. Korzystanie ze Skype w poczcie Outlook lub SKYPE online ze strony <https://www.skype.com/pl/>
- Rozmowy między uczestnikami
- Konfiguracja połączenia
- Zapraszanie innych do rozmowy lub czatu

Korzystanie z komunikatora internetowego Hangout

- Dodawanie kontaktów.

ĆWICZENIE: Prowadzenie wideo rozmowy i czatu z wykorzystaniem Hangout. Instalacja Hangout. Korzystanie ze Hangout na koncie Google. www.hangouts.google.com

- Rozmowy między uczestnikami
- Konfiguracja połączenia
- Zapraszanie innych do rozmowy lub czatu
- Dodawanie kontaktów.

ĆWICZENIE: Czat oraz darmowe wideorozmowy w Facebook Messengerze

- Zasady korzystania z komunikatorów internetowych
- W jakim celu można z nich skorzystać na co dzień

ĆWICZENIE: Korzystanie z aplikacji WhatsApp na telefonie z systemem Android

Cel: Nabycie umiejętności korzystania z różnych urządzeń mobilnych

- Nabycie wiedzy, nt. wykorzystanie urządzeń do nauki i zabawy.

ĆWICZENIE: Instalacja i konfiguracja komunikatora WhatsAppa telefonie. Zasady korzystania z aplikacji

Korzystanie z czatu na Facebooku

ZADANIE_ Czat na Facebooku - Określ poziom dostępności grupy:

- **otwarta** - każdy użytkownik Facebooka będzie mógł przeglądać stronę grupy i stać się jej członkiem. Cała zawartość (np. zdjęcia, pliki wideo i dyskusje) są widocznie dla wszystkich osób wyświetlających grupę;
- **zamknięta** - każdy użytkownik Facebooka może przeglądać stronę grupy, natomiast administratorzy muszą zatwierdzić każdą prośbę o wpisanie na listę członków grupy

lub osobiście wysłać zaproszenia. Wpisy na tablicy, forum dyskusyjne oraz zdjęcia i pliki wideo są widoczne wyłącznie dla członków grupy;

- **prywatna** - nie pojawia się w wynikach wyszukiwania i jej strony nie mogą być przeglądane przez osoby, które nie są członkami tych grup. Nazwa grupy nie jest wyświetlana w profilach jej członków. Członkostwo w grupie można uzyskać wyłącznie poprzez zaproszenie

ZADANIE_- Tworzenie listy znajomych

- Otwórz **Czat**, następnie kliknij zakładkę **Listy znajomych**
- W oknie **Utwórz nową listę** wpisz nazwę tworzonej grupy i kliknij **Enter**
- Żeby dodać znajomych do listy kliknij **Edytuj** znajdujące się przy nazwie danej grupy, po najechnaniu na nią myszką; wtedy pojawi się okno z Twoimi znajomymi
- Zaznacz w nim tych znajomych, których chcesz dodać do grupy, a następnie kliknij **Zapisz listę**
- Aby usunąć kogoś z danej listy wykonaj czynności 1. do 4., ale w punkcie **odznaczyć** osoby i kliknij **Zapisz listę**

3. Prowadzenie konta na kanale YouTube.



CELE I KOMPETENCJE CYFROWE

- Poznanie zasad prowadzenia kanału YouTube.
- Nabycie wiedzy i umiejętności w zakresie zakładania kont na portalach i stronach
- Nabycie wiedzy i umiejętności w zakresie obsługi i konfiguracji kont społecznościowych.
- Wykorzystanie YT w dziennikarstwie.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Prowadzenie konta na kanale YouTube

YouTube – serwis internetowy⁷ założony w lutym 2005 roku, który umożliwia bezpłatne umieszczanie, odtwarzanie strumieniowe, ocenianie i komentowanie filmów.

Prezesem od 2014 roku jest Susan Wojcicki.

Każde konto Google automatycznie otrzymuje „w pakiecie” **konto YouTube**. Jest to duże udogodnienie, dzięki czemu nie trzeba zapamiętywać dodatkowych loginów i haseł oraz tworzyć kolejnych kont. Dodatkową wygodą, jest to że możemy prowadzić kilka kanałów **YouTube** w ramach jednego konta Google. Wystarczy tylko przetaczać się pomiędzy kontami YouTube.

Dla każdego posiadacza kanału YouTube istotna jest jego atrakcyjność, aby wzbudzał zainteresowanie wśród użytkowników sieci. Dlatego należy zadbać o oryginalną i przyciągającą uwagę grafikę. Tworząc taką grafikę musimy dostosować się do szablonu dostarczonego przez projektantów tej usługi. Do tego posłuży program Photoshop, ponieważ tylko pliki z rozszerzeniem *.psd są w stanie dopasować się podczas wyświetlania zarówno na ekranie monitora, tabletu oraz telewizora. Stąd różne wymagania co do wielkości.

Oficjalny plik z szablonem dostępny jest pod adresem: https://storage.googleapis.com/support-kms-prod/SNP_C806A91A0D63EB04E3814E2D7AF07C58FCD4_2990562_en_v2

Drugim ważnym elementem kanału jest chwytliwy adres, inaczej mówiąc **NIESTANDARDOWY ADRES URL**. Jest to wymyślona przez nas nazwa, która ma zastąpić automatycznie wygenerowany adres przez system.

Na stronie https://www.youtube.com/account_advanced mamy możliwość zmiany adresu klikając w link: **UTWÓRZ NIESTANDARDOWY URL**.



Należy przy tym pamiętać, że czynność ta możliwa jest do wykonania tylko raz, a zmian nie można już cofnąć. Co zmusza nas do przemyślenia nazwy.

Skuteczne zarządzanie kanałami YouTube, polega na odpowiedniej automatyzacji, która pozwoli na oszczędność czasu oraz na samoistne publikowanie materiałów na kolejnych portalach takich jak Google+ czy Facebook. W tym celu należy połączyć swoje konta Facebook oraz Twitter (Google+ automatycznie publikuje Twój контент), by automatycznie

⁷ **Serwis internetowy, witryna internetowa** – grupa powiązanych ze sobą, w celu zwiększenia funkcjonalności, stron internetowych. Serwisy internetowe, poza treścią statyczną, często mają sekcję wiadomości oraz oferują możliwość logowania się i zapamiętywania preferencji odbiorców w celu dostosowania treści do indywidualnych upodobań. W serwisie mogą występować obiekty interaktywne, na przykład formularze, aplikacje. Serwisy mogą być tematyczne, a więc poświęcone jednej dziedzinie lub kwestii, albo ogólne. https://pl.wikipedia.org/wiki/Serwis_internetowy

udostępniać nowe materiały w sieciach społecznościowych. Takiej konfiguracji dokonasz na stronie: https://www.youtube.com/account_sharing

Dla ułatwienia wyszukiwania naszego kanału przez innych użytkowników należy wpisać takie słowa kluczowe w opcjach **KANAŁY**, aby Internauci bez problemu odszukali nasz produkt. Kluczowe słowa muszą być ściśle związane z treściami (zawartością) naszego kanału.

Aby tego dokonać należy wejść na stronę https://www.youtube.com/advanced_settings **TWOJE KONTO GOOGLE+**

Kolejnym ważnym elementem jest **weryfikacja**. Dzięki niej system będzie traktował Cię jak człowieka korzystającego z systemu, a nie robota automatycznie zakładającego konta.

Prawidłowej weryfikacji dokonasz na stronie: [youtube.com/verify](https://www.youtube.com/verify)

podczas weryfikacji należy podać numer telefonu na który otrzymasz wiadomość SMS bądź połączenie automatyczne. Po weryfikacji konta otrzymasz duży **upgrade**⁸ funkcjonalności, czyli od tego momentu będziesz miał **możliwość upload'u⁹ plików dłuższych niż 15 minut!**

Ostatnim bardzo ważnym zadaniem jest:

1. **Opisanie swojego kanału w kilku zdaniach** – dobry opis stanowi źródło cennych informacji o kanale oraz w znacznym stopniu wpływa na wyszukiwanie. Należy zawrzeć w nim odpowiednie, prawdziwe informacje ujmując słowa kluczowe.
2. **Dodanie linków społecznościowych oraz danych kontaktowych**, tak by każdy mógł bez kłopotu do Ciebie zadzwonić lub napisać wiadomość.

Po takich zabiegach Twój kanał jest gotowy na to, by zacząć przyciągać subskrybentów, wgrywać dziesiątki filmów oraz budować zaangażowaną społeczność.



PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

⁸ **Upgrade** (z ang: poprawiać, ulepszać) **Upgrade** może to być ulepszenie sprzętu czyli wymiana gorszego sprzętu, na nowy lepszy z lepszymi częstotliwościami i parametrami. <https://pl.wikipedia.org/wiki/Upgrade>

⁹ **Upload** - proces przeciwny do pobierania danych, polegający na wysłaniu **plików** lub innych danych do serwera lub komputera należącego do innego użytkownika. Często łącze internetowe jest umownie dzielone na dwa kanały: kanał wysyłania i kanał pobierania. <https://pl.wikipedia.org/wiki/Upload>

ĆWICZENIE: Przeglądanie zasobów YouTube

- Poszukaj dowolnego filmu, muzyki lub gry.

ĆWICZENIE: Tworzenie kanału YouTube

- Za pomocą opcji APLIKACJE GOOGLE utwórz kanał YouTube.
- Skonfiguruj konto
- Utwórz film lub posta na dowolnie wybrany temat, który chciałbyś zrealizować jako dziennikarz.

4. Prowadzenie transmisji internetowych w serwisach społecznościowych



CELE I KOMPETENCJE CYFROWE

- Opanowanie umiejętności w zakresie korzystania z komunikatorów, prowadzenia wideokonferencji, rozmów na czacie.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Każdy redaktor powinien umieć korzystać z mediów strumieniowych, czyli relacjonować ciekawe wydarzenia na żywo.

Prowadzenie transmisji internetowych w serwisach społecznościowych

- Wprowadzenie pojęcia: Streaming - Media strumieniowe
 - Dźwięk, obraz oraz dodatkowe dane opisowe, to najczęściej przesyłane dane w postaci mediów strumieniowych:
 - dźwięk - radio internetowe,
 - obraz - telewizja internetowa,
 - dodatkowe dane opisowe - napisy do filmu albo nazwy piosenek



PRZYKŁAD Transmisja spotkania/konferencji na żywo. Podczas zmiany prelegentów w krótkiej przerwie technicznej w tle odtwarzany jest utwór muzyczny. Wystarczy kilka sekund i transmisja zostaje zablokowana za złamanie praw autorskich. Mimo, że dźwięk był jedynie fragmentem tła, można pogrążyć każdą transmisję



UWAGA! W transmisji nie można emitować reklam. Wszelkie wątpliwości w tej kwestii rozstrzygane są na niekorzyść nadawcy. **Karą jest zablokowanie transmisji, a nawet**

może się zdarzyć, że zostaniemy zablokowani na organizowanie transmisji na kolejne 90 dni.



DYSKUSJA, POGADANKA, POKAZ:

- co to jest koder i do czego służy
- konfiguracja Kodera
- Przykładowe kodery: **Epiphan Webcaster X2, XSplit Broadcaster, XSplit Gamecaster, Wirecast Play** i inne. Zobacz na stronie:
<https://support.google.com/youtube/answer/2907883?hl=pl>. Jest też oprogramowanie **opensource'owe: Open Broadcaster Software**,
- Rodzaje dostępu do mediów strumieniowych
- Mediastrumieniowe, a typy treści multimedialnych



UWAGA! Włączenie transmitowania na żywo po raz pierwszy może zająć do 24 godzin. Gdy ta funkcja zostanie włączona, transmisję na żywo będzie można rozpocząć od razu.

- Rozpoczynanie transmisji
- Prowadzenie transmisji na żywo
- Nawiązywanie kontaktu z publicznością przez [czat na żywo](#).
- Zakończenie transmisji
- Potrzebny sprzęt do przeprowadzenia transmisji



TUTORIALE, SAMOUCZKI, FILMY INSTRUKTAŻOWE

<https://lenovozone.pl/blog/jak-zaczac-streamowac/> Jak zacząć streamować?

Przykłady innych serwisów społecznościowych - serwisy społecznościowe, z których korzystamy najczęściej

1. **Facebook** - Gromadzi ogromne ilości danych i korzysta z niego około 1,4 miliarda użytkowników z całego świata. W Polsce jest to serwis społecznościowy numer jeden. Jego użytkownicy mogą udostępniać treści i zdjęcia oraz reagować na nie, tworzyć grupy i wydarzenia, a także podejmować działania reklamowe w obrębie strony
2. **YouTube** - to niezwykle popularny serwis, który służy do udostępniania i oglądania materiałów wideo. Umożliwia subskrybowanie kanałów oraz komentowanie i ocenianie

treści. Znajdziemy w nim tysiące twórców, którzy dzielą się vlogami o różnej tematyce. Jest to, po Google, druga największa wyszukiwarka

3. **Snapchat** - to aplikacja mobilna, którą pokochali młodzi użytkownicy mediów społecznościowych, służąca do wysyłania znikających wiadomości do wybranych osób lub umieszczania ich w sekcji Stories. Znajdziemy tam geofiltry, maski, naklejki i inne narzędzia, które sprawią, że nasze kilkusekundowe treści będą jeszcze bardziej atrakcyjne w odbiorze
4. **Instagram** - to jeden z najpopularniejszych serwisów społecznościowych na świecie, który umożliwia publikowanie zdjęć i krótkich filmików. Obsługuje sekcję Stories oraz tworzenie albumów. Obecnie jest wiodącym narzędziem reklamowym dla wielu marek.
5. **LinkedIn** - to sieć społecznościowa dla profesjonalistów. Pozwala na nawiązanie kontaktów zawodowych, dzielenie się w ramach profilu informacjami o naszych umiejętnościach, które mogą być potwierdzone przez innych użytkowników, a także na publikowanie ofert pracy, interakcje i dyskusje grupowe oraz udostępnianie wartościowych treści
6. **Google+** - zadebiutowało w 2011 roku i jest siecią społecznościową, która w Polsce jest nieco mniej popularna i raczej niedoceniana. W ramach strony możemy dzielić się informacjami, tworzyć kręgi znajomych, zintegrować profil z albumem zdjęć Picasa Web czy organizować wideospotkania
7. **Twitter** - to dobrze znany serwis społecznościowy umożliwiający mikroblogowanie. Jego cechą charakterystyczną jest limit wpisu w postaci 140 znaków oraz używanie hashtagów, które pozwalają na agregację treści do odpowiednich znaczników, co znacznie ułatwia wyszukiwania interesujących nas tweetów
8. **Kik** - to darmowa aplikacja do szybkiej komunikacji, szczególnie popularna wśród młodych użytkowników. Użytkownicy mogą porozumiewać się ze sobą indywidualnie lub grupowo, używając nazw profili Kik zamiast numeru telefonu. Mogą wysłać wiadomości tekstowe, jak i multimedialne. Program daje także możliwość dobierania użytkowników na podstawie podobnych zainteresowań
9. **WhatsApp** - to aplikacja, która oferuje łatwą i bezpieczną komunikację oraz bezpłatne połączenia głosowe i wideo przy użyciu internetu. Wykorzystuje nasz numer telefonu, a użytkownicy mogą zezwolić na połączenie z książką telefoniczną, po to, aby nasze kontakty pojawiały się także w aplikacji. Jakiś czas temu do komunikatora

wprowadzono szyfrowanie treści, dzięki czemu wiadomość może przeczytać tylko jej nadawca oraz odbiorca, nikt poza tym

10. Musica.ly - to platforma twórcza, która umożliwia udostępnianie krótkich teledysków i dzielenie się nimi z przyjaciółmi i ze światem. Dostępne są takie kategorie jak muzyka, komedia, talent, vlog czy zwierzęta. Użytkownicy, którzy używali tej samej ścieżki dźwiękowej mogą także łączyć swoje wykonania w duety.



PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

ĆWICZENIE: Podziel uczestników na dwie konkurencyjne redakcje. Poproś aby wykonały telewizyjnego newsa ze szkolenia wykorzystując w tym celu smartfony. Dodatkowym utrudnieniem będzie zmontowanie „offa”, czyli głosu czytającego newsa w tle oraz wstawienia kilku „setek”, czyli wypowiedzi uczestników czy prowadzącego.

ĆWICZENIE: Konfiguracja i uruchomienie własnej transmisji na własnym kanale. Ćwiczenie wykonywane pod nadzorem trenera/opiekuna.

5. Rodzaje licencji (licencje otwarte, komercyjne) na których mogą być udostępnione treści i oprogramowanie.



CELE I KOMPETENCJE CYFROWE

- Poznanie rodzajów licencji oprogramowania.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Jako użytkownicy komputerów i różnych urządzeń mobilnych, stykamy się z aplikacjami, począwszy od prostych komunikatorów, przez rozbudowane programy, gry komputerowe, po systemy operacyjne. Każdy z tych programów objęty jest umową pomiędzy ich wydawcą, a konsumentami - nami. Umowa taka, nazywana jest potocznie licencją¹⁰.

¹⁰ *Licencje komputerowe to dokumenty, które porządkują sposób korzystania z programów komputerowych, Bez nich, w świecie oprogramowania zapanowałby totalny chaos. Dzięki nim wiadomo, kto może używać danej aplikacji, w jakim celu, określają one, co można z programem zrobić, regulują prawa własności. Warto wiedzieć,*

Podstawowym podziałem w kwestii licencjonowania oprogramowania jest podział na:

- model zamknięty (oprogramowanie własnościowe, prawnie zastrzeżone, zamknięte)
- model otwarty (oprogramowanie o otwartym kodzie źródłowym).

Przeciwwagą dla systemu zamkniętych licencji jest model otwarty, w przypadku którego większość praw jest dana użytkownikowi. Najistotniejszą cechą oprogramowania na otwartej licencji rozpowszechniane w postaci kodu źródłowego, **co umożliwia jego zmiany i jego udoskonalanie**. Użytkownik ma prawo swobodnie korzystać z oprogramowania udostępnionego na otwartej licencji. Zasady korzystania z oprogramowania (lub jego elementów) różnią się w zależności od typu licencji.

Licencja komercyjna¹¹ z kolei, to licencja pozwalająca na użytkowanie, często markowych, produktów (w tym programów) w celach komercyjnych. Obejmuje ona m.in. programy oparte na innych niekomercyjnych licencjach, które mogą zostać użyte w celach zarobkowych dopiero po wykupieniu licencji komercyjnej. Ograniczenia w tych licencjach dotyczą prawa użytkowania, kopiowania, rozpowszechniania, modyfikowania programów oraz często zabezpieczają ich kody źródłowe.

Mianem **wolnego oprogramowania** można określać aplikacje spełniające określone warunki. Przede wszystkim, każdy może uruchamiać je w dowolnym celu. Mogą być one również bez ograniczeń rozkładane na czynniki pierwsze i dostosowywane do własnych potrzeb. Nie ma także żadnych ograniczeń w kopiowaniu, rozpowszechnianiu kopii oraz udoskonalaniu i rozpowszechnianiu własnych wersji aplikacji. To po części podejście filozoficzne. W odróżnieniu od tego, otwarte oprogramowanie koncentruje się na podejściu praktycznym, z nieograniczonym dostępem do źródeł, ale bez wykluczenia częściowego komercyjnego wykorzystania otwartych aplikacji.

Od nazw niektórych licencji wzięty również nazwę niektóre rodzaje oprogramowania. Tak na przykład jest z licencjami i programami shareware czy freeware. Często również pojęcie licencji używane jest błędnie, gdyż używany termin określa jedynie rodzaj oprogramowania. Przykładem może być stealware, który oznacza program okradający użytkownika. Aplikacja tego typu to rodzaj wirusów, instalowane są bez wiedzy i zgody osób

jakie prawa dają i jakie obowiązki nakładają różne umowy licencyjne. <https://www.pcworld.pl/news/Swiat-licencji-oprogramowania,382093.html>

¹¹ https://pl.wikipedia.org/wiki/Licencja_komercyjna

zainteresowanych, śledzą ich działania na komputerze, wykradają dane, podmieniają numery kont podczas dokonywania płatności internetowych. Nazwa jest więc pochodną sposobu działania, a nie licencjonowania.

BOX - Najbardziej znana i najczęściej stosowana licencja. Potocznie zwana - pudełkową, lub pełną. Oferuje produkty zapakowane wraz ze wszelkim wymaganym wyposażeniem. Najczęściej stosowana w przypadku aplikacji multimedialnych, gier czy muzyki. Produkty oparte na licencji BOX są najdroższe ze wszystkich prezentowanych.

OEM - Bardzo rozpowszechniona licencja za sprawą Windowsa. Ta pozwala nam zakupić program przypisany jedynie do jednego komputera. Podczas zmiany jego podzespołów bądź zakupienia innej maszyny, licencja natychmiast traci ważność.

Shareware - Nazwa pochodzi od angielskiego słowa oznaczającego aplikacje, którą można się dzielić z innymi. Ten rodzaj licencji pozwala nam na korzystanie z programu rozpowszechnianego za darmo lub za niewielką opłatą. Jego użytkowanie często wiąże się z limitem czasowym. Po przekroczeniu wspomnianego limitu, użytkownik powinien zakupić pełną wersję produktu.

Adware - Programy typu Adware najczęściej są darmowe ale posiadają pewną, najczęściej sporą ilość niewyłączalnych reklam. To właśnie na nich zarabia autor aplikacji. Dobrym przykładem takiego programu jest Lavasoft służący do wyszukiwania wszelkiego szkodliwego oprogramowania na naszym dysku.

Trial - tzw. "wersja testowa". Oferuję wszystko to co w pełni działający program, jednak jak w przypadku shareware -po upływie czasu aplikacja blokuje do siebie dostęp. W takim wypadku pozostaje nam już tylko kupno pełnego produktu - oczywiście jeśli spełnia nasze wymagania.

Freeware - Jest to jedna z najbardziej lubianych licencji przez użytkowników, a tym samym jedna z najczęściej występujących. Dlaczego? To proste. Licencja ta pozwala nam na darmowe korzystanie z danego produktu. Jedynym wymaganiem jest całkowity zakaz czerpania korzyści majątkowej z takiego oprogramowania oraz jego modyfikowania.

GPL - Jest to licencja wolnego i otwartego oprogramowania. Oznacza to, że użytkownik może uruchamiać program objęty tą licencją w dowolnym celu, dostosowywać go do własnych potrzeb, a nawet rozpowszechniać już zmodyfikowaną wersję.

Abandonware - tzw. "porzucone oprogramowanie". Najczęściej jego autor nie pobiera już za nie pieniędzy co wiąże się z brakiem jakiegokolwiek wsparcia. Najlepszym przykładem programów tego typu są stare gry komputerowe, których właściciele i twórcy już od dawna nie zajmują produkcją komputerowej rozrywki.



CIEKAWOSTKA - Prawa autorskie¹² na program komputerowy w Polsce wygasają 70 lat po śmierci autora lub 70 lat po jego pierwszym opublikowaniu jeżeli autor nie rozpowszechnił go osobiście lub gdy nie jest znany W praktyce więc nie ma jeszcze programów, które nie są już chronione.

Licencja Creative Commons¹³

Licencje Creative Commons są standardowym sposobem, za pomocą którego twórcy treści przyznają innym prawo do korzystania ze swojej pracy. YouTube pozwala użytkownikom oznaczać filmy jako objęte licencją Creative Commons CC BY.

Jeżeli Twój film jest oznaczony jako objęty licencją CC BY, zachowujesz swoje prawa autorskie, a inni użytkownicy mogą wykorzystywać Twoją pracę zgodnie z warunkami licencji.

Creative Commons w YouTube¹⁴

Wszyscy użytkownicy mogą korzystać z możliwości oznaczania przestanych filmów jako objętych licencją Creative Commons.

Domyślnie wszystkie przesyłane filmy mają ustawioną standardową licencję YouTube. Warunki standardowej licencji YouTube znajdziesz w Warunkach korzystania z usługi.

¹² Ustawa o prawie autorskim i prawach pokrewnych - to akt prawny zabezpieczający prawa twórców i wydawców w Polsce. Reguluje on między innymi stosunki między podmiotami udostępniającymi oprogramowanie w ramach jakiejś licencji i licencjobiorcami. Chroni autorskie prawa osobiste (niezbywalne i niewygasające prawo do wiązania autora z jego dziełem) oraz autorskie prawa majątkowe (zbywalne prawo związane wynagrodzeniem za korzystanie z utworu). Zabezpiecza wizerunek, adresatów korespondencji i tajemnicę informacji. W stosunku do oprogramowania i licencji precyzuje pola eksploatacji takie jak zakres, miejsce i czas korzystania z utworu. Nie narzuca jednak sztywnych reguł, które mogą być dowolnie kształtowane przez strony umowy

¹³ <https://support.google.com/youtube/answer/2797468?hl=pl>

¹⁴ <https://support.google.com/youtube/answer/2797468?hl=pl>

Licencje Creative Commons są przeznaczone dla Twoich oryginalnych treści, dlatego nie możesz oznaczyć swojego filmu jako objętego taką licencją, jeśli zgłoszono do niego roszczenie z systemu Content ID.

Oznaczając swój własny film jako dostępny na licencji Creative Commons, dajesz całej społeczności YouTube prawo do jego edytowania i ponownego wykorzystywania.

Jakie materiały można oznaczyć jako dostępne na licencji Creative Commons¹⁵

Pamiętaj, że przesłany przez Ciebie film może zostać oznaczony jako objęty licencją Creative Commons tylko wtedy, gdy zawiera wyłącznie treści, które można udostępnić na licencji CC BY. Oto przykłady materiałów, które można udostępnić na tej licencji:

- Oryginalne materiały Twojego autorstwa
- Inne filmy oznaczone jako dostępne na licencji CC BY
- Filmy z domeny publicznej

Przykłady wyszukiwarek z możliwością określenia licencji na wykorzystanie

- www.search.creativecommons.org
- wspomniana wcześniej www.google.com , zakładka **GRAFIKA**
- Przykłady banków zdjęć:
 - www.frepik.com
 - www.1001freedowlands.com
 - www.caboompics.com
 - www.picjumbo.com
 - www.publicdomainarchive.com
 - www.splitshire.com

Najczęściej do łamania praw autorskich dochodzi w Internecie. Dlatego warto wiedzieć czym są prawa autorskie i jakie konsekwencje grożą za brak ich przestrzegania.



PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

ĆWICZENIE: Sprawdzanie licencji oprogramowania

¹⁵ <https://support.google.com/youtube/answer/2797468?hl=pl>

Uruchom stronę www.dobreprogramy.pl i wyszukaj dowolny program z licencją freeware, trial i shareware. Skopiuj linki do tych programów.

ĆWICZENIE: Sprawdzanie licencji commons

Obejrzyj film „Czym są licencje Creative Commons?”

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

[WRImA](#)

6. Bezpieczeństwo i prawa autorskie



CELE I KOMPETENCJE CYFROWE

- Poznanie zasad bezpieczeństwa w sieci.
- Nabycie wiedzy o prawach autorskich.
- Nabycie umiejętności rozpoznawania zagrożeń w sieci



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Najczęściej do łamania praw autorskich dochodzi w Internecie. Dlatego warto wiedzieć czym są prawa autorskie i jakie konsekwencje grożą za brak ich przestrzegania.

Utwór - Zasady korzystania z cudzych utworów uregulowane są ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24 poz. 83), zwaną prawem autorskim. Zgodnie z art. 1 przedmiotem prawa autorskiego jest *każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia*. Jest to definicja uniwersalna dla wszystkich dzieł twórczych. Tak rozumiany utwór podlega ochronie prawnej, niejako automatycznie, już od chwili jego ustalenia. Jako przykład wskazać należy teksty publikowane w Internecie, filmy, nagrania muzyczne, programy komputerowe, itp. Ich autorom przysługuje ochrona a tym samym możliwość egzekwowania odpowiedzialności cywilnej i karnej¹⁶.

¹⁶ Artykuł: Ochrona praw autorskich w Internecie - <http://www.infor.pl/prawo/prawo-karne/ciekawostki/325443,Ochrona-praw-autorskich-w-Internecie.html>

Prawo autorskie to dyscyplina prawa cywilnego, czyli zespół norm prawnych wchodzących w skład prawa własności intelektualnej¹⁷, a także ogół praw przysługujących autorowi utworu (lub innemu uprawnionemu podmiotowi) upoważniających go do decydowania o eksploatacji utworu i czerpaniu z niej korzyści finansowych¹⁸.

Prawa autorskie dzielimy na osobiste i majątkowe.

1. **Osobiste prawa autorskie** nie wygasają, są niezbywalne, nieprzenoszalne i nie można się ich zrzec. Poza tym polegają na powiązaniu nazwiska twórcy z jego dziełem i gwarantują autorowi prawo do zachowania niezmienionej treści i formy utworu lub anonimowości autora. Twórca dzieła jest osobą uprawnioną do korzystania i rozporządzania go. Tylko on na mocy licencji lub innej umowy może upoważnić także inne osoby.
2. **Majątkowe prawa autorskie** wygasają wraz z upływem 70 lat od śmierci twórcy i ogranicza je zasada dozwolonego użytku (prywatnego i publicznego).

Dozwolony użytek osobisty

Art. 23 Ustawy o prawie autorskim i prawach pokrewnych¹⁹ o dozwolonym użytku osobistym, określa:

1. Bez zezwolenia twórcy wolno nieodpłatnie korzystać z już rozpowszechnionego utworu w zakresie własnego użytku osobistego. Przepis ten nie upoważnia do budowania według cudzego utworu architektonicznego i architektoniczno-urbanistycznego oraz do korzystania z elektronicznych baz danych spełniających cechy utworu, chyba że dotyczy to własnego użytku naukowego niezwiązanego z celem zarobkowym.

¹⁷ **Prawo własności intelektualnej** – termin obejmujący elementy różnych działów prawa, regulujące zasady korzystania z tzw. własności intelektualnej. https://pl.wikipedia.org/wiki/Prawo_w%C5%82asno%C5%9Bci_intelektualnej

¹⁸ https://pl.wikipedia.org/wiki/Prawo_autorskie

¹⁹ USTAWA z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 Nr 24 poz. 83)

2. Zakres własnego użytku osobistego obejmuje korzystanie z pojedynczych egzemplarzy utworów przez krąg osób pozostających w związku osobistym, w szczególności pokrewieństwa, powinowactwa lub stosunku towarzyskiego.

Najczęściej w Internecie sięgamy po pliki multimedialne (piosenki, filmy, seriale). Jeżeli utwór jest już rozpowszechniony, to samo ściąganie (czyli pobieranie) utworu, nie stanowi naruszenia prawa. Zgodnie z ww. ustawą mieści się ono w zakresie pojęcia dozwolonego użytku osobistego, czyli można nieodpłatnie z niego korzystać, a co za tym dalej idzie nie potrzebujemy wyrażenia zgody ze strony twórcy. Należy przy tym pamiętać, że udostępnianie takich plików jest już przestępstwem. Zgodnie z obowiązującym prawem dozwolony użytek osobisty nie może naruszać zasad korzystania z utworu ani godzić w interesy twórcy.

Plagiat i prawo cytatu. Szybki dostęp do informacji zamieszczonych w sieci oraz łatwość z jaką można je zdobyć stwarza sytuacje sprzyjającego do tworzenia plagiatu. I choć nie ma prawnej definicji na to zjawisko, to możemy go sklasyfikować jako jawny i ukryty ale zawsze świadomy. Plagiat to powielenie cudzej pracy (twórczości) w całości lub jej części, czyli mówimy tu np. o kradzieży własności intelektualnej.

Tworząc własną stronę internetową lub bloga pamiętajmy, że gdy zamieszczamy czyjeś teksty lub grafikę, to bezwzględnie podajemy ich autora, czyli źródło właściwe. Nie przywłaszczamy sobie cudzej własności intelektualnej, ponieważ grożą za to kary i poważne konsekwencje. Autor skradzionego utworu ma prawo domagać się:

- opublikowania przeprosin,
- wycofania plagiatu z obrotu,
- rekompensaty finansowej.

Za udowodniony plagiat może ponadto grozić kara grzywny, a nawet ograniczenia wolności do lat 3.



Zobacz więcej: <https://poradnikprzedsiębiorcy.pl/-czym-jest-plagiat-i-jakie-sa-jego-konsekwencje>

W Internecie jest wiele systemów sprawdzających czy dane dzieło jest już plagiatem, czy jeszcze nie. Oto przykład strony, z której korzystają również uczelnie wyższe. Takie strony

zazwyczaj są komercyjne, jednak niektóre z nich mają opcje jednorazowego sprawdzenia pracy lub pliku.



PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

DYSKUSJA: Bazy Legalnych Źródeł – umiejętność rozróżniania źródeł treści legalnych od nielegalnych.

- Pogadanka na temat czym są Bazy Legalnych Źródeł i jak z nich korzystać (zasady korzystania) – korzystanie z funkcji sortowania „darmo”, „odpłatnie”,
- Omówienie zasad ściągania plików multimedialnych (piosenki, filmy, seriale) za pośrednictwem Internetu

ĆWICZENIE: Przeglądanie Bazy Legalnych Źródeł za pomocą zaawansowanych funkcji wyszukiwarki Google - wprowadzenie pojęcia: „licencja”, „dozwolony użytek osobisty”, „prawa autorskie”, „utwór”

ĆWICZENIE: Sprawdź czy w kategorii FILMY serwis ADAPTER jest bezpłatny.

Uwaga!!! Przypomnij uczestnikom, że pobieranie zdjęć, filmów, tekstów jest niedozwolone i nie wolno ich wykorzystywać bez sprawdzenia, na jakich warunkach zostały opublikowane

- Przykłady wyszukiwarek z możliwością określenia licencji na wykorzystanie www.search.creativecommons.org oraz wspomniana wcześniej www.google.com, zakładka **GRAFIKA**



UWAGA!!! – informacje, o których należy bezwzględnie pamiętać. Jest wiele popularnych serwisów zdjęciowych, które oferują zdjęcia do komercyjnego wykorzystania, np. na blogach, czy stronach internetowych. Należy jednak pamiętać, iż każda z nich określa zasady korzystania i pobierania plików. W tym celu należy zapoznać się z regulaminem i zaakceptować go.

ĆWICZENIE: Jak rozpoznać czy obraz, film, treść jest chroniona prawami autorskimi?

Cel – wyjaśnienie uczestnikom, czym są prawa do użytkowania



Uwaga!!! W trakcie wykonywania ćwiczenia należy krótko omówić co oznaczają i jakie dają możliwości poszczególnych filtrów, wprowadzić definicję praw autorskich²⁰ oraz omówić prawo do użytkowania²¹.

- oznaczone do ponownego wykorzystania z modyfikacją (czyli możemy je przerobić),
- oznaczone do ponownego wykorzystania (niekoniecznie można przerobić),
- oznaczone do ponownego wykorzystania w celach niekomercyjnych z modyfikacją,
- oznaczone do ponownego wykorzystania w celach niekomercyjnych.

- Ćwiczenia należy wykonać na kilku różnych wyszukiwarkach



Uwaga!!! Należy wspomnieć o różnicach w sposobie wyświetlania tych samych wyników wyszukiwania w różnych wyszukiwarkach:

1. **JAHO!** – Images/Public Domain

2. **Bing** – Obrazy/Licencja"

3. **Flickr** - zawiera wiele zdjęć chronionych prawami autorskimi. Niezależnie od tego możemy na nim znaleźć zdjęcia na licencji Creative Commons. Część z tych zdjęć można remiksować i wykorzystywać nawet komercyjnie. W czasie przeglądania zdjęć na Flickrze po lewej stronie widzimy link "Any License". Oznacza to, że przeglądamy zdjęcia na wszystkich dostępnych licencjach.

DYSKUSJA: darmowe serwisy zdjęć i banki zdjęć, klipów, dźwięków

- Omówienie co to są banki zdjęć i jakie są ich rodzaje
- Omówienie zasad korzystania z serwisów darmowych zasobów
- Podanie stron darmowych banków:

<https://unsplash.com/>

<https://pixabay.com/pl/>

- Przykłady banków zdjęć (nie wszystkie z nich są darmowe): [Unsplash](#), [Picjumbo](#), [Shutterstock](#), [Dreamstime](#), [IstockPhoto](#), [ThinkStockPhotos](#), [Gratisography](#), [IM Free](#),

²⁰ **Prawo autorskie** - przysługuje twórcy utworu. Istnieje domniemanie, że jest nim osoba, której nazwisko w tym charakterze uwidoczniło na egzemplarzach utworu lub której autorstwo podano do publicznej wiadomości w jakikolwiek inny sposób, w związku z rozpowszechnianiem utworu.

[Death to the Stock Photo](#), [Little Visuals](#), regulaminy tych banków określają zasady pobierania zdjęć za darmo.

DYSKUSJA: Zdjęcia i grafika

- Omówienie zasad korzystania z serwisu Pixabay
- Zaprezentowanie narzędzi serwisu
- Wykonanie zadania wprowadzającego w tajniki korzystania i pobierania darmowych zdjęć

ZADANIE: Pixabay - wyszukiwanie darmowych filmów wideo oraz grafiki wektorowej

1. Uruchom stronę <https://pixabay.com/pl/> i wyfiltruj filmy wideo o zwierzętach wg. kategorii **Nadchodzące**
2. Wyszukaj grafikę wektorową na dowolny temat w kategorii **Najnowsze** – to samo zadanie wykonaj również w dowolnie wybranej wyszukiwarce (np. JAHOO!, Bing, czy Mozilla)
 - Omówienie funkcji Wikipedii jako źródła darmowych zdjęć z uwzględnieniem zalet i wad
 - Wprowadzenie pojęcia „licencji stanowiących domenę publiczną, na licencji Creative Commons oraz GNU FDL”, „licencja komercyjna”
 - Omówienie zobowiązań jakie musimy spełnić w przypadku z korzystania ze zdjęć na tych licencjach (obowiązek dołączenia pełnego tekstu licencji - uznanie tych licencji jest uszanowaniem autora, który zrezygnował z wynagrodzenia.



Uwaga!!! – Wiele źródeł multimediów na wolnych licencjach jest zebrane na stronie commons.wikimedia.org.

DYSKUSJA, POKAZ: Muzyka, filmy, książki

- Prezentacja portali do oglądania filmów, słuchania muzyki
- Wprowadzenie pojęcia „streaming” i jego zalet w aspekcie zachowania praw autorskich i poszanowania własności intelektualnej
- Omówienie źródeł informacji o filmach i serwisach filmowych (na potrzeby szkolenia omówiony zostanie serwis VOD <https://vod.pl/filmy>)
- Podanie przykładów serwisów www.filmweb.pl
www.kinomaniak.pl
www.stopklatka.pl
- Omówienie technik wyszukiwania filmów

- Wykonanie ćwiczenia – wyszukiwanie filmów na dowolnie wybranym serwisie

ĆWICZENIE: Wyszukiwanie filmu na dowolnie wybranym serwisie

Wspólne spędzanie czasu z rodziną można uatrakcyjnić ciekawym filmem.

1. Znajdź na dowolnym serwisie film z uwzględnieniem następujących filtrów:
gatunek – Familijne, sortuj – Rok produkcji.
 2. Wyszukaj inny film wg. własnych filtrów zgodnie z zainteresowaniami.
- Rozmowa z uczestnikami na temat wspierania dzieci i młodzieży w zakresie tematyki oglądanych filmów, słuchanej muzyki czy książek ze względu na ich prawidłowy rozwój psychiczny i osobowościowy
 - Wskazanie stron internetowych zawierających recenzje różnych pozycji
 - Recenzje muzyczne <https://audio.com.pl/muzyka/recenzje>
<https://muzyka.onet.pl/recenzje>
 - Recenzje książek <http://lubimyczytac.pl>,
<http://dzieci.pl>
<https://www.strefapsotnika.pl>

DYSKUSJA: Dozwolony użytek osobisty

- Wprowadzenie pojęcia: dozwolony użytek osobisty, licencji
- Podstawa prawna - Art. 23 Ustawy o prawie autorskim i prawach pokrewnych o dozwolonym użytku osobistym
- Zasady pobierania i korzystania ze zbiorów w Internecie
- Serwisy: [Unsplash.com](https://unsplash.com) oraz [Pexels.com](https://pexels.com), które oferują zdjęcia na licencji [CC0](https://creativecommons.org/licenses/by/4.0/).
Jedynym warunkiem serwisu Pexels jest, by zdjęcia nie były wykorzystywane "w złym świetle"

DYSKUSJA: Wprowadzenie pojęcia: plagiat

- Konsekwencje łamania praw:
- Autor skradzionego utworu ma prawo domagać się:
 - opublikowania przeprosin,
 - wycofania plagiatu z obrotu,
 - rekompensaty finansowej.



Uwaga!!! Za udowodniony plagiat może ponadto grozić kara grzywny, a nawet ograniczenia wolności do lat 3. Więcej na stronie:

<https://poradnikprzedsiębiorcy.pl/-czym-jest-plagiat-i-jakie-sa-jego-konsekwencje>

- serwis do sprawdzania czy dzieło jest już plagiatem

<https://poradnikprzedsiębiorcy.pl/-czym-jest-plagiat-i-jakie-sa-jego-konsekwencje>

ĆWICZENIE: Sprawdzanie dzieła pod kątem plagiatu Zaloguj się do systemu.

<https://poradnikprzedsiębiorcy.pl/-czym-jest-plagiat-i-jakie-sa-jego-konsekwencje>

- Wgraj plik, który chcesz sprawdzić.
- Wygeneruj raport.
- Dokonaj oceny.

7. Tworzenie własnego BLOGA



CELE I KOMPETENCJE CYFROWE

- Poznanie zasad praw autorskich i konsekwencji w przypadku braku przestrzegania.
- Nabycie umiejętności zakładania i prowadzenia strony internetowej – bloga.
- Nabycie umiejętności konfiguracji ustawień bloga.
- Poznanie zasad prowadzenia bloga.
- Tworzenie własnych postów i ich modyfikacji.
- Poznanie narzędzi Bloggera.
- Poznanie powiązań między kontami Google i Blogger.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Każde konto Google automatycznie otrzymuje „w pakiecie” platformę **BLOGGERRA**. Dzięki temu nie trzeba zapamiętywać dodatkowych loginów i haseł oraz tworzyć kolejnych kont. Dodatkową wygodą, jest to że możemy prowadzić kilka BLOGÓW w ramach jednego konta Google.

Darmowy blog można zakładamy na platformie **Blogger**, która należy do Google o adresie **blogger.com** czy też inaczej **blogspot.com**. Ten serwis blogowy znany jest na całym świecie. Ma mnóstwo użytkowników i ogromną społeczność. Najważniejszą jego zaletą tej usługi jest darmowa wersja i prostota obsługi. Poza tym jest brak reklam.



UWAGA!!! Podczas zakładania nowego konta bloga, należy zwrócić uwagę aby adres nie zawierał polskich liter oraz znaków specjalnych (spacji, przecinków, gwiazdek ... itd). Może zawierać litery, cyfry i myślniki. Jeśli wpiszeć coś nie tak, to dostaniecie informację o błędzie wraz z czerwonym wykrzyknikiem

Ten adres bloga jest nieprawidłowy lub nie jest obsługiwany.

Wpisywany adres może być już zajęty, czyli istnieje już taki blog. Dostaniecie wtedy informację wraz z żółtym znakiem wykrzyknika:

Niestety, ten adres bloga nie jest dostępny.

Gdy podany adres będzie prawidłowy i nie jest zajęty:

Ten adres bloga jest dostępny.

Osoby prowadzące blogi zrzeszają się w społeczności na różnych forach internetowych w celu wymiany doświadczeń, samodoskonalenia i pogłębiania swoich umiejętności i wiedzy.

- <https://forum.blogowicz.info/>
- <http://niepoprawni.pl/blog/2110/forum-dla-blogerow>
- <http://progrupa.webd.pl/zamkniete-forum-dla-blogerow-co-zyskujesz/>
- Polskie serwisy - Blox.pl lub Blog.pl
- Serwis koncernu Google Blogger.pl

Jak zabezpieczyć własne treści w regulaminie bloga przed dowolnym wykorzystaniem.

DYDSKUSJA: Zasady zabezpieczania własnych treści w regulaminie bloga/strony.

- Prawo do własności intelektualnej
- Zasady korzystania i podstawa prawna

„Zarówno układy treści zawarte na Portalu, jak i poszczególne jego części, takie jak materiały pisemne, zdjęcia, grafika i inne, korzystają na ogólnych zasadach z ochrony udzielanej przez przepisy ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity – Dz. U. z 2006 r. nr 90, poz. 631 ze zm.). Każdy z Użytkowników zobowiązany jest do poszanowania praw autorskich pod rygorem odpowiedzialności cywilnoprawnej oraz karnej wynikającej z przepisów tej ustawy”.
- Przykładowy tekst klauzuli zaczerpnięty ze strony <https://jakchronicinformacje.pl/regulamin-bloga-oraz-polityka-prywatnosci/>

1. „Można korzystać z tekstów zawartych na Blogu w zakresie własnego dozwolonego użytku osobistego. Wykorzystanie tekstów zawartych na Blogu w innym celu nie wymaga zgody **IMIĘ I NAZWISKO** pod warunkiem umieszczenia na każdej kopii imienia i nazwiska autora danego materiału i informacji w następującym brzmieniu „Tekst pochodzi z bloga jakchronicinformacje.pl”. Teksty udostępniane są na licencji CC BY-NC-ND 3.0 PL (zapoznaj się z nią)
2. Powyższa zgoda nie dotyczy zdjęć oraz innych materiałów nie będących tekstami.
3. Zdjęcia wykorzystywane do postów pochodzą z banków zdjęć płatnych lub darmowych udostępnianych na licencji CC lub pochodzą z domeny publicznej.”

W dzisiejszych czasach korzystanie z zasobów sieci niesie również wiele zagrożeń. Celem ataku mogą stać się wszystkie informacje, które udostępniamy, np. na swoim blogu. Użytkownicy profili sieciowych muszą pamiętać, że ich bezpieczeństwo w znacznym stopniu zależy od ustawień prywatności na portalu i ustawień prywatności jego znajomych.

Podstawowe zagrożenia:

- Zbieranie danych o użytkownikach, (cyfrowe dossier, czyli tzw. CV). Są to informacje typu: miejsca zamieszkania, wykształcenie, wykonywana praca, kontakty, statusy, zdjęcia, polubione strony lub linki. Wszystkie te dane mogą zostać użyte przeciw publikującym je osobom.

PRZYKŁADY: odzyskiwanie hasła do profilu użytkownika.

- Zbieranie danych historycznych - mogą zostać w niekorzystny sposób wykorzystane.
- Trudności z całkowitym usuwaniem kont na portalach społecznościowych. Nawet w przypadku usunięcia profilu, kopia tych danych pozostaje, ponieważ przechowywana jest na serwerze zewnętrznym.
- **Rozpoznawanie twarzy** – (często wykorzystywane na Facebooku i innych portalach poprzez oznaczanie na zdjęciach znajomych). Zdjęcia mogą posłużyć również do oznaczania lokacji geograficznych, przedmiotów i innych cech.
- **Kradzież tożsamości** - przejmowanie profili i szarganie reputacji
- **Phishing** - taktyki socjotechniczne do wydobywania od użytkowników ich sekretnej informacji.
- **Spam**, czyli niechciane wiadomości i reklamy.

- **Wirusy oraz robaki** - to zagrożenia typu XSS (ang. cross site scripting).
- **Agregatory** SNS (ang. social networking service), powielające portale społecznościowe - są sposobem na pozyskiwanie lub wyciąganie informacji.
- Szczególnie dokuczliwym zagrożeniem jest wykorzystywana niekiedy możliwość zwyczajnego **znęcania się**, poprzez wysyłanie obraźliwych wiadomości, szantaż i nękanie użytkowników i osób.



PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

DYSKUSJA: Rozpowszechnianie w sieci informacji o swoim blogu lub stronie internetowej

- Wprowadzenie pojęcia „blogosfera”
- Omówienie rodzajów blogów,
- Przykłady blogów specjalistycznych i firmowych. Blogi tematyczne
- Na czym polega pozycjonowanie blogów
- Wskazówki do pozycjonowania bloga – internetowe instrumenty promocji (reklamy)
- Korzystanie z Goole Analytics - analizowanie ruchu na prowadzonej witrynie internetowej
- Strona do nauki pozycjonowania <http://naukapozycjonowania.pl/> darmowe kursy
- Przykłady wyszukiwarek blogowych:
 - na świecie: Technorati.com, 9rules.com, Wikio.com, BlogSearch.Google.com
 - w Polsce: BlogFrog.pl, 10przykazan.com, Blogbox.com.pl, Blogowisko.org
- Zalety bloga – wspólne omówienie zalet.

DYSKUSJA: Ochrona wizerunku oraz prawa autorskie na portalach społecznościowych.

- Dyskusja na temat zagrożeń wynikających z korzystania z portali społecznościowych – wymiana doświadczeń i spostrzeżeń

DYSKUSJA: Typy zagrożeń dla informacji na portalach społecznościowych.

- Omówienie typów zagrożeń dla informacji na portalach, typu: zbieranie danych o użytkownikach, rozpoznawanie twarzy, pozyskiwanie danych, spam, wirusy, robaki, agregatory SNS, phishing, XSS, przejmowanie profili, utrata reputacji i inne
- Rozumienie zjawisk i zagadnień dotyczących zjawiska hate, fake news, ochrony wizerunku

- Uświadomienie rodzicom, iż największą luką w zabezpieczeniach portali są sami użytkownicy

DYSKUSJA: Ustawienia prywatności na blogu.

- Zabezpieczenia na blogach – bezpieczeństwo w treści oraz danych osobowych

ĆWICZENIE: Ustawienie prywatności na blogu

- Rola użytkownika w zapewnieniu bezpieczeństwa



Uwaga! W zakresie bezpieczeństwa w sieci największą rolę do odegrania ma sam użytkownik. To od niego zależy jakie i ile informacji udostępni. Dlatego zaleca się rozważę, aby nie zostać celem ataku lub nienawiści.

DYSKUSJA: Bezpieczne korzystanie z portali społecznościowych i zarządzanie tożsamością oraz własnym wizerunkiem w sieci.

- Omówienie zasad zachowania bezpieczeństwa w sieci,
- Rozmowa na temat zagrożeń wynikających z korzystania z portali społecznościowych.
- Typy zagrożeń dla informacji: zbieranie danych o użytkownikach, zbieranie danych historycznych, rozpoznawanie twarzy - pozyskiwanie danych i informacji.

8. Tworzenie własnej strony internetowej



CELE I KOMPETENCJE CYFROWE

- Poznanie przydatnych aplikacji do tworzenia strony internetowej.
- Wykorzystanie aplikacji SWAY do szeroko rozumianej promocji oraz rozpowszechniania informacji w sieci.
- Wykorzystanie darmowego kreatora WIX do projektowania strony internetowej.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Cele i zadania strony internetowej. Każda strona musi mieć swoje przeznaczenie. Najważniejszym elementem prac wstępnych jest określenie celów jaki ma służyć dane dzieło i do jakiej grupy adresatów jest kierowana. W dziennikarstwie jest to szczególnie ważny element projektowania strony.

Do niedawna, aby stworzyć stronę internetową, trzeba było znać języki programowania. Obecnie na rynku dostępna jest wiele kreatorów stron internetowych. My na potrzeby szkolenia zaproponowaliśmy – [Wix](#).

„Wix to platforma, który umożliwia tworzenie zindywidualizowanych, nowoczesnych stron www. Kreator Wixa jest bardzo intuicyjnym narzędziem. Edycja szablonu wymaga jedynie podstawowych zdolności obsługi komputera. Dodawanie nowych elementów (np. sekcji, obszarów tekstowych, przycisków, obrazków) działa na zasadzie „drag and drop” (czyli przeciągnij i upuść). Równie proste jest wyposażanie stron w nowe funkcjonalności: zarządzanie nimi odbywa się przy pomocy czytelnego, bocznego menu.

Wix oferuje także tysiące gotowych szablonów oraz bibliotekę z bezpłatnymi zdjęciami. Za jego pomocą internauci tworzą strony internetowe, blogi czy sklepy internetowe”²².

Wix oferuje wiele możliwości projektowania stron. Użytkownicy z łatwością mogą dodawać różne elementy, np. pola tekstowe, obrazy, przyciski, galerie, filmy wideo, moduły mediów społecznościowych, formularze kontaktowe czy menu. Strony można rozbudowywać o nowe sekcje, a także podstrony. Wix oferuje ponad 500 bezpłatnych szablonów, gotowych do edycji. Natomiast ci, którzy nie posiadają własnych zdjęć, mają do dyspozycji bibliotekę darmowych obrazów Wixa. Poza tym platforma Wix posiada wiele bezpłatnych funkcjonalności, np. moduły mediów społecznościowych, galerie, komentarze, forum, formularze, rezerwacje czy płatności. Ponadto takie opcje jak moduły pogody, liczniki, kalendarze, zegary, mapy, czy narzędzia analityczne.

Wix to doskonała propozycja dla osób, które chcą zaistnieć w Internecie, ale z różnych względów nie mogą zainwestować w stronę internetową. Do tego grona można zaliczyć np. gminne samorządowe ośrodki kultury, które chcą zorganizować warsztaty z dziennikarstwa internetowego.



TUTORIALE, SAMOUCZKI, FILMY INSTRUKTAŻOWE

- <https://www.youtube.com/watch?v=5l2XwYQnhfE> Jak zrobić stronę na www.wix.com
- https://www.youtube.com/watch?v=8Gy_zpelyN0 Kreator Stron HTML | Pierwsze kroki z Edytorem Wix

²² <https://www.offon.pl/baza-wiedzy/strony-internetowe-wix/>

- <https://www.youtube.com/watch?v=sIBKDTazJIY> Wix jak stworzyć stronę www



UWAGA!!! Na szczególną uwagę zasługuje fakt, że Wix to bezpieczeństwo strony jeśli chodzi o ataki hakerskie. Poza tym użytkownika nie interesują aktualizacje, tak jak w przypadku WordPress, czy kompatybilności wtyczek.

Posiadanie własnej strony internetowej jest początkiem działań promocyjnych swoich działań, zainteresowań, pasji, czy firmy. Przed tworzeniem strony internetowej, bloga warto skrupulatnie zaprojektować jej układ i strukturę oraz wybrać odpowiednią domenę. Dobrze w adresie strony umieścić słowa kluczowe związane z tematyką strony, co ułatwia wyszukiwanie przez innych użytkowników sieci naszego bloga w wyszukiwarkach.

Najlepiej wybierać domeny krótkie, takie które łatwo zapamiętać. Użytkownicy na ogół intuicyjne wpisują krótkie hasła tematyczne w okno przeglądarki. Aby zaistnieć w sieci należy uruchomić własny serwer lub skorzystać z usługi firmy, która świadczy usługi hostingowe. Jedną z podstawowych zasad posiadania strony internetowej, jest odpowiedni dobór słów kluczowych, aby zwiększyć efektywność wyszukiwania, co ma ogromny wpływ na promocję produktu. Ważna jest przy tym:

- aktualizacja informacji,
- grafika strony
- łatwość w odnajdowaniu z innych informacji.

Prowadzenie bloga to nic innego jak prowadzenie strony internetowej. Blogowanie, nazywane webloggingiem stało się dzisiaj modne i jest stałym elementem nowych mediów.

Sway - Tworzenie wyróżniających się wizualnie biuletynów, prezentacji i dokumentacji w kilka minut

Aplikacja Sway to narzędzie wchodzące w skład pakietu Office. Służy do tworzenia prezentacji multimedialnych zwanych wizytówkami, biuletynów, raportów i dokumentacji. Interfejs przygotowano w taki sposób by dało się go obsługiwać także z poziomu przeglądarek dla smartfonów i tabletów.

Aby skorzystać z aplikacji niezbędne jest posiadanie konta w usługach Microsoftu poprzez dowolnego e-maila. Po zalogowaniu się zyskujemy dostęp do wcześniej

stworzonych prezentacji, a nowo powstałe są zapisywane w chmurze. Projekty rozpoczęte na innym urządzeniu możemy z poziomu wersji mobilnej edytować oraz prezentować.

Ilość dostępnych narzędzi jest spora, i w dużej mierze opiera się na dodawaniu treści z różnych źródeł. Podczas tworzenia cały czas towarzyszy nam podgląd na efekt naszej pracy. Dodatkowo z poziomu programu możemy pobrać samouczki, które przybliżą nam działanie aplikacji oraz poszczególnych opcji.

Obsługa, tworzenie i edytowanie prezentacji, wszystkie te operacje możemy wykonać w wygodny sposób zarówno na ekranie tabletu jak i za pomocą myszki oraz klawiatury. To właśnie prosta obsługa oraz łatwa nawigacja i udostępnianie stanowią największą zaletę Sway'a. Program dostępny jest za darmo w sklepie z aplikacjami dla systemu Windows 10.



PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

ZADANIE: *Dokonaj analizy popularnych stron internetowych. Jakie elementy znajdujące się na nich planujesz wykorzystać na swojej stronie WWW?*

ZADANIE: *Spróbuj zapoznać się z kodem źródłowym dowolnej strony. W tym celu otwórz ją w przeglądarce i wybierz z menu kontekstowego (widocznego po naciśnięciu prawego klawisza myszy) opcję **Pokaż źródło strony** (Firefox) lub **Pokaż źródło** (Internet Explorer). Zapewne zdziwi cię długość i stopień skomplikowania kodu.*

ĆWICZENIE: *Uruchom kreator Wix i zapoznaj się z narzędziami. Wybierz odpowiedni szablon i stwórz prostą wizytówkę warsztatów dziennikarskich.*

ĆWICZENIE: *Za pomocą graficznego edytora stron WWW wykonaj stronę internetową na temat zlecony przez prowadzącego zajęcia lub promujący jedną z dziedzin życia lokalnego. Po wykonaniu strony zapoznaj się z jej kodem źródłowym.*

ĆWICZENIE: *Stwórz wizytówkę swojej okolicy w aplikacji SWAY.*

9. Ochrona komputera i innych urządzeń przed złośliwym oprogramowaniem.



CELE I KOMPETENCJE CYFROWE

- Poznanie różnych stron z darmowymi programami.
- Poznanie sposobów jak wyszukiwać programy na stronach www.
- Opanowanie umiejętności instalowania i konfigurowania oprogramowania.
- Nabycie wiedzy jak prawidłowo zabezpieczyć komputer przed złośliwym oprogramowaniem.
- Nabycie wiedzy na temat szkodliwego oprogramowania.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Wirus komputerowy – program komputerowy posiadający zdolność powielania się, tak jak prawdziwy wirus, stąd jego nazwa. Wirus do swojego działania potrzebuje i wykorzystuje system operacyjny, aplikacje oraz tożsamość użytkownika komputera. Wirusa komputerowego zalicza się do szkodliwego oprogramowania (malware)²³.

Bardzo często wirusy komputerowe rozprzestrzeniają się w załącznikach do wiadomości e-mail lub przy użyciu wiadomości błyskawicznych. Z tego względu nie należy otwierać załączników wysyłanych przez nieznanymi, których otrzymanie nie było oczekiwane. Wirusy mogą być zamaskowane jako śmieszne obrazy, pocztówki i pliki audio/wideo. Mogą też rozprzestrzeniać się w plikach pobieranych z Internetu. Wirusy mogą być ukryte w pirackim oprogramowaniu i innych plikach dostępnych w sieci²⁴.

Instalacja programów antywirusowych

Darmowe programy antywirusowe można pobrać ze stron internetowych. W tym celu w wyszukiwarkę GOOGLE wpisujemy nazwę szukanego programu, np. **avast free** i klikamy klawisz **ENTER** lub wpisujemy kryterium wyszukiwania typu **darmowe programy antywirusowe**. Po czym wybieramy odpowiedni link z wyników wyszukiwania. Najbezpieczniej jednak pobierać programy bezpośrednio ze stron producenta.

Istnieją również strony internetowe, z których można pobrać darmowe oprogramowanie, należą do nich m.in. <https://www.dobreprogramy.pl/>. Wybieramy przycisk **Pobierz bezpłatnie** i postępujemy zgodnie z instrukcją, zgodnie z kreatorem instalacji.

²³ [Wirus komputerowy – Wikipedia, wolna encyklopedia - https://pl.wikipedia.org/wiki/Wirus_komputerowy](https://pl.wikipedia.org/wiki/Wirus_komputerowy)

²⁴ <https://support.microsoft.com/pl-pl>

Przykładowe programy antywirusowe na Androida

Aby być aktywnym użytkownikiem portali społecznościowych, trzeba korzystać z bezpiecznych urządzeń mobilnych. Dlatego należy zadbać, aby nasze urządzenia zawierały programy antywirusowe. Oto kilka darmowych propozycji. Każdy z tych programów można pobrać ze strony **GOOGLE PLAY** na urządzeniu na którym chcemy zainstalować oprogramowanie, po czym należy wybrać opcje **ZAINSTALUJ**.

Sophos Mobile Security - Bez zarzutu radzi sobie z zagrożeniami, nie obciąża zbytnio systemu, Dostępne funkcje to: ochrona przed złośliwym oprogramowaniem, filtrowanie sieci, blokowanie spamu i dostępu do aplikacji, tworzenie i przechowywanie haseł, możliwość zdalnego blokowania, czyszczenie oraz lokalizowania sprzętu.

AVAST Mobile Antivirus & Security - Avast w wersji w języku polskim, łatwy w obsłudze.

Security Master - Pakiet zabezpieczający smartfona od Cheetah Mobile, wyposażony w skaner z antywirusem. którego skuteczność została potwierdzona w niezależnych testach. Aplikacja pozwala też usuwać śmieci. Funkcje: darmowy VPN (czyli możliwość ukrycia swojej lokalizacji podczas przeglądania Internetu), blokada aplikacji, zdjęcie intruza.

Bitdefender Antivirus Free - Bitdefender - sprawdzona, bardzo skuteczna technologia skanowania w chmurze.

Avira Antivirus Security - Avira – intuicyjna obsługa, wbudowany skaner antywirusowy, klasyfikuje zainstalowane programy, zdalna blokada dostępu i śledzenie lokalizacji.



PRZYKŁADOWE ZADANIA I ĆWICZENIA PRAKTYCZNE

ĆWICZENIE: Instalacja programów

Pobierz program Avast Free Antivirus. Zainstaluj go na dysku pamiętając o opcji **Skanowanie podczas uruchamiania systemu**. Zeskanuj komputer. Jeżeli zainstalowanie jest niemożliwe obejrzyj filmy:



TUTORIALE, SAMOUCZKI, FILMY INSTRUKTAŻOWE,

- <https://www.youtube.com/watch?v=7tqITP26gvE> Instalacja Avast Free Antivirus
- <https://www.youtube.com/watch?v=LbOhUpTG0Lg> Windows 10: Instalacja Avast Free Antivirus.
- <https://www.youtube.com/watch?v=cMflh3LOR0U> Instalacja i konfiguracja darmowego antywirusa Avast



UWAGA!!! Podczas instalacji domyślnie instalowana jest również specjalna przeglądarka, możemy jednak usunąć zaznaczenie przy zgodzie na jej instalację.

7. METODYKA SZKOLEŃ OSÓB DOROSŁYCH Z ZAKRESU KOMPETENCJI CYFROWYCH:

Głównym założeniem programu szkoleniowego jest udzielenie wsparcia i wyprofilowanie zajęć do poziomu zaawansowania uczestników szkolenia w kształtowaniu kompetencji cyfrowych na podstawie indywidualnych konsultacji i diagnozy wstępnej. Szkolenie w zakresie zdobywania kompetencji cyfrowych w ramach projektu będzie bazować na segmentacji tematycznej co pozwoli zapewnić manewrowanie treściami, metodami, formami i ćwiczeniami praktycznymi adekwatnie do różnego poziomu wiedzy uczestników w zakresie konkretnego zagadnienia. Zadaniem trenera jest dostosowanie ćwiczeń, zadań praktycznych oraz obserwacja reakcji uczestników w trakcie szkolenia, a także dostosowanie tempa do możliwości grupy. Zarówno konstrukcja, jak i skuteczność prowadzonych zajęć zależą będzie od doświadczenia i intuicji trenera, który musi nie tylko regulować poziom merytoryczny zajęć, ale również wykazywać się empatią.

Podstawą metodyki szkolenia jest dywersyfikacja kanałów komunikacyjnych, ponieważ skuteczność warsztatów nie tylko zależy od założeń merytorycznych, ale również od doboru optymalnej formy i metod przekazywania wiedzy. W związku z tym, że proces kształtowania kompetencji cyfrowych obejmuje różne style uczenia się, zajęcia będą wspomagane różnorodnymi metodami i formami, takimi jak: prezentacje multimedialne, tutorial, ćwiczenia opierające się na czytaniu, pisaniu, żywej rozmowie oraz wykonywaniu konkretnych czynności. Warto podkreślić, że ze względu na charakter szkolenia jedna forma przekazywania wiedzy (tj. ćwiczenia praktyczne z wykorzystaniem nowoczesnych technologii) siłą rzeczy staje się dominująca, jednak kanały komunikacji należy

dywersyfikować, aby uniknąć monotonii i nie zmęczyć uczestników. Zatem częste reakcje i natychmiastowa weryfikacja nowo zdobytych informacji pozwoli na szybkie i skuteczne przyswajanie wiedzy i umiejętności przez uczestników. Ze względu na fizjologiczne uwarunkowania utrzymania koncentracji na przerabianym zagadnieniu zajęcia będą prowadzone poprzez dozowanie praktycznej wiedzy w kilkunastominutowych interwałach teorii połączonej z dyskusją opartą na doświadczeniach własnych uczestników, a także interesującymi ćwiczeniami praktycznymi. Różnorodność taka ma sprzyjać efektywnej aktywizacji słuchaczy podczas zajęć. Co półtorej, dwie godziny wskazane są przerwy, aby uczestnicy mogli się odprężyć oraz uzupełnić deficyty kalorii spowodowane wysiłkiem umysłowym.

Na zajęciach będzie obowiązywała zasada KISS (Keep It Simple and Short), czyli krótko, treściwie i na temat. Wobec tego trener powinien posługiwać się słownictwem zrozumiałym dla wszystkich, aby uniknąć niedomówień oraz zapewnić słuchaczom komfort podczas warsztatów. Styl komunikacji trenerskiej powinny cechować spójność, jednoznaczność oraz forma oszczędna w dygresje. Poza tym trener powinien być otwarty na pytania uczestników, stwarzać odpowiednie warunki sprzyjające swobodnej wymianie doświadczeń, dopuszczać możliwość zdobywania kompetencji cyfrowych poprzez samodzielne eksperymentowanie (poszukiwanie rozwiązań) głównie z użyciem nowoczesnych technologii. Na rozwiązanie danego problemu powinien zaproponować do wyboru różne metody i sposoby wykorzystania narzędzi informatycznych i komunikacyjnych, po to by uczestnicy mogli wybrać odpowiednią dla siebie metodę. Wszystkie zadania powinny być realizowane w oparciu o instruktaż słowny ze strony trenera, projekcję zadań z wykorzystaniem projektora multimedialnego oraz pokaz slajdów i tutoriali. Dorośli nowe umiejętności nabywają przez pryzmat wiedzy już posiadanej. Trener w trakcie szkolenia pełni niejako funkcję moderatora koordynującego przebieg całego procesu, ale nie narzuca swojego zdania i nie podsuwa gotowych odpowiedzi. Uczestnicy szkolenia niejako konstruują wiedzę drogą poszukiwań, osiągania i przekształcania napływających informacji - głównie dzięki współdziałaniu i osobistemu doświadczeniu. W takim procesie kształcenia podkreślany jest aspekt samodzielności działania i świadomego samodoskonalenia. Natomiast podział materiału szkoleniowego na konkretne zadania zapewni sukcesywne opanowanie wydzielonych w małych partiach zagadnień i pozwoli na systematyczną weryfikację trudności, które należy powtórzyć a nawet przeanalizować z uczestnikami raz

jeszcze. Wszystkie ćwiczenia i rozwiązywane problemy należy podsumować i zewaluować wspólnie z kursantami, co zapewni informację zwrotną trenerowi na temat poprawności doboru metod i form pracy z daną grupą szkoleniową. Po takiej analizie trener powinien zwrócić uwagę na mocne i słabe strony każdej ze stosowanych przez siebie metod, nawiązując przy tym do procesów grupowych i dynamiki grupy szkoleniowej.

8. ZASADY RÓWNOŚCI SZANS I NIEDYSKRIMINACJI, W TYM DOSTĘPNOŚCI DLA OSÓB Z NIEPEŁNOSPRAWNOŚCIAMI ORAZ RÓWNOŚCI SZANS KOBIECI I MĘŻCZYŹN W KONTEKŚCIE REALIZOWANYCH SZKOLEŃ:

Program szkolenia jest zgodny z zasadami równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz zasadami równości szans kobiet i mężczyzn. **Założenia programowe przewidują udział osób z niepełnosprawnościami na równi z innymi uczestnikami szkolenia. Metody i formy pracy są tak dostosowane, aby wszyscy uczestnicy mieli zapewnione odpowiednie wsparcie w zakresie zdobywania kompetencji cyfrowych.** Pomieszczenia w których będą odbywały się zajęcia warsztatowe będą w pełni przystosowane dla osób niepełnosprawnych. Budynek wyposażony jest w podjazdy, windy dla osób niepełnosprawnych, szatnię oraz infrastrukturę sanitarną przystosowaną do korzystania przez osoby z niepełnosprawnością ruchową. Wszystkie szkolenia adresowane są w takim samym stopniu do kobiet, jak i do mężczyzn na zasadzie równości szans. Grupy szkoleniowe będą mieszane, co będzie sprzyjało budowaniu przyjaznej atmosfery oraz poznaniu sytuacji obu płci na rynku zawodowym oraz pozycji w społeczeństwie.

Zasada równości szans kobiet i mężczyzn:

- dotyczy podejmowania działań (przeszkolenia) na rzecz zdobywania kompetencji cyfrowych pozwalających na poprawę jakości ich życia w społeczeństwie informacyjnym,
- kobietom i mężczyznom przypisuje się taką samą wartość społeczną, równe prawa i obowiązki oraz gdy mają oni równy dostęp do zasobów (środki finansowe, szanse rozwoju, dostęp do informacji), z których mogą korzystać;

- udział w szkoleniu ma pomóc wyeliminować bariery i ograniczenia utrudniające równy dostęp do zasobów i dóbr społecznych;
- unikanie sztucznych podziałów na role i obszary wyłącznie „kobiece” lub wyłącznie „męskie”, np. prowadzenie firmy, korzystanie z komunikatorów internetowych w celu przeprowadzania rozmów służbowych, rozwijanie zainteresowań dzieci itp.
- zaprezentowanie sposobów pozyskiwania informacji, które mogą przyczynić się do rozwiązania konkretnych problemów w zakresie równości szans kobiet i mężczyzn.

9. PROCEDURY OSIĄGANIA SZCZEGÓŁOWYCH CELÓW EDUKACYJNYCH:

Ujęte w programie treści zostały tak ułożone, aby każdy uczestnik szkolenia mógł stosować różne metody korzystania z usług Katalogu cyfrowego usług polskiej administracji i rozwijać umiejętności myślenia i uczenia się, a w efekcie nabyte umiejętności i wiadomości wykorzystać podczas realizacji różnych zadań z wykorzystaniem technologii cyfrowych, a przede wszystkim podczas prowadzenia warsztatów dziennikarskich z dziećmi i młodzieżą. Strategie prowadzenia zajęć szkoleniowych:

- **strategia dydaktyczna** – opiera się na wykładzie i wyjaśnieniach trenera bazujących na pytaniach dodatkowo zadawanych przez uczestników szkolenia; w tej strategii nadrzędną rolą jest sprawdzenie przez prowadzącego rozumienia jego słów;
- **strategia pytań opierających się na faktach** – jej głównym celem jest ustalenie faktów; interakcja między prowadzącym a kursantami bazuje głównie na wyrażaniu przez trenera aprobaty, bądź też uwag na temat wykonania zadania;
- **strategia pytań skłaniających do myślenia, zwana też dialogiczną** – jest oparta na dialogu, celem tej strategii jest zachęcenie beneficjentów do myślenia i rozbudzenie w nich potrzeby dyskusji; trener uczestniczy w rozmowie na równi z uczestnikami szkolenia, komentuje lub uzupełnia wypowiedzi, może także w trakcie dyskusji zmienić stanowisko wobec omawianego problemu; ta strategia jest oparta na formułowaniu otwartych pytań ożywiających (czyli poszukujących, skłaniających do myślenia), dzięki którym zwiększa się interakcja między kursantami;

10. ZALECANE WARUNKI I SPOSÓB REALIZACJI

Na etapie szkolenia kompetencji cyfrowych uczestnicy poznają nieformalne znaczenie wybranych pojęć związanych z wyszukiwaniem informacji w sieci oraz biegłym wykorzystywaniem zasobów Internetu do korzystania w pełni z usług administracji publicznej, w tym wypełniania obowiązków dziennikarza internetowego. Zajęcia mają pobudzić ich do kreatywnego działania i poszukiwania rozwiązań stawianych im problemów. Tymi pojęciami są m.in.: *prawo autorskie, chmura, usługi on-line, blog, czat, e-mail, wideorozmowa, a także pojęcia wynikające z bezpieczeństwa w Internecie typu, fake news, hate i wiele innych*. Kolejnym etapem poszerzania kompetencji cyfrowych jest posługiwanie się komputerem w korelacji z pozostałymi obszarami życia codziennego i kompetencjami kluczowymi. Każde stanowisko powinno być tak skonfigurowane, aby spełniało następujące kryteria:

1. zainstalowana przynajmniej jedna przeglądarka internetowa,
2. zainstalowana kamera internetowa,
3. głośniki i mikrofon jeżeli zestaw nie ma wbudowanych,
4. dostęp do drukarki, jako zewnętrznego urządzenia peryferyjnego,
5. ekran lub tablica interaktywna, rzutnik multimedialny,
6. dostęp do Internetu.

11. EWALUACJA PROGRAMU

Ewaluacja programu oraz prowadzonych zajęć w ramach szkolenia kompetencji cyfrowych dla pracowników gminnych samorządowych instytucji kultury, którzy pragną zdobyć lub poszerzyć swoje kompetencje cyfrowe z zakresie pracy w sieci zostanie przeprowadzona w oparciu o wyniki ankiety ewaluacyjnej oraz na podstawie opinii samych uczestników, a także w oparciu o bieżące obserwacje zajęć.

AUTORSKI PROGRAM
SZKOLENIA KOMPETENCJI CYFROWYCH
DLA PRACOWNIKÓW GMINNYCH SAMORZĄDOWYCH INSTYTUCJI KULTURY

**SCENARIUSZ NR 2: BEZPIECZNE ZACHOWANIE W SIECI - W ŻYCIU PRYWATNYM, SPOŁECZNYM
ORAZ W EDUKACJI**
**„ZNAJĄC NIEBEZPIECZEŃSTWA I SPOSOBY ICH UNIKNIĘCIA MOŻNA BEZPIECZNIE KORZYSTAĆ
Z INTERNETU”.**

*Program powstał w na potrzeby projektu realizowanego w ramach
Działania 3.2 Innowacyjne rozwiązania na rzecz aktywizacji cyfrowej Program Operacyjny
Polska Cyfrowa 2014-2020*

Autorzy programu:

Elżbieta Fim – Szkoła Podstawowa im. Stefana Wyszyńskiego w Nasutowie

Barbara Gnysińska – Szkoła Podstawowa im. Zofii Trzcіńskiej – Kamińskiej w Leścach

WPROWADZENIE

Dynamiczny rozwój technologii komputerowej oraz ciągle wzrastające znaczenie Internetu w życiu codziennym spowodowały konieczność systematycznego rozwoju kompetencji cyfrowych niemal wszystkich osób. Rozwój kompetencji cyfrowych musi następować zarówno w zakresie korzystania z technologii cyfrowych, jaki i posługiwania się nimi we wszystkich sferach życia zawodowego i prywatnego.

Nabywanie tych umiejętności pozwala na:

- lepszą i sprawniejszą komunikację między społeczeństwem,
- korzystanie z e-usług administracji publicznej (załatwianie on-line spraw urzędowych - o dogodnej dla siebie porze, bez konieczności wychodzenia i odwiedzania urzędów),
- umiejętne publikowanie i zamieszczanie informacji na różnych portalach społecznościowych, stronach internetowych, blogach i innych multimediami,
- nowe style promocji i prezentacji,
- nowe style spędzania czasu wolnego lub jego organizacji,
- korzystanie ze wsparcia zamieszczonego w zasobach Internetu.

Samorządowe instytucje kultury w dobie cyfryzacji stanęły przed bardzo trudnym zadaniem, a mianowicie stworzenie oferty kulturalno-edukacyjnej zgodnej z oczekiwaniami współczesnego odbiorcy wychowanego w świecie informacyjnym.

Obecnie ponad 500 usług można załatwić drogą elektroniczną, dlatego kompetencje cyfrowe²⁵ stały się celem samym w sobie i konieczne dla każdego obywatela w dobie postępu komunikacyjno-informacyjnego. Poza tym stosowanie nowych technologii kształtuje podstawowe kompetencje kluczowe oraz pozytywne postawy społeczne wśród użytkowników ze względu na obowiązującą netykietę oraz rozbudza świadomość na temat praw autorskich, cyberprzemocy, zjawisk fake news oraz hate.

²⁵**Kompetencje informatyczne (cyfrowe)**, to jeden z najważniejszych obszarów 8 kompetencji kluczowych w procesie uczenia się przez całe życie, które są niezbędne do pełnego uczestnictwa w życiu coraz bardziej scyfryzowanego społeczeństwa. W tym ujęciu kompetencje cyfrowe można zdefiniować jako swobodne i krytyczne korzystanie z technologii informacyjno-komunikacyjnych, aby osiągać cele związane pracą, zatrudnieniem, nauką, wypoczynkiem i uczestnictwem w życiu społecznym. Kompetencje cyfrowe należą do umiejętności przekrojowych, czyli występują i są wręcz niezbędne w nabywaniu kompetencji w pozostałych obszarach (np. umiejętnościach nauki języków, umiejętności uczenia się czy świadomości kulturowej). <http://vccsystem.eu/system-certyfikacji/kompetencje-cyfrowe/>

1. KATALOG KOMPETENCJI CYFROWYCH.

Proponowany program ma na celu sprostać oczekiwaniom współczesnego społeczeństwa i przygotować pracowników samorządowych instytucji kultury do stworzenia oferty zgodnej oraz podejmowania działań przygotowujących dzieci, młodzież i dorosłych do życia w sieci technologii cyfrowej i informacyjnej. Aby móc korzystać z dobrodziejstw cyfryzacji należy się do tego przygotować i opanować wiele kompetencji z „Katalogu cyfrowych usług polskiej administracji”, które opracowało Ministerstwo Cyfryzacji. Katalog dostępny jest na stronie www.gov.pl, który zawiera m.in. zestawienie wszystkich usług elektronicznych, z jakich Polacy mogą obecnie korzystać na najpopularniejszych portalach rządowych - <https://mc.gov.pl/aktualnosci/katalog-cyfrowych-uslug-polskiej-administracji-aktualizacja>. Tematyka programu szkolenia w zakresie zdobywania kompetencji cyfrowych w ramach projektu oparty jest na kompetencjach zamieszczonych we wcześniej wspomnianym katalogu.

Poniższa tabela prezentuje zestaw kompetencji cyfrowych w 5 kategoriach, które uwzględniają treści proponowanego programu.

Tabela nr 1. Zestaw kompetencji cyfrowych w 5 kategoriach

Kategoria	Rodzaj kompetencji
UMIEJĘTNOŚCI INFORMACYJNE	4. Przeglądanie, szukanie i filtrowanie informacji 5. Ocena informacji 6. Przechowywanie i wyszukiwanie informacji
UMIEJĘTNOŚCI KOMUNIKACYJNE	7. Komunikacja z wykorzystaniem narzędzi cyfrowych i aplikacji 8. Dzielenie się informacjami i zasobami 9. Aktywność obywatelska online 10. Współpraca z wykorzystaniem narzędzi cyfrowych

	<p>11. Netykieta</p> <p>12. Zarządzanie tożsamością cyfrową</p>
TWORZENIE TREŚCI	<p>5. Tworzenie treści</p> <p>6. Integracja i przetwarzanie treści.</p> <p>7. Przestrzeganie prawa autorskiego i licencji</p> <p>8. Programowanie</p>
BEZPIECZEŃSTWO	<p>5. Narzędzia służące ochronie</p> <p>6. Ochrona danych osobowych</p> <p>7. Ochrona zdrowia fizycznego i psychicznego przed zagrożeniami wynikającymi z korzystania z technologii informacyjno-komunikacyjnych</p> <p>8. Ochrona środowiska</p>
ROZWIĄZYWANIE PROBLEMÓW	<p>5. Rozwiązywanie problemów technicznych</p> <p>6. Rozpoznawanie potrzeb i narzędzi niezbędnych do rozwiązywania problemów</p> <p>7. Innowacyjność i twórcze wykorzystywanie technologii</p> <p>8. Rozpoznawanie braków w zakresie kompetencji cyfrowych</p>

Powodzenie realizacji zadań w zakresie korzystania z nowoczesnych technologii oraz zasobów sieci zależeć będzie od gotowości i przygotowania pracowników gminnych samorządowych instytucji kultury. Proponowany program szkolenia kompetencji cyfrowych adresowany jest do wszystkich pracowników GOK-ów, chcących swobodnie poruszać się po zasobach Internetu oraz poszukujących nowych metod i form na organizację warsztatów z wykorzystaniem stron internetowych i blogów oraz wiele innych. Poza tym ma stanowić **wsparcie dla rozwoju w zakresie kompetencji cyfrowych** i ich wykorzystywania w życiu codziennym. Program realizowany będzie w następującym zakresie:

1. Bazy Legalnych Źródeł – umiejętność rozróżniania treści źródeł legalnych od nielegalnych
2. Korzystanie z usług publicznych
3. Ochrona komputera i innych urządzeń przed złośliwym oprogramowaniem
4. Wideorozmowy

5. Zagrożenia internetowe

2. ZAŁOŻENIA PROGRAMU:

7. Rodzaj zajęć – zajęcia warsztatowe

8. Grupa docelowa:

- **I ETAP szkolenia** - pracownicy gminnych samorządowych ośrodków kultury
- **II ETAP szkolenia** – dzieci i młodzież uczestniczące w warsztatach z dziennikarstwa online

9. Liczebność grupy –max. 12 osób.

10. Liczba godzin – 30 godzin zajęć grupowych (zorganizowanie 15 spotkań w cyklu 2 - godzinnym).

11. Wsparcie – w celu lepszej i sprawniejszej komunikacji oraz merytorycznego i metodycznego wsparcia realizacja projektu będzie dodatkowo wzmocniona o wyszukane propozycje materiałów, tutoriali i filmików instruktażowych zamieszczonych w zasobach Internetu. Poza tym pierwszy etap projektu będzie obejmować działania mające na celu podniesienie kompetencji pracowników GOK w takim stopniu, aby mogli oni docelowo samodzielnie lub w asyście trenera przeprowadzić szkolenia dla dzieci i młodzieży. Po zakończeniu szkolenia, każdy pracownik GOK, który zrealizuje pełen kurs nauczania, otrzyma wsparcie co najmniej w postaci mentoringu (doradztwa) zorientowanego na odkrywanie i rozwijanie jego potencjału, a także bezpłatną aktualizację materiałów dydaktycznych.

Wydzielone krótkie partie materiału zapewniają indywidualizację pracy z beneficjentami oraz możliwość modyfikacji zadań w zakresie kolejności realizowanych treści. Natomiast różnorodność ćwiczeń pozwoli uniknąć stanu zniechęcenia.

Bezpośredni kontakt z mentorem-szkoleniowcem stworzy warunki na nabycie doświadczenia pod okiem fachowca w zakresie podstawowych kompetencji TIK, do których m.in. należą: wykorzystanie komputera lub tabletu, aplikacji lub programów oraz biegłość poruszania się w sieci.

Dobre zrozumienie tematyki szkoleń oraz systemu działania w sieci spełni założone cele i zaowocuje świadomym i celowym wykorzystaniem kompetencji

cyfrowych w zakresie podstawowych kompetencji kluczowych (m.in.: korzystanie z darmowych aplikacji GOOGLE, korzystania z portali społecznościowych jako funkcjonowanie w grupie, czy bezpiecznego korzystania z zasobów Internetu oraz korzystania z portali edukacyjnych w ramach samorealizacji i rozwoju potencjału osobistego).

12. Środowisko:

- **sala komputerowa lub sala multimedialna wyposażona przynajmniej w ekran i projektor** – 1 komputer albo tablet dla każdego uczestnika szkolenia
- **materiały dydaktyczne** - dla każdego uczestnika
- **dostęp do Internetu**, dowolna przeglądarka internetowa,

3. CEL OGÓLNY:

Rozwój kompetencji cyfrowych, w tym zwiększenie stopnia oraz poprawa umiejętności korzystania z Internetu w tym e-usług publicznych,

- edukacja w zakresie zachowania bezpieczeństwa w Sieci,
- edukacja dorosłych pracujących z dziećmi w zakresie zasad bezpieczeństwa dzieci w Internecie.
- podniesienie świadomości na temat zagrożeń występujących w cyberprzestrzeni, przeciwdziałanie tego rodzaju zagrożeniom oraz promowanie świadomego i bezpiecznego korzystania z internetu.

6.1. CEL DŁUGOOKRESOWY:

3. stworzenie trwałej struktury dostępu do wiedzy w zakresie prowadzenia i animowania aktywności cyfrowej oraz podwyższania kompetencji cyfrowych na poziomie gminnych instytucji kultury;
4. wzrost aktywności cyfrowej społeczności lokalnej, która będzie mogła liczniej i częściej uczestniczyć w oferowanych zajęciach i wydarzeniach organizowanych przez gminne samorządowe jednostki kultury.

6.2. CEL KRÓTKOOKRESOWY:

3. zwiększenie kompetencji cyfrowych pracowników gminnych samorządowych instytucji kultury
4. rozwijanie kompetencji cyfrowych dzieci i młodzieży w wieku 10 - 18 lat poprzez organizację zajęć szkoleniowych w w/w instytucjach

3.3. CELE SZCZEGÓŁOWE:

- rozwój kompetencji cyfrowych umożliwiających stworzenie popytu na Internet oraz technologie informacyjno-komunikacyjne wśród obywateli Polski,
 - nabycie umiejętności korzystania z e-usług, począwszy od nauki obsługi komputera i Internetu jak i rozwijanie umiejętności bardziej zaawansowanych,
 - stworzenie trwałych mechanizmów podnoszenia kompetencji cyfrowych na poziomie lokalnym
 - Pokazanie dzieciom, **jakie zachowania w Internecie mogą być dla nich niebezpieczne** i w jaki sposób można unikać zagrożeń, a także jak powinny reagować, kiedy się z nimi zetkną;
 - **Zapoznanie** dorosłych z **możliwościami, jakie daje Internet, oraz ze związanymi z nim zagrożeniami**, w szczególności tymi, na które narażone są dzieci;
 - Uświadomienie , że Sieć zaczyna stanowić jedną z istotnych płaszczyzn życiowych człowieka, i w związku z tym **powinniśmy zdawać sobie sprawę z zachowań dzieci w Internecie**, przede wszystkim po to, by zapewnić im bezpieczeństwo;
- a) Przedstawienie uczniom rodzajów zagrożeń, jakie niesie ze sobą korzystanie z Internetu (uzależnienie od Internetu i gier komputerowych, kontakt z osobami niebezpiecznymi, dostęp do treści sprzecznych z normami wychowania, nieumiejętność odróżniania rzeczywistości wirtualnej od świata realnego, przestępczość, nieuczciwość).
 - b) Upowszechnianie zasad bezpiecznego i właściwego zachowywania się w Internecie, głównie poprzez **promowanie internetowej etykiety**.
- **Wyrobienie postawy dystansu wobec przekazów elektronicznych i krytycyzmu wobec treści informacji.**
 - Wyrabianie umiejętności klasyfikowania i wartościowania wiadomości zdobytych w Internecie.
 - Uświadomienie uczniom faktu, że anonimowość w Sieci jest tylko pozorna.

- Uczulenie trenerów na problem bezpieczeństwa dzieci w Sieci.

4. METODOLOGIA:

Szkolenie opiera się na metodologii uczenia dorosłych. Uczenie przez doświadczenie i eksperymentowanie oznacza, że szkolenie ma charakter głównie warsztatowy. Wykład i pokaz są w niewielkim stopniu wykorzystywane jedynie jako wsparcie i mają na celu ukierunkowanie uczestnika szkolenia na samodzielne eksperymentowanie i poszukiwanie rozwiązań.

Metody pracy:

8. **Obserwacja** (pokaz)
9. **Dyskusja** (wymiana poglądów i pomysłów)
10. Metoda „**Praktycznego działania**”
11. Metoda **kierowania korzystaniem z materiałów źródłowych i narzędzi TIK**
12. Metoda **projektów** (zadań)
13. Metoda **podająca** (instrukcje do zadań)
14. Metody **aktywizując**

5. FORMY PRACY:

4. Zajęcia warsztatowe
5. Indywidualna
6. Grupowa (zespołowa)

6. ZAKRES TREŚCI NAUCZANIA:

Charakterystyka

Proponowany program szkolenia przeznaczony jest dla wszystkich osób, które zainteresowane są działalnością w sieci, również w ramach różnych portali społecznościowych. Prezentowany materiał szkoleniowy poświęcony jest przygotowaniu odpowiedzialnego i przewidującego konsekwencje swoich działań użytkownika Internetu. Założenia programowe mają stanowić wsparcie w rozwijaniu świadomości zagrożeń wynikających z cyberprzestrzeni i kompetencji językowych. Dzięki tym materiałom każdy uczestnik szkolenia pozna filozofię i sposób funkcjonowania sieci społecznościowych oraz wykorzystania ich w działalności na rzecz swojej społeczności lokalnej lub prywatnie oraz w obronie własnej tożsamości. Zrozumie jak ochronić swoją prywatność w sieci, czym są prawa autorskie, własność intelektualna, a także pozna jakie konsekwencje kradzież treści. Nabędzie umiejętności pozwalające na bezpieczne poruszanie się w świecie wirtualnym, w tym m.in jak nawiązywać i kontynuować swoje znajomości, kształtować swój wizerunek lub najbliższego środowiska, wykorzystywać i dzielić się swą twórczością.

Dzięki tym materiałom każdy użytkownik pozna wartościowe i pochodzące z legalnych źródeł treści, zrozumie jak zapewnić bezpieczeństwo sobie w sieci i swoim dzieciom. Poza tym pozna gdzie szukać darmowego wsparcia w Internecie oraz gdzie szukać pomocy w sytuacjach trudnych i stwarzających różnego rodzaju zagrożenia. Zrozumie jak zapewnić bezpieczeństwo dziecku w sieci (pozna jakie konsekwencje niesie ze sobą HATE, TROLLING, GROOMING, FAKE NEWS, kradzież treści).

Ważnym aspektem szkolenia będzie poznanie praktycznych podstaw prawa autorskiego, niezbędnego do korzystania z zasobów sieci i zdobycie umiejętności wyszukiwania legalnych źródeł tj.: film, muzyka, książki i inne. Uczestnicy szkolenia zapoznają się z zasadami działania grup dyskusyjnych. Poza tym w ramach realizacji treści programowych dostępne będą instruktaże, komentarze głosowe, pokaz slajdów, platformy e-learningowe, demo serwisów oraz portale i serwisy internetowe, takie jak:

Obywatel.gov.pl; Biznes.gov.pl, Praca.gov.pl, Emp@tia, Platforma Ministerstwa Sprawiedliwości.

ŚRODOWISKO PRACY: laptop dla każdego uczestnika (zestaw komputerowy) lub tablet z dostępem do Internetu oraz zainstalowaną przeglądarką internetową, ekran, projektor multimedialny, głośniki, kamerki internetowe w przypadku stanowisk stacjonarnych.

MATERIAŁY POMOCNICZE W RAMACH WSPARCIA: instrukcje słowne, elementy wykładu lub teorii, filmy instruktażowe (tutorial).

6.1.2. ZAKRES TREŚCI PROGRAMOWYCH ORAZ UWAGI O REALIZACJI

Informacje wstępne: Zajęcia prowadzone głównie na zasadzie zajęć praktycznych na urządzeniach cyfrowych poparte wykładem i instruktażem słownym Trenera. Podstawą równomiernej pracy wszystkich uczestników szkolenia jest prowadzenie warsztatów z wykorzystaniem pokazu/projeksi wykonywanych ćwiczeń i zadań.

Bazy Legalnych Źródeł – umiejętność rozróżniania treści źródeł legalnych od nielegalnych



CELE I KOMPETENCJE CYFROWE

- Nabycie wiedzy na temat sposobów i metod wyszukiwania informacji w sieci.
- Kształtowanie umiejętności pozyskiwania informacji w sieci.
- Nabycie umiejętności wyszukiwania stron internetowych z zawartością kulturalno - oświatową,
- Nabycie umiejętności obsługi komputera i korzystania z przeglądarki internetowej.
- Kształtowanie sprawności w przeglądaniu najpopularniejszych stron i serwisów związanych z kulturą.
- Nabycie umiejętności korzystania z narzędzi portali edukacyjnych.
- Nabycie umiejętności odbywania wycieczek wirtualnych po wirtualnym muzeum.
- Nabycie wiedzy na temat systemu PEGI oraz które gry są wartościowe pod kątem edukacyjno-kulturalnym.
- Poznanie czym są Legalne Bazy Źródeł

- Omówienie zasad ściągania plików multimedialnych (piosenki, filmy, seriale) za pośrednictwem Internetu
- Nabycie umiejętności korzystania z narzędzi GOOGLE ARTS & CULTURE.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Istnieją dwa rodzaje sytuacji, gdy wykorzystywanie cudzych zdjęć w internecie będzie odbywało się **zgodnie z prawem** (przy założeniu, że mamy do czynienia z fotografią, która jest w ogóle utworem prawa autorskiego). Oto one:

- wykorzystywanie zdjęć na zasadzie licencji Creative Commons,
- wykorzystywanie zdjęć, które znajdują się w tzw. domenie publicznej.

Licencje CC to tak zwane **licencje otwarte**, które upoważniają użytkownika danego utworu (licencjobiorcę) do legalnego korzystania z utworów w sposób nieodpłatny, także poza granicami wyznaczonymi przepisami o dozwolonym użytku. Licencje CC zezwalają na dowolne wykorzystywanie, przesyłanie, a nawet modyfikowanie zdjęć.

Cztery podstawowe warunki licencji typu Creative Commons to:

- **uznanie autorstwa** (chodzi o poszanowanie autorskich praw osobistych twórcy): CC-BY;
- **użycie niekomercyjne** (utwór nie może być wykorzystywany dla celów handlowych, w celu osiągnięcia zysków): CC-BY-NC;
- **bez utworów zależnych** (utworu nie wolno zmieniać, przekształcać ani tworzyć na jego podstawie nowych dzieł, utwór może być eksploatowany wyłącznie w oryginalnej, niezmienionej postaci): CC-BY-ND;
- **na tych samych warunkach** (utwory zależne powstałe na podstawie danego utworu mogą być rozpowszechniane tylko na takiej samej licencji co utwór pierwotny): CC-BY-SA.

Niezależnie od typu licencji, w przypadku wykorzystywania zdjęć na zasadzie licencji CC należy podać informacje o autorze utworu (zdjęcia), podać typ licencji oraz (dla pełnego bezpieczeństwa) podać link do treści licencji.

Domena publiczna

Domena publiczna w kontekście prawa własności intelektualnej oznacza zbiór dzieł, które nie są chronione prawem autorskim. Najczęstszym powodem przejścia utworu do domeny

publicznej jest upływ określonego czasu . Po upływie określonego okresu czasu dzieło trafia do tzw. wolnego publicznego użytku. Dzieło nie jest już chronione przez prawo i może być swobodnie wykorzystywane w każdym czasie i miejscu. Od kilku lat istnieje (także w Polsce) Dzień Domeny Publicznej? Dzień Domeny Publicznej przypada 1 stycznia każdego roku, a jego celem jest zwrócenie uwagi opinii publicznej na rolę domeny publicznej w budowaniu kultury i otwieraniu dostępu do wiedzy. Na początku każdego roku na całym świecie otwiera się dostęp do nowych zasobów, które przestały podlegać ograniczeniom prawa autorskiego i przeszły do domeny publicznej. 1 stycznia 2015 r. do domeny publicznej „dołączyły” dzieła m.in.: norweskiego malarza, twórcy słynnego obrazu „Krzyk” Edvarda Muncha, rosyjskiego artysty i grafika Wassily’ego Kandinsky’ego oraz dzieła Antoine de Saint-Exupéry ,ego – autora m.in. wielkiego „Małego Księcia”).²⁶

Materiały pobrane ze strony: <https://lookkreatywni.pl/baza-wiedzy/o-swobodnym-wykorzystywaniu-zdjec/>

Serwisy z darmowymi zdjęciami oraz korzystanie z banków zdjęć, klipów, dźwięków

- Omówienie co to są banki zdjęć i jakie są ich rodzaje
- Omówienie zasad korzystania z serwisów darmowych zasobów
- Podanie stron darmowych banków:

<https://unsplash.com/>

<https://pixabay.com/pl/>

Jak bezpiecznie korzystać ze zdjęć znalezionych w sieci?

W kwestii legalnego wykorzystywania zdjęć z internetu zdania opinii publicznej są mocno podzielone. Duża część młodych ludzi uważa, że „ze wszystkiego, co znajduje się w sieci można korzystać dowolnie” (badania jakościowe przeprowadzone w Instytucie Socjologii UW). Są i tacy, którzy stoją na stanowisku, że korzystanie ze zdjęć i ilustracji znalezionych w internecie to zawsze łamanie prawa. Jak jest naprawdę?

Odpowiedzią na tak postawione pytanie niech będzie ulubione sformułowanie wszystkich prawników: **to zależy**. W niektórych przypadkach wstawianie zdjęć będzie zgodne z prawem, zaś w wielu innych takie działanie zostanie uznane jako bezprawne²⁷.

²⁶ <https://lookkreatywni.pl/baza-wiedzy/o-swobodnym-wykorzystywaniu-zdjec/>

²⁷ <https://lookkreatywni.pl/baza-wiedzy/o-swobodnym-wykorzystywaniu-zdjec/>

Materiały pobrane ze strony: <https://lookkreatywni.pl/baza-wiedzy/o-swobodnym-wykorzystywaniu-zdjec/>

- Przykłady banków zdjęć (nie wszystkie z nich są darmowe): [Unsplash](#), [Picjumbo](#), [Shutterstock](#), [Dreamstime](#), [IstockPhoto](#), [ThinkStockPhotos](#), [Gratisography](#), [IM Free](#), [Death to the Stock Photo](#), [Little Visuals](#), regulaminy tych banków określają zasady pobierania zdjęć zadarmo.

DYSKUSJA: Zdjęcia i grafika

- Omówienie zasad korzystania z serwisu Pixabay
- Zaprezentowanie narzędzi serwisu
- Wykonanie zadania wprowadzającego w tajniki korzystania i pobierania darmowych zdjęć

DYSKUSJA: Muzyka, filmy, książki, Skąd brać muzykę za darmo?

W Internecie bardzo modne stają się materiały rozpowszechniane na licencji Creative Commons. Założeniem organizacji, która rozpowszechnia tę licencję jest maksymalne uproszczenie tematyki praw autorskich. Jeśli autor uzna, że udostępnia swoje dzieła innym, to są udostępnione. Tutaj wystarcza wyłącznie wola twórcy oraz informacja powiązana z utworem, nie potrzeba nic więcej, poza wzmianką o autorstwie np w opisie filmu albo napisach końcowych. Utwory czasem rozpowszechniane są na licencji niekomercyjnej, albo wymagane jest rozpowszechnianie filmu na tej samej licencji co użytkowany utwór. Więcej informacji można znaleźć tutaj: <https://creativecommons.org/licenses/>

1. [Audionautix.com](#). Jest to spora baza utworów stworzonych przez jedną osobę. Utwory posegregowane są wg gatunku, tempa i powiązanych emocji. Wyszukiwanie jest bardzo proste, a utwory dobrej jakości. Strona niestety znajduje się na niezbyt szybkim serwerze.
2. [Incompetech.com](#). To również strona jednego autora – twierdzi on, że utworów jest tak wiele, że ze sporym prawdopodobieństwem nie były w stanie przypomnieć sobie ich nazw, gdyby został o nie zapytany. Jakość brzmienia jest bardzo dobra, kompozycje są zróżnicowanej jakości, ale na szczególną uwagę zasługuje dział World Music. Na tej stronie nie utworów z wokalem.

7. [Jamendo.com](https://www.jamendo.com). To rozwiązanie dla osób które mają dużo czasu i cierpliwości. Koniecznie ustawcie w wyszukiwarce opcję przeszukiwania wyłącznie utworów na licencji Creative Commons (ustawcie odpowiedni filtr, w zależności od tego czy wykorzystujecie muzykę komercyjnie czy nie). W zamian za przebrnięcie przez przepastne katalogi Jamendo, możecie otrzymać muzykę fantastycznej jakości... jeśli będziecie mieć szczęście.

Sposoby, jak znaleźć piosenkę, o której nic nie wiemy²⁸

PRZYKŁAD: *Słyszysz świetną piosenkę zupełnie przypadkiem. Wpada Ci w ucho, nie daje o sobie zapomnieć. Ale jak znaleźć piosenkę, o której nic nie wiesz?*

Oto 10 odpowiedzi, jak można to zrobić.

Muzyka towarzyszy nam niemal zawsze i wszędzie. Zwykle słuchamy tego, co lubimy – ulubione albumy w Spotify, ukochanego artystę w plikach mp3, pobudzające rano/wyciszające wieczorem piosenki w popularnej stacji radiowej. Muzyki słuchamy też w autobusie, w telewizji, podczas seansu, u fryzjera czy na zakupach w sklepie.

DYSKUSJA: *Jak znaleźć piosenkę po melodii czy po kilku słowach? Jak znaleźć piosenkę z radia czy z telewizji? Kto pomoże rozszyfrować soundtrack z reklamy czy filmu?*

1. **Zainstaluj aplikację rozpoznawania muzyki.** Aplikacje są dobre na wszystko! Są też oczywiście takie, które rozpoznają dowolny utwór w kilka sekund. Jest ich trochę, m.in. [Shazam](#), [Soly](#), [Music Recognition](#), taka opcja jest też w Google Music Play. Wystarczy, że uruchomisz aplikację i przytrzymasz telefon blisko źródła dźwięku, a po chwili otrzymasz wynik. Aplikacja analizuje dźwięki piosenki i rozpoznaje ją, jeśli ma ją w swojej bazie nagrań.
2. **Nagraj utwór.** Nagranie możesz puścić znajomym – możesz ktoś rozpoznać piosenkę lub utwór. Możesz też wrzucić nagranie do [AudioTag](#) – wystarczy nawet kilka sekund nagrania, żeby piosenkę rozpoznać. W AudioTag możesz też wkleić po prostu link do nagrania znalezione w sieci.
3. **Zaśpiewaj albo zanuć to, co wpadło Ci w ucho.** Aplikacja [SoundHound](#) przeanalizuje melodię i da Ci listę możliwych opcji. Na komputerze podobnie zadziała [Midomi](#) – pamiętaj tylko, żeby włączyć mikrofon. Te programy bez problemu poradzą sobie z

²⁸ <http://splashmedia.pl/blog/skad-brac-muzyke-do-filmow/>

utworami współczesnymi, ale gdybyś chciał/a znaleźć piosnkę, którą nucił Twój dziadek, to może być problem;)

4. **Zapisz nuty albo rytm.** Jeśli znasz nuty to dla Ciebie jest [Musipedia](#) – możesz zapisać linię melodyczną, tylko jej zarys, albo podać jedynie rytm. Z uwagi na specyfikę tego narzędzia i bazę utworów, na której ono pracuje, wyszukasz tu raczej instrumentalną muzykę klasyczną i inne typy muzyki nie popularnej.
5. **Nie pamiętasz melodii, ale pamiętasz kilka słów?** Super! Wpisz w wyszukiwarkę słowa i dodaj do nich wyraz „lyrics”. Zapamiętane słowa najlepiej wpisz w cudzysłowie – ograniczysz w ten sposób wyniki i będzie łatwiej.
6. **Nic nie pamiętasz poza kontekstem?** Spróbuj skorzystać z wyszukiwarki. Jeśli szukasz utworu z telewizji/filmu/reklamy warto wpisać pytanie typu „piosenka z reklamy ING” albo „utwór z Big Brother”. Można też spróbować opisać artystę/zespół, który piosenkę wykonuje i wyłović sylwetkę i jej nagrania, które będą najbliższe zapamiętanym szczegółom.
7. **Piosenkę usłyszałeś w radio!** O, to jest najłatwiejsze. Przypomnij sobie stację, dzień i porę, a potem odnajdź stronę radia i sprawdź jego playlistę danego dnia. Możesz też skorzystać ze strony [Odsłuchane](#) – tu masz wszystkie stacje radiowe w jednym miejscu.
8. **Słuchasz muzyki w internecie?** Sprawdź, czego aktualnie słuchasz za pomocą wtyczki do przeglądarki, np. [AHA Music – Music Identifier](#). Wystarczy uruchomić przycisk podczas trwania utworu i po chwili otrzymasz odpowiedź.
9. **Zapytaj innych.** To często najlepszy sposób, choć może chwilę potrwać. W sieci swoje nagranie lub piosenkę możesz wrzucić na portal [WatZatSong](#). Wśród mnóstwa użytkowników, na pewno znajdzie się taki, który rozpozna wrzucony przez ciebie kawałek. W Stanach działa mega forum – [AdTunes](#). W Polsce pasjonaci zagadek muzycznych skupiają się na dwóch miejscach: [Muzyka z reklam](#) i [rozpoznajemy.pl](#). Warto też czytać komentarze, np. pod filmami na Youtube – jest bardzo prawdopodobne, że już ktoś przed tobą szukał tej samej piosenki.
10. **Szukasz muzyki z reklam/filmów/gier/programów telewizyjnych?** Tu można spróbować wszystkich sposobów podanych wcześniej. Warto zajrzeć na fora, o których napisałam punkt wyżej. Możesz poszukać też stron dedykowanych stricte

reklamom, np. [TvAdMusic](#). Sprawdź też mega portal [Tunefind](#) – tu odkryjesz wszystko, co pojawiło się m.in. w filmach i grach.

Materiał zaczerpnięty ze strony: <http://splashmedia.pl/blog/skad-brac-muzyke-do-filmow/>
DYSKUSJA, POKAZ

- Prezentacja portali do oglądania filmów, słuchania muzyki
- Wprowadzenie pojęcia „**streaming**” i jego zalet w aspekcie zachowania praw autorskich i poszanowania własności intelektualnej
- Omówienie źródeł informacji o filmach i serwisach filmowych (na potrzeby szkolenia omówiony zostanie serwis VOD<https://vod.pl/filmy>)
- Podanie przykładów serwisów www.filmweb.pl
www.kinomaniak.pl
www.stopklatka.pl
- Omówienie technik wyszukiwania filmów
- Wykonanie ćwiczenia – wyszukiwanie filmów na dowolnie wybranym serwisie

DYSKUSJA, POKAZ: Gdzie znaleźć darmowe e-booki w Polsce?

Polskie platformy z darmowymi e-bookami:

ktoczyta.pl, [nexto](http://nexto.pl), [publio](http://publio.pl), [virtualo](http://virtualo.pl), [woblink](http://woblink.pl), cdp.pl, [ebookpoint](http://ebookpoint.pl), [koobe](http://koobe.pl), [ZłoteMyśli](http://ZloteMyśli.pl)

Praktycznie każdy polski sklep z e-bookami posiada u siebie katalog z darmowymi książkami elektronicznymi.

Katalog DARMOWE na bookto.pl

W katalogu zebraliśmy wszystkie darmowe e-booki, jakie znajdują się aktualnie w ofercie platform, z którymi współpracujemy. Możecie przejrzeć większość darmowych książek elektronicznych dostępnych na rynku polskim. Oczywiście, konkretne e-booki pobieracie już bezpośrednio z konkretnej platformy, na której znajduje się wybrany przez Was e-book.

Wolne lektury

To projekt prowadzony przez fundację Nowoczesna Polska. W zbiorach znajduje się obecnie 2666 darmowych ebooków, głównie klasycznych utworów literackich, w tym wiele znajdujących się na liście lektur szkolnych. Książki są w formatach: HTML , TXT , PDF, EPUB, MOBI, FB2. Na stronach serwisu znajduje się także kilkaset audiobooków, czytanych przez takich aktorów jak: Danuta Stenka, Jan Peszek czy Andrzej Chyra.

FantastykaPolska.pl

Prywatna strona [Robert J. Szmidta](#), pisarza SF i fantasy, założyciela a zarazem redaktora naczelnego miesięcznika [Science Fiction](#). Autor zgromadził ponad 500 opowiadań, powieści z kategorii fantastyka napisanych przez znanych polskich autorów, które ukazały się drukiem na łamach istniejących w ostatnich latach czasopism albo w książkach znanych wydawnictw. Wśród autorów m.in.: [R. Dębski](#), [M. Mortka](#), [Ł. Orbitowski](#), [A.W. Sawicki](#), [D. Sokołowski](#), [R. Szmidt](#), [A. Zimniak](#).

Pamięć.pl Publikacje historyczne i naukowe IPN

Baza darmowych publikacji historycznych IPN. Obecnie zawiera kilkadziesiąt pozycji. Lista jest na bieżąco aktualizowana. Dostępne formaty: epub, mobi, pdf. Pliki do pobrania bez logowania.

Chmura czytania

Projekt prowadzony przez fundację Festina Lente. Kilkadziesiąt tytułów, głównie klasyka literatury polskiej i zagranicznej. Dostępne są e-booki (epub, mobi) i audiobooki (mp3). Katalog bardzo przejrzysty w nawigacji.

RW2010

Oficyna wydawnicza przeznaczona do samodzielnego, darmowego publikowania utworów literackich niezależnych autorów. Baza zawiera ok. 400 darmowych e-booków autorów współpracujących z RW2010. Niestety, serwis nie posiada odrębnego katalogu z darmowymi książkami. Aby dotrzeć do darmowej oferty, należy ustawić filtr z ceną rosnącą.

Czytaj za free

Kilkaset darmowych e-booków (klasyka, niezależni autorzy). Serwis współpracuje z Wydawnictwem Nowy Świat.

Wydaje.pl

Darmowe publikacje niezależnych polskich autorów, głównie krótkie opowiadania. Można pobierać ebooki bez logowania.

ebooks43.pl

Kilkadziesiąt darmowych e-booków niezależnych autorów. Publikacje dostępne tylko na stronach serwisu.

Korzystanie z utworów podczas zajęć

Prowadząc **zajęcia** w szkołach (państwowych lub prywatnych), wykładając na wyższej uczelni lub dając indywidualne lekcje, korzystamy z różnych **chronionych materiałów**, takich jak nagrania, nuty utworów lub filmy.

W związku z tym często zastanawialiście się **czy można** legalnie odtworzyć w czasie zajęć nagranie lub puścić film? Czy można skserować nuty i dać je uczniom? A zeskanować? Czy ma znaczenie, że nuty są wypożyczone z biblioteki? Czy można materiały przesyłać mailem albo umieścić je na własnej stronie internetowej?

Jak legalnie korzystać z materiałów chronionych przez prawo autorskie w działalności dydaktycznej?

Poniżej **podstawowe zasady**, których należy się trzymać²⁹.

1. Możesz **korzystać** z każdego rozpowszechnionego materiału (filmu na płycie, z YouTube, książki, muzyki, nut), niezależnie od źródła z którego pochodzi, o ile dzieje się to **w ramach wykładów lub zajęć**. Nie można takich materiałów rozpowszechniać poza grupą uczniów/studentów.
2. Utwór jest **rozpowszechniony**, gdy został już wcześniej legalnie udostępniony publicznie. Warto zadbać, by źródło pochodzenia materiału było legalne. .
3. Możesz **kopiować** (kserować, skanować i wysyłać mailem, nagrywać na pendrive) **fragmenty** dowolnych utworów (filmów, książek, muzyki) swoim uczniom/studentom do celów edukacyjnych.
4. Warto **zwrócić uwagę** na to, że dozwolone kopiowanie ogranicza się do fragmentów utworów (np. partii jednego instrumentu, części utworu).
5. Jeśli chcesz **dzielić się** utworami w celach edukacyjnych w sieci, musisz pamiętać, że rozpowszechnianie ich nie może wykroczyć poza grupę Twoich uczniów/studentów. Na przykład możesz przestać materiały w mailach, przekazać je w zamkniętym kursie elearningowym lub poprzez wirtualny dysk (Dropbox, Google Drive), do którego mają dostęp jedynie Twoi uczniowie/studentenci. Jeżeli chcesz umieścić materiały na swojej **stronie internetowej**, to muszą być one zabezpieczone hasłem, by dostęp do nich mieli tylko Twoi uczniowie/studentenci.

²⁹ <https://lookkreatywni.pl/baza-wiedzy/o-swobodnym-wykorzystywaniu-zdjec/>

6. W ramach zajęć, lekcji, prac domowych można **modyfikować** dowolny utwór (wiersz, piosenkę) nie pytając o zgodę uprawnionego, o ile nie dojdzie do rozpowszechnienia wykorzystanych utworów poza zajęciami.
7. Podczas **impresz szkolnych** (np. koncertów dyplomowych, audycji, koncertów uczniów z Twojej klasy) mogą być wykonywane rozpowszechnione utwory, o ile wstęp na te imprezy jest bezpłatny, a wykonawcy nie uzyskują żadnego wynagrodzenia.
8. Nie wystarczy sam fakt, że impreza odbywa się w budynku szkoły/uczelni. Musi to być impreza związana z działalnością dydaktyczną. Trzeba zwrócić uwagę na to, że chodzi wyłącznie o **wykonania** utworów przez artystów wykonawców. Nie jest dozwolone odtwarzanie nagrań lub filmów w czasie imprez szkolnych.

(Materiały pobrane ze strony: <https://lookreatywni.pl/baza-wiedzy/o-swobodnymwykorzystywaniu-zdjec/>)



PRZYKŁADY ZADAŃ I ĆWICZEŃ

ĆWICZENIE: Jak rozpoznać czy obraz, film, treść jest chroniona prawami autorskimi?

Cel – wyjaśnienie uczestnikom, czym są prawa do użytkowania



Uwaga!!! W trakcie wykonywania ćwiczenia należy krótko omówić co oznaczają i jakie dają możliwości poszczególne filtry, wprowadzić definicję praw autorskich³⁰ oraz omówić prawo do użytkowania³¹.

- oznaczone do ponownego wykorzystania z modyfikacją (czyli możemy je przerobić),
- oznaczone do ponownego wykorzystania (niekoniecznie można przerobić),
- oznaczone do ponownego wykorzystania w celach niekomercyjnych z modyfikacją,
- oznaczone do ponownego wykorzystania w celach niekomercyjnych.

Ćwiczenia należy wykonać na kilku różnych wyszukiwarkach

³⁰**Prawo autorskie** - przysługuje twórcy utworu. Istnieje domniemanie, że jest nim osoba, której nazwisko w tym charakterze uwidoczniło na egzemplarzach utworu lub której autorstwo podano do publicznej wiadomości w jakikolwiek inny sposób, w związku z rozpowszechnianiem utworu.



Uwaga!!! Wspomnieć o różnicach w sposobie wyświetlania tych samych wyników wyszukiwania w różnych wyszukiwarkach:

1. **JAHOO!** – Images/Public Domain
2. **Bing** – Obrazy/Licencja"
3. **Flickr** - zawiera wiele zdjęć chronionych prawami autorskimi. Niezależnie od tego możemy na nim znaleźć zdjęcia na licencji Creative Commons. Część z tych zdjęć można remiksować i wykorzystywać nawet komercyjnie. W czasie przeglądania zdjęć na Flickrze po lewej stronie widzimy link "Any License". Oznacza to, że przeglądamy zdjęcia na wszystkich dostępnych licencjach.

ĆWICZENIE: Wyszukiwanie darmowych filmów wideo oraz grafiki wektorowej na Pixabay

3. Uruchom stronę <https://pixabay.com/pl/> i wyfiltruj filmy wideo o zwierzętach wg. kategorii **Nadchodzące**
4. Wyszukaj grafikę wektorową na dowolny temat w kategorii **Najnowsze** – to samo zadanie wykonaj również w dowolnie wybranej wyszukiwarce (np. JAHOO!, Bing, czy Mozilla)
 - Omówienie funkcji Wikipedii jako źródła darmowych zdjęć z uwzględnieniem zalet i wad
 - Wprowadzenie pojęcia „licencji stanowiących domenę publiczną, na licencji Creative Commons oraz GNU FDL”, „licencja komercyjna”
 - Omówienie zobowiązań jakie musimy spełnić w przypadku korzystania ze zdjęć na tych licencjach (obowiązek dołączenia pełnego tekstu licencji - uznanie tych licencji jest uszanowaniem autora, który zrezygnował z wynagrodzenia.



Uwaga!!!– Wiele źródeł multimediów na wolnych licencjach jest zebrane na stronie commons.wikimedia.org.

- Przykłady innych banków zdjęć:
 - www.frepik.com
 - www.1001freedowlands.com
 - www.cabooompics.com
 - www.picjumbo.com
 - www.publicdomainarchive.com
 - www.splitshire.com

ĆWICZENIE: Wyszukiwanie filmu na dowolnie wybranym serwisie

Wspólne spędzanie czasu z rodziną można uatrakcyjnić ciekawym filmem.

3. Znajdź na dowolnym serwisie film z uwzględnieniem następujących filtrów:
gatunek – Familijne, sortuj – Rok produkcji.
 4. Wyszukaj inny film wg. własnych filtrów zgodnie z zainteresowaniami.
- Rozmowa z uczestnikami na temat wspierania dzieci i młodzieży w zakresie tematyki oglądanych filmów, słuchanej muzyki czy książek ze względu na ich prawidłowy rozwój psychiczny i osobowościowy
 - Wskazanie stron internetowych zawierających recenzje różnych pozycji
 - Recenzje muzyczne <https://audio.com.pl/muzyka/recenzje>
<https://muzyka.onet.pl/recenzje>
 - Recenzje książek <http://lubimyczytac.pl>,
<http://edziecei.pl>
<https://www.strefapsotnika.pl>

ĆWICZENIE: Szukamy ciekawych książek dla siebie i dla dzieci

1. Znajdź na stronie <http://lubimyczytac.pl> książkę „Aru Shah i koniec czasu” autorstwa Roshani Chokshi
2. Następnie znajdź dla siebie ciekawą pozycję.

Corzystanie z usług publicznych



CELE I KOMPETENCJE:

- Nabycie wiedzy i umiejętności w zakresie rejestrowania konta w ePUAP.
- Poznanie możliwości wykorzystania profilu zaufanego.
- Poznanie zalet i zasad pracy wykorzystując usługi online w życiu codziennym



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

DYSKUSJA: Umiejętności korzystania z usług publicznych. Karta Dużej Rodziny

- Omówienie programu KDR
- Przykłady serwisów, w których można załatwić sprawy urzędowe online z pomocą profilu zaufanego: www.obywatel.gov.pl, www.gov.pl, www.biznes.gov.pl,

www.ePUAP.gov.pl, www.empatia.mpips.gov.pl, www.zus.pl, Portal podatkowy - <https://ppuslugi.mf.gov.pl/>

- Omówienie co to jest ePUAP i profil zaufany
- Zakładanie konta w ePUAP na profilu zaufanym
- Omówienie jakie sprawy można załatwić z wykorzystaniem profilu zaufanego oraz jak przebiega proces składania wniosków przez profil
- Omówienie jakie urzędy i jakie sprawy obsługuje ePUAP

DYSKUSJA: Składanie wniosku o przyznanie KDR

- Omówienie kto może ubiegać się o Kartę Dużej rodziny
- Korzyści wynikające z posiadania KDR
- Umiejętności korzystania z usług publicznych. Karta Dużej Rodziny
- Omówienie programu KDR –



film <https://www.youtube.com/watch?v=2Xy0kKuxeVo>

Wykaz dokumentów, które mogą się przydać podczas składania wniosku o KDR

- Składanie wniosku o KDR

Program Rodzina 500+, 2.1. Składanie wniosku Rodzina 500+



Składanie wniosku Rodzina 500+ - film

<https://www.youtube.com/watch?v=H63kFE97oUo> (dla przykładu PKO)

- **Składanie innych wniosków:**
 - Składanie wniosku o dowód osobisty (obywatel.gov.pl)
 - Wydanie karty EKUZ Omówienie zasad składania wniosku o kartę EKUZ <http://www.nfz.gov.pl/dla-pacjenta/zalstw-sprawe-krok-po-kroku/jak-wyrobic-karte-ekuz/>

- **Sprawdzanie punktów karnych za mandaty –**



film <https://www.youtube.com/watch?v=uGgT-92sok>

- Założenie działalności gospodarczej z wykorzystaniem CEIDG. –
- film <https://www.youtube.com/watch?v=haYg5ecwDUk>

Zakładanie konta ePUAP

ePUAP (elektroniczna Platforma Usług Administracji Publicznej) – ogólnopolska platforma teleinformatyczna służąca do komunikacji obywateli i przedsiębiorców z jednostkami administracji publicznej w ujednolicony, standardowy sposób. Platforma służy również do komunikacji pomiędzy jednostkami administracji publicznej³².

Aby rozpocząć proces zakładania konta na platformie ePUAP (bezpłatna usługa) należy wejść na stronę ePUAP <http://epuap.gov.pl>, a następnie wybrać opcję **Zarejestruj się**.

1. Wypełnij formularz rejestracji konta.
3. Prawidłowo zdefiniuj **Adres e-mail** i **hasło**.



UWAGA!!! Użytkownik po zarejestrowaniu konta może w dowolnym momencie zmienić **Sposób logowania** z hasła na certyfikat i odwrotnie z certyfikatu na hasło.

4. Wyraż zgodę na przetwarzanie danych osobowych
5. System automatycznie składa wnioski o Profil Zaufany.
6. Odbierz powiadomienie mailowe potwierdzające złożenie wniosku o Profil Zaufany.
7. Osobiście potwierdź złożenie wniosku na swój **Profil Zaufany** w jednym z Punktów Potwierdzających, po okazaniu dowodu osobistego lub paszportu.
8. Potwierdź numer telefonu.
9. Zakończ proces rejestracji.
10. Zostałeś automatycznie zalogowany do systemu.
11. Wraz z założeniem konta utworzono Ci w **STREFIE KLIENTA Skrzynkę - Moja Skrzynka**.
12. W skrzynce gromadzone są dokumenty które:
 - będziesz odbierał od urzędu,
 - dokumenty które będziesz wysłał,
 - kopie robocze tworzonych pism.
 - Skrzynka przechowuje pobrane z dysku pliki oraz umożliwia przechodzenie do innych utworzonych skrzynek.

³² https://epuap.gov.pl/wps/wcm/connect/epuap2/PL/Strefa+Klienta_Pomoc/Co+to+jest+ePUAP/

13. Odbierz z podanego przy rejestracji adresu e-mail **powiadomienie** o tym, że zarejestrowałeś konto na platformie ePUAP.

14. **Założenie konta nie jest jednoznaczne z posiadaniem Profilu Zaufanego³³.**



UWAGA!!! Jeśli użytkownik poprawnie wypełnił pole **PESEL** podczas rejestracji konta, system automatycznie złożył za niego wniosek o **Profil Zaufany**. Jeśli natomiast nie wypełnił tego pola, to po zalogowaniu na swoje konto, może złożyć wniosek o Profil Zaufany.

DYSKUSJA, POKAZ: Wykorzystanie profilu zaufanego.

Wnioski, które można złożyć za pośrednictwem profilu zaufanego ePUAP:

- zgłoszenie narodzin dziecka,
- rejestracja auta,
- dopisanie do spisu wyborców,
- zgłoszenie działalności gospodarczej,
- i inne

DYSKUSJA, POKAZ: E-usługi za pomocą profilu zaufanego

- Składanie i sprawdzanie dokumentów rozliczeniowych w ZUS i US
- Zgłaszanie utraty dokumentu tożsamości
- Składanie wniosku o rejestrację działalności gospodarczej
- Załatwianie spraw urzędowych dla swojej rodziny: becikowe, świadczenia rodzicielskie, Karta Dużej Rodziny, Świadczenie o Funduszu Alimentacyjnym
- Wystąpienie o Europejską Kartę Ubezpieczenia Zdrowotnego
- Uzyskanie odpisu aktu stanu cywilnego
- Dziesiątki innych spraw.

Elektroniczna Platforma Usług Administracji Publicznej (w skrócie **ePUAP**) portal www.epuap.gov.pl skierowany jest zarówno do osób fizycznych, przedsiębiorców, jak i

³³ **Profil Zaufany** jest to **odpowiednik bezpiecznego podpisu elektronicznego**, to bezpłatna metoda potwierdzania tożsamości w elektronicznych kontaktach z administracją. Wykorzystując Profil Zaufany obywatel może załatwić sprawy administracyjne (np. wnoszenie podań, odwołań, skarg) drogą elektroniczną bez konieczności osobistego udania się do urzędu.

instytucji administracji publicznej. Platforma ta ma ułatwić i unowocześnić komunikację pomiędzy:

- obywatelami a administracją,
- przedsiębiorcami a administracją,
- instytucjami administracji publicznej.

Wykorzystanie profilu zaufanego³⁴ przy wysłaniu pisma do systemu ePUAP

1. Celem wysłania pisma z użyciem profilu zaufanego obywatel loguje się do systemu ePUAP na stronie www.epuap.gov.pl.
2. Wybranie z Katalogu Usług usługi oraz realizującego ją urzędu oraz wypełnienie elektronicznego formularza udostępnionego przez urząd, celem utworzenia pisma urzędowego.
3. Podpisanie pisma za pomocą profilu zaufanego oraz potwierdzenie operacji kodem autoryzującym wysłanym przez system ePUAP na konto e-mail podane podczas zakładania profilu zaufanego.
4. Wysyłanie pisma, które automatycznie kierowane jest na Elektroniczną Skrzynkę Podawczą. Otrzymanie Urzędowego Poświadczenia Odbioru.
5. Obsługa pisma przez urzędnika zgodnie z procedurą obowiązującą dla usługi w danym urzędzie. Wysłanie pisma na konto ePUAP obywatela.
6. Podpisanie odbioru pisma i odczytanie pisma przez obywatela.
7. Odbiór Urzędowego Poświadczenia Odbioru

Jakie urzędy i jakie sprawy obsługuje ePUAP

Coraz więcej spraw możesz załatwić przez Internet, bo coraz więcej urzędów udostępnia swoje usługi na ePUAP. Są to między innymi:

- samorządy, w tym urzędy gminy — wniosek o dowód dla siebie lub dziecka; zgłoszenie utraty lub zniszczenie dowodu albo prawa jazdy; zawiadomienie o sprzedaży samochodu; dopisanie się do spisu wyborców,
- USC (urzędy stanu cywilnego) — odpisy aktów: małżeństwa, urodzenia, zgonu, lub inne dokumenty; zgłoszenie urodzenie dziecka,

³⁴ Ministerstwo Spraw Wewnętrznych i Administracji | ul. Batorego 5, 02-591 Warszawa | www.epuap.gov.pl – „elektroniczna Platforma Usług Administracji Publicznej - Proces wykorzystania profilu zaufanego”

- ZUS (Zakład Ubezpieczeń Społecznych) — sprawdź, czy pracodawca cię ubezpieczył i jaką dostaniesz emeryturę; przejrzyj swoje zwolnienia lekarskie i składki,
- NFZ (Narodowy Fundusz Zdrowia) — karta EKUZ (Europejska Karta Ubezpieczenia Zdrowotnego),
- US (urzędy skarbowe) — rozliczenia podatkowe; zgłoszenie spadku lub darowizny,
- KRK (Krajowy Rejestr Karny) — zaświadczenie o niekaralności,
- UP (urzędy pracy) — zarejestruj się jako osoba bezrobotna i korzystaj ze szkoleń,
- Rejestr PESEL i Rejestr Dowodów Osobistych — sprawdź swoje dane i dokumenty,
- inne urzędy administracji publicznej (centralne, regionalne i lokalne) oraz instytucje publiczne — zarejestruj działalność gospodarczą; złóż wniosek o Kartę Dużej Rodziny; wyślij pismo ogólne, gdy nie ma formularza do załatwienia twojej sprawy.

Składanie wniosku o dowód osobisty (obywatel.gov.pl)

Ministerstwo Cyfryzacji stworzyło możliwość składania różnych wniosków przez Internet.

Wystarczy wejść na stronę www.obywatel.gov.pl.

Dowód osobisty to dokument, który pozwala potwierdzić twoją tożsamość oraz polskie obywatelstwo. Każdy pełnoletni obywatel, który mieszka w Polsce, musi mieć dowód osobisty. Dodatkowo, z dowodem możesz podróżować bez paszportu między innymi do krajów Unii Europejskiej. Sprawdź podstawowe informacje na temat dowodu osobistego. Dowód osobisty musi mieć każdy pełnoletni obywatel, który mieszka w Polsce. Dowód może mieć również osoba, która nie ukończyła jeszcze 18 lat (na przykład jeśli chce podróżować za granicę do krajów, w których nie jest wymagany paszport)³⁵.

Przykłady serwisów, w których można załatwić sprawy urzędowe online z pomocą profilu zaufanego:

- obywatel.gov.pl
- biznes.gov.pl
- ePUAP.gov.pl
- empatia.mpips.gov.pl
- zus.pl
- Portal podatkowy <https://www.finanse.mf.gov.pl/web/wp/pp>

³⁵ <https://obywatel.gov.pl/dokumenty-i-dane-osobowe/dowod-osobisty-informacja-o-dokumentacie>



PRZYKŁADY ZADAŃ I ĆWICZEŃ

ĆWICZENIE: Załóż konto w ePUAP i na profilu zaufanym



/Uwaga: zgodnie z instruktażem trenera/

ĆWICZENIE: Wymień poznane sprawy jakie obsługuje e-PUAP.

ĆWICZENIE: Do jakich spraw można wykorzystać profil zaufany, podaj przykłady

ĆWICZENIA: ZAKŁADANIE KONTA ePUAP



<https://www.youtube.com/watch?v=pO5PoGzKxAo> ePUAP - co to jest i jak założyć?

– film

- Składanie wniosku o przyznanie KDR - korzyści wynikające z posiadania KDR
- Wykaz dokumentów, które mogą się przydać podczas składania wniosku o KDR

Ochrona komputera i innych urządzeń przed złośliwym oprogramowaniem



CELE I KOMPETENCJE CYFROWE

- Poznanie sposobów jak prawidłowo zapewnić kontrole rodzicielską.
- Poznanie różnych stron z darmowymi programami.
- Opanowanie umiejętności instalowania i konfigurowania oprogramowania.
- Nabycie wiedzy jak prawidłowo zabezpieczyć komputer przed złośliwym oprogramowaniem.
- Nabycie wiedzy na temat szkodliwego oprogramowania.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

DYSKUSJA, POKAZ: Ochrona komputera i innych urządzeń przed złośliwym oprogramowaniem

- Omówienie co to jest wirus komputerowy i złośliwe oprogramowanie
- Rodzaje wirusów
- Rodzaje złośliwego oprogramowania

Instalacja programów antywirusowych

- Sposoby wyszukiwania programów antywirusowych
- Pobieranie darmowych i płatnych programów
- Instalacja i rejestracja programu antywirusowego
- Zwrócenie uwagi, iż najlepiej pobierać ze strony producenta

Korzystanie z narzędzi kontroli rodzicielskiej na komputerach

- Wyszukiwanie programów do kontroli rodzicielskiej
- Pobieranie i instalacja programu
- Konfiguracja kontroli rodzicielskiej na komputerze
- Korzystanie z narzędzi programu

Filmy edukacyjne w sieci – rozwijanie świadomości zagrożeń jakie niesie ze sobą Internet.

- <https://www.saferinternet.pl/menu/materialy-edukacyjne/materialy-multimedialne/owce-w-sieci.html>
- <https://sieciaki.pl>
- <https://www.pcformat.pl/>
- <http://www.instalki.pl/>
- <http://www.edulider.pl/edukacja/jakie-programy-komputerowe-warto-znac>
- <https://www.dobreprogramy.pl>

Co to jest złośliwe oprogramowanie?

- Złośliwe oprogramowanie (malware) to szeroki termin, obejmujący fragmenty kodu i programy, które szkodzą systemom.
- Wrogie, inwazyjne i celowo dokuczliwe złośliwe oprogramowanie ma na celu inwazję, uszkodzenie lub dezaktywację komputerów, systemów komputerowych, sieci, tabletów i urządzeń przenośnych, często przez częściowe przejęcie kontroli nad działaniem urządzenia. Podobnie jak ludzka grypa, zakłóca funkcjonowanie.
- Złośliwe oprogramowanie ma na celu nielegalne zarabianie pieniędzy. Złośliwe oprogramowanie nie może uszkodzić fizycznie sprzętu systemu lub sprzętu sieciowego, jednak może ono ukraść, zaszyfrować lub usunąć dane, zmienić lub przechwycić podstawowe funkcje komputera i szpiegować Twoje działania na komputerze bez Twojej wiedzy i akceptacji

Jak mogę sprawdzić, czy mam złośliwe oprogramowanie?



- Obecność złośliwego oprogramowania może się przejawiać na wiele różnych sposobów:
- Oto kilka znaków ostrzegawczych, które świadczą o tym, że w Twoim systemie znalazło się złośliwe oprogramowanie:
- Komputer działa wolniej. Złośliwe oprogramowanie najczęściej powoduje znaczne spowolnienie działania systemu operacyjnego.
- Natłok denerwujących reklam, które nie powinny być wyświetlane na ekranie. Nieoczekiwane wyskakujące reklamy to typowy objaw zainfekowania złośliwym oprogramowaniem. Zwykle są one powiązane z rodzajem złośliwego oprogramowania znanego pod nazwą adware. Jeśli więc zobaczysz w okienku coś w rodzaju „GRATULACJE! WYGRAŁEŚ DARMOWĄ WIZYTĘ U JASNOWIDZA!”, nie klikaj tego. Bez względu na to, jaką darmową nagrodę obiecuje reklama, na pewno będzie Cię drogo kosztować.
- Twój system często się zawiesza, zamraża lub wyświetla niebieski ekran (BSOD, Blue Screen of Death), który może wystąpić w systemach Windows po wystąpieniu błędu fatalnego.
- Zauważasz tajemniczą utratę miejsca na dysku.
- Ma miejsce dziwny wzrost aktywności internetowej Twojego systemu.
- Wykorzystanie zasobów systemowych jest nienormalnie wysokie, a wentylator komputera zaczyna działać z pełną prędkością — aktywność złośliwego oprogramowania pochłania zasoby systemowe w tle
- Strona startowa przeglądarki zmieniła się bez Twojego pozwolenia. Odsyłacze, które klikasz, również wysyłają Cię do miejsc innych niż oczekiwane. Zwykle oznacza to kliknięcie w takim okienku z „gratulacjami” i pobranie niechcianego oprogramowania.
- Przeglądarka może działać bardzo wolno. W przeglądarce nieoczekiwanie pojawiają się paski narzę Program antywirusowy przestaje działać i nie można go zaktualizować, system jest niezabezpieczony przed podstępny złośliwym oprogramowaniem, które go blokuje.
- Mamy do czynienia z boleśnie oczywistym, celowo nieukrywanym atakiem złośliwego oprogramowania. Tak zachowuje się słynne oprogramowanie

ransomware, które oznajmia, że jest zainstalowane, informuje, że ma Twoje dane, i żąda okupu za zwrot Twoich plików, rozszerzenia lub wtyczki.

- Nawet jeśli wydaje się, że wszystko działa dobrze w Twoim systemie, nie popadaj w samozadowolenie, ponieważ brak informacji niekoniecznie jest dobrą wiadomością. Potężne złośliwe oprogramowanie może ukryć się głęboko w komputerze i rozpocząć niszczycielską działalność bez fanfar i oklasków: łamie hasła, kradnie poufne pliki lub używa komputera do rozprzestrzeniania się na inne komputery
- Powód złośliwego oprogramowania na urządzeniu:
 - surfujesz po przejętych stronach internetowych,
 - klikasz wersje demonstracyjne gier,
 - pobierasz zainfekowane pliki audio,
 - instalujesz nowe paski narzędzi od nieznanego dostawcy,
 - instalujesz i konfigurujesz oprogramowanie z nieznanego źródła,
 - otwierasz złośliwy załącznik do wiadomości e-mail lub robisz cokolwiek innego, co wiąże się z pobieraniem plików z Internetu na urządzenie niewystarczająco zabezpieczone przed złośliwym oprogramowaniem

Jakiego rodzaju złośliwe oprogramowanie występuje najczęściej? Oto najczęściej spotykane „złośliwe oprogramowanie”:

- [Adware](#) jest niechcianym oprogramowaniem służącym do wyświetlania reklam na Twoim ekranie. Zazwyczaj programy te wykorzystują różne metody podszywania się pod żądane aplikacje lub podczepiają się do nich, aby skłonić nas do zainstalowania ich na swoim komputerze, tablecie lub urządzeniu mobilnym.
- [Oprogramowanie szpiegujące](#) to złośliwe oprogramowanie, które potajemnie obserwuje działania użytkownika komputera bez jego zgody i zgłasza je autorowi oprogramowania.
- [Wirus](#) to złośliwe oprogramowanie, które dołącza się do innego programu, a po uruchomieniu — zazwyczaj przypadkowo — sam się powiela, modyfikując inne programy komputerowe i zarażając je własnymi bitami kodu.
- [Robaki](#) to złośliwe oprogramowanie podobne do wirusów, samopowielające się i infekujące inne komputery przez sieć. Zwykle powoduje szkody, niszcząc dane i pliki.

- [Trojan](#) lub koń trojański to jeden z najniebezpieczniejszych typów złośliwego oprogramowania. Zazwyczaj podszywa się pod coś pożytecznego, aby cię oszukać. Po uruchomieniu systemu napastnicy dysponujący koniem trojańskim uzyskują nieautoryzowany dostęp do zaatakowanego komputera. Dlatego koń trojański może być wykorzystywany do kradzieży informacji finansowych lub instalowania zagrożeń, takich jak wirusy i oprogramowanie ransomware.
- [Ransomware](#) to złośliwe oprogramowanie, które blokuje urządzenie i/lub szyfruje Twoje pliki, a następnie zmusza Cię do zapłacenia okupu, aby je odzyskać. Oprogramowanie ransomware czasem jest nazywane bronią cyberprzestępców, ponieważ żąda szybkiego, wysokiego haraczu w trudnej do śledzenia [kryptowalucie](#). Kod oprogramowania ransomware łatwo zdobyć na rynkach przestępczych online, a obrona przed nim jest bardzo trudna.
- [Rootkit](#) to rodzaj złośliwego oprogramowania, który nadaje atakującemu uprawnienia administratora w zainfekowanym systemie. Zwykle jest niewidoczne dla użytkownika, oprogramowania, a nawet dla systemu operacyjnego. [Keylogger](#) to złośliwe oprogramowanie, które zapisuje wszystkie naciśnięcia klawiszy użytkownika na klawiaturze, zazwyczaj przechowuje zebrane informacje i wysyła je do atakującego, który wyszukuje poufne informacje, takie jak nazwy użytkownika, hasła czy dane karty kredytowej
- [Złośliwy cryptomining](#), określany czasem jako drive-by mining lub [cryptojacking](#), to coraz bardziej rozpowszechnione złośliwe oprogramowanie instalowane zazwyczaj przez konia trojańskiego. Umożliwia ono atakującemu wykorzystywanie Twojego komputera do zdobywania kryptowalut, takich jak bitcoin lub monero. Następnie zamiast umieścić pieniądze na Twoim koncie kryptominer wysyła zebrane pieniądze na własne konta. Zasadniczo złośliwy kryptominer kradnie Twoje zasoby, aby zarabiać pieniądze.
- [Exploity](#) to rodzaj złośliwego oprogramowania, które wykorzystuje błędy i [słabe punkty](#) w systemie, aby umożliwić przejęcie kontroli autorowi oprogramowania wykorzystującego luki w programach. Podobnie jak inne zagrożenia, exploity są powiązane ze [złośliwymi reklamami](#) atakującymi przez legalną stronę, która nieświadomie pobiera szkodliwe treści ze złej strony. Następnie szkodliwa treść próbuje zainstalować samą siebie na Twoim komputerze w ataku typu drive-by download. Nie

są potrzebne żadne kliknięcia. Wszystko, co musisz zrobić, to odwiedzić dobrą stronę pewnego pechowego dnia.

Jak mogę usunąć złośliwe oprogramowanie?

Po pierwsze, jeśli jeszcze go nie masz, to pobierz oryginalny program do [zwalczania złośliwego oprogramowania](#), taki jak [Malwarebytes for Windows](#), [Malwarebytes for Mac](#), [Malwarebytes for Android](#) lub [jeden z naszych produktów dla przedsiębiorstw](#). Następnie zainstaluj go i przeprowadź skanowanie. Programy takie jak te mają na celu wyszukanie i wyeliminowanie złośliwego oprogramowania na urządzeniu.

Gdy urządzenie zostanie wyczyszczone, warto zmienić hasło, nie tylko do komputera i urządzenia mobilnego, ale także do konta e-mail, kont w mediach społecznościowych, ulubionych sklepach, na stronach banków i internetowych centrów rozliczeniowych

W jaki sposób mogę się bronić przed złośliwym oprogramowaniem?

- W przypadku wszystkich urządzeń należy zwracać szczególną uwagę na wczesne objawy infekcji złośliwym oprogramowaniem, aby zapobiec jego skutecznemu ukryciu się.
- Unikaj klikania wyskakujących reklam podczas przeglądania Internetu. Nigdy nie otwieraj nieoczekiwanych załączników do wiadomości e-mail, nie pobieraj oprogramowania z niepewnych stron internetowych lub sieci transferu plików peer-to-peer.
- Nie klikaj dziwnych, niezweryfikowanych łączy w wiadomościach e-mail, tekstowych i WhatsApp o nieznanym pochodzeniu. Należy również unikać dziwnych łączy od znajomych i innych kontaktów, chyba że wiesz, że są bezpieczne.
- Tak więc zanim coś zaatakuje Twój komputer, urządzenie mobilne lub sieć firmową, zabezpiecz się, pobierając dobry [program antywirusowy zapewniający cyberbezpieczeństwo](#), taki jak:
 - [Malwarebytes for Windows](#),
 - [Malwarebytes for Mac](#),
 - [Malwarebytes for Android](#),
 - [Malwarebytes na urządzenia przenośne](#) lub jeden z [produktów Malwarebytes dla przedsiębiorstw](#).

10 sposobów na zabezpieczenie nowego komputera

1. Antywirus, antyspyware oraz firewall

Brzmi dość prosto i naprawdę tak jest, jednak wciąż może dziwić liczba osób, które z takich programów nie korzystają. Każdy komputer z dostępem do internetu powinien korzystać z **antywirusa**, **oprogramowania antyspyware** oraz **firewall**. Szczególnie ważne jest utrzymywanie ich w aktualnych wersjach oraz regularne skanowanie komputera

2. Zabezpieczenia behawioralne

Oprócz podstawowych aplikacji, w ofercie wielu firm znajdują się też inne programy zabezpieczające, takie jak **behawioralne aplikacje zabezpieczające** wykorzystujące także tradycyjne sprawdzanie sygnatur wirusów.

Jako pierwsza linia obrony, sprawdzanie sygnatur jest niedoścignione. Chodzi o moment kiedy kod programu próbującego coś zmienić w naszym komputerze jest porównywany z bazą danych, znanych już szkodliwych aplikacji. Umożliwia to bardzo często usunięcie programu zanim zdąży on narobić w naszym OS-ie jakiegokolwiek szkody.

3. Usuń śmieci i próbki

Twój komputer może być dostarczony z masą darmowych triali, które po skończeniu się okresu próbnego zaczną nachalnie zachęcać do kupna pełnych wersji. Nie ma w tym nic niebezpiecznego, jednakże takie "pop-upy" mogą znieczulić użytkownika na przeróżne, irytujące komunikaty. Taką formę "reklamy" często przyjmują także wirusy niewykryte przez przestarzałe oprogramowanie zabezpieczające.

4. Aktualizuj swoje oprogramowanie

Brak utrzymywania "świeżości" swojego oprogramowania spowoduje, że Twój komputer będzie "dziurawy". Wiele programów wymaga aktualizacji. Producenci naprawiają w ten sposób błędy, które mogą wykorzystać programiści od złośliwego oprogramowania. Popularne programy takie jak Adobe Flash czy Firefox, jak również system operacyjny Windows, wymagają regularnych aktualizacji, ponieważ ich brak skutecznie obniża poziom bezpieczeństwa.

5. Załóż konto do kontroli wszystkich kont

Jednym z najłatwiejszych sposobów poprawienia bezpieczeństwa jest korzystanie z konta o ograniczonych możliwościach tak, aby nie było możliwe dokonanie żadnych krytycznych zmian w systemie. Aby to zrobić, na początku należy stworzyć konto administratora i ustawić aby tylko ono było w stanie dokonywać ważnych zmian. Następnie założyć chronione hasłem konto o ograniczonych możliwościach, które będzie wykorzystywane na co dzień.

6. Zabezpiecz sieć oraz przeglądarkę

Istnieje kilka rzeczy jakie możesz zrobić w celu zabezpieczenia komputera przez zagrożeniami płynącymi z sieci. Pierwsza to zabezpieczenie swojego routera. Mimo iż standardowo posiada on hasło, to często brzmi ono "1234" lub "0000". Ustawmy więc jakieś bardziej skomplikowane, najlepiej szyfrowane w **standardzie WPA2**. W samej przeglądarce, zabezpieczenia mogą zostać ustawione na te najbardziej restrykcyjne.

7. Ustaw punkt przywracania systemu

Punkt przywracania systemu jest swego rodzaju zakładką, która jest tworzona po znaczącej zmianie w twoim komputerze. Windows Updates tworzy je po instalacji większych aktualizacji. Często punkt przywracania tworzony jest również w określonych odstępach czasowych np. co tydzień. Jeśli czasem pójdzie coś źle i np. wprowadzone zostaną bardzo niekorzystne ustawienia, punkty te umożliwią powrót do poprzedniego momentu, bez straty wielu ważnych danych.

8. Uświadom innych użytkowników komputera



Podstawowym i największym zagrożeniem dla komputera jest jego użytkownik. Najłatwiejszym natomiast sposobem na zainfekowanie sprzętu wirusem jest dopuszczenie nieświadomego użytkownika, który wejdzie w nieodpowiedni link lub ściągnie plik niewiadomego pochodzenia.

Element ludzki nigdy nie zostanie całkowicie wyeliminowany, jednakże można ograniczyć niebezpieczeństwo uzgadniając kilka podstawowych zasad dotyczących użytkownika Twojego nowego komputera. Powinni ich przestrzegać wszyscy, również Ty. Strony, które uważasz za nieodpowiednie można bezproblemowo dodać do czarnej listy przy pomocy darmowych programów takich jak **Windows Family Safety**. Zatrzymaj prawa administratora tylko dla siebie. Zaznacz, że ściąganie plików niewiadomego pochodzenia nie będzie tolerowane, hasła powinny być zróżnicowane i nie banalne.

9. Fizyczne zabezpieczenie

Laptopy mają jeden poważny minus: łatwo je ukraść. Powinniśmy zastosować się do dwóch prostych zasad, aby temu zapobiec. Jeśli to możliwe trzymać sprzęt blisko łóżka w którym śpimy i koniecznie przechowywać go w miejscu odległym od okien i niewidocznym z ulicy. Kolejnym sposobem może być inwestycja w **zabezpieczenie Kensington** i fizyczne przyczepienie komputera do czegoś. Nikt z pewnością nie chciałby się zorientować, że jego idealnie zabezpieczony komputer został fizycznie ukradziony.

10. Bądź uważny i rozważny

Żadna z powyższych rad nie zagwarantuje bezpieczeństwa waszemu systemowi. Jednak zestawione razem spowodują, że ewentualny cyberprzestępca będzie miał dużo bardziej ograniczony dostęp do waszego komputera, a w najgorszym przypadku do waszego portfela. Kluczem do tego wszystkiego jest zachowanie czujności.

Twój nowy komputer jest przecież po to, by cieszyć. Internet to genialne źródło informacji i nie powinniśmy żyć w strachu. Ale szczypta zdrowego sceptycyzmu i odrobina ostrożności we wszystkim co związane z komputerem z pewnością nie zaszkodzi.

Jak działają programy antywirusowe?

W jaki sposób odbywa się rozpoznanie potencjalnie groźnych programów? Firma będąca producentem antywirusa tworzy bazę danych składającą się z sygnatur znanego złośliwego oprogramowania. Sygnatury te to charakterystyczne części kodu wirusa, dzięki którym można go zidentyfikować i odróżnić od zwykłych aplikacji. Antywirus pobiera i na bieżąco, nawet codziennie, aktualizuje tę bazę, aby móc rozpoznawać najnowsze zagrożenia. Posiadając aktualną bazę danych, skanuje znajdujące się na dysku pliki w poszukiwaniu tych określonych fragmentów kodu. Po ich znalezieniu wyświetla komunikat na ekranie komputera o wykryciu zagrożenia. Następnie albo sam podejmuje decyzję o usunięciu zainfekowanych plików lub zostawia tę decyzję użytkownikowi.

Jak zapewnić maksymalną ochronę przy pomocy programu antywirusowego?

- Podstawową kwestią jest upewnienie się, że sygnatury są na bieżąco aktualizowane. Opcja automatycznego pobierania nowych baz danych znajduje się w ustawieniach każdego programu antywirusowego i powinna być domyślnie włączona. Wyszukiwanie wirusów odbywa się na dwa podstawowe sposoby: za pomocą automatycznej ochrony w czasie rzeczywistym i skanowania dysku.
- **Ochrona w czasie rzeczywistym** polega na skanowaniu wszystkich aktualnie używanych przez użytkownika plików, w tym tych wykorzystywanych przez uruchomione programy. Dzięki temu na przykład pobrany z internetu plik zostanie automatycznie sprawdzony pod kątem podejrzanych sygnatur. Takie działanie wykorzystuje przez cały czas część mocy obliczeniowej komputera, ale zapewnia wysoki poziom bezpieczeństwa. Dlatego należy upewnić się, że ta opcja również jest włączona.

- **Skanowanie dysku** polega natomiast na szukaniu złośliwego oprogramowania na wszystkich znajdujących się na nim plikach, także tych, które nie są aktualnie używane. Zdarza się, że wirusy znajdują się na dysku w stanie uśpienia i nie wykonują aktualnie żadnych działań. Ta czynność pozwala je znaleźć i unieszkodliwić, zanim zdążą spowodować szkody. Można je uruchomić ręcznie za pomocą odpowiedniej opcji w antywirusie zarówno dla całego dysku, jak i poszczególnych folderów. W wielu programach znajduje się jednak możliwość ustawienia automatycznego skanowania na przykład raz w tygodniu, ponieważ maksymalną ochronę komputera zapewni połączenie obu sposobów wyszukiwania szkodliwego oprogramowania.

Co to jest wirus komputerowy i jak działa?

Wirusa komputerowego w najprostszy sposób określić można jako program komputerowy bądź złośliwe oprogramowanie, stworzone z zamiarem wyrządzenia przeróżnych szkód na „zainfekowanym” urządzeniu. Każdy istniejący wirus cechuje się zdolnością do samopowielania, co jest elementem niezbędnym, aby program mógł zostać sklasyfikowany jako wirus. Wirusy komputerowe rozprzestrzeniane są poprzez „zarażone” wcześniej pliki, które następnie – zazwyczaj nieświadomie – umieszczane są w komputerach. Wirusy są w stanie wyrządzić **szereg niepożądanych i szkodliwych** efektów, takich jak:

- utrata kontroli nad zainfekowanym komputerem przez jego właściciela,
- wykradnięcie przechowywanych danych (wszystkich, włącznie z poufnymi, jak numery kont bankowych)
- kasowanie danych,
- spowalnianie pracy komputera (a także całkowite uniemożliwienie pracy na zainfekowanym urządzeniu),
- rozsyłanie tzw. „spamu” bez zgody oraz wiedzy właściciela urządzenia,
- występowanie niepożądanych elementów graficznych czy ścieżek dźwiękowych.

Jak zapobiegać występowaniu wirusów?

- Walka z wirusami trwa nieprzerwanie od lat, a pracują nad tym zarówno amatorzy, jak i specjaliści. W celu odpowiedniego zabezpieczenia swojego komputera zaleca się:
- **Korzystanie z programów antywirusowych** – na rynku istnieje cała masa programów stworzonych z myślą o bezpieczeństwie komputera. Z roku na rok jest

ich coraz więcej, oraz są coraz bardziej skuteczne. Programy antywirusowe pomagają zarówno wykryć zagrożenie wirusowe, uniemożliwić jego rozprzestrzenienie, a także je usunąć. Programy antywirusowe są ogólnodostępne, a wiele mogą być wykorzystywane przez użytkowników za darmo.

- **Ostrożność** – niewskazany jest pobieranie plików oraz otwieranie korespondencji internetowej z niezweryfikowanych źródeł. W pobieranych plikach bądź wiadomościach kryć mogą się niezwykle groźne wirusy. Dodatkowym zaleceniem jest zapoznawanie się z wszystkimi komunikatami, które pojawiają się na naszym urządzeniu.
- **Profilaktykę** – ważnym jest regularne skanowanie dysków za pomocą programów antywirusowych oraz aktualizowanie oprogramowania i systemu operacyjnego.

Jaki program antywirusowy wybrać? 10 najpopularniejszych programów. Ranking 2019

Avast Free Antivirus 2019

Avira Free Antivirus 2019

ClamWin Free Antivirus

Adaware Antivirus Free

Bitdefender Antivirus Free

Panda Dome

Kaspersky Free 2019

AVG AntiVirus FREE 2019

Instalacja programu avast! Free Antivirus

Aplikacja jest przeznaczona do użytku domowego i ma polskojęzyczny interfejs. Można ją pobrać ze strony producenta (www.avast.com).[Instalacja](#) zgodnie z instrukcją producenta

Strona z dostępem do darmowych programów antywirusowych

<http://di.com.pl/krok-po-kroku-instalacja-darmowego-programu-antywirusowego-37450>



UWAGA!!! - Instrukcja – instalacja programu antywirusowego. Wspólna instalacja programu antywirusowego na podstawie załączonej instrukcji/

Kontrola rodzicielska³⁶. Program do kontroli rodzicielskiej daje możliwość kontrolowania dzieci przy komputerze przez rodziców i opiekunów. Oprogramowanie kontroli rodzicielskiej pozwala blokować dostęp do stron pornograficznych oraz innych niestosownych materiałów. Rodzice mogą również ograniczyć korzystanie z danych programów, jak i ustawić limity czasowe, w których dzieci mogą logować się do komputera.

Przeglądanie Internetu³⁷. Tu zarządzać możemy dostępem naszej pociechy do witryn internetowych. Po pierwsze, możemy wyłączyć ogólnie dostęp do nieodpowiednich treści (seks, przemoc, wulgaryzmy). Te są definiowane za pomocą całkiem skutecznej techniki SafeSearch. Jeżeli jednak mamy wątpliwości, możemy też ręcznie dodać do listy witryny, do których na pewno dziecko może mieć dostęp, jak i te które mają zawsze być blokowane.

Aplikacje, gry i multimedia. W tej sekcji możemy definiować czy gry nieodpowiednie dla wieku naszej pociechy mają być blokowane, czy też nie. Dodatkowo możemy ogólnie zakazać dostępu do dowolnej wskazanej przez nas gry i aplikacji.

Godziny korzystania z urządzeń. W tej sekcji możemy dokładnie definiować ile czasu nasza pociecha może spędzać z komputerem lub konsolą. Możemy zarówno wskazywać to ogólnie (na przykład: trzy godziny dziennie) jak i bardzo konkretnie (na przykład: od 18:00 do 20:00). Ustawienie może być globalne lub dla każdego z dni tygodnia osobno. Możemy też osobno definiować dostęp do każdego z urządzeń (PC, konsola Xbox).

Zakupy i wydatki. Niektóre gry i aplikacje są płatne lub umożliwiają robienie zakupów. Jeżeli chcemy, możemy z poziomu tego menu naładować złotówkami konto naszego dziecka, by mogło robić zakupy do kwoty którą wpłaciliśmy. Możemy też kategorycznie zablokować jakiegokolwiek funkcje płatności w systemie, grach i aplikacjach.

Znajdź swoje dziecko. Ta funkcja, niestety, nie przyda nam się za bardzo, gdyż wymaga by nasza pociecha posiadała telefon z Windows 10 Mobile (patrząc po statystykach: raczej nie posiada). Jeżeli jednak jakimś cudem jest inaczej, to tu w każdej chwili możemy zobaczyć gdzie nasza pociecha aktualnie się znajduje.

³⁶ <https://www.spidersweb.pl/2017/09/jak-skonfigurowac-komputer-dla-dziecka.html>

³⁷ <https://www.spidersweb.pl/2017/09/jak-skonfigurowac-komputer-dla-dziecka.html>

Konfiguracja komputera dla dziecka jest prosta. Nie ma więc żadnego wytłumaczenia na brak uwagi poświęconej dziecięcemu kontu. To raptem kilkanaście klików myszką, dzięki którym naszej pociesze nie grozi uzależnienie od komputera ani ekspozycja na treści dla niej nieodpowiednie. Warto temu poświęcić naszą uwagę, korzyści są nie do przecenienia.

Informacje ze strony: <https://www.spidersweb.pl/2017/09/jak-skonfigurowac-komputer-dla-dziecka.html>



<https://www.youtube.com/watch?v=K8--mztOu9s> - film „Kontrola rodzicielska „

Popularne programy do kontroli rodzicielskiej

Alladyn 1.0 - Bezpieczna przeglądarka internetowa Alladyn jest przeznaczona dla dzieci w wieku przedszkolnym. Alladyn jest w pełni "profesjonalną" przeglądarką. Jediną różnicą jest brak wyszukiwarek "dla dorosłych" typu Google, Yahoo, itp. Zamiast, posiada tak znakomite wyszukiwarki stron dla dzieci jak Mamuu i Lupiko.

Anti-Porn - Program kontroluje i blokuje dostęp do gier komputerowych oraz innych programów zawierających treści nieodpowiednie dla danego użytkownika korzystającego z komputera. Aplikacja jest bardzo przydatna, jeżeli z jednego komputera korzysta cała rodzina. Wówczas można szybko zabezpieczyć dostęp do niechcianych stron lub innych elementów systemowych.

Anti-Porn rejestruje również wszystkie odwiedzane strony i zapisuje je w formie zrzutów ekranowych na dysku twardym komputera. Aplikacja nie posiada języka polskiego, ale nie stanowi to żadnego kłopotu, bowiem interfejs użytkownika jest prosty i bardzo czytelny.

Program dostępny jest w wersji testowej i pozwala na 7 dni darmowego użytkowania. Najczęściej pobierane narzędzia pozwalające kontrolować poczynania dziecka to [Beniamin](#), [Visual Porn Blocker Free](#) i [Opiekun Dziecka w Internecie](#).

/Wspólna instalacja programu do kontroli rodzicielskiej/



PRZYKŁADY ZADAŃ I ĆWICZEŃ

ĆWICZENIE:__ Zainstaluj wybrany przez siebie program antywirusowy według instruktażu trenera

ĆWICZENIE: Korzystając z zainstalowanego programu do kontroli rodzicielskiej zablokuj dostęp do stron pornograficznych, oraz ustaw dostęp do logowania dla dzieci – limit czasowy 2 godziny w sobotę i niedzielę.

Wideorozmowy



CELE I KOMPETENCJE:

- Umiejętność wykorzystania narzędzi komunikatorów oraz stron społecznościowych.
- Opanowanie umiejętności w zakresie korzystania z komunikatorów, prowadzenia wideokonferencji, rozmów na czacie.
- Nabycie umiejętności nawiązania rozmowy online z innymi użytkownikami portali społecznościowych.
- Poznanie portali społecznościowych.



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Czat oraz darmowe wideorozmowy w Facebook Messengerze

Portal społecznościowy Facebook w 2015 roku zaoferował swoim użytkownikom nową funkcję w aplikacji mobilnej Messenger służącej do obsługi chatu. Dzięki czemu użytkownicy największego portalu społecznościowego na świecie za pomocą swoich smartfonów i tabletów mogą prowadzić między sobą wideo rozmowy.

Messenger³⁸ to aplikacja Facebooka służąca do komunikacji pomiędzy użytkownikami portalu.

Do niedawna na urządzeniach mobilnych można było wykonywać jedynie połączenia głosowe. Teraz jednak usługodawca umożliwił użytkownikom prowadzenie rozmów wideo na Facebooku z aplikacji Messenger. To rozwiązanie może zastąpić komunikatory takie jak Skype, Hangouts i Facetime.

³⁸ **Facebook Messenger** - komunikator internetowy stworzony przez Facebooka. Służy do wysyłania wiadomości, zdjęć, filmów, naklejek i innych plików, a także pozwala reagować na wiadomości znajomych (tz. reakcje) oraz wchodzić w interakcje z botami. Usługa pozwala również na połączenia głosowe (także grupowe) oraz na wideorozmowy. Aplikacja ma możliwość szyfrowania wiadomości oraz grania w minigry.

DYSKUSJA, POKAZ: Przeprowadzanie wideorozmowy w aplikacji Facebook Messenger

Uczestniczenie w czacie na Facebook

Zaloguj się na swoje konto Facebook



UWAGA!!! Dla bezpieczeństwa swoich danych nigdy nie zapamiętuj hasła.

1. Przeprowadź rozmowę z dowolnie wybraną osobą

Przydatne aplikacje do wykorzystania – jak ich szukać?

Prowadząc konto na portalu społecznościowym, blog lub kanał na YouTube warto poznać możliwości innych programów i aplikacji, które pomogą nam w tworzeniu ciekawych i atrakcyjnych plików do zamieszczania ich na naszej stronie. Jeżeli interesujemy się jakąś dziedziną w życiu to warto stworzyć dobry podkład muzyczny lub grafikę naszej strony. Posłuża do tego różne darmowe programy, które bez problemu pobierzemy w darmowej wersji ze strony <https://www.dobreprogramy.pl>

Poniżej prezentujemy przykład instalacji programu do tworzenia filmów.



PRZYKŁADOWE ZADANIA I ĆWICZENIA

ĆWICZENIE: Instalacja programu GOM Mix Pro

1. Przed instalacją sprawdź jaki masz zainstalowany system na swoim komputerze
2. Sprawdź jaki masz typ systemu, czyli procesor: 32-bit, 64-bit
3. Uruchom stronę <https://www.dobreprogramy.pl>
4. Szukaj programu, który przeznaczony jest na taki typ systemu jak Twój.
5. W opcji licencji wybierz **BEZPŁATNA**
6. Wybierz jeden program, np. **GOM Mix Pro**
7. Uruchom plik instalacyjny z dysku i postępuj zgodnie kreatorem instalacyjnym.
8. Uruchom program – od tego momentu możesz montować własne filmy.

Zagrożenia internetowe



CELE I KOMPETENCJE CYFROWE:

- Nabycie wiedzy na temat zagrożeń w sieci, cyberprzemocy oraz zjawisk hate, fake news i innych.

- Poznanie typów zagrożeń dla informacji na portalach społecznościowych.
- Poznanie różnych grup i portali społecznościowych
- Nabycie umiejętności rozpoznawania zagrożeń w sieci
- Kształtowanie sprawności w przeglądaniu najpopularniejszych stron związanych z rozumieniem zjawiska hate, fake news, prawa autorskiego oraz ochrony wizerunku.
- Nabycie wiedzy na temat właściwego zachowania się w internecie



ZAKRES TREŚCI PROGRAMOWYCH I UWAGI O REALIZACJI

Zagrożenia w sieci (omówienie zagrożeń)

Bezpieczne korzystanie z portali społecznościowych i zarządzanie tożsamością oraz własnym wizerunkiem w sieci.

- Dyskusja na temat zagrożeń wynikających z korzystania z portali społecznościowych – wymiana doświadczeń i spostrzeżeń

Typy zagrożeń dla informacji na portalach społecznościowych.

- Omówienie typów zagrożeń dla informacji na portalach, typu: rozpoznawanie twarzy, pozyskiwanie danych, spam, wirusy, robaki, agregatory SNS, phishing, przejmowanie profili, utrata reputacji i inne
- Uświadomienie rodzicom, iż największą luką w zabezpieczeniach portali są sami użytkownicy
- Uboczne skutki dla dziecka wynikające z dostępu do nieodpowiednich treści.

Zawieranie znajomości w Internecie, zjawisko groomingu

Cyberprzemoc (agresja elektroniczna)

Zjawisko hate - mowa nienawiści (ang. hate speech)

Zjawisko fake news

Fake news – forma przekazywania informacji, która opiera się na celowej dezinformacji lub oszustwie, rozprzestrzeniana poprzez drukowane i nadawcze serwisy informacyjne, media elektroniczne czy serwisy społecznościowe³⁹. Informacje te są pisane i publikowane w celu

³⁹ **Serwis społecznościowy** – służy do budowania sieci społecznych oraz stosunkach społecznych, które opierają się na podobnych zainteresowaniach, wspólnym życiu zawodowym lub prywatnym, itp. Umożliwia kontakt ze znajomymi oraz dzielenie się informacjami, zainteresowaniami, itp. Różnorodność serwisów społecznościowych dostępnych obecnie w Internecie stwarza wyzwanie do stworzenia jednej definicji, istnieją jednak pewne cechy wspólne: serwisy społecznościowe opierają się na aplikacjach internetowych; treści tworzone przez użytkowników są siłą napędową

Najważniejsze niebezpieczeństwa na jakie może być narażone dziecko w Internecie.

Kontakt z nieodpowiednimi treściami

Korzystając z Internetu dziecko może zostać narażone na kontakt z nieodpowiednimi dla niego treściami (materiały pornograficzne, rasistowskie, propagujące przemoc, informacje o sektach i in.), a także może być zachęcane do podejmowania działań, które są nielegalne lub niebezpieczne.

Molestowanie fizyczne i wykorzystywanie seksualne

Istnieje ryzyko, iż korzystając z sieci, dziecko może dostarczyć obcym osobom informacji lub zaaranżować spotkanie, które może stanowić zagrożenie dla jego bezpieczeństwa lub bezpieczeństwa jego rodziny. W wielu przypadkach pedofile wykorzystują pocztę elektroniczną, chat roomy, grupy dyskusyjne, aby zdobyć zaufanie dziecka, a następnie zorganizować spotkanie w prawdziwym świecie.

Najczęstsze formy wykorzystywania seksualnego dzieci z użyciem Internetu to: prezentowanie dzieciom materiałów pornograficznych, pornografia dziecięca

(produkcja, dystrybucja, posiadanie), uwodzenie dzieci, prostytutka dziecięca, wirtualny seks.

Łamanie prawa

Dziecko może również zaangażować się w działalność, która jest nielegalna lub pociągą za sobą straty finansowe. Korzystając z aukcji internetowych, podając dane karty kredytowej rodziców itp. dziecko często staje się ofiarą różnych oszustów. Młodzi ludzie bywają nie tylko ofiarami nękania czy niewybrednych żartów, ale także bardzo często sami są ich autorami. Łamią prawo przesyłając wirusy, nielegalne treści, uprawiając hazard, jak również kopiując filmy i muzykę (m.in. za pośrednictwem programów P2P).

Zachęcanie do używania alkoholu, nikotyny, narkotyków

Niektóre strony www i grupy dyskusyjne zawierają informacje, które zachęcają dzieci i młodzież do korzystania ze środków uzależniających takich, jak: alkohol, nikotyna czy narkotyki.

portali; użytkownicy tworzą własne profile; usługi społecznościowe ułatwiają rozwój internetowych sieci społecznych poprzez łączenie profilu użytkownika z innymi osobami lub podmiotami o podobnych zainteresowaniach lub w jakimś stopniu z nimi powiązanymi.

Internet to wspaniałe narzędzie dla łatwego kontaktu z narkotykami. W 2007 roku znaleziono 238 , a w 2008 roku 347 polskich stron i adresów o narkotykach.

- wymiana informacji np. blogi (wspomnienia ponarkotykowe - „mój pierwszy raz”),
- wskazówki praktyczne np. jak brać lub jak uprawiać narkotyki,
- oferty handlowe bezpośrednio i pośrednio,
- upowszechnianie nowych środków – pseudonarkotyki (brak ich na liście narkotyków)
- top listy – ranking stron oferujących marihuanę - muzik listy – muzyka, która wpływa na podświadomość- młodzieży.

Kluby samobójców

W Internecie można znaleźć na forach lub blogach informacje jak skutecznie i bezboleśnie popełnić samobójstwo skupiające ludzi zagubionych w życiu, dość często szukających jak skutecznie pozbawić się życia.

Komercyjne wykorzystywanie dzieci

Rynek reklam kierowanych do dzieci rozszerza obecnie swój zasięg obejmując już nie tylko telewizję, ale także Internet. O ile jednak reklamy telewizyjne skierowane były na dzieci jako całość, reklamy online adresowane są często do konkretnego klienta. Zwiększa to znacznie prawdopodobieństwo sprzedaży danego produktu. Przykładem może tu być wykorzystanie bohatera popularnej kreskówki, który zwraca się do dziecka po imieniu, łamiąc w ten sposób tradycyjne bariery sprzedaży.

Zmiany w zdolności do odróżniania rzeczywistości od fantazji

Wiele dzieci korzysta z chat roomów, gdzie spotyka się wielu użytkowników np. biorących udział we wspólnej zabawie, grze. Przybierają oni różnorodne tożsamości i wcielają się w różne role. Badanie wskazują, iż niektóre dzieci uczestniczące w takich grach mogą stracić zdolność do odróżniania prawdziwego życia od komputerowej symulacji. Z czasem zaczynają coraz mocniej angażować się w tego typu wirtualne interakcje i spędzają coraz więcej czasu przed ekranem komputera

Uzależnienie od Internetu

Oprócz wielkich korzyści postępująca informatyzacja przyniosła nowe zagrożenia. Rośnie bowiem stale liczba osób uzależnionych od Internetu i gier komputerowych. Popularność gier przekroczyła wszelkie oczekiwania i oceniana jest jako prawdziwy fenomen

socjologiczny lub wręcz zjawisko kulturowe. Ale też powodowane przez nie efekty destrukcyjne stają się poważnym problemem społecznym i zdrowotnym.

Do niedawna uzależnienie od komputera stanowiło w Polsce problem czysto teoretyczny, który interesował głównie specjalistów. W ciągu ostatnich dwóch lat stało się problemem realnie występującym, z którym trzeba będzie się zmierzyć. Należy się spodziewać, że wzrastająca dostępność komputerów, a więc także Internetu i gier, oraz upowszechnienie umiejętności posługiwania się medium informatycznym spowodują narastanie typowych zaburzeń, zwłaszcza u dzieci i młodzieży. Bowiem w Polsce, w odróżnieniu od krajów wysoko uprzemysłowionych, statystyczny użytkownik komputera jest człowiekiem bardzo młodym. Jak wiadomo proces uzależniania się osób młodych, z nie do końca uformowaną osobowością, przebiega znacznie szybciej.

Gry komputerowe

Coraz młodsze dzieci uczą się obsługiwać komputer, który stanowi dla nich interesującą zabawkę. Zaczynają zwykle od najprostszych symulacyjnych gier sprawnościowych (odbijanie piłeczki, detonowanie min czy prowadzenie samochodu). Z czasem przechodzą do gier przygodowych czy bardziej skomplikowanych gier strategicznych wymagających umiejętności planowania. Zabawa okazuje się niezwykle wciągająca i łatwo prowadzi do uzależnienia się. Dumni ze sprawności swego dziecka rodzice, zwłaszcza ci, którzy sami nie potrafią posługiwać się komputerem, często nie są świadomi negatywnych konsekwencji nadmiernego zainteresowania grami i nie kontrolują dostatecznie działań dzieci. Spędzają one coraz więcej czasu przy monitorze tracąc zainteresowanie innymi rodzajami aktywności. T. Zyss i J. Boroń z Collegium Medicum UJ badając mechanizm uzależnienia od gier postawili pytanie, jakie gratyfikacje uzyskuje osoba grająca, które motywują ją do ciągłego podejmowania gry, i które rekompensują jej zmęczenie fizyczne oraz ograniczenie kontaktów interpersonalnych. Z przeprowadzonej analizy wynika, iż komputer jest traktowany przez

grającego jako bezpieczny i niezwykle atrakcyjny partner.

Umożliwia zaspokajanie różnorodnych potrzeb i popędów niemożliwych do zrealizowania w rzeczywistości (np. potrzeby osiągnięć, więzi czy potrzeby seksualnej).

Podobnej satysfakcji i poczucia bezpieczeństwa nie zapewniają kontakty z ludźmi, którzy mogą obrażać się, wyszydzać, znudzić i spowodować poczucie odrzucenia i przegranej. Poza tym kontakt z komputerem stwarza możliwość interakcji dając iluzję kontaktu

interpersonalnego. Autorzy stwierdzają, że świat gier jest szczególnie atrakcyjny dla osób młodych, sfrustrowanych i zagubionych, szukających dowartościowania. Bardzo pociąga on osobowości histeryczne i narcystyczne żyjące w świecie wyobraźni i mające trudności z oceną własnej wartości. Wymienione grupy osób łatwo wpadają w pułapkę uzależnienia.



TUTORIALE, SAMOUCZKI, FILMY INSTRUKTAŻOWE

<https://www.youtube.com/watch?v=nI1DBZ6KNB4> – film „Co to jest PEGI

<https://www.youtube.com/watch?v=iDxUPmlQaNk> – film „Jak rozpoznać, że jesteśmy uzależnieni od gier komputerowych”

Chorzy na Internet

Sieć internetowa ma bardzo bogatą ofertę i dla wielu osób przebywanie w niej jest ogromnie wciągające. Problem zaczyna się wówczas, gdy czas i sposób użytkowania Internetu wymyka się spod kontroli. Sieć niepostrzeżenie zaczyna rządzić użytkownikiem. Dla zjawiska nałogowego, kompulsywnego przebywania w sieci ukuto już wiele nazw. Często używa się terminów: sieciorizm, infoholizm, dataholizm albo netmania. Uważa się, że powstała nowa jednostka zaburzeń psychicznych, jeszcze nie do końca zbadana, która wkrótce zostanie wpisana do międzynarodowych systemów klasyfikacji zaburzeń DSM IV i ICD-10. Ostatnio w pracach amerykańskich najwięcej zwolenników zyskuje termin Internet Addiction Disorder (w skrócie IAD), który można przetłumaczyć jako Zespół Uzależnienia od Internetu. Mechanizm powstawania zaburzenia jest taki sam jak w uzależnieniach od środków psychoaktywnych.

Zagrożenia zdrowia fizycznego

nadwyrężony kark, wada postawy, zmęczony wzrok, brak sprawności ruchowej, hałas – nadmierne powoduje zmęczenie układu nerwowego – 35-70 db.

Następstwa IAD (Zespół uzależnienia od Internetu) są bardzo poważne. W sferze fizycznej obserwuje się następujące objawy: zaburzenia wzroku, trwałe wady kręgosłupa, zwiotczenie mięśni (z braku ruchu), anemię (nie ma czasu na jedzenie), zaburzenie rytmów dobowych, bezsenność. U dzieci i młodzieży może wystąpić również „padaczka ekranowa” wywołana przez intensywne, szybko zmieniające się bodźce świetlne emitowane przez ekran. Najważniejsze skutki psychologiczne i społeczne to: niepokój, lęk, stany depresyjne, rozdrażnienie, zaburzenia koncentracji uwagi i pamięci, częste kłamstwa, konflikty z

otoczeniem, zanik więzi emocjonalnych z bliskimi osobami (wyczerpujący opis IAD zawiera praca K. Świrzbina (<http://infoholizm.e-sfera.pl/>)).

Cyberprzemoc (agresja elektroniczna) – stosowanie przemocy poprzez: prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem Internetu i narzędzi typu elektronicznego takich jak: SMS, e-mail, witryny internetowe, fora dyskusyjne w Internecie, portale społecznościowe i inne⁴⁰.

Cyberprzemoc niesie ze sobą równie zgubne konsekwencje, jak przemoc ze świata realnego. To że nie mamy kontaktu fizycznego i wzrokowego z prześladowcą nie oznacza że jesteśmy bezpieczni. Dzięki technologii narodził się nowy sposób na przemoc. Zatrważająca jest szybkość z jaką się rozpowszechnia. To może być kompromitujące zdjęcie lub nieprawdziwa informacja. Nie ma znaczenia pora dnia i nocy, bo w każdej chwili z łatwością mogą dołączyć do grupy agresorów nowe osoby. Całkowite usunięcie tych treści często bywa trudne a czasem wręcz niemożliwe. Najbardziej na cyberprzemoc narażone są dzieci i młodzież, dlatego że dorośli często nie zdają sobie sprawy co dzieje się w ich sieciowym świecie.

Cyberprzemoc zawiera w sobie nowe zjawiska jakim jest hate i fake news

Zjawisko hate

Mowa nienawiści (ang. hate speech) jest zjawiskiem, które polega na używaniu języka w celu rozbudzenia, rozpowszechniania czy usprawiedliwiania nienawiści i dyskryminacji, jak również przemocy wobec konkretnych osób, grup osób, przedstawicieli mniejszości czy jakiegokolwiek innego podmiotu będącego „na celowniku” danej wypowiedzi. Akceptacja mowy nienawiści w wymiarze społecznym prowadzi do utrwalania się stereotypów, uprzedzeń i powodując mniejszą akceptację przedstawicieli grup 'hejtowanych' może także prowadzić do tzw. przestępstw z nienawiści (ang. hate crimes). Mowa nienawiści przyjmuje różne formy i dlatego istnieje trudność w jednoznacznym określeniu czym ona dokładnie jest. Mimo iż żadna z wielu powstałych dotychczas definicji tego zjawiska nie jest powszechnie akceptowana i używana, to dosyć często mowę nienawiści rozumie się zgodnie z definicją Rady Europy⁴¹.

⁴⁰ <https://pl.wikipedia.org/wiki/Cyberprzemoc>

⁴¹ <http://uprzedzuprzedzenia.org/czym-mowa-nienawisci/>



TUTORIALE, SAMOUCZKI, FILMY INSTRUKTAŻOWE

https://www.youtube.com/watch?v=MIhfiQ_SV4 - film – „Czym jest przestępstwo na tle nienawiści?”

Zjawisko fake news

Fake news – forma przekazywania informacji, która opiera się na celowej dezinformacji lub oszustwie, rozprzestrzeniana poprzez drukowane i nadawcze serwisy informacyjne, media elektroniczne czy serwisy społecznościowe⁴². Informacje te są pisane i publikowane w celu wprowadzenia w błąd, albo w celu uzyskania finansowych lub politycznych korzyści. Często stosują chwytliwe nagłówki w celu zwrócenia możliwie dużej uwagi. Należy rozróżnić nieprawdziwe i wprowadzające w błąd fałszywe wiadomości od satyry lub parodii, która jest przeznaczona dla humoru, ale nie ma na celu wprowadzenia w błąd odbiorców

Materiały do wykorzystania podczas zajęć:

Do stwierdzenia uzależnienia można posłużyć się Testem Kimberly Young⁴³:

1. Czy stajesz się ożywiony, gdy myślisz o ostatniej lub następnej sesji z Internetem?
2. Czy czujesz potrzebę stałego zwiększania czasu spędzonego w Sieci?
3. Czy próbowałeś kilkakrotnie i bez powodzenia kontrolować, zmniejszać lub w ogóle zaprzestać korzystania z Internetu?
4. Czy czujesz się niespokojny, podirytowany lub bliski depresji, gdy próbujesz zredukować ilość i długość trwania sesji
5. Czy pozostajesz w sieci dłużej, niż pierwotnie planowałeś?
6. Czy z powodu Internetu naraziłeś na szwank związki z bliskimi, pracę lub szkołę?
7. Czy kłamałeś, aby ukryć, jak wiele czasu spędzasz w Internecie?
8. Czy używasz sieci jako sposobu na ucieczkę przed problemami lub na uśmierzanie przykrego nastroju (poczucia bezradności, winy, niepokoju, depresji)?

⁴² **Serwis społecznościowy** – służy do budowania sieci społecznych oraz stosunkach społecznych, które opierają się na podobnych zainteresowaniach, wspólnym życiu zawodowym lub prywatnym, itp. Umożliwia kontakt ze znajomymi oraz dzielenie się informacjami, zainteresowaniami, itp. Różnorodność serwisów społecznościowych dostępnych obecnie w Internecie stwarza wyzwanie do stworzenia jednej definicji, istnieją jednak pewne cechy wspólne: serwisy społecznościowe opierają się na aplikacjach internetowych; treści tworzone przez użytkowników są siłą napędową portali; użytkownicy tworzą własne profile; usługi społecznościowe ułatwiają rozwój internetowych sieci społecznych poprzez łączenie profilu użytkownika z innymi osobami lub podmiotami o podobnych zainteresowaniach lub w jakimś stopniu z nimi powiązanymi.

⁴³ <https://poradniapraxis.pl/skale-samooceny,32.html>

Interpretacja wyników.

Za uzależnioną uznaje się osobę, która odpowie twierdząco na co najmniej pięć pytań. Jednak odpowiedzi mogą zostać zafałszowane przez krzepiące autooszustwa badanego! Opierając się na kryteriach diagnostycznych uzależnień wg ICD-10 uzależnienie od Internetu rozpoznaje się wówczas, kiedy w okresie ostatniego roku stwierdzono obecność co najmniej trzech objawów z poniższej listy:

1. silną potrzebę lub poczucie przymusu korzystania z Internetu;
2. subiektywne przekonanie o mniejszej możliwości kontrolowania zachowań związanych z Internetem, tj. upośledzenie kontroli nad powstrzymywaniem się od korzystania z Internetu oraz nad długością spędzania czasu w Internecie;
8. występowanie, przy próbach przerwania lub ograniczenia korzystania z Internetu, niepokoju, rozdrażnienia czy gorszego samopoczucia oraz ustępowanie tych stanów z chwilą powrotu do komputera;
9. spędzanie coraz większej ilości czasu w Internecie w celu uzyskania zadowolenia czy dobrego samopoczucia, które poprzednio osiągnąć było w znacznie krótszym czasie;
10. postępujące zaniedbywanie alternatywnych źródeł przyjemności lub dotychczasowych zainteresowań na rzecz Internetu;
11. korzystanie z Internetu pomimo szkodliwych następstw (fizycznych, psychicznych i społecznych), o których wiadomo, że mają związek ze spędzaniem czasu w Internecie

Wskazówki dla rodziców, nauczycieli i osób dorosłych przebywających z dzieckiem, w tym pracowników GOK prowadzących zajęcia z dziećmi.

1. Postaraj się, aby komputer, z którego korzysta twoje dziecko stał we wspólnym pomieszczeniu.
2. Ustal zasady korzystania z Internetu:
 - rozmawiaj z dzieckiem na temat tego, co może i czego nie może robić korzystając z sieci
 - ustal z dzieckiem co wolno, a czego nie i egzekwuj to. Ustalając zasady bądź wyrozumiały i miej rozsądne wymagania. Staraj się zrozumieć potrzeby twojego dziecka, jego zainteresowania i naturalną ciekawość
3. Rozmawiaj z dzieckiem o potencjalnych zagrożeniach:

- .zapoznaj je z zasadami bezpiecznego korzystania z Sieci (możesz je znaleźć na stronach tego poradnika pod hasłem Wskazówki dla dzieci i Wskazówki dla nastolatków
- naucz je krytycznego podejścia do informacji przeczytanych w Internecie. Twoje dziecko powinno mieć świadomość □, że nie wszystkie informacje znalezione w Sieci są wiarygodne i warto czasem je zweryfikować korzystając z innych źródeł takich, jak encyklopedie, słowniki itp.)

4. Interesuj się tym, co twoje dziecko robi w sieci i rozmawiaj z nim o tym:

- surfuj po sieci razem z dzieckiem
- poproś je, aby pokazało ci swoje ulubione strony
- .wskaz mu ciekawe i przyjazne strony (listę takich stron możesz znaleźć w edukacyjnym serwisie internetowym – <http://www.sieciaki.pl/>, <http://www.kidprotect.pl/> lub <http://www.strefawiedzy.polska.pl/>)

5. Postaraj się poznać internetowych przyjaciół twojego dziecka, tak jak robisz to w przypadku innych jego kolegów. W przypadku małego dziecka sprawdzaj e-maile, które otrzymuje.

6. Jeśli twoje dziecko korzysta z czatów lub e-maila:

- naucz je, by nie podawało w Internecie swoich danych osobowych takich jak: imię i nazwisko, adres domowy, telefon, adres szkoły
- naucz je, by nie odpowiadało na obraźliwe lub niebezpieczne e-maile, czaty i in.

7. Ustal, że nie wolno umawiać się z osobami poznanymi w sieci bez twojej zgody.

8. wyjaśnij dziecku, że osoba poznana w sieci nie zawsze musi być tym za kogo się podaje („12-letnia dziewczynka" może okazać się 40-letnim mężczyzną) jeśli dziecko chce się spotkać z internetowym znajomym, zadbaj o to, aby spotkanie odbyło się w miejscu publicznym, w twojej obecności lub gdy dziecko jest starsze – w obecności koleżanki lub kolegi

8. Naucz swoje dziecko, że zawsze może przyjść do ciebie, jeśli znajdzie w Internecie lub w swojej poczcie treści, które go zaniepokoją, zawstydzą lub sprawią, że poczuje się skrępowane. Zgłoście taki incydent do punktu kontaktowego <http://www.hotline.org.pl/>

9. Przypominaj dziecku, że w Internecie również obowiązują zasady dobrego wychowania, że należy być uprzejmym, miłym, nie używać obraźliwego słownictwa itp. (zasady NETYKIETY znajdziesz na stronie <http://www.sieciaki.pl/>)

10. Korzystaj z programów filtrujących i przeglądark:

- programy filtrujące mają za zadanie chronić dzieci blokując wyświetlanie dziecku stron ze szkodliwymi treściami, najpopularniejsze obecnie na rynku to – Cenzor, Opiekun oraz x-Guard
- przeglądarki internetowe (np. Internet Explorer) pozwolą ci sprawdzić jakie strony odwiedza twoje dziecko

11. Korzystaj z pomocy specjalistów:

- jeśli coś wzbudziło twoje wątpliwości, czujesz, że coś niepokojącego dzieje się z twoim dzieckiem, poproś o pomoc specjalistę – kogoś, kto zna się na komputerach, psychologa czy pedagoga
- możesz zwrócić się np., do Fundacji Dzieci Niczyje <http://www.fdn.pl/> lub do Fundacji Kidprotect <http://www.kidprotect.pl/>.
- Pamiętaj, że Internet to nie tylko niebezpieczeństwo i zagrożenia, ale również doskonałe źródło wiedzy i rozrywki.

Zasady bezpiecznego korzystania z Internetu – dla nastolatków

Cyberprzestrzeń jest jak wielkie miasto. Możesz znaleźć tam biblioteki, uniwersytety, muzea, miejsca rozrywki oraz możliwość spotkania wielu wspaniałych ludzi. Niestety możesz tam spotkać ludzi lub sprawy, których powinieneś unikać. **Znając niebezpieczeństwa i sposoby ich uniknięcia możesz bezpiecznie korzystać z Internetu.**

- Ustal wspólnie z rodzicami zasady korzystania z Internetu. Ustalcie kiedy i jak długo możesz przebywać w Sieci, z jakich serwisów internetowych możesz korzystać. Umowa z rodzicami nie oznacza rezygnacji z twojej prywatności czy twoich praw. Jest ona po prostu uzgodnieniem waszego wspólnego stanowiska opartego na wzajemnym zaufaniu i zrozumieniu.
- Chroń swoją prywatność w Sieci. Jeśli bierzesz udział w jakimkolwiek forum publicznym w internecie, nie podawaj swojego nazwiska, adresu mailowego, numeru telefonu, nazwy szkoły oraz innych informacji, które mogłyby pozwolić na ustalenie twojej tożsamości (dotyczy to również danych twoich rodziców, rodzeństwa, znajomych).
- Nie wysyłaj swoich zdjęć osobom, których nie znasz, bez porozumienia z rodzicami.
- Odpowiadaj mądrze na otrzymane wiadomości. Nigdy nie odpowiadaj na wiadomości (e-maile, komentarze na czacie, IM, grupy dyskusyjne, itp.), które sprawiają, że czujesz się skrępowany, zmieszany lub zaniepokojony. Gdy otrzymasz



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



taką wiadomość, powiedz o tym rodzicom lub innym dorosłym, do których masz zaufanie. Zgłoście taki incydent do punktu kontaktowego <http://www.hotline.org.pl/>

- Bądź ostrożny korzystając z chat roomów. Chat room jest prawdopodobnie najbardziej niebezpiecznym obszarem w Internecie. Nigdy nie możesz mieć pewności z kim naprawdę rozmawiasz. Możesz spotkać tam wielu przyjaznych i ciekawych ludzi. Pamiętaj jednak, że czaty są również wykorzystywane przez pedofili do poszukiwania swoich ofiar, szczególnie wśród nastolatków. Nigdy nie podawaj swoich danych osobowych i nie organizuj spotkań w „realu” bez wiedzy rodziców.
- Nigdy nie umawiaj się z osobami, które poznałeś w Sieci, bez zgody rodziców. Pamiętaj, że ludzie nie zawsze są tymi za kogo się podają. Jeśli jednak chcesz się spotkać z internetowym znajomym, porozmawiaj o tym najpierw z rodzicami i nigdy nie idź na takie spotkanie sam. Zadbaj o to, aby spotkanie odbyło się w miejscu publicznym, które dobrze znasz.
- Bądź podejrzliwy, jeśli ktoś, kogo poznałeś na czacie próbuje nastawiać cię przeciwko rodzicom, opiekunom, nauczycielom czy przyjaciołom. Niektóre czaty wykorzystywane są przez pedofili, sekty i inne niebezpieczne grupy do nakłaniania młodych ludzi, by zrobili coś, czego nie chcieliby robić
- Bądź ostrożny, jeśli ściągasz coś do swojego komputera ze strony www. Niektóre strony www proszą o pozwolenie na załadowanie jakiegoś programu lub „podłączenie się”. Programy te w niektórych przypadkach mogą być wykorzystywane później do przesyłania ci jedynie irytujących reklam. Niestety często są również używane do ingerowania w twoją prywatność, śledzenia tego, co robisz w danej chwili w sieci czy wprowadzania wirusów do twojego komputera. Mogą one zamienić twój komputer w serwer, z którego ktoś nieznajomy będzie mógł swobodnie korzystać, np. pobierając bez twojej zgody twoje fotografie, prywatne dokumenty i in. Nie wgrzywaj żadnych programów, jeśli nie masz pewności, że pochodzą one z godnego zaufania źródła.
- Jeśli masz swój blog, musisz mieć świadomość, że jest on dostępny każdemu kto korzysta z Internetu. Pamiętaj o tym zamieszczając w blogu informacje o sobie. Zastanów się, jakie wiadomości na swój temat chciałbyś tam umieścić i czy naprawdę powinieneś to zrobić. Wszystko, co umieścisz w blogu może być nie tylko przeczytane przez innych użytkowników sieci, ale także z łatwością kopiowane i

przechowywane, a w przyszłości może zostać wykorzystane przeciwko tobie. To, co teraz wydaje ci się fajne i zabawne, może okazać się niestosowne i kłopotliwe kilka lat później, np. gdy będziesz się starał o przyjęcie do szkoły czy pracy. Powinieneś też uważać, co mówisz o członkach swojej rodziny, znajomych i przyjaciółach, aby nie sprawić im przykrości czy wręcz narazić na niebezpieczeństwo.

- Pamiętaj, że w Internecie również obowiązują zasady dobrego wychowania. Nie rób niczego, co mogłoby urazić innych użytkowników lub byłoby sprzeczne z prawem.

BIBLIOGRAFIA

- Andrzejewska A., Bednarek J., Szarżała D., *Cyberprzestrzeń – szanse, zagrożenia, uzależnienia*, Wydaw. Pedagogium, Warszawa 2007.
- Andrzejewska A., *Dziecko w cyberprzestrzeni*, Wydaw. Pedagogium, Warszawa 2007.
- Andrzejewska, *(Nie)bezpieczny komputer*, Wydaw. APS, Warszawa 2008.
- Bednarek J., *Multimedia w kształceniu*, Wydaw. PWN, Warszawa 2006.
- Gała A., Ulfik I. (red.), *Oddziaływanie „agresywnych” gier komputerowych na psychikę dzieci*, Wydaw. UMCS, Lublin 2000

Aby bezpieczniej korzystać z Internetu, wykorzystuj następujące metody:

1. *Bądź anonimowy.* Jeśli nie musisz podawać swoich danych prywatnych — nie rób tego. Im mniej informacji o tobie jest w sieci, tym jesteś bezpieczniejszy.
2. *Ustaw „silne” hasła.* Ważne, aby twoje hasła były jak najdłuższe. Miej wiele haseł i czasem je zmieniaj.
3. *Sprawdzaj, czy łączyz się bezpiecznie (przez połączenie https://).* Bezpieczne połączenia oznacza się za pomocą zielonego zaznaczenia lub kłódeczki koło paska adresu. Czasem występuje problem z bezpieczeństwem połączenia i pojawiają się ostrzeżenia o błędach certyfikatu. Nie ignoruj ich, zwłaszcza jeśli witryna nie jest godna zaufania lub wcześniej nie pojawiał się na niej błąd.
4. *Zainstaluj program: Adblock, NoScript, Flashblock, Cookie Monster.* Te programy blokują niepożądane elementy stron. Np. Adblock nie tylko usunie reklamy, lecz także ograniczy przepływ informacji o historii przeglądania.
5. *Stosuj tryb prywatny w przeglądarkach.* Jest przydatny, jeśli korzystasz z komputera dostępnego dla innych osób. Po zakończeniu sesji kasowana jest cała jej historia oraz ciasteczka.

6. Wyloguj się po pracy. Nie można o tym zapomnieć!

DYSKUSJA:

- *Jak rodzice mogą pomóc dzieciom w zminimalizowaniu tych zagrożeń?*
- *Gdzie szukać pomocy, jak rozpoznać zagrożenie?*
- Zapoznanie się z edukacyjno-informacyjną zawartością serwisu
- Wprowadzenie pojęcia grooming, pornografia dziecięca, cyberprzemoc,
- Skutki zawierania znajomości w Internecie
- Dziecko jako ofiara cyberprzestępstwa
- Rodzaje i źródła przemocy
- Gdzie szukać pomocy? Jakie kroki podjąć
- *Kontakt z Policją jeśli doszło do złamania prawa*
- www.helpline.org.pl
- *zadzwoń pod bezpłatny numer telefonu 0 800 100 100. Jest to bezpłatna i anonimowa pomoc telefoniczna i online dla rodziców i nauczycieli, którzy potrzebują wsparcia i informacji w zakresie przeciwdziałania i pomocy dzieciom przeżywającym kłopoty i trudności wynikające cyberprzemocy, agresji i innych*
- *FDN „Ogólnopolski telefon zaufania dla dzieci i młodzieży 116 111”.*
- www.safeinternet.pl
- www.nask.pl
- www.dbi.pl
- *Jaką pomoc powinna dać szkoła gdy dziecko stało się ofiarą cyberprzemocy*
- *Ochrona dzieci- Sposoby na zapewnienie bezpieczeństwa dziecku w Internecie warto dostosować do jego wieku. Młodszym dzieciom warto towarzyszyć podczas korzystania z Internetu, a komputer w domu ustawić w widocznym miejscu. Zawsze warto zabezpieczyć sprzęt i mieć kontrolę nad stronami, jakie odwiedza dziecko oraz wskazać strony dedykowane młodszym internautom, gdzie dostęp do szkodliwych treści jest zniwelowany. - Warto zainstalować bezpłatną przeglądarkę stron www BeSt dedykowaną dzieciom w wieku od 3 do 10 lat. Jest ona dostępna także w wersji na urządzenia mobilne działające na systemie Android. Znajdź informację o rekomendowanych stronach dla dzieci i młodzieży w wiarygodnych serwisach, np. bestapp.fdn.pl (katalog aplikacji dziecięcych, w którym można pobierać*

bezpieczne aplikacje dla dzieci w wieku przedszkolnym). - Jeśli dziecko często korzysta z przeglądarki Google, zainstaluj filtry blokujące grafikę i filmy zawierające elementy pornografii. Skorzystaj jednocześnie z oprogramowania filtrującego, narzędzi kontroli rodzicielskiej i ustawień bezpieczeństwa w urządzeniach mobilnych, co pozwoli na lepszą kontrolę oglądanych treści, bez zaglądania dziecku przez ramię. - Pokaż dziecku, jak należy weryfikować dostępne treści, zainteresuj się informacją, jakie dziecko lubi oglądać filmy lub grać w gry. Sprawdzaj również limity wieku na grach i filmach (tzw. PEGI umieszczone na opakowaniach), którym dziecko poświęca czas.- Rodzice powinni zwracać szczególną uwagę na zmiany w zachowaniu dziecka i pamiętać że długie korzystanie z komputera szkodzi zdrowiu. Dziecko musi mieć zapewnione inne zajęcia, które pozwolą się bawić, odpoczywać i rozwijać na wielu płaszczyznach. - Starsze dzieci potrzebują więcej autonomii i tu rodzice muszą wiedzieć, jak je chronić, ale nie burzyć jego potrzeby samodzielności i samodecydowania. Kluczowa jest rozmowa, kontakt, ustalenie zasad i konsekwentne ich przestrzeganie. -Rodzice nie zawsze wiedzą, jak pomóc dziecku unikać szkodliwych treści, na co zwrócić uwagę. Wynika to z ich dorastania w świecie bez tylu wirtualnych atrakcji co dziś, jednak by uniknąć późniejszych kłopotów, warto sięgnąć po wiedzę i skupić się na tym temacie dla dobra dziecka.

- Kursy dla rodziców: Jeżeli chcesz dowiedzieć się więcej na temat tego, jak pomóc dzieciom unikać szkodliwych treści w Internecie, skorzystaj z bezpłatnego kursu internetowego dla rodziców Bezpiecznie Tu i Tam, który przygotowała Fundacja Orange. Kurs dostępny jest pod adresem: <http://www.fundacja.orange.pl/kurs>.

Przykłady różnych serwisów społecznościowych

- Serwisy i portale dla rodziców
 - <https://dyzurnet.pl/>
 - <http://www.edziecko.pl/>
 - <http://dzidziusiowo.pl/>
- Fora dla rodziców:
 - <http://www.familie.pl/Forum-3-170-1>
 - <http://dzidziusiowo.pl/forum>
 - <https://www.maluchy.pl/forum/>

- o <http://forum.mamotoja.pl/forum/>

[GoldenLine](#), [Profeo.pl](#), [MySpace](#), [Wykop](#), [Twitter](#), [Blip](#), [Fotka.pl](#), [Digart.pl](#)

- Broszura dla rodziców „Chroń dziecko w sieci”



TUTORIALE, SAMOUCZKI, FILMY INSTRUKTAŻOWE - Zagrożenia dla dzieci i młodzieży związane z treściami internetowymi (filmy)

- <https://www.youtube.com/watch?v=FIAILWDITj0> – film „Monitorowanie Internetu pod kątem nielegalnych treści”
- <https://www.youtube.com/watch?v=ExpTrtluTic> – film „Dyżurnet.pl - zgłoś nielegalne treści z sieci”
- <https://www.youtube.com/watch?v=N8jw5RpW73E> – film „Zainspirowani - Magazyn WTK | #56 - dyżurnet.pl ostrzega przed wrzuceniem zdjęć dzieci do sieci”
- <https://www.youtube.com/watch?v=K8--mztOu9s> - film „Kontrola rodzicielska – Android”

DYSKUSJA: wymienienie sytuacji z życia:

- w których najmniej dba się o bezpieczeństwo korzystania z internetu,
- w których należy pozostać anonimowym albo ujawnić swoją tożsamość.

Netykieta to zbiór zasad przyzwoitego zachowania w Internecie.

Na poziomie komunikacji elektronicznej zarówno na blogach, stronach internetowych, jak i poczcie elektronicznej powinno się przestrzegać określonych zasad. Są to:

- zakaz stosowania wulgaryzmów,
- zakaz wysyłania SPAMU,
- duże załączniki w e-mailu pakujemy programem do kompresji, żeby nie zapychać odbiorcy skrzynki,
- nie cytujemy całych wiadomości,
- wiadomości powinny mieć temat,
- listy e-mailowe piszemy w formacie tekstowym, a nie HTML-u
- unikamy błędów w tekście listu, używamy narzędzi do sprawdzania pisowni,
- nie piszemy tekstów dużymi literami,
- na forach dyskusyjnych należy pisać konkretnie i na temat
- szanujemy prywatność innych – nie piszemy np. na blogu o prywatnych sprawach znajomych,

- nie wolno kopiować, plagiatować i wklejać cudzych tekstów bez podawania przypisu czy źródła.

Działania, odpowiedzialnego rodzica kiedy dziecko padło ofiarą cyberprzemocy

- **Nie ograniczaj dziecku dostępu do Internetu**, nie zabraniaj mu korzystać ze smartfona. Może odebrać to jako karę (nawet jeśli Twoją intencją jest ochrona przed dalszymi atakami). Następnym razem, gdy coś złego spotka je w sieci, nie zwróci się do Ciebie o pomoc.
- Pamiętaj, że **cyberprzemoc często realizowana jest wieloma kanałami** równocześnie – mailowo, na portalach społecznościowych, z użyciem specjalnie tworzonych w tym celu fałszywych stron www, poprzez komunikatory (również w grach komputerowych), SMSy i MMSy.
- Porozmawiajcie o tym, co się wydarzyło. **Ustal jak najwięcej szczegółów** dotyczących przebiegu wydarzeń. To może być dla dziecka bardzo trudne – wykaż zrozumienie i spróbuj je przekonać, że tylko znając całą sytuację możesz mu pomóc. Nie komentuj wypowiedzi, a w żadnym razie nie sugeruj, że może „zastąpiło” na takie zachowanie (to powodują np. pytania w stylu „A co zrobiłaś/eś wcześniej, czy ta osoba może być na ciebie zła?”).
- Umów się z dzieckiem, aby zgłaszało Ci każdą sytuację nękania w sieci. Poproś je również, aby nigdy nie kasowało wiadomości, komentarzy czy zdjęć. Niech je przekazuje Tobie. Zapewnij je, że nie będziesz go oceniać, niezależnie od tego, jak przykre, zawstydzające czy upokarzające materiały Ci pokaże. Wyjaśnij, że jest to potrzebne, by mogło otrzymać Twoją pomoc!
- **Zabezpiecz dowody** – zapisz i wydrukuj wszystkie wiadomości i zdjęcia, zapisz filmy. Zrób kopie stron internetowych i portali, na których pojawiły się obraźliwe treści, zapisz adresy stron i nazwy użytkowników.
- Jeśli cyberprzemoc ma charakter mowy nienawiści (np. związanej z wyznaniem, kolorem skóry czy pochodzeniem dziecka) – **zgłoś incydent**. Możesz także zgłosić niewłaściwe treści do usunięcia administratorowi strony.
- Jeśli przemoc online trwa i nasila się, **powiadom policję**.
- Poradź dziecku, aby **nie utrzymywało kontaktu ze sprawcą cyberprzemocy**, nie odpowiadało na obraźliwe komentarze itp.

- **Zasugeruj zmianę ustawień** komunikatorów czy profili w mediach społecznościowych. Chodzi o to, by nikt spoza listy kontaktów nie mógł do niego pisać.
- **Porozmawiaj ze szkolnym psychologiem lub pedagogiem.** Jeśli podejrzewasz lub wiesz, że sprawcą cyberprzemocy jest inne dziecko ze szkoły, przekaz tę informację. Poproś o podjęcie interwencji (usunięcie obraźliwych treści, adekwatne przeprosiny, ew. podjęcie interwencji wychowawczej wobec sprawcy cyberprzemocy). Dobrym pomysłem może być też przeprowadzenie warsztatów uwrażliwiających na zjawisko cyberprzemocy itp.

Najważniejsze: nie zostawiaj dziecka samego z problemem, zabezpiecz dowody i nie bój się interweniować!



PRZYKŁADOWE ZADANIA I ĆWICZENIA

ĆWICZENIE: Ustal hierarchię bezpieczeństwa w Internecie:

- a — bardzo bezpieczne
- b — średnio bezpieczne
- c — najmniej bezpieczne

Hasło:

-czarny
-czarnyKotBiałyKoT
-czarny01

Podawanie prawdziwych danych w internecie:

-podczas zakupów on-line na zaufanej stronie
-na stronie, gdzie można się dowiedzieć, ile się będzie miało dzieci w przyszłości
-żeby móc podyskutować na forum

Aktualizacja programów zabezpieczających system (np. antywirus):

-jak sobie przypomnę
-nigdy o tym nie pamiętam
-aktualizują się automatycznie

ĆWICZENIE: Wyszukaj w Internecie informacje o trzech wybranych przez siebie zagrożeniach internetowych. Stwórz własny zestaw zasad dotyczący bezpieczeństwa przed tymi zagrożeniami.



/UWAGA: ćwiczenie wykonujemy po zapoznaniu się z wszystkimi omówionymi zagrożeniami/

ĆWICZENIE: Rozwiązywanie testu „Podstawy bezpieczeństwa w Internecie” na stronie <http://www.fundacja.orange.pl/kurs>

7. METODYKA SZKOLEŃ OSÓB DOROSŁYCH Z ZAKRESU KOMPETENCJI CYFROWYCH:

Głównym założeniem programu szkoleniowego jest udzielenie wsparcia i wyprofilowanie zajęć do poziomu zaawansowania uczestników szkolenia w kształtowaniu kompetencji cyfrowych na podstawie indywidualnych konsultacji i diagnozy wstępnej. Szkolenie w zakresie zdobywania kompetencji cyfrowych w ramach projektu będzie bazować na segmentacji tematycznej co pozwoli zapewnić manewrowanie treściami, metodami, formami i ćwiczeniami praktycznymi adekwatnie do różnego poziomu wiedzy uczestników w zakresie konkretnego zagadnienia. Zadaniem trenera jest dostosowanie ćwiczeń, zadań praktycznych oraz obserwacja reakcji uczestników w trakcie szkolenia, a także dostosowanie tempa do możliwości grupy. Zarówno konstrukcja, jak i skuteczność prowadzonych zajęć zależą będzie od doświadczenia i intuicji trenera, który musi nie tylko regulować poziom merytoryczny zajęć, ale również wykazywać się empatią.

Podstawą metodyki szkolenia jest dywersyfikacja kanałów komunikacyjnych, ponieważ skuteczność warsztatów nie tylko zależy od założeń merytorycznych, ale również od doboru optymalnej formy i metod przekazywania wiedzy. W związku z tym, że proces kształtowania kompetencji cyfrowych obejmuje różne style uczenia się, zajęcia będą wspomagane różnorodnymi metodami i formami, takimi jak: prezentacje multimedialne, tutorial, ćwiczenia opierające się na czytaniu, pisaniu, żywej rozmowie oraz wykonywaniu konkretnych czynności. Warto podkreślić, że ze względu na charakter szkolenia jedna forma przekazywania wiedzy (tj. ćwiczenia praktyczne z wykorzystaniem nowoczesnych technologii) siłą rzeczy staje się dominująca, jednak kanały komunikacji należy dywersyfikować, aby uniknąć monotonii i nie zmęczyć uczestników. Zatem częste reakcje i

natychmiastowa weryfikacja nowo zdobytych informacji pozwoli na szybkie i skuteczne przyswajanie wiedzy i umiejętności przez uczestników. Ze względu na fizjologiczne uwarunkowania utrzymania koncentracji na przerabianym zagadnieniu zajęcia będą prowadzone poprzez dozowanie praktycznej wiedzy w kilkunastominutowych interwałach teorii połączonej z dyskusją opartą na doświadczeniach własnych uczestników, a także interesującymi ćwiczeniami praktycznymi. Różnorodność taka ma sprzyjać efektywnej aktywizacji słuchaczy podczas zajęć. Co półtorej, dwie godziny wskazane są przerwy, aby uczestnicy mogli się odprężyć oraz uzupełnić deficyty kalorii spowodowane wysiłkiem umysłowym.

Na zajęciach będzie obowiązywała zasada KISS (Keep It Simple and Short), czyli krótko, treściwie i na temat. Wobec tego trener powinien posługiwać się słownictwem zrozumiałym dla wszystkich, aby uniknąć niedomówień oraz zapewnić słuchaczom komfort podczas warsztatów. Styl komunikacji trenerskiej powinny cechować spójność, jednoznaczność oraz forma oszczędna w dygresje. Poza tym trener powinien być otwarty na pytania uczestników, stwarzać odpowiednie warunki sprzyjające swobodnej wymianie doświadczeń, dopuszczać możliwość zdobywania kompetencji cyfrowych poprzez samodzielne eksperymentowanie (poszukiwanie rozwiązań) głównie z użyciem nowoczesnych technologii. Na rozwiązanie danego problemu powinien zaproponować do wyboru różne metody i sposoby wykorzystania narzędzi informatycznych i komunikacyjnych, po to by uczestnicy mogli wybrać odpowiednią dla siebie metodę. Wszystkie zadania powinny być realizowane w oparciu instruktaż słowny ze strony trenera, projekcją zadań z wykorzystaniem projektora multimedialnego oraz pokaz slajdów i tutoriali. Dorośli nowe umiejętności nabywają przez pryzmat wiedzy już posiadanej. Trener w trakcie szkolenia pełni niejako funkcję moderatora koordynującego przebieg całego procesu, ale nie narzuca swojego zdania i nie podsuwa gotowych odpowiedzi. Uczestnicy szkolenia niejako konstruują wiedzę drogą poszukiwań, osiągania i przekształcania napływających informacji - głównie dzięki współdziałaniu i osobistemu doświadczeniu. W takim procesie kształcenia podkreślany jest aspekt samodzielności działania i świadomego samodoskonalenia. Natomiast podział materiału szkoleniowego na konkretne zadania zapewni sukcesywne opanowanie wydzielonych w małych partiach zagadnień i pozwoli na systematyczną weryfikację trudności, które należy powtórzyć a nawet przeanalizować z uczestnikami raz jeszcze. Wszystkie ćwiczenia i rozwiązywane problemy należy podsumować i zewaluować

wspólnie z kursantami, co zapewni informację zwrotną trenerowi na temat poprawności doboru metod i form pracy z daną grupą szkoleniową. Po takiej analizie trener powinien zwrócić uwagę na mocne i słabe strony każdej ze stosowanych przez siebie metod, nawiązując przy tym do procesów grupowych i dynamiki grupy szkoleniowej.

8. ZASADY RÓWNOŚCI SZANS I NIEDYSKRYMINACJI, W TYM DOSTĘPNOŚCI DLA OSÓB Z NIEPEŁNOSPRAWNOŚCIAMI ORAZ RÓWNOŚCI SZANS KOBIECI I MĘŻCZYŹN W KONTEKŚCIE REALIZOWANYCH SZKOLEŃ:

Program szkolenia jest zgodny z zasadami równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz zasadami równości szans kobiet i mężczyzn. **Założenia programowe przewidują udział osób z niepełnosprawnościami na równi z innymi uczestnikami szkolenia. Metody i formy pracy są tak dostosowane, aby wszyscy uczestnicy mieli zapewnione odpowiednie wsparcie w zakresie zdobywania kompetencji cyfrowych.** Pomieszczenia w których będą odbywały się zajęcia warsztatowe będą w pełni przystosowane dla osób niepełnosprawnych. Budynek wyposażony jest w podjazdy, windy dla osób niepełnosprawnych, szatnię oraz infrastrukturę sanitarną przystosowaną do korzystania przez osoby z niepełnosprawnością ruchową. Wszystkie szkolenia adresowane są w takim samym stopniu do kobiet, jak i do mężczyzn na zasadzie równości szans. Grupy szkoleniowe będą mieszane, co będzie sprzyjało budowaniu przyjaznej atmosfery oraz poznaniu sytuacji obu płci na rynku zawodowym oraz pozycji w społeczeństwie.

Zasada równości szans kobiet i mężczyzn:

- dotyczy podejmowania działań (przeszkolenia) na rzecz zdobywania kompetencji cyfrowych pozwalających na poprawę jakości ich życia w społeczeństwie informacyjnym,
- kobietom i mężczyznom przypisuje się taką samą wartość społeczną, równe prawa i obowiązki oraz gdy mają oni równy dostęp do zasobów (środki finansowe, szanse rozwoju, dostęp do informacji), z których mogą korzystać;
- udział w szkoleniu ma pomóc wyeliminować bariery i ograniczenia utrudniające równy dostęp do zasobów i dóbr społecznych;

- unikanie sztucznych podziałów na role i obszary wyłącznie „kobiece” lub wyłącznie „męskie”, np. prowadzenie firmy, korzystanie z komunikatorów internetowych w celu przeprowadzania rozmów służbowych, rozwijanie zainteresowań dzieci itp.
- zaprezentowanie sposobów pozyskiwania informacji, które mogą przyczynić się do rozwiązania konkretnych problemów w zakresie równości szans kobiet i mężczyzn.

9. PROCEDURY OSIĄGANIA SZCZEGÓŁOWYCH CELÓW EDUKACYJNYCH:

Ujęte w programie treści zostały tak ułożone, aby każdy uczestnik szkolenia mógł stosować różne metody korzystania z usług Katalogu cyfrowego usług polskiej administracji i rozwijać umiejętności myślenia i uczenia się, a w efekcie nabyte umiejętności i wiadomości wykorzystać podczas realizacji różnych zadań z wykorzystaniem technologii cyfrowych, a przede wszystkim podczas prowadzenia warsztatów dziennikarskich z dziećmi i młodzieżą. Strategie prowadzenia zajęć szkoleniowych:

- **strategia dydaktyczna** – opiera się na wykładzie i wyjaśnieniach trenera bazujących na pytaniach dodatkowo zadawanych przez uczestników szkolenia; w tej strategii nadrzędną rolą jest sprawdzenie przez prowadzącego rozumienia jego słów;
- **strategia pytań opierających się na faktach** – jej głównym celem jest ustalenie faktów; interakcja między prowadzącym a kursantami bazuje głównie na wyrażaniu przez trenera aprobaty, bądź też uwag na temat wykonania zadania;
- **strategia pytań skłaniających do myślenia, zwana też dialogiczną** – jest oparta na dialogu, celem tej strategii jest zachęcenie beneficjentów do myślenia i rozbudzenie w nich potrzeby dyskusji; trener uczestniczy w rozmowie na równi z uczestnikami szkolenia, komentuje lub uzupełnia wypowiedzi, może także w trakcie dyskusji zmienić stanowisko wobec omawianego problemu; ta strategia jest oparta na formułowaniu otwartych pytań ożywiających (czyli poszukujących, skłaniających do myślenia), dzięki którym zwiększa się interakcja między kursantami;

10. ZALECANE WARUNKI I SPOSÓB REALIZACJI

Na etapie szkolenia kompetencji cyfrowych uczestnicy poznają nieformalne znaczenie wybranych pojęć związanych z wyszukiwaniem informacji w sieci oraz biegłym wykorzystywaniem zasobów Internetu do korzystania w pełni z usług administracji publicznej. Zajęcia mają pobudzić ich do kreatywnego działania i poszukiwania rozwiązań stawianych im problemów. Tymi pojęciami są m.in.: *prawo autorskie, usługi on-line, blog, czat, e-mail, wideorozmowa, a także pojęcia wynikające z bezpieczeństwa w Internecie typu, grooming, fake news, hate i wiele innych*. Kolejnym etapem poszerzania kompetencji cyfrowych jest posługiwanie się komputerem w korelacji z pozostałymi obszarami życia codziennego i kompetencjami kluczowymi. Każde stanowisko powinno być tak skonfigurowane, aby spełniało następujące kryteria:

1. zainstalowana przynajmniej jedna przeglądarka internetowa,
2. zainstalowana kamerka internetowa,
3. głośniki i mikrofon jeżeli zestaw nie ma wbudowanych,
4. dostęp do drukarki, jako zewnętrznego urządzenia peryferyjnego,
5. ekran lub tablica interaktywna, rzutnik multimedialny,
6. dostęp do Internetu.

11. EWALUACJA PROGRAMU

Ewaluacja programu oraz prowadzonych zajęć w ramach szkolenia kompetencji cyfrowych dla pracowników gminnych samorządowych instytucji kultury, którzy pragną zdobyć lub poszerzyć swoje kompetencje cyfrowe z zakresie pracy w sieci zostanie przeprowadzona w oparciu o wyniki ankiety ewaluacyjnej oraz na podstawie opinii samych uczestników, a także w oparciu o bieżące obserwacje zajęć.

- Czy po przeprowadzonych zajęciach uczestnicy są przekonani, że warto dbać o , bezpieczeństwo swoich danych, haseł, sprzętu, przez który łączą się z Internetem, połączenia internetowego, szczególnie, gdy przesyłają ważne informacje czy robią transakcje finansowe?
- Czy mają świadomość ewentualnych skutków i odpowiedzialności, jaka ciąży na nich w momencie publikowania informacji i materiałów dotyczących ich samych lub innych osób?



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- Czy wiedzą, kiedy lepiej działać w Internecie pod nazwiskiem, a kiedy zachować anonimowość?
- Czy są świadomi, że anonimowość w sieci może być pozorna, jeśli się o nią odpowiednio nie zadba?)
- a także w oparciu o bieżące obserwacje zajęć.