Dr Agnieszka Skulimowska
Dr Waldemar Wysocki
Uniwersytet w Siedlcach
Wydział Nauk Ścisłych i Przyrodniczych

I. INTERNET

WSTĘP

Internet nie tylko ułatwia dostęp do informacji i usług, ale także kształtuje kluczowe aspekty naszej codzienności – m.in. komunikację, edukację, pracę i finanse – oraz sektory specjalistyczne, takie jak przemysł czy medycyna. Do tego globalnego systemu można dołączyć praktycznie każde urządzenie codziennego użytku m.in.: lodówkę, pralkę, system oświetleniowy, samochód bądź termostat. Pozwala to zdalnie nimi sterować, monitorować oraz automatyzować ich funkcje i nazywa się Internetem Rzeczy (ang. *Internet of Things*, w skrócie IoT).

W niniejszym rozdziale czytelnik pozna ogólną charakterystykę Internetu, zagrożenia związane z cyberbezpieczeństwem, programy antywirusowe i licencje Creative Commons. Opracowanie zawiera także praktyczne przykłady zaawansowanego wyszukiwania informacji i zarządzania nimi oraz korzystania z wybranych baz danych dostępnych online na przykładzie Biblioteki Głównej Uniwersytetu w Siedlcach.

1. OGÓLNA CHARAKTERYSTYKA

Sieci komputerowe to systemy urządzeń połączonych mediami transmisyjnymi oraz zestawami reguł i procedur (protokołami) w celu wymiany danych oraz współdzielenia zasobów. Ze względu na zasięg dzielimy je na:

1. LAN (ang. *Local Area Network*) - sieć lokalna, obejmuje ograniczony obszar, taki jak budynek, biuro lub dom, wykorzystuje połączenia przewodowe lub bezprzewodowe.
2. MAN (ang. *Metropolitan Area Netwok*) - miejska sieć komputerowa, łączy sieci lokalne (LAN) w obrębie miasta lub regionu geograficznego.
3. WAN (ang. *Wide Area Network*) - rozległa sieć, zawiera wiele sieci LAN i MAN, zapewnia połączenia między krajami czy kontynentami, wykorzystuje różne media transmisyjne, w tym światłowody oraz łączność satelitarną.

Internet to sieć komputerowa o zasięgu globalnym, składa się z milionów sieci lokalnych (stąd też nazwa **sieć sieci**), a także miliardów komputerów oraz innych urządzeń połączonych ze sobą przewodowo i bezprzewodowo. System opiera się na protokole **TCP/IP** (ang. Transmission Control Protocol/Internet Protocol), który działa warstwowo:

1. TCP segmentuje dane na mniejsze fragmenty i dołącza do nich nagłówki m.in. z numerami porządkowymi.
2. IP obudowuje segmenty TCP własnym nagłówkiem, tworząc pakiety (datagramy**)**, które zawierają m.in. adres nadawcy i odbiorcy.
3. Routery sprawdzają te adresy i kierują pakiety najlepszą możliwą trasą.
4. Odbiorca potwierdza nadawcy otrzymane dane, a TCP sortuje je i składa w całość.
5. Brak informacji zwrotnej w wymaganym czasie powoduje, że TCP retransmituje brakujące pakiety.

Adres IP stanowi główną część protokołu internetowego (IP) i jest niepowtarzalnym numerem identyfikującym każde urządzenie w sieci komputerowej. W wersji 4 (IPv4) składa się z 32 bitów

i ma postać czterech liczb dziesiętnych z zakresu 0-255 oddzielonych kropkami, np. 212.77.98.9. Pula adresów oferowanych przez ten format jest bliska wyczerpaniu, co sprawiło powstanie standardu IPv6. Jest on 128-bitowy, zapisywany szesnastkowo z wykorzystaniem dwukropków, np. 3FFE:FFFF:7654:FEDA:1245:BA98:3210:4562. Takie ciągi cyfr są trudne do zapamiętania, dlatego zastępują je adresy domenowe, a jedne na drugie przekładają serwery DNS (ang. *Domain Name System*).
Na przykład, jeśli wpiszemy onet.pl, a w pamięci podręcznej przeglądarki, systemu operacyjnego lub dostawcy Internetu nie ma zapisanego odpowiadającego adresu IP, to zapytanie trafia do serwerów DNS, które wyszukują go rekurencyjnie. Po uzyskaniu odpowiedzi przeglądarka łączy się, używając protokołu TCP/IP, pobiera i wyświetla stronę.
Adresy IP klasyfikuje się m.in. jako:

1. Publiczne - umożliwiają bezpośredni dostęp do Internetu, są unikalne w skali globalnej.
2. Prywatne - zapewniają komunikację wewnątrz sieci lokalnych i są w nich niepowtarzalne.
3. Statyczne - przypisane na stałe do urządzenia.
4. Dynamiczne - na czas łączenia z Internetem są wybierane automatycznie, a po rozłączeniu z siecią wracają do puli i mogą być wykorzystane przez innego użytkownika.

Przykład 1. Sprawdź publiczny adres IP komputera.

1. Wpisz w Google hasło: moje ip.



1. Wyświetlany adres IP na stronie ip.pc.pl

2. Wybierz jedną z propozycji.
3. Odczytaj publiczny adres IP komputera: 91.210.51.212 (il. 1).

Przykład 2. Skorzystaj z wiersza poleceń i komendy **ping**, aby sprawdzić, jaki adres IP wyświetli się dla domeny google.pl?

1. Naciśnij klawisz **Windows** lub ikonę **Start**.
2. Napisz **cmd** i kliknij **Enter** (il. 2).



2. Otwieranie wiersza polecenia

3. Do okna wiersza polecenia wprowadź komendę **ping google.pl**.
4. Po kliknięciu **Enter** pokazał się adres IP 142.251.98.94[1] (il. 3).

```
C:\Users\Student>ping google.pl

Pinging google.pl [142.251.98.94] with 32 bytes of data:
Reply from 142.251.98.94: bytes=32 time=11ms TTL=112
Reply from 142.251.98.94: bytes=32 time=12ms TTL=112
Reply from 142.251.98.94: bytes=32 time=7ms TTL=112
Reply from 142.251.98.94: bytes=32 time=14ms TTL=112

Ping statistics for 142.251.98.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 14ms, Average = 11ms
```

3. Wynik polecenia ping nazwa_domeny

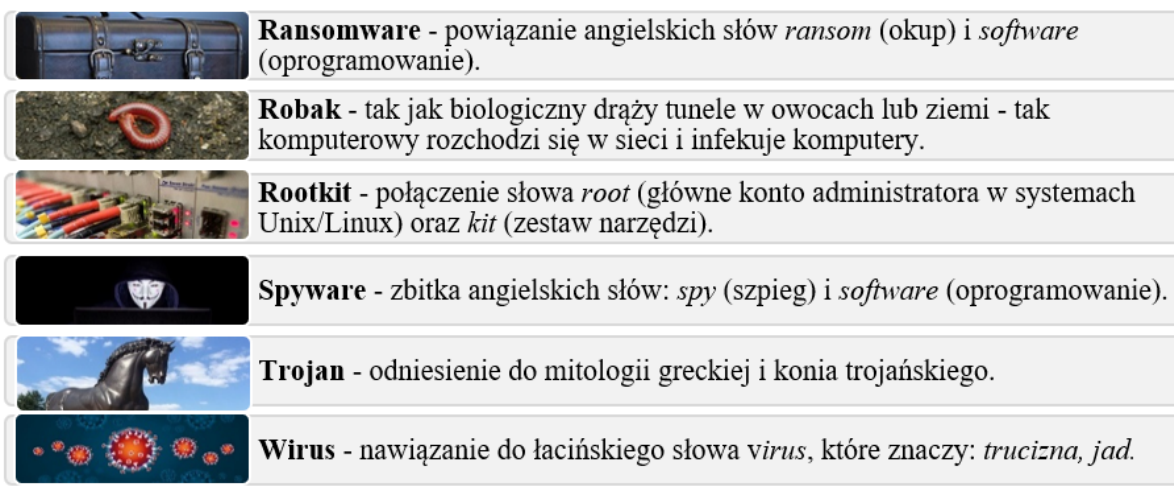
[1] Google dysponuje milionami adresów IP w standardzie IPv4, jak i IPv6. Są one przypisywane zależnie od lokalizacji użytkownika i obciążenia serwerów.

2. ZAGROŻENIA W INTERNECIE I PROGRAMY ANTYWIRUSOWE

Rozwój technologii sprawia, że użytkownicy Internetu są narażeni na coraz więcej niebezpieczeństw. Należą do nich m.in. złośliwe oprogramowanie (tzw. malware), phishing[2], kradzież danych, fałszywe strony (np. sklepy), cyberprzemoc, uzależnienie, czy nieodpowiednie treści, w szczególności dla dzieci. **Malware** to wszystkie programy zaprojektowane do powodowania szkód, kradzieży danych, zakłócania pracy urządzeń bądź przejmowania nad nimi kontroli. Działają bez wiedzy użytkownika, a do ich istotnych rodzajów należą[3]:

1. **Ransomware** - szyfruje dane bądź blokuje dostęp do urządzenia domagając się okupu.
2. **Robak** (ang. *worm*) - samodzielny program, który automatycznie tworzy swoje kopie i rozprowadza je między urządzeniami przez sieci; używa luk w zabezpieczeniach (niezaktualizowane systemy operacyjne lub aplikacje).
3. **Rootkit** - w sposób zdalny i ukryty kontroluje system komputerowy, niejednokrotnie przejmuje najważniejsze zadania, a przy tym jest trudny do wykrycia.
4. **Spyware -** oprogramowanie szpiegujące; po kryjomu gromadzi loginy, hasła, historię przeglądania, dane finansowe, lokalizację, a nawet nagrywa obraz z kamery czy dźwięk z mikrofonu i przekazuje cyberprzestępcom. Przykładem jest **keylogger**, który rejestruje wybierane przyciski na klawiaturze.
5. **Trojan** - bazuje na socjotechnice, udaje pożyteczny program bądź pliki, a po uruchomieniu przez użytkownika uzyskuje nieautoryzowany dostęp do systemu i realizuje szkodliwe działania.
6. **Wirus** - potrzebuje nosiciela i dlatego dołącza się do plików, a gdy użytkownik je uruchamia aktywują się, powielają i rozprzestrzeniają. Najczęstsza metoda infekcji to otwieranie podejrzanych załączników e-mailowych, klikanie linków w wiadomościach od nieznanych nadawców, pobieranie plików z niepewnych źródeł także z pendrive'ów, a nawet odwiedzanie fałszywych stron ze złośliwymi reklamami.

Pionowa lista obrazów (il. 4) przybliża pochodzenie nazw złośliwego oprogramowania, a grafika[4] ułatwia ich zapamiętanie.



4. Popularne zagrożenia malware

Łatwość oraz szybkość udostępniania treści, a także poczucie anonimowości i bezkarności przyczyniają się do wzrostu zjawiska **cyberprzemocy**. Polega ono na celowym i powtarzającym się nękaniu, zastraszaniu lub wyśmiewaniu osób przy użyciu urządzeń elektronicznych oraz Internetu, w celu wyrządzenia im krzywdy, wywołania wstydu czy strachu. Ten rodzaj agresji jest wielowymia-

[2] Informacje na temat złośliwego oprogramowania i pojęć: phishing, ransomware, botnet znajdziesz w rozdziale III (3.1. Współczesne formy ataków).

[3] https://www.malwarebytes.com/pl/malware, data dostępu: 22.02.2026.

[4] https://pixabay.com/photos/suitcase-leather-leather-suitcase-2534787/, https://pixabay.com/photos/worm-animal-ground-nature-955467/, https://pixabay.com/photos/fiber-optic-light-waveguide-4393369/, https://pixabay.com/photos/anonymous-collective-secret-hacker-4165613/, https://pixabay.com/photos/horse-trojan-horse-statue-1574780/, https://pixabay.com/photos/corona-symbol-coronavirus-virus-5025009/, data dostępu: 28.03.2026.

rowy, dotyczy zróżnicowanych działań, sięga po bezprawne wkraczanie w życie osobiste i złożone manipulacje. Poniżej często spotykane przejawy oraz formy cyberprzemocy[5]:

1. **Doxing** - publiczne ujawnianie wszelkich prywatnych informacji, często wrażliwych.
2. **Hejt** - agresywne, wrogie, obraźliwe, poniżające komentarze bądź zachowania kierowane do osób lub grup, np. *Ale się ubrałaś, jak wieśniara*. **Flaming** - zamierzone zaognianie i eskalowanie kłótni online, np. wulgaryzmy. **Trolling** - celowe publikowanie prowokacyjnych treści, aby zakłócać dyskusję i denerwować uczestników, np. *Graj dalej, jesteś mierny.*
3. **Naruszenie wizerunku** - wykorzystanie bez zgody zdjęć, głosu, filmu.
4. **Nękanie** - uporczywe i powtarzające się działania, m.in. nachodzenie, śledzenie, wysyłanie niechcianych wiadomości oraz dręczenie telefonami (**stalking**).
5. **Podszywanie się** - tworzenie fałszywych tożsamości w sieci z użyciem cudzych informacji i zdjęć lub włamania na konta w celu oszukania, szantażowania, poniżania, ośmieszania dla zabawy bądź korzyści finansowych.
6. **Sexting** - wymiana wiadomości tekstowych, zdjęć, filmów o charakterze seksualnym, która zmienia się w cyberprzemoc, jeśli treści te są ujawniane wbrew woli nadawcy i wykorzystywane do szantażu (**sextortion**) lub hejtu.
7. **Wykluczenie** - celowe i wielokrotne usuwanie osoby z grup online, czatów bądź blokowanie jej dostępu do społeczności wirtualnych w celu izolacji społecznej.
8. **Zniesławienie** - publiczne rozpowszechnianie nieprawdziwych lub kompromitujących informacji o osobie, firmie lub instytucji, aby zaszkodzić reputacji, naruszyć dobre imię lub narazić na utratę zaufania niezbędnego do funkcjonowania.

Przykład 3. Przy każdym zdaniu, w nawiasach kwadratowych, nazwij formę cyberprzemocy.

1. Przestępca przejął konto użytkownika i prosi znajomych o kod BLIK, pisząc, że jest w sklepie i nie ma pieniędzy. [Podszywanie się].
2. Kobieta grozi byłemu partnerowi, że jeśli nie spełni jej żądań, wyśle znajomym jego intymne zdjęcia. [Sextortion].
3. Pod udostępnionym zdjęciem na Facebooku pojawił się obraźliwy komentarz *Jesteś gruba, wyglądasz jak wieloryb*. [Hejt].
4. Założyciel grupy na WhatsAppie usunął ją, utworzył nową pod nazwą *Poza Janem* i nie zaprosił do niej jednej osoby z poprzedniego składu. [Wykluczenie].
5. Oszust założył konto na Messengerze, wykorzystuje zdjęcie oraz imię jednego z użytkowników i wysyła obraźliwe wiadomości do jego znajomych. [Podszywanie się].
6. Pracownica rozpowszechnia w mediach społecznościowych zmyślone informacje o życiu prywatnym byłego przełożonego. [Zniesławienie].

Podczas korzystania z sieci warto zadbać o własne bezpieczeństwo. Podstawą jest tworzenie silnych haseł, aktualizowanie na bieżąco oprogramowania, w szczególności antywirusowego.
Najczęstszym sposobem weryfikacji tożsamości i pierwszą zaporą przed nieautoryzowanym dostępem do kont oraz danych jest hasło[6]. Na ile jest bezpieczne można zweryfikować dzięki darmowym narzędziom online.
Uwaga! Na stronach, do których nie ma się całkowitego zaufania lub ich nie zna **nigdy** nie kontroluje się używanego hasła, ale takie o podobnej strukturze.

Przykład 4. Zweryfikuj siłę wymyślonego hasła, używając dwóch różnych testerów online. Czy uzyskane wyniki są identyczne?

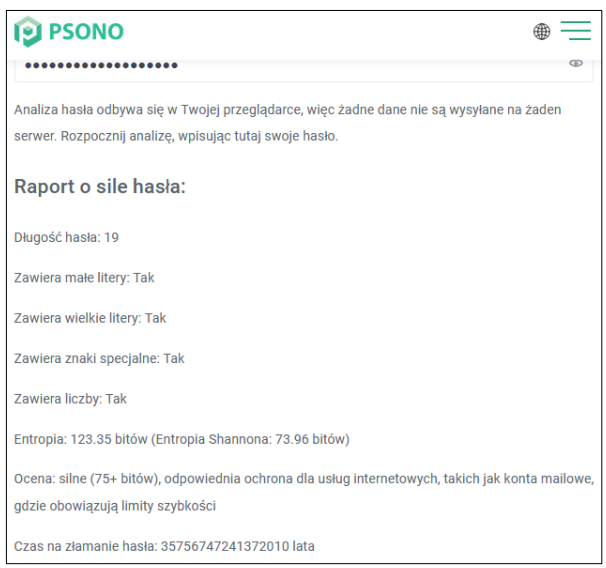
1. Poszukaj stron dla frazy: **tester siły hasła**.
2. Otwórz wybraną propozycję.
3. Wpisz hasło i odczytaj wynik (il. 5).

[5] https://cyberprzemoc.pl/, data dostępu: 20.01.2026.
[6] Informacje na temat haseł znajdziesz w rozdziale III (3.2. Bezpieczeństwo w systemie Windows).



5. Informacja o sile hasła[7]

4. Przejdź do strony z innym testerem.
5. Wprowadź hasło i sprawdź jego analizę (il. 6).



6. Ocena siły hasła[8]

6. Wyniki dla tego samego hasła nie są identyczne. Pierwsze narzędzie online informuje m.in., że jest ono bardzo silne i trzeba 880 lat, aby je złamać, natomiast drugie, że jest silne i czas na jego rozszyfrowanie wynosi 35 756 747 241 372 010 lat.

Oprogramowanie antywirusowe stanowi fundament strategii bezpieczeństwa w Internecie. Do jego podstawowych zadań należy:

1. **Wykrywanie zagrożeń:** skanowanie plików, aplikacji a także ruchu sieciowego w poszukiwaniu złośliwego oprogramowania i podejrzanych działań, np. logowania w niespotykanych godzinach albo z nieznanych lokalizacji.
2. **Ochrona w czasie rzeczywistym**: nieustanne kontrolowanie systemu, plików, operacji i przeciwdziałanie próbom uruchomienia malware'u bądź pobrania go.
3. **Skanowanie na żądanie:** ręczne uruchamianie przez użytkownika tego, co i kiedy chce przeskanować.
4. **Zwalczanie**: pozbycie się wykrytego zagrożenia przez izolację plików (kwarantanna), naprawę (dezynfekcja) bądź kasację.

[7] https://www.strongpasswordgenerator.org/pl/password-strength-checker/; data dostępu: 28.02.2026.
[8] https://psono.com/pl/password-strength-test, data dostępu: 28.02.2026.

5. **Aktualizacje:** systematyczne pobieranie nowych definicji nieustannie ewoluujących wirusów i bycie na bieżąco z zagrożeniami.

Programy różnią się między sobą skutecznością wykrywania, zakresem funkcji, stopniem obciążenia systemu, modelem działania, interfejsem i ceną. Wersje darmowe zapewniają podstawową ochronę. Płatne oferują dodatkowe funkcje, takie jak firewall, ochrona płatności i tożsamości oraz zabezpieczenie przed szpiegowaniem poprzez szyfrowanie danych i maskowanie adresu IP. Przy wyborze należy brać też pod uwagę zgodność z systemem operacyjnym, profesjonalne recenzje, niezależne testy wydajnościowe i liczbę urządzeń, które można zabezpieczyć. Poniżej przykłady antywirusów:

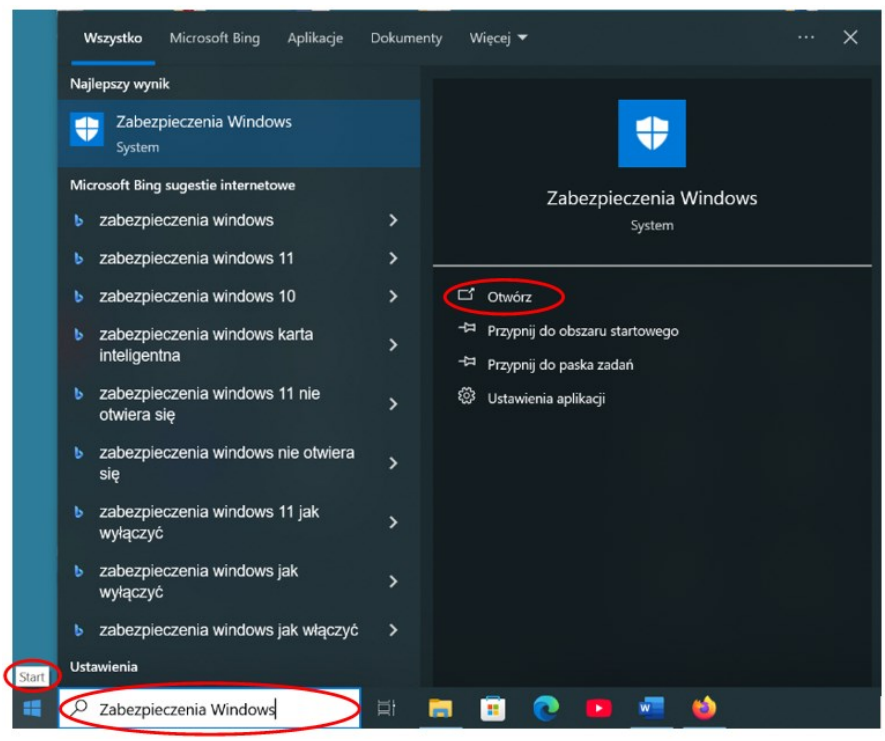
1. Darmowe: Avast Free, AVG Free, Avira Free Security, Bitdefender Free, Microsoft Defender.
2. Płatne: Avast Premium, Bitdefender, ESET, Kaspersky, Norton 360.

Systemy Windows 10/11 mają wbudowany bezpłatny program antywirusowy o nazwie Microsoft Defender Antivirus (wcześniej Windows Defender), który chroni w czasie rzeczywistym przed zagrożeniami i ma domyślnie włączoną zaporę sieciową (Firewall). Nie ma go w **Ustawieniach** i sekcji **Aplikacje i funkcje**, a jest dostępny m.in. w menu **Start** jako **Zabezpieczenia Windows** lub po wpisaniu takiej nazwy do wyszukiwarki systemowej. Jeśli użytkownik zainstaluje inny program antywirusowy, to w celu zapobiegania konfliktom, Defender automatycznie przełącza się w tryb pasywny i nie zapewnia ochrony w czasie rzeczywistym.

Uwaga! Nie istnieją stuprocentowe metody zabezpieczeń przed potencjalnymi źródłami zagrożeń. Najskuteczniejszą strategią pozostaje obrona wielowarstwowa, czyli łączenie antywirusa z ostrożnością użytkownika, aktualizacjami systemu i silnymi hasłami.

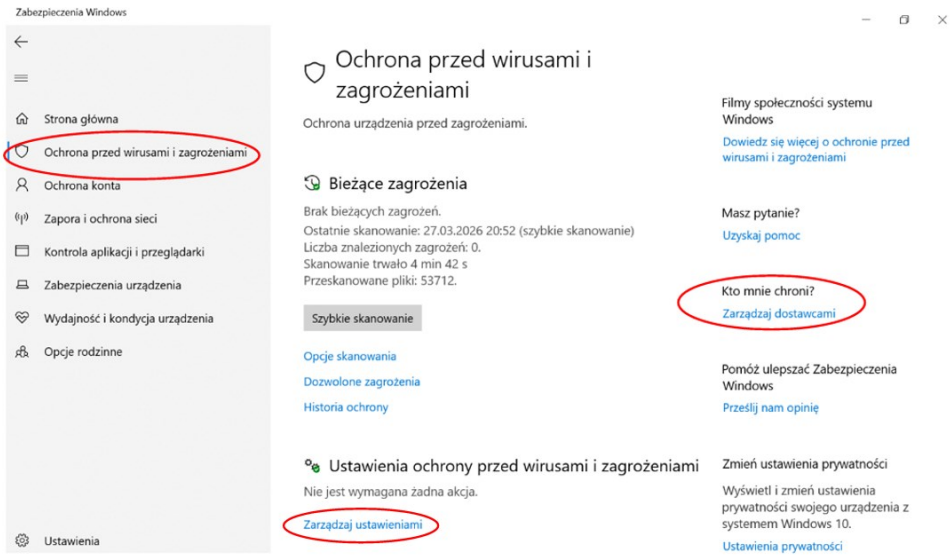
Przykład 5. W aplikacji **Zabezpieczenia Windows** i sekcji **Dostawcy zabezpieczeń** sprawdź ochronę komputera przed złośliwym oprogramowaniem.

1. Wybierz kolejno: **Start** > **Ustawienia** > **Aktualizacja i zabezpieczenia** > **Zabezpieczenia Windows** lub naciśnij: **Start** i w polu **Wyszukaj** na pasku zadań wpisz **Zabezpieczenia Windows**, a potem **Otwórz** albo **Enter** (il. 7).



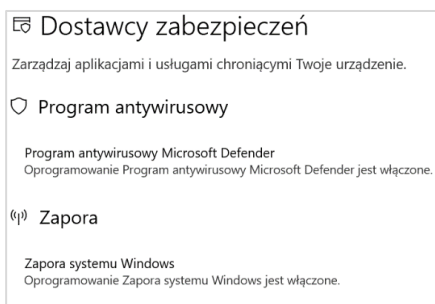
*7. Menu wyszukiwania dla frazy **Zabezpieczenia Windows***

2. Z lewej strony wskaż **Ochrona przed wirusami i zagrożeniami**.



*8. Zakładka **Ochrona przed wirusami i zagrożeniami** okna **Zabezpieczenia Windows***

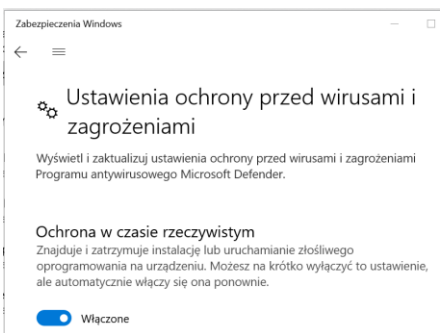
3. W obszarze **Kto mnie chroni?** kliknij **Zarządzaj dostawcami** (il. 8).
4. Przed złośliwym oprogramowaniem chroni komputer włączony program antywirusowy **Microsoft Defender** oraz **Zapora systemu Windows** (il. 9).



*9. Sekcja **Dostawcy zabezpieczeń***

Przykład 6. Skontroluj, czy Microsoft Defender chroni komputer w czasie rzeczywistym?

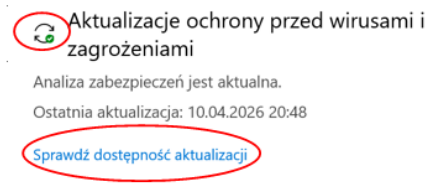
1. Na pasku zadań w prawym dolnym rogu ekranu kliknij dwukrotnie na ikonie tarczy . Jeśli jej nie widzisz wybierz strzałkę **Pokaż ukryte ikony**.
2. Z lewej strony wskaż **Ochrona przed wirusami i zagrożeniami**.
3. W sekcji **Ustawienia ochrony przed wirusami i zagrożeniami** kliknij **Zarządzaj ustawieniami** (il. 8).
4. Funkcja **Ochrona w czasie rzeczywistym** jest włączona (il. 10).



*10. **Ochrona w czasie rzeczywistym** w **Zabezpieczeniach Windows***

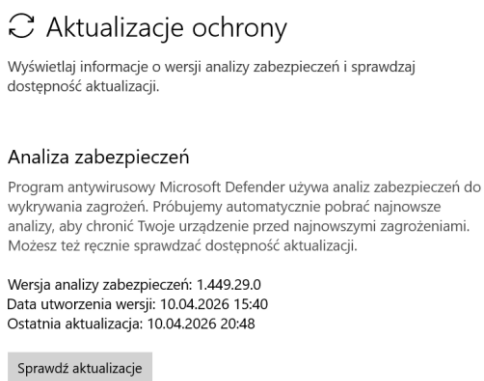
Przykład 7. Sprawdź, czy Microsoft Defender korzysta z najnowszej aktualizacji zabezpieczeń?

1. Wybierz kolejno: **Start** > **Ustawienia** > **Aktualizacja i zabezpieczenia** > **Zabezpieczenia Windows**.
2. Przejdź do zakładki **Ochrona przed wirusami i zagrożeniami** (il. 8).
3. Odszukaj sekcję **Aktualizacje ochrony przed wirusami i zagrożeniami** (il. 11).



11. Sprawdzanie analizy zabezpieczeń

4. Zielony kolor znaku graficznego informuje, że definicje wirusów są aktualne (il. 11), żółty trójkąt z wykrzyknikiem sugeruje podjęcie działania, a czerwone kółko z krzyżykiem sygnalizuje konieczność natychmiastowej reakcji.
5. Kliknij:
   5.1. **Sprawdź dostępność aktualizacji** (il. 11).
   5.2. **Sprawdź aktualizacje**, aby pobrać nowe sygnatury (il. 12).



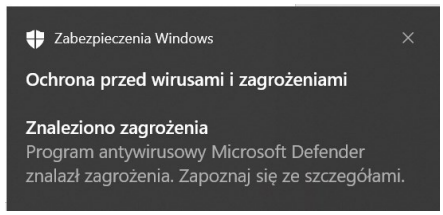
12. Sprawdzanie aktualizacji

6. Z ręcznego sprawdzenia aktualizacji wynika, że Microsoft Defender używa najnowszej dostępnej w danej chwili bazy sygnatur zagrożeń (il. 12).

Można w prosty i bezpieczny sposób sprawdzić, czy oprogramowanie antywirusowe działa poprawnie i wykrywa zagrożenia. Służy do tego nieszkodliwy plik testowy EICAR[9], który prawie wszystkie antywirusy rozpoznają jako złośliwe oprogramowanie.

Przykład 8. Utwórz plik testowy EICAR[10] i użyj go, aby przetestować ochronę w czasie rzeczywistym.

1. Skopiuj ciąg: X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
2. Wklej do Notatnika i zapisz jako EICAR.txt.
3. Windows Defender natychmiast zareagował na zagrożenie (il. 13).

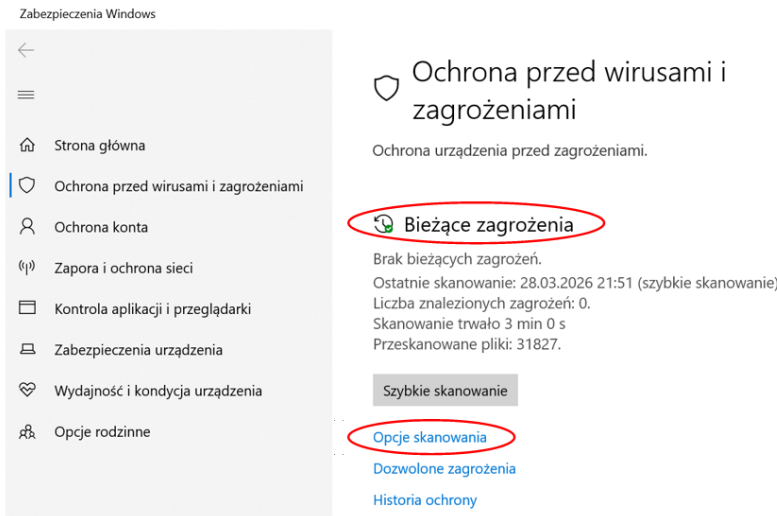


13. Komunikat o wykryciu zagrożenia

[9] https://learn.microsoft.com/pl-pl/defender-endpoint/validate-antimalware, data dostępu: 11.03.2026.
[10] Ibidem.

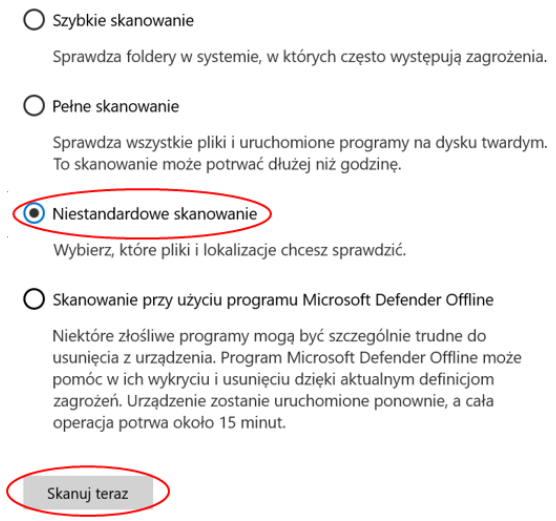
Przykład 9. Użyj programu Microsoft Defender do przeskanowania wybranego folderu.

1. Otwórz aplikację **Zabezpieczenia Windows** (**Start** > **Ustawienia** > **Aktualizacja i zabezpieczenia**).
2. Przejdź do **Ochrony przed wirusami i zagrożeniami**.
3. W strefie **Bieżące zagrożenia** wybierz **Opcje skanowania** (il. 14).



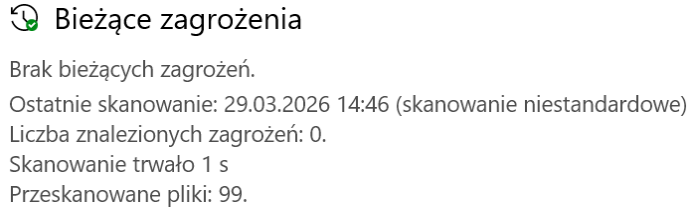
14. Zabezpieczenia Windows - ochrona urządzenia przed zagrożeniami

4. Zaznacz **Niestandardowe skanowanie** i kliknij **Skanuj teraz** (il. 15).



15. Opcje skanowania

5. Wskaż folder, który chcesz sprawdzić.
6. Kliknij **Wstecz**, aby wrócić do **Bieżących zagrożeń** i informacji podsumowujących proces (il. 16).



16. Raport ze skanowania niestandardowego

3. ZAAWANSOWANE METODY WYSZUKIWANIA INFORMACJI

Dynamiczny rozwój sieci komputerowych przyczynia się do ogromnego wzrostu ilości dostępnych treści. Wymaga to od użytkownika umiejętności znajdowania rzetelnych źródeł, krytycznej oceny wiadomości oraz ich weryfikacji, w tym m.in. sprawdzenia[11]:

1. Autora (osoba anonimowa czy z kwalifikacjami, a może znana instytucja).
2. Wiarygodności źródła (godne zaufania domeny np. gov.pl, edu.pl czy prestiżowe media).
3. Daty publikacji (aktualność).
4. Czy dane opierają się na dowodach, faktach, cytatach? Czy przedstawiają wiele punktów widzenia, czy tylko jeden? Czy linki prowadzą do materiałów źródłowych, czy przetworzonych?
5. Czy treść jest powiązana z celem (np. sprzedaż)?
6. Czy tekst jest neutralny, czy nacechowany emocjonalnie? Używane słownictwo pozytywne (np. koteczek), negatywne (kocur) i oceniające ujawnia podejście autora do przedstawianego tematu.
7. Czy podane informacje przekazują też inne zaufane źródła?
8. Transparentności, np. kto finansuje publikację?
9. Faktów za pomocą takich narzędzi, jak np. https://demagog.org.pl/, https://konkret24.tvn24.pl/, https://oko.press/.

Przeglądarka internetowa (ang. web browser) to program umożliwiający pobieranie i wyświetlanie stron WWW, plików oraz odtwarzanie treści multimedialnych. Do najpopularniejszych należą: Google Chrome, Firefox, Microsoft Edge, Safari, Opera. Różnią się one m.in. szybkością działania, wykorzystaniem zasobów komputera, dostępnymi funkcjami (np. historia, zakładki), obsługą rozszerzeń (np. blokowanie reklam, menedżer haseł), a także poziomem bezpieczeństwa i prywatności. Wybór zależy od indywidualnych potrzeb użytkownika.

Większość przeglądarek oferuje **tryb prywatny**, do którego łatwo jest przejść z menu umieszczonego w prawym górnym rogu okna (≡ lub ···) bądź za pomocą skrótów klawiaturowych (tabela 1). Z tej funkcji warto korzystać np. na urządzeniach publicznych bądź używanych przez kilka osób, i w ten sposób zapobiec przechowywaniu historii, ciasteczek, danych logowania, reklam dopasowanych do preferencji użytkownika oraz personalizacji wyników wyszukiwania. Tryb nie zabezpiecza przed złośliwym oprogramowaniem, zaawansowanym śledzeniem i nie daje pełnej anonimowości online, bo nie ukrywa adresu IP.

Tabela 1. Tryb prywatny wybranych przeglądarek

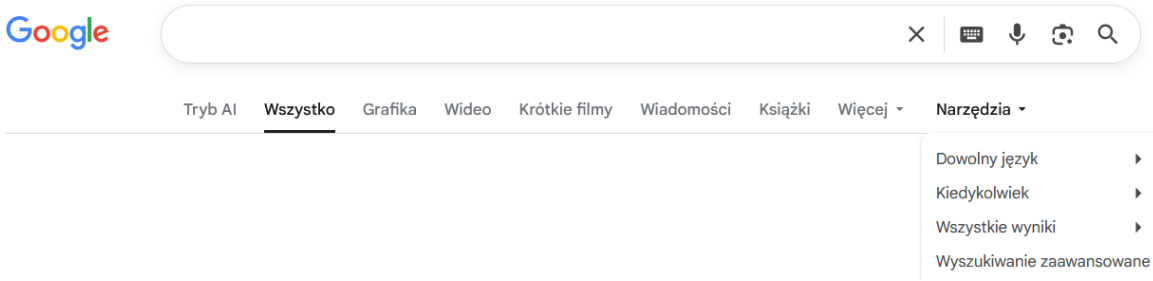
L.p.	Przeglądarka	Symbol	Skrót	Tryb
1.	Google Chrome		Ctrl+Shift+N	Incognito
2.	Firefox		Ctrl+Shift+P	Prywatny
3.	Microsoft Edge		Ctrl+Shift+N	InPrivate

Wyszukiwarka internetowa (ang. *search engine*) to program komputerowy lub strona internetowa, która umożliwia znajdowanie w sieci globalnej informacji jak najlepiej skorelowanych z frazą wpisaną przez użytkownika. Swoje działanie opiera na specyficznych programach, które automatycznie indeksują zasoby sieciowe, oraz na złożonych algorytmach dopasowujących zapytania do indeksu i porządkujących wyniki wyszukiwania. Najbardziej znane to: Google, Bing, DuckDuckGo, Yahoo!, Baidu, Yandex.

Przeglądarka jest potrzebna do wyświetlania stron, a wyszukiwarka pomaga je znaleźć w sieci, gdy nie znamy ich adresu. Na świecie i w Polsce liderem jest Google, który pozwala na zawężanie uzy-

[11]https://blog.google/intl/pl-pl/nowosci-firmie/programy-inicjatywy/miedzynarodowy-dzien-sprawdzania-faktow-jak-weryfikowac-informacje-w-internecie/, data dostępu: 7.03.2026.

skanych rezultatów przy użyciu filtrów[12]. Poniżej wpisanych słów kluczowych można wybrać typ wyniku, np.: Tryb AI, Wszystko, Grafika, Krótkie filmy, Wideo, Wiadomości (il. 17).

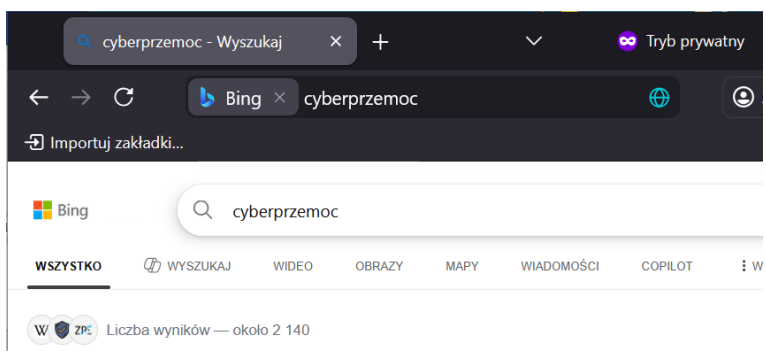


17. Zawężanie wyników wyszukiwania w Google

Użycie polecenia **Narzędzia** udostępnia opcje zależne m.in. od wyszukiwanego hasła i wskazanego typu treści, a nawet zalogowania na konto Google. W szczególności dla **Wszystko** to np.: język, data publikacji strony czy przejście do szukania zaawansowanego (il. 17), a dla **Grafiki** m.in.: rozmiar, kolor, prawa do użytkowania bądź typ.

Przykład 10. Skorzystaj z przeglądarki internetowej **Firefox** w trybie prywatnym i dla słowa kluczowego **cyberprzemoc** porównaj liczbę rezultatów otrzymanych za pomocą wyszukiwarki **Bing** oraz **Google**. W obu przypadkach wyniki ogranicz do typu **Wszystko**.

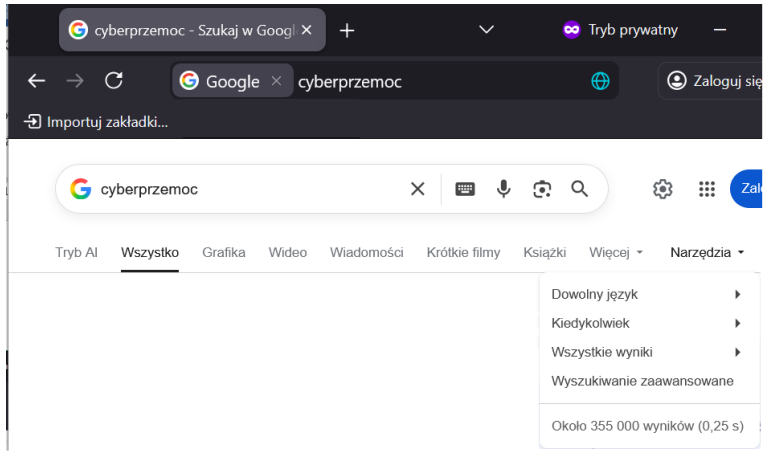
1. Uruchom przeglądarkę Firefox i użyj skrótu klawiaturowego [Ctrl] + [Shift] + [P], aby przejść do trybu prywatnego.
2. Przejdź do strony www.bing.com.
3. Wpisz **cyberprzemoc** i wybierz **Wszystko** (il. 18).



18. Bing i liczba wyników dla hasła[13]

4. Otwórz stronę www.google.com.
5. Powtórz czynność z punku 3 (il. 19).
6. Rozwiń listę **Narzędzia**, aby zobaczyć liczbę rezultatów (il. 19).

[12] https://support.google.com/websearch/answer/142143, data dostępu: 11.03.2026.
[13] Data dostępu: 10.03.2026.

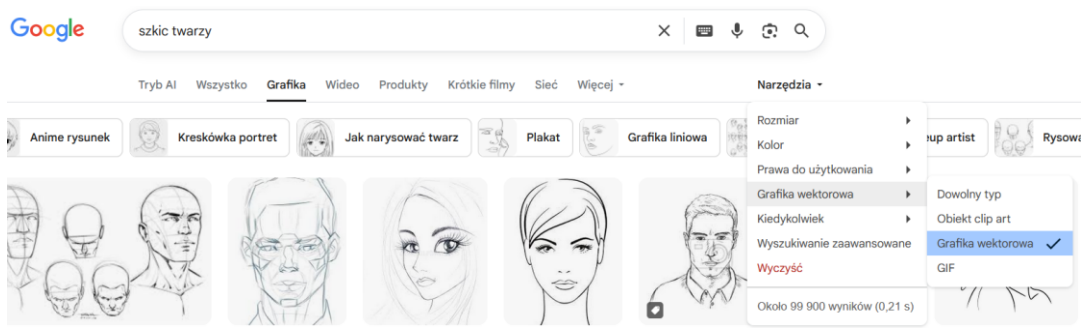


19. Google i liczba rezultatów dla hasła[14]

7. Wyszukiwarka Bing znalazła 2 140 wyników (il. 18), a Google 355 000 (il. 19).

Przykład 11. Znajdź w Google grafiką wektorową dla hasła **szkic twarzy**.

1. Wpisz adres www.google.pl, a potem **szkic twarzy** (il. 20).
2. Kliknij przycisk:
   2.1. **Grafika**.
   2.2. **Narzędzia** i z menu **Typ** wybierz **Grafika wektorowa** (il. 20).



20. Wyszukane grafiki wektorowe

Do wpisywanych słów kluczowych wolno bezpośrednio dodawać operatory wyszukiwania zaawansowanego (tabela 2) i doprecyzować wyniki.

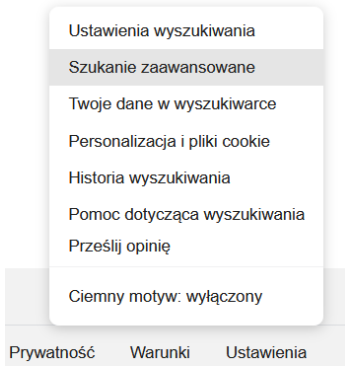
Tabela 2. Wybrane operatory szukania zaawansowanego w Google

L. p.	Operator	Znaczenie	Przykład
1.	„”	Wyszukuje dokładnie wpisane hasło, w przypadku ciągu słów zachowuje kolejność. Korzystanie może powodować, że nie widzi się przydatnych treści z blisko powiązanymi słowami.	„stypendium socjalne”
2.	-	Wyklucza dane słowo lub wyrażenie z wyników.	zupa -pomidorowa.
3.	+	Wymusza uwzględnienie konkretnego słowa w wynikach wyszukiwania.	kawa +rozpuszczalna
4.	*	Zastępuje treść między wpisanymi frazami, gdy brakuje wyrazów w cytatach czy nazwach.	sukces to * bez utraty entuzjazmu

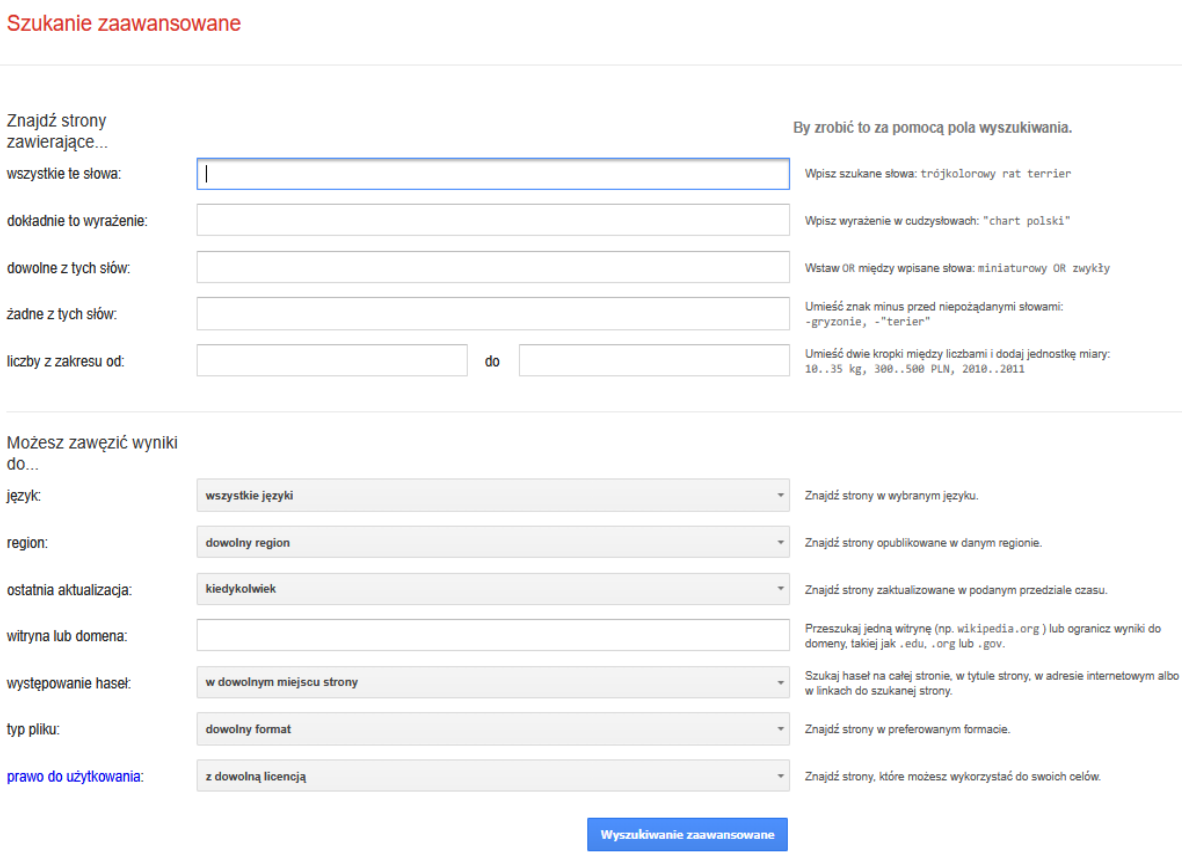
[14] Data dostępu: 10.03.2026.

5.	filetype:	Zawęża rezultaty do podanych typów plików.	poznaj ptaki filetype:pdf
6.	allintitle:	Wyszukuje strony z wyrazami w tytule.	allintitle:Uniwersytet w Siedlcach
7.	in	Zamienia jednostki m.in. miar, wag, walut, temperatur.	300 USD in EUR
8.	site:	Ogranicza wyniki do konkretnej witryny lub domeny.	administracja site:uws.edu.pl, olimpiady site:edu.pl

Można nie pamiętać słów lub symboli (tabela 2) i korzystać z formularza (il. 22), który jest dostępny po kliknięciu **Ustawienia** w prawym dolnym rogu strony www.google.pl oraz polecenia **Szukanie zaawansowane** (il. 21).



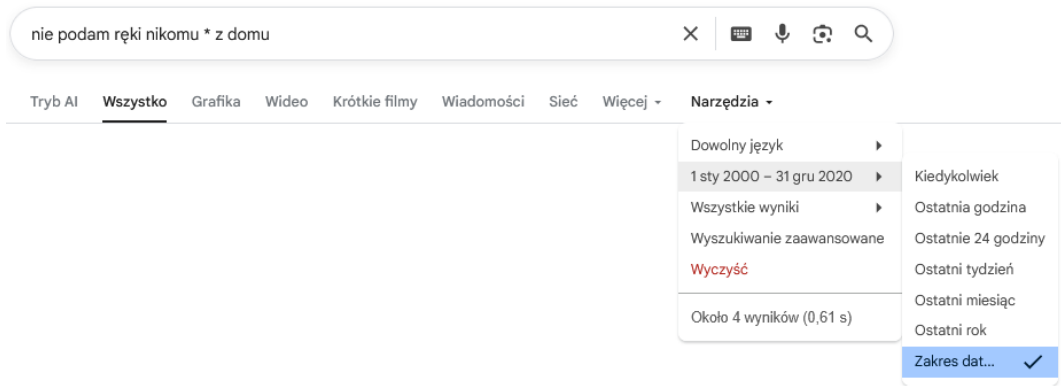
21. Otwieranie formularza szukania zaawansowanego



22. Formularz szukania zaawansowanego w Google

Przykład 12. Uzupełnij cytat Melchiora Wańkowicza, który zaczyna się od słów **nie podam ręki nikomu** a kończy na **z domu**. Zawęź wyszukiwanie do zakresu dat 1.01.2000 - 31.12.2020.

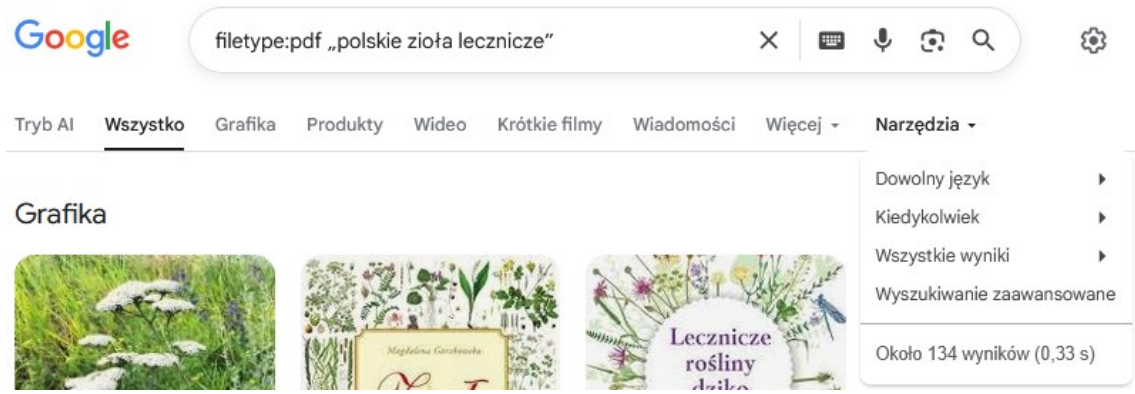
1. Na stronie www.google.pl w polu wyszukiwania wpisz: **nie podam ręki nikomu * z domu** (il. 23).
2. Z **Narzędzi** wybierz opcję **Zakres dat** i wprowadź je: **1.01.2000** oraz **31.12.2020** (il. 23).
3. Uzupełniony cytat: **Nie podam ręki nikomu, kto nie wie jak jego prababka z domu**.



23. Wyszukiwanie z symbolem „gwiazdki" i zakresem dat

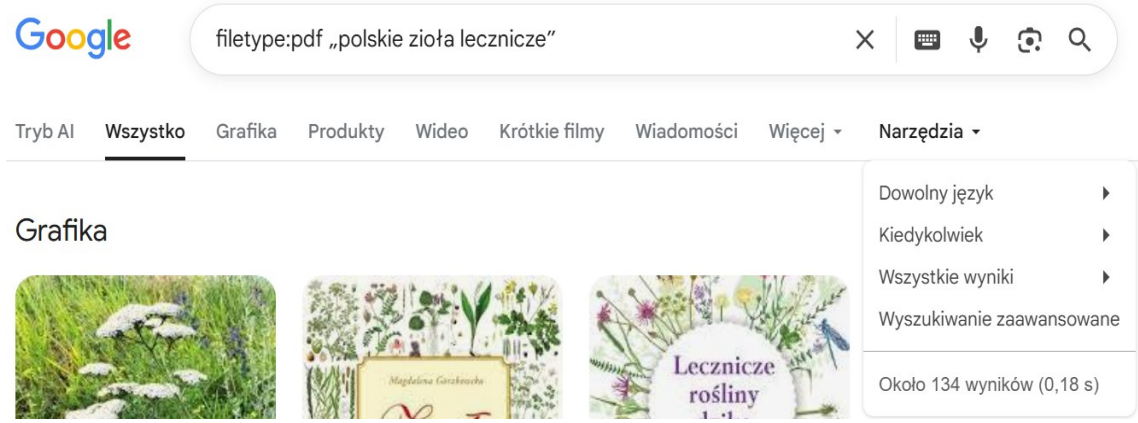
Przykład 13. Porównaj szybkość działania przeglądarek Firefox oraz Microsoft Edge na przykładzie szukania z Google stron internetowych dla dokładnego wyrażenia **polskie zioła lecznicze**, ogranicz wyniki do plików **pdf**.

1. Otwórz przeglądarkę Firefox i stronę www.google.pl.
2. Wpisz **filetype:pdf „polskie zioła lecznicze"** (il. 24). Zwróć uwagę, że nie ma spacji między operatorem filetype a formatem pliku pdf. Możesz też uruchomić formularz szukania zaawansowanego i skorzystać z pól **dokładnie to wyrażenie** oraz **typ pliku** (il. 22).



24. Firefox i czas szukania

3. W opcjach **Narzędzi** sprawdź czas (il. 24).
4. Otwórz przeglądarkę Microsoft Edge i stronę www.google.pl.
5. Powtórz czynności z punktów 2-3 (il. 25).



25. Edge i czas szukania

6. Przeglądarka Firefox znalazła rezultaty w ciągu 0,33 sekundy, a Microsoft Edge w 0,18 sekundy.

Przykład 14. Znajdź w wyszukiwarce Google strony z wyrazem **stypendium**, wyniki ogranicz do witryny uws.edu.pl.

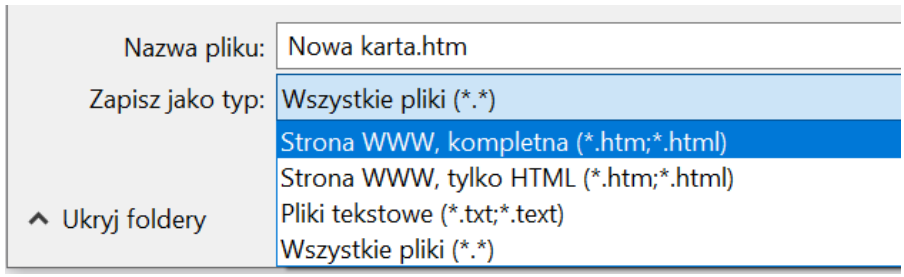
1. Otwórz stronę www.google.pl i wpisz **site:uws.edu.pl stypendium**. Zwróć uwagę, że między operatorem **site** a domeną nie ma spacji.
2. Opcjonalnie możesz skorzystać z formularza i pól **wszystkie te słowa** oraz **witryna lub domena** (il. 22).

4. ZARZĄDZANIE INFORMACJĄ

Wyszukane strony internetowe można m.in. zapisywać, aby czytać je w późniejszym czasie offline lub tworzyć do nich zakładki, ale też pobierać za pomocą specjalistycznych programów.

Przykład 15. W przeglądarce Firefox zapisz dowolną stronę internetową, korzystając z dostępnych typów.

1. Otwórz Firefox i wybraną stronę internetową.
2. W prawym górnym rogu paska adresu kliknij ikonkę menu , a potem **Zapisz stronę jako**.
3. Określ lokalizację, opcjonalnie zmień nazwę pliku.
4. W polu **Zapisz jako typ** wybierz opcję (il. 26):
   - 4.1. **Strona WWW, kompletna**: powstają dwa elementy - plik html i powiązany folder o tej samej nazwie zawierający grafiki, style, skrypty potrzebne do wyświetlenia strony offline.
   - 4.2. **Strona WWW, tylko HTML**: pojedynczy plik z kodem html i linkami, bez obrazów i stylów.
   - 4.3. **Pliki tekstowe**: ekstrakcja samej treści tekstowej.
   - 4.4. **Wszystkie pliki**: podobnie jak **Strona WWW, tylko HTML**, ale w oknie zapisu użytkownik może ręcznie określić rozszerzenie pliku.

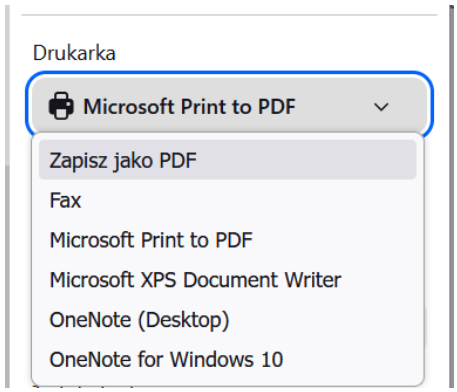


26. Firefox i opcje zapisu strony WWW

5. Kliknij **Zapisz**.

Przykład 16. W przeglądarce Firefox zapisz stronę Wikipedii o historii swojego miasta jako plik PDF.

1. Otwórz Firefoksa.
2. Wpisz słowa kluczowe i z rezultatów wybierz stronę Wikipedii.
3. W prawym górnym rogu pasku adresu wskaż menu i polecenie **Drukuj** lub użyj skrótu klawiaturowego [Ctrl]+[P].
4. Z listy wybierz **Zapisz jako PDF** (il. 27), a potem **Zapisz**.
5. Ustal miejsce, ewentualnie nazwę pliku i kliknij **Zapisz**.

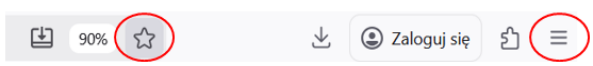


27. Firefox i wydruk do pliku PDF

Zakładki pozwalają zapisywać łącza do często odwiedzanych stron internetowych i umożliwiają szybki do nich dostęp, bez pamiętania adresu. Z myślą, aby nie zajmowały one zbyt dużo miejsca na pasku można nie wpisywać ich nazw, a wtedy będą identyfikowały je tylko ikony stron internetowych (favicon). Zbyt duża liczba zakładek utrudnia znajdowanie przydatnych informacji, dlatego warto je grupować w foldery.

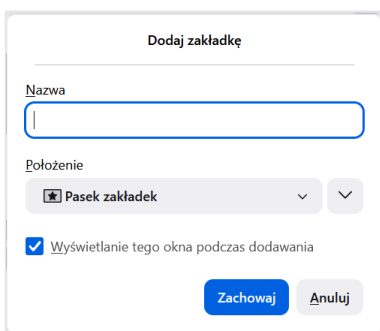
Przykład 17. W Firefox dodaj zakładki bez nazw dla stron: www.uws.edu.pl, ti.ii.uws.edu.pl, allegro.pl oraz www.olx.pl. Umieść je w utworzonych folderach **Studia** i **Zakupy** na **Pasku zakładek**.

1. Otwórz przeglądarkę Firefox.
2. Przejdź do strony internetowej.
3. Kliknij:
   3.1. Gwiazdkę na pasku adresu (il. 28). Możesz też wskazać menu (il. 28) i polecenia **Zakładki > Dodaj zakładkę do tej karty** bądź użyć skrótu klawiaturowego [Ctrl]+ [D].



28. Firefox i dodawanie strony do zakładek

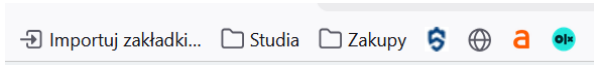
   3.2. W polu **Nazwa**, aby usunąć domyślny tekst (il. 29).



29. Edytowanie zakładki

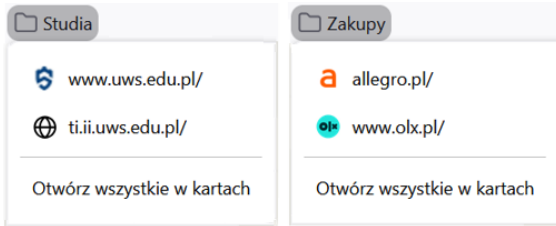
   3.3. **Zachowaj** (il. 29).
4. Powtórz czynności z punktów 2-3, aby utworzyć zakładki do wszystkich wymienionych stron.

5. Na **Pasku zakładek**, z menu kontekstowego, wybierz **Dodaj folder** i nazwij go **Studia**. Tak samo utwórz katalog **Zakupy** (il. 30).



30. Pasek zakładek z folderami i ikonami stron internetowych

6. Metodą przeciągnij i upuść zmień położenie ikon, strony z domeną uws.edu.pl przenieś do folderu **Studia**, a pozostałe do **Zakupy** (il. 31).



31. Zakładki pogrupowane w foldery

5. LICENCJE CREATIVE COMMONS

Prawa autorskie chronią twórców i ich oryginalne utwory o indywidualnym charakterze, bez względu na postać (np. pisemną, cyfrową, dźwiękową), wartość, przeznaczenie oraz sposób wyrażenia[15]. Przykładami takich dzieł są m.in. książki, wiersze, piosenki, malarstwo, rzeźby, zdjęcia, filmy, programy komputerowe. Nie każda praca człowieka podlega ochronie - dotyczy to np. dokumentów urzędowych, formularzy, prostych tabel, jednostkowych informacji, odkryć naukowych czy wzorów matematycznych.

W Polsce prawa autorskie dzielą się na majątkowe i osobiste. Na mocy pierwszych twórca eksploatuje dzieło w sposób komercyjny i bez jego zgody nikt z niego nie może czerpać korzyści finansowych. Ponieważ te prawa są zbywalne, wolno je choćby sprzedać, udzielić licencji, podarować czy odziedziczyć. Obowiązują za życia oraz 70 lat po śmierci twórcy; potem wygasają, a utwór przechodzi do tzw. domeny publicznej i jest dostępny dla wszystkich bez ograniczeń. Natomiast prawa osobiste nigdy nie przemijają, zapewniając łączność autora z dziełem.

Można korzystać z już rozpowszechnionych utworów bez zgody twórcy czy właściciela praw autorskich w ramach tzw. **dozwolonego użytku** osobistego bądź publicznego[16]. Pierwszy pozwala zaspokajać potrzeby własne oraz osób pozostających w relacjach rodzinnych lub towarzyskich. Dla przykładu wolno pożyczyć książkę babci, wykonać jej kopię ksero dla siebie, czy oglądać film na platformie streamingowej z przyjaciółmi w domu. Przepisów tych nie stosuje się do utworów nieupublicznionych, programów komputerowych (w tym gier), budowania zgodnie z cudzym projektem architektonicznym, chronionych baz danych oraz eksploatacji komercyjnej. Natomiast dozwolony użytek publiczny obejmuje korzystanie z dzieła w celach edukacyjnych, naukowych, informacyjnych lub kulturalnych. Umożliwia on np. bibliotekom udostępnianie zbiorów, odtwarzanie muzyki na akademiach szkolnych oraz wykorzystanie fragmentów utworów w twórczości własnej. Oczywiście nie zwalania to z podania imienia i nazwiska twórcy a także źródła, jeśli to możliwe.

W celu odchodzenia od reguły **wszystkie prawa zastrzeżone** do **pewne prawa zastrzeżone** powstały bezpłatne licencje prawne Creative Commons[17]. Pozwalają one twórcom dzielić się swoim dorobkiem z innymi przy określeniu czterech podstawowych warunków:

Uznanie autorstwa (BY) - konieczność wskazania twórcy.

Użycie niekomercyjne (NC) - nie wolno korzystać do osiągania zysków finansowych.

Na tych samych warunkach (SA) - zastosownaie identycznej licencji do utworów zależnych.

[15] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 Nr 24 poz. 83).

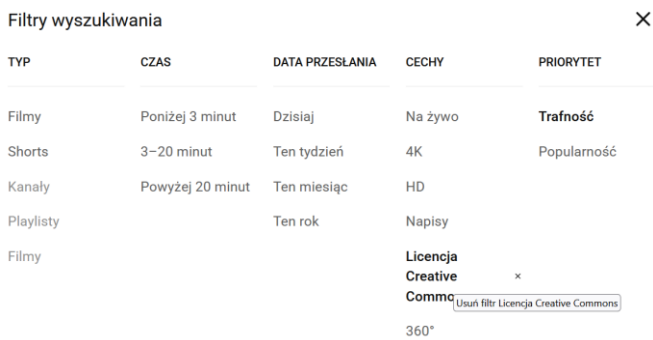
[16] https://www.legalnakultura.pl/pl/strefa-edukacji/strefa-dla-uczniow/warto-wiedziec/dozwolony-uzytek#gsc.tab=0, data dostępu: 11.03.2026.

[17] https://creativecommons.pl/poznaj-licencje-creative-commons/, data dostępu: 11.03.2026.

Bez utworów zależnych (ND) - zakaz tworzenia dzieł pochodnych, tylko oryginalna postać. Utwory zależne (inaczej pochodne) to twórcze przeróbki, adaptacje lub tłumaczenia dzieł pierwotnych, w których elementy oryginału zostały uzupełnione o nowy kreatywny wkład. Kombinacje wymienionych licencji określają zasady korzystania z dzieł, wskazując co jest dozwolone, a co nie, np. CC BY-NC-ND (Uznanie autorstwa - Użycie niekomercyjne - Bez utworów zależnych). Jeśli twórca zrzeka się praw autorskich, to utwór oznacza znakiem: CC0 (CC Zero) i tym samym przenosi go do domeny publicznej. Licencje CC są zaprojektowane do wytworów kultury, tekstów, obrazów, muzyki oraz innych treści cyfrowych, ale nie do programów komputerowych. Jeśli materiały mają być opublikowane na stronach WWW warto z narzędziem creativecommons.org/choose wygenerować część kodu HTML, który rozpoznają wyszukiwarki internetowe, np. Google[18]. Polska witryna https://creativecommons.pl/ umożliwia m.in. obejmowanie własnych prac wspomnianymi standardami prawnymi oraz znajdowanie treści dostępnych na tych zasadach.

Przykład 18. Poszukaj w serwisie YouTube materiałów dla hasła **sekretne miejsca**, skorzystaj z filtrów, aby uwzględnić licencję Creative Commons.

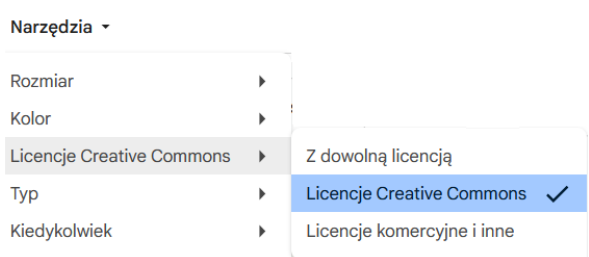
1. Otwórz stronę www.youtube.com.
2. Wpisz hasło przedmiotowe **sekretne miejsca**.
3. W prawym, górnym rogu rozwiń **Filtry wyszukiwania** Filtry.
4. W części **Cechy** wybierz **Licencja Creative Commons** (il. 32), a wyświetlą się wyniki wyszukiwania.



32. YouTube i filtr Licencja Creative Commons

Przykład 19. Skorzystaj z wyszukiwarki Google i licencji Creative Commons, aby znaleźć grafiki dla hasła **Oscar Wilde**. Wybierz zdjęcie z pomnikiem w Dublinie z serwisu Flickr (il. 34). Na jakich warunkach można korzystać z fotografii?

1. Otwórz stronę www.google.com, wpisz słowa kluczowe: **Oscar Wilde** i naciśnij Enter.
2. Kliknij:
   2.1. **Grafika**.
   2.2. **Narzędzia > Prawa do użytkowania** > **Licencje Creative Commons** (il. 33).



*33. Wyszukiwanie obrazów na licencjach **Creative Commons***

3. Wybierz zdjęcie z serwisu internetowego Flickr (il. 34).

[18] https://creativecommons.pl/instrukcja-dokument/, data dostępu: 11.03.2026.

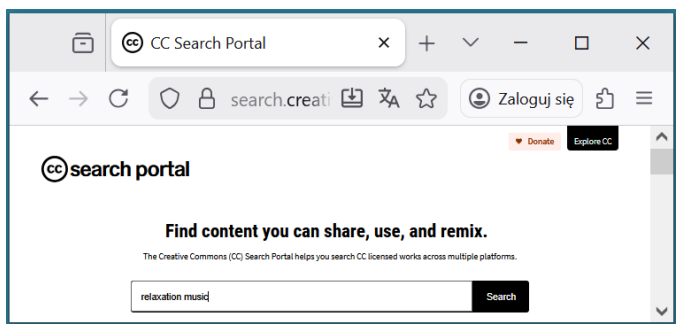


34. Pomnik Wilde'a w Dublinie[19]

4. Oznaczenie fotografii . Licencja CC BY-NC-ND (Uznanie autorstwa - Użycie niekomercyjne - Bez utworów zależnych) umożliwia bezpłatne pobieranie, udostępnianie, kopiowanie oraz pokazywanie fotografii o ile wskaże się autora (BY), nie wykorzysta do celów komercyjnych (NC) i nie przerobi zdjęcia, czyli pozostawi jego oryginalny wygląd (ND).

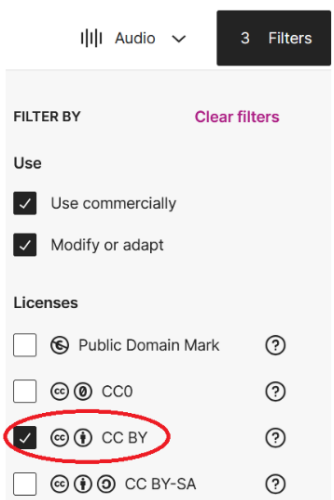
Przykład 20. Skorzystaj z witryny https://creativecommons.pl/ i znajdź muzykę relaksacyjną dostępną na licencji Creative Commons, która wymaga jedynie uznania autorstwa (CC BY).

1. Wpisz adres **creativecommons.pl** i przejdź do witryny.
2. Kliknij kolejno **Znajdź zasoby > Wyszukiwarka Creative Commons**.
3. Wprowadź hasło przedmiotowe **relaxation music** i naciśnij **Search** (il. 35).



35. Okno wyszukiwania na stronie https://search.creativecommons.org/

4. Kliknij przycisk **Audio** i zaznacz licencję CC BY (il. 36).



36. Zastosowane filtry

[19] https://www.flickr.com/photos/anaxila/375475382, data dostępu: 10.04.2026.

5. Poniżej trzy pierwsze wyszukane propozycje (il. 37).



37. Początkowe rezultaty szukania

6. KORZYSTANIE Z BAZ UNIWERSYTETU W SIEDLCACH

Wiele uporządkowanych zbiorów informacji gromadzą i udostępniają internetowe bazy danych. Można je przeszukiwać za pomocą formularzy, które wysyłają zapytania i prezentują wyniki.

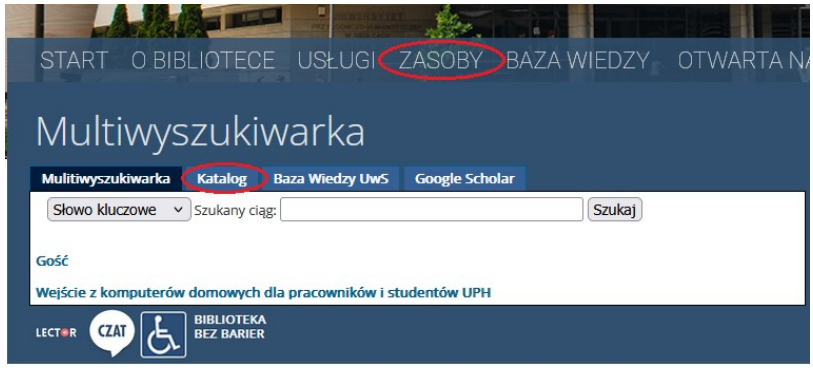
Biblioteka Główna Uniwersytetu w Siedlcach pozyskuje i udostępnia zasoby potrzebne do realizacji badań naukowych oraz procesu dydaktycznego. Korzystają z nich pracownicy, studenci, a ze względu na ich uniwersalny zakres tematyczny także mieszkańcy miasta i regionu[20]. Oprócz zbiorów tradycyjnych, do których należą m.in. książki, czasopisma, broszury, są też specjalne, np. płyty analogowe, książki CD czy wydawnictwa tzw. drugiego obiegu. Instytucja subskrybuje również abstraktowe, bibliograficzne, pełnotekstowe bazy danych, e-książki oraz e-czasopisma, a dostęp do większości licencjonowanych treści cyfrowych zapewniają komputery w sieci uczelnianej[21].

Elektroniczny katalog INTEGRO pozwala korzystać online z zasobów bibliotecznych. Umożliwia ich przeglądanie według indeksów wyszukiwawczych: **Wszystkie pola**, **Tytuł**, **Autor** czy **Temat** albo znajdowanie konkretnego egzemplarza po wpisaniu numeru, pełnego lub tylko części, inwentarza bądź sygnatury. Pozwala również sprawdzać dostępność publikacji, a zalogowanym użytkownikom – zamawiać je przez Internet, rezerwować wypożyczone oraz przedłużać termin ich zwrotu (prolongata). Rezultaty jednego zapytania pochodzą z wielu źródeł m.in. Biblioteki Cyfrowej UWS, IBUK Libry, Repozytorium UWS, czy bezpłatnej biblioteki internetowej Wolne Lektury[22]. Wyniki wyszukiwania można zawęzić za pomocą faset widocznych w lewym panelu do: Roku publikacji, Agendy, Typu dokumentu, Autora, Tematu, Lokalizacji, Położenia, Języka, Kraju, Formy dzieła, Okresu powstania, Dziedziny, Odbiorcy, Serii, Klasyfikacji wewnętrznej. Pozwala to na stopniowe ograniczanie wyboru przez korzystanie z wielu filtrów równocześnie.

> Przykład 21. W katalogu INTEGRO Biblioteki Głównej Uniwersytetu w Siedlcach znajdź publikacje, które w **tytule** zawierają frazę: **jak radzić sobie ze stresem**. Uwzględnij następujące ograniczenia: Rok publikacji: 2000 – 2025; Agenda: Biblioteka – Wyp.Gł.; Temat: Poradnik; Dziedzina: Psychologia, Edukacja i pedagogika. Zrób zrzut ekranu z aktywnymi filtrami dla użytej frazy.

1. Otwórz stronę https://bg.uws.edu.pl/ (il. 38).

[20] https://bg.uph.edu.pl/o-bibliotece/misja-i-zbiory/, data dostępu: 21.02.2026.
[21] https://bg.uph.edu.pl/zasoby/, data dostępu: 11.03.2026.
[22] https://bg.uws.edu.pl/images/OIN/PDF/Przewodnik_2023.pdf, data dostępu: 7.02.2026.



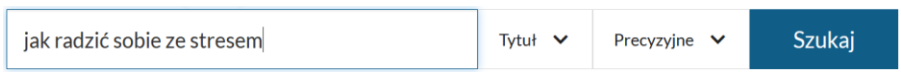
38. Widok strony Biblioteki Głównej Uniwersytetu w Siedlcach

2. Wybierz zakładkę **Katalog** (il. 38). Możesz wskazać też **Zasoby** (il. 38) i po stronie lewej **Katalogi**, a następnie przycisk **INTEGRO** (il. 39).



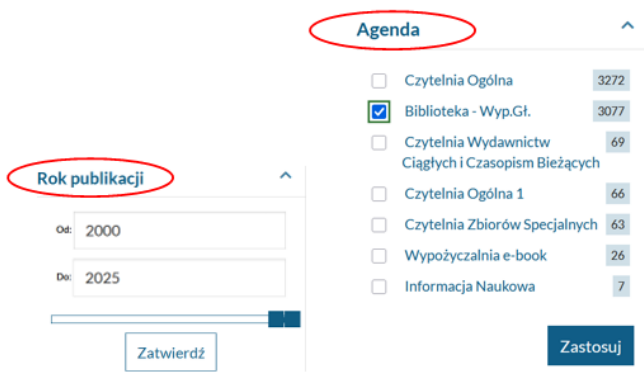
*39. Widok zakładki **Katalogi** na stronie Biblioteki Głównej Uniwersytetu*

3. W oknie wyszukiwania wpisz: **jak radzić sobie ze stresem**, po stronie prawej wskaż z listy kryterium **Tytuł** i naciśnij **Szukaj** (il. 40).



40. Okno wyszukiwania katalogu INTEGRO

4. Do otrzymanych wyników wykorzystaj filtry, za każdym razem użyj przycisku Zatwierdź lub Zastosuj:
   4.1. **Rok publikacji**: 2000-2025 (il. 41).



*41. Filtry **Rok publikacji** i **Agenda***

4.2. **Agenda**: Biblioteka – Wyp.gł. (il. 41).
4.3. **Temat**: Poradnik.
4.4. **Dziedzina**: Psychologia oraz Edukacja i pedagogika.

5. Kliknięcie tytułu wybranej pozycji wyświetla jej szczegóły (np. sygnaturę i dostępność), a zalogowanym użytkownikom pozwala na jej zamówienie lub rezerwację.
6. Poniżej zrzut fragmentu ekranu z aktywnymi filtrami (il. 42).



42. Użyte filtry do szukanej frazy w tytule

Biblioteka Uniwesytetu w Siedlcach posiada dostęp m.in. do elektronicznych książek i czasopism z wielu dziedzin nauki w postaci różnorodnych baz danych m.in.:

1. Bibliograficznych; obejmują one opisy dokumentów (autor, tytuł, źródło) i abstrakty. Są polecane do przygotowania przeglądu literatury bądź szukania źródeł na określony temat.
2. Pełnotekstowych; zapewniają wgląd do całych treści i warto z nich korzystać, aby szybko zapoznać się z konkretnym artykułem.
3. Faktograficznych; zawierają gotowe informacje np. liczby, wzory, tabele. Są używane, aby uzyskać bezpośrednie odpowiedzi i konkretne dane.

Coraz częściej zacierają się granice między tymi narzędziami, np. bazy pełnotekstowe posiadają możliwości przeszukiwania jak bibliograficzne, a te z kolei zawierają linki do pełnych tekstów. Biblioteka oferuje także dostęp do zasobów Ibuk Libra, tj. czytelni online e-booków naukowych i akademickich z różnych dziedzin[23].

Przykład 22. W pełnotekstowej bazie danych **Lex** znajdź obowiązującą ustawę: **Prawo o szkolnictwie wyższym i nauce**. Zapisz ją w formacie **.docx**, wybierz czcionkę Arial, 11 pt.

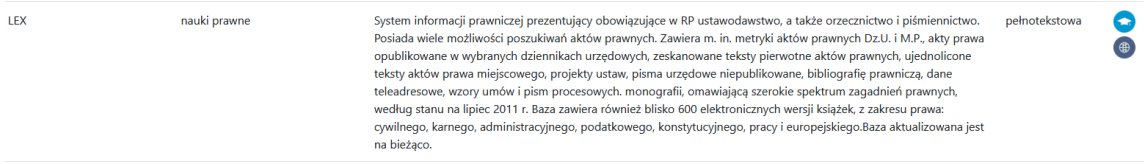
1. Wpisz adres bg.uws.edu.pl, kliknij kartę **Zasoby** (il. 38), a potem **Wyszukiwarka e-źródeł** (il. 39, 43).



43. Wyszukiwarka e-źródeł z pierwszymi bazami

[23] https://bg.uws.edu.pl/zasoby/ibuk-libra; data dostępu: 13.03.2026.

2. Znajdź bazę **Lex** i z prawej strony wybierz **Dostęp z sieci UwS** (il. 44).



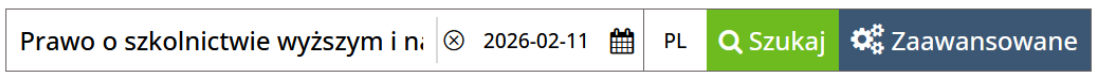
44. Wyszukiwarka e-źródeł i baza danych Lex

3. Zaloguj się, podając numer karty bibliotecznej i hasło.
4. Kliknij w obszarze pola (il. 45), aby przejść do wyszukiwania.



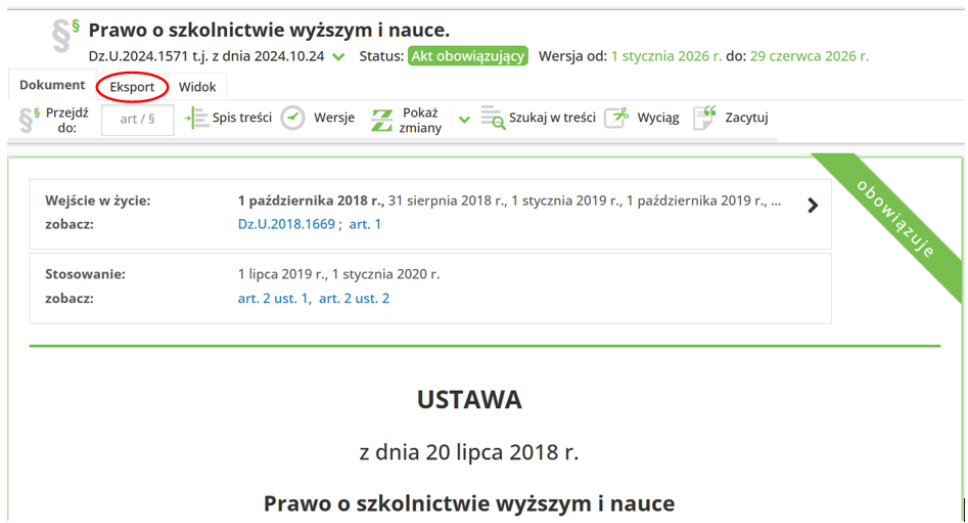
45. Wejście do programu

5. Wpisz hasło: **Prawo o szkolnictwie wyższym i nauce** (il. 46).



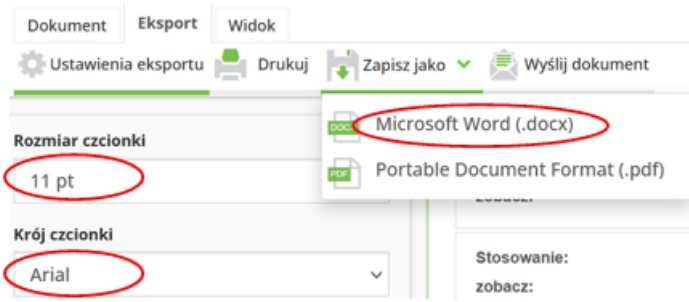
46. Okno wyszukiwarki głównej LEX

6. Wybierz:
   6.1. **Szukaj** (il. 46).
   6.2. W lewym górnym rogu kartę **Eksport** (il. 47).



47. Znaleziona ustawa w oknie szukania zaawansowanego bazy Lex

7. Rozwiń **Zapisz jako** i wskaż **Microsoft Word (.docx)** (il. 48).



48. Karta Eksportu bazy Lex

8. Po lewej stronie ustal czcionkę Arial 11 pt (il. 48).
9. Dokument pojawi się w folderze **Pobrane**.

Przykład 23. W bazie danych ProQuest znajdź artykuł **David Kennedy: The Impact of Neuroinformatics** i pobierz pełny jego tekst w formacie PDF na dysk lokalny komputera.

1. Otwórz stronę bg.uph.edu.pl, kliknij **Zasoby** (il. 38) i **Wyszukiwarka e-źródeł** (il. 39).
2. Znajdź bazę **ProQuest** i wskaż **Dostęp z sieci UwS** .
3. Przejdź z wyszukiwania prostego do zaawansowanego (il. 49).



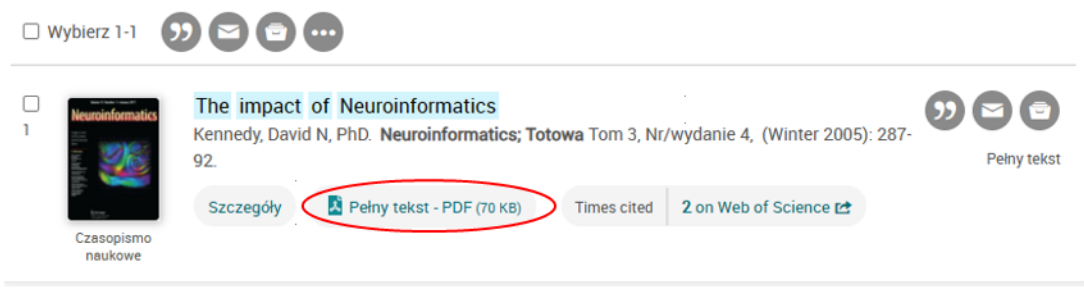
49. Wyszukiwanie proste w bazie ProQuest

4. Wpisz:
   4.1. **The Impact of Neuroinformatics**, a po prawej stronie z listy wybierz **Tytuł dokumentu – TITLE** (il. 50).
   4.2. **David Kennedy** i z rozwijanej listy wskaż **Autor – AUTHOR** (il. 50).



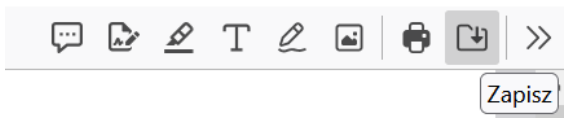
50. Okno wyszukiwania zaawansowanego w bazie ProQuest

5. Zaznacz opcję **Pełny tekst** (il. 50) i naciśnij **Wyszukaj**.
6. W oknie z wyświetlanym artykułem kliknij **Pełny tekst – PDF** (il. 51).



51. Baza ProQuest i wyszukany artykuł

7. Wybierz **Zapisz** (il. 52) i wskaż lokalizację pliku na komputerze.



52. Pasek narzędzi widoczny nad artykułem

7. ZADANIA

Pliki do zadań 4, 5, 9 i 13.1 zapisz w folderze na pulpicie, a dla pozostałych punktów wklej zrzuty ekranu do dokumentu Word.

1. Użyj wiersza poleceń (cmd) i sprawdź adres IP dla domeny www.uws.edu.pl.
2. Otwórz aplikację Zabezpieczenia Windows i skontroluj datę ostatniej aktualizacji analizy zabezpieczeń w Microsoft Defender.
3. Wybierz tester online i zweryfikuj siłę wymyślonego hasła (minimum 14 znaków).
4. Na podstawie charakterystycznych symboli zidentyfikuj programy antywirusowe i podaj ich nazwy (il. 53). Skorzystaj z pliku Internet I_4-5.docx umieszczonego w folderze Zadania.



53. Graficzne oznaczenia wybranych antywirusów

5. Na przykładzie frazy **technologia informacyjna** sprawdź, jak wpływają na wyniki wyszukiwania operatory Google, takie jak cudzysłów, plus i minus. Obok każdego przykładu zapisz liczbę znalezionych stron internetowych (tabela 3). Użyj pliku Internet I_4-5.docx, który znajduje się w folderze Zadania.

Tabela 3. Wpływ wybranych operatorów na wyniki wyszukiwania

l.p.	Szukana fraza	Liczba wyników
1.	technologia informacyjna	
2.	„technologia informacyjna”	
3.	technologia -informacyjna	
4.	technologia +informacyjna	

6. Wyszukaj w Google:
   6.1. Grafiki dla słów kluczowych **postacie z gier komputerowych**; spośród kolorów zastosuj przezroczyste.
   6.2. Strony dla hasła **organizacja roku akademickiego**; wyniki ogranicz do witryny **uws.edu.pl** i czasu **ostatni rok**.

   W zrzutach ekranu uwzględnij wykorzystane filtry i operatory.
7. Użyj tej samej przeglądarki w trybie prywatnym/incognito i porównaj liczbę rezultatów, jakie zwracają wyszukiwarki Bing i Google dla hasła **antywirusy**. W obu przypadkach wyniki ogranicz do typu **Wszystko**.

8. Porównaj czas wczytywania wyników przez dwie wybrane przeglądarki w trybie prywatnym/incognito po wpisaniu w Google nazwy studiowanego kierunku i przefiltrowaniu do plików pdf.
9. W przeglądarce Microsoft Edge znajdź przepis na zupę grzybową i zapisz stronę internetową jako plik pdf.
10. Na pasku zakładek przeglądarki utwórz folder **Studia** i umieść w nim zakładki do uczelnianej poczty oraz systemu USOSweb.
11. Przeszukaj zbiory Biblioteki Głównej Uniwersytetu w Siedlcach z katalogiem INTEGRO. Wybierz indeks wyszukiwawczy **Temat** i jako hasło wpisz nazwę studiowanego kierunku. Zawęź wyniki wyszukiwania do:
    11.1. Roku publikacji: od 2000 do najbliższego obecnemu.
    11.2. Agendy: Biblioteka – Wyp.Gł.
    11.3. Dziedziny: odpowiedniej do zdobywanej wiedzy oraz umiejętności zgodnie z dyscypliną naukową.
    Zrzut ekranu z szukaną frazą oraz aktywnymi filtrami wklej do dokumentu.
13. Z pełnotekstowych baz danych:
    13.1. BazHum pobierz artykuł **Aleksandra Aleksandrowicza** zatytułowany **Pamiętnik**, który został opublikowany w czasopiśmie **Niepodległość i Pamięć** (1996 rok, tom 3, nr 2).
    13.2. ProQuest wyszukaj wyniki dla hasła **sztuczna inteligencja** i zastosuj filtry: Ograniczenie do: Pełny tekst, Typ źródła: Czasopisma naukowe, Data publikacji: Ostatnie 12 miesięcy, Rodzaj dokumentu: Artykuł. Zadbaj, aby zrzut ekranu zawierał szukaną frazą, użyte filtry i widoczny pierwszy wynik.

LITERATURA

https://bg.uws.edu.pl/images/OIN/PDF/Przewodnik_2023.pdf, data dostępu: 7.02.2026.

https://blog.google/intl/pl-pl/nowosci-firmie/programy-inicjatywy/miedzynarodowy-dzien-sprawdzania-faktow-jak-weryfikowac-informacje-w-internecie/, data dostępu: 7.03.2026.

https://creativecommons.pl/poznaj-licencje-creative-commons/, data dostępu: 11.03.2026.

https://cyberprzemoc.pl/, data dostępu: 20.01.2026.

https://support.google.com/websearch/answer/142143, data dostępu: 11.03.2026.

https://www.legalnakultura.pl/pl/strefa-edukacji/strefa-dla-uczniow/warto-wiedziec/dozwolony-uzytek#gsc.tab=0, data dostępu: 11.03.2026.

https://www.malwarebytes.com/pl/malware, data dostępu: 22.02.2026.

SPIS TREŚCI

Wstęp 1
1. Ogólna charakterystyka 1
2. Zagrożenia w Internecie i programy antywirusowe 3
3. Zaawansowane metody wyszukiwania informacji 10
4. Zarządzanie informacją 15
5. Licencje Creative Commons 17
6. Korzystanie z baz Uniwersytetu w Siedlcach 20
7. Zadania 25
Literatura 26