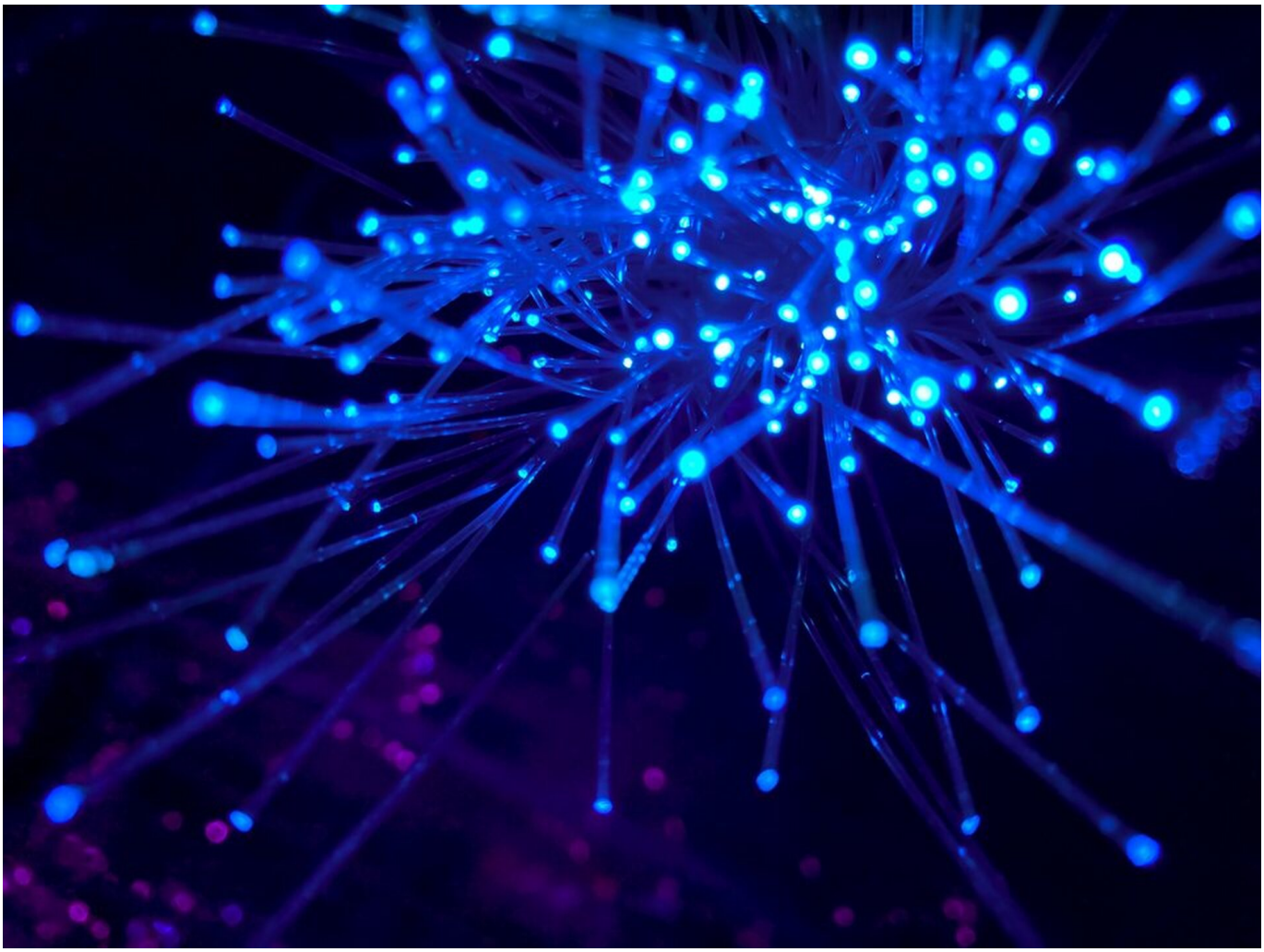


Wirtualna sieć prywatna

Źródło: JJ Ying, dostępny w internecie: unsplash.com, domena publiczna.

Wiele osób nie zdaje sobie sprawy, jak dużo informacji o ich przyzwyczajeniach, upodobaniach, codziennych obowiązkach albo lokalizacji trafia do firm, które twierdzą, że „za darmo" oferują usługi w internecie. W rzeczywistości każdy przejaw aktywności internauty da się wyśledzić i przeanalizować, a następnie wykorzystać choćby w celach reklamowych.

Firmy, takie jak Google albo Facebook, zbierają olbrzymie ilości danych na temat osób, które korzystają z ich na pozór bezpłatnych kont, komunikatorów oraz innych usług. Później zarabiają dzięki tym informacjom miliardy dolarów, ponieważ są w stanie dostarczyć użytkownikom spersonalizowane reklamy.

Jako użytkownicy sieci powinniśmy mieć świadomość, że w internecie nie jesteśmy anonimowi: zawsze pozostawiamy za sobą jakieś ślady. Na szczęście istnieją metody pozwalające zachować nieco prywatności w sieci i utrudnić szpiegowanie naszych poczynań.

> **Twoje cele**
>
> - Przeanalizujesz, jak wiele informacji na twój temat gromadzą firmy świadczące usługi w internecie.
> - Wymienisz sposoby zapewnienia sobie anonimowości.

- Wyjaśnisz potrzebę stosowania szyfrowanej komunikacji w sieciach komputerowych.

Przeczytaj

Internet odcisnął piętno na tym, jak pracujemy, uczymy się i spędzamy czas wolny. Globalna sieć pozwala komunikować się ze znajomymi, wymieniać z nimi dane (na przykład zdjęcia i filmy), a nawet wirtualnie podróżować po świecie.

Korzystając z tych wszystkich udogodnień, często zapominamy o jednym z ważniejszych zagadnień związanych z cyberprzestrzenią, a mianowicie o bezpieczeństwie cyfrowym.

Czym jest bezpieczeństwo cyfrowe?

Użytkownicy internetu codziennie generują olbrzymie ilości danych i coraz częściej świadomie (bądź nie) udostępniają je nie tylko znajomym, ale również firmom, z których usług korzystają. Zgromadzone w ten sposób informacje okazują się niezwykle cenne.

Czy przypuszczacie, że wszystkie „darmowe" usługi w internecie są naprawdę bezpłatne? Z tego, że w większości przypadków nie płacimy za nie gotówką, kartą kredytową czy kodami BLIK, nie wynika, że nie ponosimy żadnych kosztów. Otóż usługodawcy pobierają opłaty – tyle, że nie w postaci pieniędzy, lecz danych użytkowników.

Dzięki zebranym informacjom firmy oferujące usługi w internecie wiedzą, jakie miejsca odwiedzamy, w których sklepach robimy zakupy, w jakich restauracjach jadamy, a także kiedy, gdzie i jakie filmy oglądamy. Pozwala to tworzyć profile użytkowników, które mają wielką wartość z punktu widzenia agencji reklamowych. Dysponując wiedzą na temat upodobań internauty, są one w stanie przygotować materiał, który zainteresuje określone grupy odbiorców.

A kto może dostarczyć profile użytkowników sieci? Podajmy dwa najbardziej spektakularne przykłady. Mowa o korporacjach Google (z „bezpłatnymi" kontami pocztowymi i wyszukiwarką) oraz Facebook (z „darmowymi" kontami w sieci społecznościowej, serwisie Instagram i komunikatorami WhatsApp albo Messenger). Szefowie obydwu firm wiedzą doskonale, że każdy dolar zainwestowany w „nieodpłatne" usługi (utrzymanie serwerów, energia elektryczna, pensje pracowników itp.) zwróci się z nawiązką dzięki reklamodawcom płacącym za precyzyjne profile użytkowników.

W internecie trzeba również liczyć się z zagrożeniami. Warto pamiętać, że nawet potężne firmy nie są w stanie uniknąć ataków hakerskich, o czym świadczy m.in. wyciek danych użytkowników portalu Facebook w kwietniu 2021 r. Mając na uwadze takie niebezpieczeństwo, wielu internautów stara się zachować anonimowość w sieci.

Notowanych jest też coraz więcej ataków hakerskich wymierzonych nie w duże firmy, lecz w przeciętnych użytkowników globalnej sieci. Niektóre z nich są bardzo wyrafinowane, a ich konsekwencje są czasami bardzo kosztowne. Dzieje się tak choćby w przypadku przejęcia danych karty kredytowej albo ataku z wykorzystaniem oprogramowania szantażującego (*ransomware*).

> **Ważne!**
>
> Unikając podejrzanych miejsc w internecie, zwiększasz poziom własnego bezpieczeństwa cyfrowego.
>
> **Jego poziom możesz również zwiększyć, korzystając z odpowiednich narzędzi i systemów komunikacji, takich jak VPN, czyli wirtualna sieć prywatna**.

Szyfrowanie i protokoły VPN

W strukturach VPN stosuje się różne metody szyfrowania danych i protokoły komunikacyjne. Część protokołów jest otwarta (dostępna dla wszystkich) i każdemu wolno stosować je we własnej sieci. Firmy oferujące komercyjne usługi VPN korzystają z otwartych protokołów, ale często zdarza się, że oferują własne protokoły i metody szyfrowania, oparte na technologiach ogólnodostępnych. Obecnie najczęściej spotykanymi protokołami i metodami szyfrowania danych w połączeniach VPN są:

- **OpenVPN** – najbardziej popularny w ostatnich latach zbiór metod i technik szyfrowania. Opiera się na otwartym kodzie źródłowym i może być zastosowany w każdej sieci. Wielu komercyjnych dostawców używa tego protokołu, ponieważ zapewnia on wysoki poziom bezpieczeństwa.
- **L2TP/IPsec** – połączenie protokołu L2TP (ang. *Layer 2 Tunnel Protocol*), służącego do zestawiania tunelowanych połączeń VPN z zapewniającym szyfrowanie protokołem IPsec. Problem związany ze stosowaniem opisanego zestawu wynika z faktu, że L2TP/IPsec może być wykrywany i blokowany przez zapory sieciowe na serwerach.
- **IKEv2/IPsec** – połączenie protokołu IKE w wersji 2 (ang. *Internet Key Exchange*) oraz mechanizmów szyfrowania stosowanych w protokole IPSec. Stanowi unowocześnią wersję zestawu protokołów L2TP/IPsec. Zapewnia duży poziom bezpieczeństwa oraz szybkość, ale również może być blokowany przez zapory sieciowe. Jest zalecany do stosowania na urządzeniach mobilnych.
- **SSTP** (ang. *Secure Socket Tunneling Protocol*) – mniej znany protokół tunelowania, będący własnością firmy Microsoft.

Słownik

> **VPN**

(ang. *Virtual Private Network*) wirtualna sieć prywatna – umożliwia szyfrowane połączenie z internetem i siecią firmową

bezpieczeństwo cyfrowe

wyeliminowanie zagrożeń związanych z korzystaniem z sieci komputerowych dzięki zastosowaniu mechanizmów chroniących dane cyfrowe

Prezentacja multimedialna

Polecenie 1

Zapoznaj się z prezentacją. W jakich sytuacjach użytkownicy sieci korzystają z serwerów VPN?

1

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

VPN (ang. Virtual Private Network) jest konstrukcją pozwalającą prowadzić szyfrowaną (kodowaną) komunikację w internecie. Między klientem a serwerem VPN zostaje utworzony wirtualny tunel, niedostępny dla urządzeń, które nie są częścią wirtualnej sieci prywatnej. Pozwala to zachować poufność komunikacji. Jeśli komukolwiek uda się przechwycić transmisję w sieci VPN, to i tak nie będzie on w stanie odczytać danych.

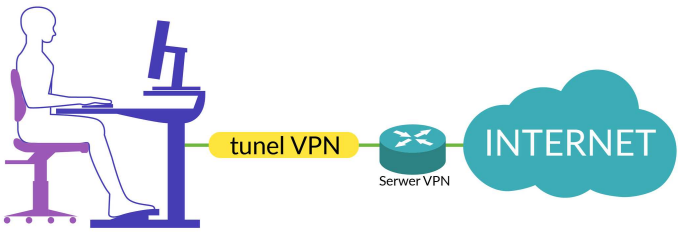
2

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

Dawniej z technologii takiej korzystały korporacje, duże firmy albo instytucje dysponujące odpowiednimi środkami finansowymi. Obecnie jest ona dostępna nawet dla osób prywatnych.

3



Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

VPN tworzy szyfrowany tunel między komputerem użytkownika a serwerem VPN, dzięki czemu osoby postronne nie mogą odczytać przesyłanych informacji.

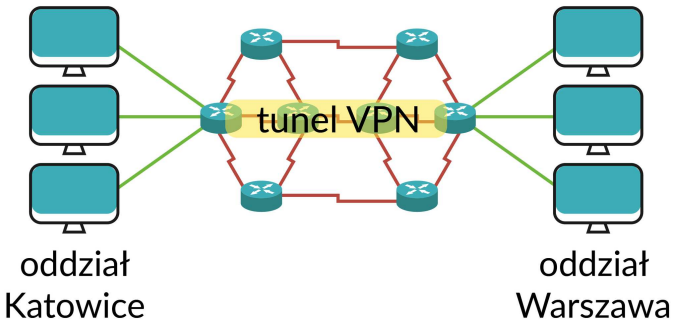
4

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

Rozwiązania VPN są najczęściej stosowane w trzech przypadkach:

5



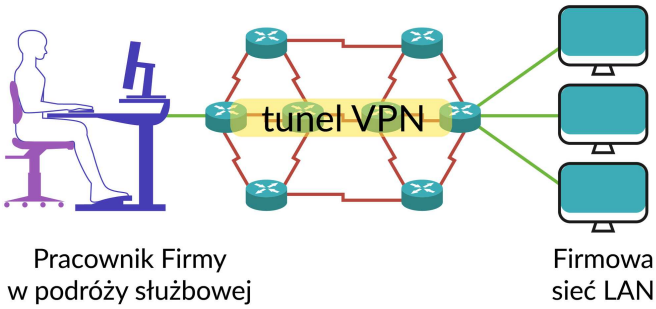
Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

Firma dysponuje dużą, rozproszoną siecią (działającą w różnych miejscach). Za pomocą tunelu VPN typu site-to-site jest możliwe

połączenie ze sobą tych lokalizacji i zapewnienie szyfrowanej komunikacji między nimi.

6



Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

Pracownicy firmy często podróżują służbowo lub pracują zdalnie. Wykorzystanie struktury VPN typu remote-access umożliwia podłączenie się pracownika do sieci lokalnej firmy przez szyfrowany tunel VPN w internecie. Dzięki temu użytkownik ma dostęp do wszystkich usług sieci firmowej, tak jakby pracował w jej siedzibie.

7

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

Użytkownicy internetu chcą zachować anonimowość i zwiększyć poziom swojego bezpieczeństwa cyfrowego. Korzystając z oprogramowania instalowanego na komputerze lub smartfonie (zwanego potocznie bramką VPN), użytkownik łączy się z internetem przez specjalny serwer, który – po pierwsze – zmienia informację o lokalizacji użytkownika, a po drugie – szyfruje całą komunikację. Bramki są oferowane przez dostawców usług VPN i pozwalają na wybór protokołu połączenia (szyfrowania), a także lokalizacji serwera, który będzie w internecie komunikował się z innymi

w naszym imieniu. Możliwe jest dzięki temu choćby ominięcie ograniczeń regionalnych (przykładem jest inna oferta filmowa w USA, a inna w Polsce). Po uruchomieniu bramki użytkownik korzysta z sieci w ten sam sposób co zwykle, ale jego komunikacja jest szyfrowana. Dzięki temu jest chroniona jego tożsamość, a zbieranie przez firmy zewnętrzne informacji o aktywności internauty mocno utrudnione.

8

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

Obecnie z usług VPN może skorzystać każdy użytkownik internetu. Istnieją firmy oferujące dostęp do VPN za darmo, inne wymagają opłacenia abonamentu.

9

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/PNbkOf7AW

W przypadku usług komercyjnych mamy do dyspozycji ofertę firm NordVPN, ExpressVPN, CyberGhost, Syrfshark albo PrivateVPN. Jeśli chodzi o usługi darmowe, warto przyjrzeć się operatorom ProtonVPN, Windescribe czy Hide.me

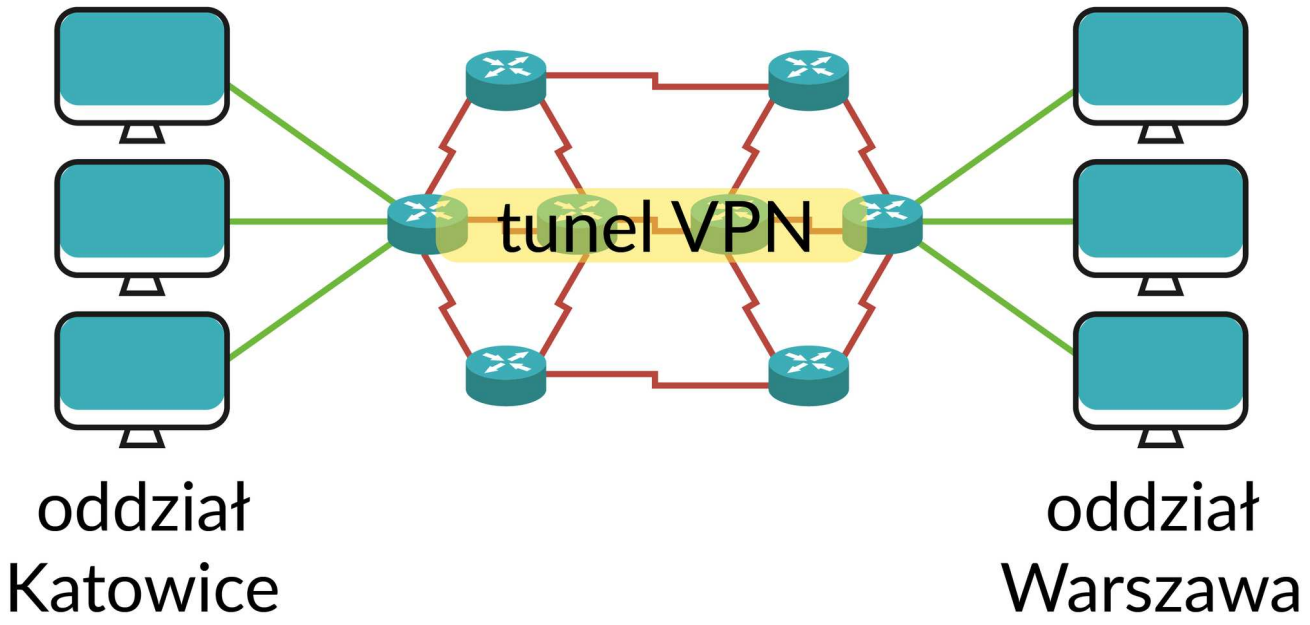
Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Dokończ zdanie.

Grafika przedstawia sieć VPN typu...



- point-to-point.
- point-to-site.
- site-to-site.
- remote access.

Ćwiczenie 2

Przyporządkuj przykładowe scenariusze do odpowiednich rozwiązań:

VPN site-to-site

VPN remote-access

- pracuję w domu i muszę mieć dostęp do plików zapisanych na firmowym serwerze
- nie chcę, aby mój dostawca internetu wiedział, jakie strony WWW przeglądam
- chcę obejrzeć na platformie streamingowej film dostępny tylko w USA
- codziennie przesyłam raporty do szefa, który rezyduje w głównej siedzibie firmy
- pracuję nad projektem wspólnie z Adamem, który rezyduje w oddziale firmy w Gdańsku
- nie chcę udostępniać swojej lokalizacji firmom świadczącym usługi sieciowe
- pracuję w biurze, ale korzystam z aplikacji, której serwery znajdują się w oddziale w Katowicach

Ćwiczenie 3

Przed jakimi zagrożeniami z sieci nie chroni VPN? Wskaż właściwą odpowiedź.

- ◯ szpiegowaniem polegającym na analizowaniu stron WWW, na które wchodzimy
- ◯ zainfekowaniem komputera przez wirusy
- ◯ zbieraniem danych o naszej aktywności w sieci przez dostawcę internetu
- ◯ śledzeniem naszej lokalizacji

Ćwiczenie 4

Uzupełnij zdanie:

Bramki [ ] pozwalają na wybór [ ], poprzez który łączymy się z [ ], a także na wybór protokołu [ ] komunikacji.

ISP | siecią LAN | serwera | bezpiecznej | szyfrowania | NAT | komunikacji | VPN | internetem

Ćwiczenie 5

Dokończ zdanie.

Między serwerem VPN a klientem jest tworzony wirtualny...

- ◯ przekop.
- ◯ ciąg komunikacyjny.
- ◯ most.
- ◯ tunel.

Ćwiczenie 6

Uzupełnij zdanie.

SSTP (ang. *Secure Socket Tunneling Protocol*) to mało znany i stosunkowo rzadko stosowany protokół tunelowania, będący własnością firmy [ ].

NordVPN | Facebook | Microsoft | ExpressVPN | Google

Ćwiczenie 7

Wskaż, co robią firmy z danymi użytkowników.

- ◯ Tworzą profile użytkowników, aby lepiej dopasować proponowane treści oraz właściwie dobierać reklamy.
- ◯ Zawsze przekazują je organom ścigania.
- ◯ Nie wykorzystują ich w żaden sposób, po 30 dnia kasują wszystkie informacje o naszej aktywności.
- ◯ Wykorzystują je wyłącznie do udoskonalania swoich usług.

Ćwiczenie 8

Wskaż, które protokoły VPN są obecnie najbardziej popularne.

- ☐ L2TP/IPsec
- ☐ OpenVPN
- ☐ IKEv2/IPsec
- ☐ SSTP
- ☐ PPTP

Dla nauczyciela

Autor: Damian Stelmach
Przedmiot: Informatyka

Temat: Wirtualna sieć prywatna

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy i rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania – wymagania szczegółowe

III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi.

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

5) wyjaśnia, od czego zależy sprawne funkcjonowanie sieci komputerowej oraz szybki dostęp do jej usług i zasobów (parametry osprzętu sieciowego, szerokość pasma, zabezpieczenia typu ściana ogniowa i programy antywirusowe, możliwości serwera).

V. Przestrzeganie prawa i zasad bezpieczeństwa.

Zakres podstawowy. Uczeń:

3) stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji;

4) opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa.

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;

- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Przeanalizujesz, jak wiele informacji na twój temat gromadzą firmy świadczące usługi w internecie.
- Wymienisz sposoby zapewnienia sobie anonimowości.
- Wyjaśnisz potrzebę stosowania szyfrowanej komunikacji w sieciach komputerowych.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych;
- ćwiczenia praktyczne.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Wirtualna sieć prywatna". Nauczyciel prosi uczniów o zapoznanie się z treściami w sekcji „Przeczytaj".

Faza wstępna:

1. Ustalenie celu lekcji i kryteriów sukcesu.

2. **Rozpoznanie wiedzy uczniów.** Nauczyciel prosi wybranego ucznia lub uczniów o przedstawienie sytuacji problemowej związanej z tematem lekcji.

Faza realizacyjna:

1. **Praca z tekstem.** Jeżeli przygotowanie uczniów do lekcji jest niewystarczające, nauczyciel prosi o indywidualne zapoznanie się z treścią zawartą w sekcji „Przeczytaj". Każdy uczestnik zajęć podczas cichego czytania wynotowuje najważniejsze kwestie poruszane w tekście.
2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Prezentacja multimedialna". Uczniowie wspólnie zapoznają się z jego treścią. Zapisują ewentualne problemy i pytania. Po czym następuje dyskusja, w trakcie której nauczyciel wyjaśnia niezrozumiałe treści.
3. **Ćwiczenie umiejętności.** Liga zadaniowa - uczniowie wykonują indywidualnie na czas ćwiczenia nr 1-8 z sekcji „Sprawdź się", a następnie omawiają zadania na forum.

Faza podsumowująca:

1. Nauczyciel ponownie wyświetla na tablicy temat lekcji zawarty w sekcji „Wprowadzenie" i inicjuje krótką rozmowę na temat zrealizowanych celów (czego uczniowie się nauczyli).

Praca domowa:

1. Uczniowie odpowiadają na pytanie postawione w Poleceniu 1 w sekcji „Prezentacja multimedialna".

Wskazówki metodyczne:

- Treści w sekcji „Przeczytaj" można wykorzystać jako podsumowanie i utrwalenie wiedzy uczniów.