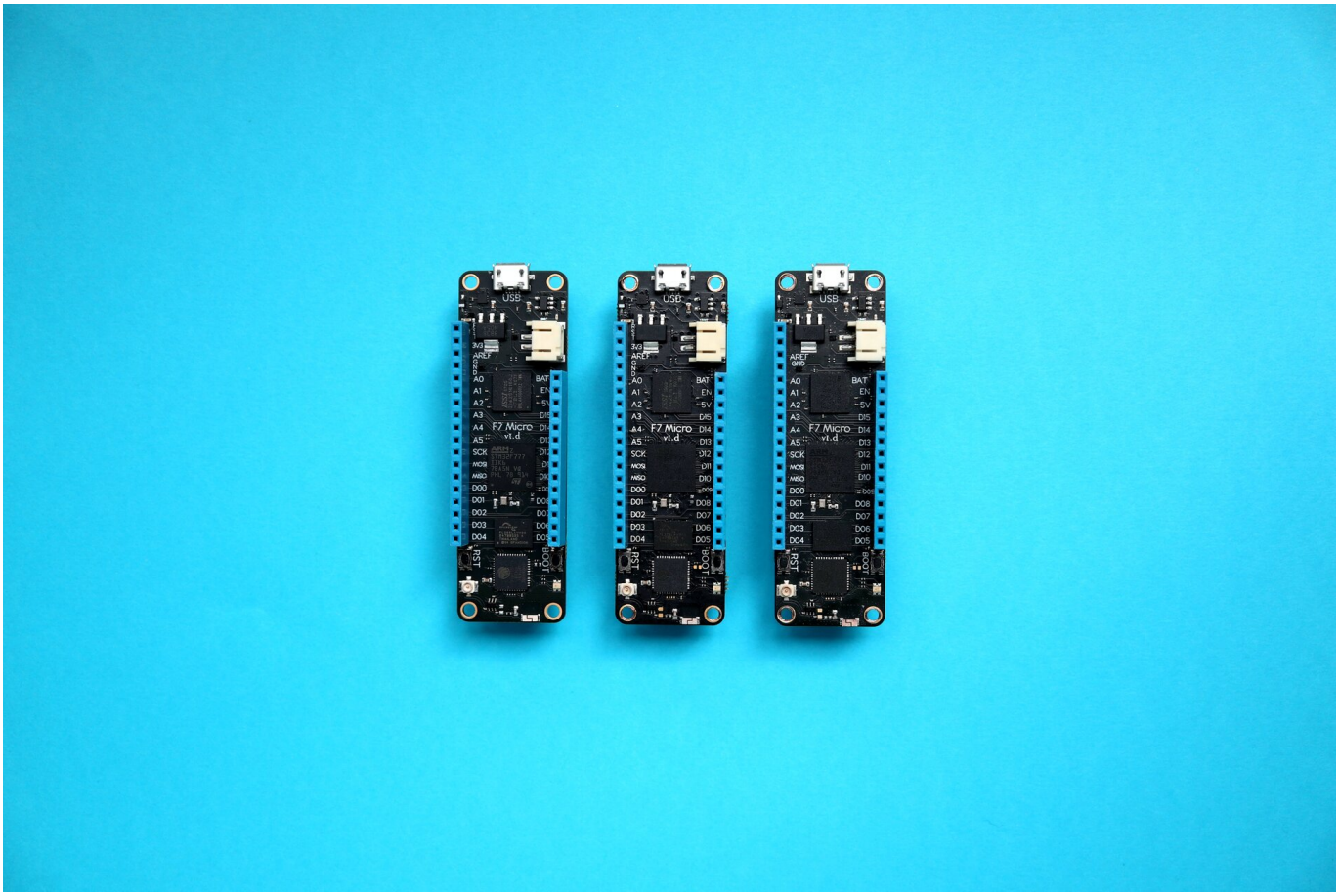

Rozwój informatyki: Internet rzeczy

- Wprowadzenie
- Przeczytaj
- Audiobook
- Sprawdź się
- Dla nauczyciela

Bibliografia:

- Źródło: Bartosz Blaicke, Artur Rot, *Bezpieczeństwo Internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie” 2017, nr 26, s. 192.

Źródło: Jorge Ramirez, domena publiczna.

Od automatu z napojami podpiętego do sieci, aż do rozległej infrastruktury inteligentnych miast. Rozwój Internetu rzeczy zaliczył w ostatniej dekadzie niewiarygodny przeskok technologiczny i wszystko wskazuje na to, iż będzie on jednym z najbardziej znaczących wynalazków ery informacji.

Wynika to z coraz większych możliwości oferowanych m.in. przez sztuczną inteligencję czy też gromadzenia oraz przesyłania danych w chmurze.

W jaki sposób wykształciła się sieć powiązanych urządzeń oraz kto stał za tym pomysłem? Jak Internet rzeczy poprawił funkcjonalność sprzętów elektronicznych? Jaką rolę technologia ta odegra w najbliższej dekadzie?

O innych aspektach rozwoju informatyki przeczytasz w e-materiałach:

- Rozwój informatyki,

- Rozwój informatyki: robotyka i mechatronika,
- Rozwój informatyki: podejście futurystyczne.

> **Twoje cele**
>
> - Dowiesz się, w jaki sposób rozwijała się technologia Internetu rzeczy na przestrzeni lat.
> - Poznasz elementy stojące za nagłym rozwojem Internetu rzeczy.
> - Przeanalizujesz skutki powszechnego zastosowania Internetu rzeczy oraz dowiesz się, w jakim kierunku rozwinie się on w przyszłości.

Przeczytaj

Rozwój Internetu rzeczy

Pomimo faktu, iż sam termin został użyty po raz pierwszy **w 1999 r.** za sprawą **Kevina Ashtona** – początki jego kształtowania możemy odnaleźć już w latach osiemdziesiątych. Wówczas na uniwersytecie *Carnegie Mellon* do automatu z napojami zostają podłączone mikroprzełączniki, które dzięki połączeniu z zewnętrznym komputerem umożliwiały bezpośrednią analizę liczby dostępnych butelek oraz stopnia schłodzenia napoju. Był to tym samym pierwszy krok na drodze ku automatyzacji urządzeń elektrycznych.

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

W kolejnych latach wraz z pojawianiem się na rynku coraz to nowszych sprzętów oraz gadżetów z możliwością połączenia do sieci, zaczęto rozważać utworzenie systemu bezpośrednich powiązań sprzętów. Tak utworzona struktura miała w założeniu zwiększyć wydajność, prostotę oraz możliwości sprzętów elektronicznych. Im więcej urządzeń podepniemy bowiem pod wspólną sieć, tym większe korzyści możemy czerpać z uwagi na intuicyjność zarządzania systemem. Sam system może również

polepszać swoje działanie poprzez wzajemną wymianę danych pomiędzy urządzeniami.

Kevin Ashton, pomysłodawca terminu określanego jako Internet rzeczy – zauważył użyteczność technologii **zdalnej identyfikacji radiowej (RFID)**, która umożliwiała m.in. odczytywanie wielu etykiet produktów przy pomocy czytnika. Technologia ta swoje główne zastosowanie znalazła w gałęzi handlu, gdzie wykorzystywana jest w celu prostego zarządzania łańcuchem dostaw.

Początkową ideą Internetu rzeczy miało być stworzenie **rozbudowanego systemu komputerów zbierającego jak najwięcej informacji o jak największej liczbie „rzeczy".** Struktura ta miała zwiększać wydajność oraz niwelować koszty głównie w obrębie wcześniej wspomnianego handlu.

Tak stworzony system mógł dostarczać informacji m.in. w zakresie:

- sprawności maszyn,
- ilości wyprodukowanego towaru,
- ilości sprzedanego towaru oraz zapotrzebowania na poszczególne produkty,
- terminu ważności produktów,
- bezpośredniej lokalizacji towaru (podczas dostawy z punktu A do punktu B).

Wszystko to przy jednoczesnym ograniczeniu ludzkiego czynnika do absolutnego minimum.

W ten sposób wchodząca w nowe millenium technologia wykształciła solidne podstawy do określenia jej mianem „rewolucyjnej". Sam jej rozkwit miał jednak dopiero nadejść, kiedy to do powszechnego użytku zaczęły wchodzić smartfony.

Internet rzeczy dziś

Właściwe narodziny Internetu rzeczy - IoT (w wymiarze, jaki znamy go dzisiaj) należy datować **na przełom lat 2008 oraz 2009.** To wtedy do internetu podłączone było więcej urządzeń oraz sprzętów elektronicznych niż ludzi na całym świecie.

To wtedy również odbyła się pierwsza oficjalna konferencja poświęcona Internetowi rzeczy, który zaczął być postrzegany jako technologia mogąca mieć niebagatelny wpływ na kształtowanie się gospodarki oraz funkcjonowania przestrzeni publicznej wielu rozwiniętych państw (zarządzanie ruchem świateł, informowanie o korkach oraz wypadkach, a także innych niebezpiecznych zdarzeniach).

Od tego czasu liczba elektroniki z dostępem do sieci wzrasta w tempie wykładniczym, zaś ich obecna wartość szacowana jest na około **50 miliardów urządzeń** (i stale rośnie). Oznacza to, że na jedną osobę na świecie przypada średnio siedem urządzeń elektrycznych, które mogą komunikować się wzajemnie z wykorzystaniem technologii Internetu rzeczy.

Co stoi za rozwojem Internetu rzeczy?

Przyczynę tak gwałtownego rozwoju niewątpliwie należy upatrywać we wprowadzeniu do powszechnego użytku nowoczesnych **smartfonów**, które obecnie pełnią rolę swoistego „centrum zarządzania" innymi przedmiotami lub gadżetami z dostępem do sieci. To za ich pomocą możemy bowiem sterować urządzeniami działającymi np. w domach inteligentnych (regulacja temperatury, oświetlenie itd.) lub analizować parametry naszego ciała, które to przesyłane są bezpośrednio ze smart opaski.

Co więcej, najnowsze modele sprzętów AGD, takich jak chociażby lodówki, pralki czy też zmywarki również są połączone z internetem. Poprzez włączanie coraz większej ilości urządzeń w struktury Internetu rzeczy, poprawia się tym samym jego funkcjonalność z uwagi na wymianę danych pomiędzy sprzętami oraz ich możliwe interakcje.

Jednocześnie, olbrzymią rolę odegrało również rozwinięcie się technologii **chmury obliczeniowej**, która przy tanich kosztach użytkowania pozwala na swobodne przechowywanie danych potrzebnych do funkcjonowania urządzeń działających w strukturze Internetu rzeczy. Jej działanie opiera się bowiem w głównym stopniu na przechowywaniu oraz przesyłaniu danych na serwer, z którego odbierana jest informacja zwrotna. W tym wypadku potrzebne jest nam jedynie stałe połączenie urządzenia z internetem.

W jaki sposób działa technologia Internetu rzeczy?

Działanie **Internetu rzeczy** opiera się na łączności urządzeń elektrycznych przy wykorzystaniu internetu, dzięki czemu możliwe jest stworzenie struktury wzajemnej wymiany, gromadzenia oraz przetwarzania informacji.

Łączność z internetem może być tym samym zapewniona w sposób **przewodowy lub bezprzewodowy** (co jest najczęstszym wyborem) m.in. za sprawą technologii:

- Wi-Fi,
- Bluetooth,
- sieci komórkowej,
- Z-Wave,
- ZigBee.

Tym samym każde urządzenie posiadające możliwość podłączenia do sieci może stać się częścią struktury Internetu rzeczy. Niekiedy zamiennie z terminem Internetu rzeczy używane jest określenie **Internet wszechrzeczy**, które w swoim ogólnym znaczeniu określa sieć ludzi, procesów oraz przedmiotów podłączonych do internetu.

Bezpieczeństwo Internetu rzeczy

IoT to technologia, która daje nam niesamowitą wygodę. Czy pamiętamy jednak o tym, żeby upewnić się, że nasze sprzęty podłączone do sieci są na pewno bezpieczne? To zagadnienie jest tym ważniejsze, że narażone jest nie tylko cyberbezpieczeństwo pojedynczych użytkowników, ale również miast, przemysłu i biznesu. Efekt ewentualnego złamania zabezpieczeń może być tym samym o wiele poważniejszy, a konsekwencje – bardziej odczuwalne.

Zagrożenia czają się na wielu poziomach. Pojawiają się pytania, np. jak przechowywać przesyłane między urządzeniami dane? Kto powinien mieć do nich dostęp? Jak uwierzytelniać użytkowników i autoryzować ich działania? Pamiętajmy, że IoT ma być przyjazny i dostępny również tym użytkownikom, którzy niekoniecznie przywiązują wagę do skomplikowanych haseł, wieloetapowych weryfikacji etc. Siłą rzeczy

prowadzi to do sytuacji, które mogą stać się źródłem wycieku danych, czy przejęcia kontroli nad urządzeniem.

Już teraz eksperci zajmujący się tematyką Internetu rzeczy mówią, że kwestie bezpieczeństwa stanowią największe wyzwanie.

Prywatność użytkowników

Firma HP przeprowadziła audyt wielu urządzeń IoT. Ich badanie wykazało, że praktycznie każde z nich nie tylko było podatne na atak, ale miało też konkretne słabe punkty w zakresie haseł, szyfrowania czy braku odpowiedniego zarządzania kontrolą dostępu.

Najczęstsze problemy wykryte przez firmę HP

> **Artur Rot, Bartosz Blaicke**
>
> **Bezpieczeństwo Internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych**
>
> Problemy z prywatnością danych – zanotowano podatności dotyczące prywatności związanej z gromadzeniem danych osobowych (imię, nazwisko, e-mail, adres zamieszkania, data urodzenia, numer karty kredytowej oraz informacje na temat zdrowia itp.). Wiele badanych systemów przechowywało nieodpowiednio zabezpieczone dane osobowe w samym produkcie, w chmurze lub w obsługującej urządzenie aplikacji mobilnej.
>
> Słabe punkty w systemie autoryzacji i uwierzytelnienia – systemy bezpieczeństwa w 80% badanych urządzeń nie wymagały haseł o odpowiedniej długości i złożoności (wiele urządzeń pozwalało na używanie trywialnych haseł).

> Brak szyfrowania transmisji danych – 70% badanych urządzeń nie szyfrowało komunikacji z Internetem i sieciami lokalnymi, a połowa aplikacji mobilnych stosowanych do obsługi tych urządzeń przesyłała niezaszyfrowane komunikaty w chmurze obliczeniowej, Internecie lub sieci lokalnej.
>
> Niebezpieczne interfejsy WWW – w 6 z 9 testowanych urządzeń zanotowano obawy związane z bezpieczeństwem interfejsów użytkownika.
>
> Niewystarczający poziom bezpieczeństwa oprogramowania – 60% urządzeń nie stosowało szyfrowania podczas aktualizacji oprogramowania.
>
> Źródło: Bartosz Blaicke, Artur Rot, *Bezpieczeństwo Internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie" 2017, nr 26, s. 192.

Warto zaznaczyć, że decydując się na instalację w naszych domach urządzeń podłączonych do IoT, częściowo sami wystawiamy się na ataki. Doniesienia na temat tego, że urządzenia typu Alexa czy Google Home nas podsłuchują, nikogo już nie dziwią. Martwić może jednak to, co z pozyskanymi na nasz temat informacjami mogą zrobić hakerzy, czy w ogóle osoby niepowołane. Przykładów manipulowania użytkownikami znamy wiele.

Ataki hakerskie

Pomimo tego, że historia IoT jest krótka, doświadczyliśmy już dotkliwych ataków hakerskich. Oto jeden z przykładów.

Bot Mirai

Atak sparaliżował wiele dużych serwisów – należał do nich między innymi Netflix czy Twitter. Komputery zainfekowane botem wyszukiwały w sieci niezabezpieczone lub słabo zabezpieczone urządzenia podłączone do IoT i za ich pomocą wysyłały

zapytania do serwerów wielu usług. W ten sposób zupełnie sparaliżowały do nich dostęp.

Jak hakerom udało się przejąć kontrolę nad kamerkami czy innymi sprzętami IoT? Część użytkowników… nie zmieniła fabrycznie ustawionych haseł. Atak był zatem banalnie prosty. Eksperci wskazują, że pomimo niedociągnięć technologicznych, to nadal człowiek jest najsłabszym ogniwem w całym łańcuchu.

Słownik

> **Internet rzeczy**
>
> (ang. *Internet of Things*) system urządzeń elektronicznych, które po podłączeniu do sieci mogą się ze sobą komunikować bez udziału człowieka

> **chmura obliczeniowa**
>
> usługa polegająca na udostępnianiu mocy obliczeniowej przez zewnętrzny serwer, do którego dostęp możliwy jest za pośrednictwem internetu

Audiobook

Polecenie 1

Wysłuchaj audiobooka, a następnie zastanów się nad przyszłością technologii Internetu rzeczy. Przeprowadź dyskusję z kolegą lub koleżanką z ławki, dotyczącą waszych wyobrażeń na temat świata w pełni zautomatyzowanego za sprawą Internetu rzeczy.

Audiobook można wysłuchać pod adresem: https://zpe.gov.pl/b/P1Gh9gsXn

---

Czy jesteśmy w stanie przewidzieć przyszłość?

Zapewne wielu z was nieraz zastanawiało się nad tym aspektem, w kontekście szans na wygranie fortuny na loterii lub w przypadku odgadnięcia prawidłowych odpowiedzi na sprawdzianie. I choć – w tych konkretnych przypadkach – technologia nie do końca pomaga, rozwój Internetu rzeczy może – w ciągu najbliższych lat – przybliżyć nas do tej futurystycznej wizji.

Przyglądając się zmianom, które nastąpiły od roku 1999 (kiedy to Kevin Ashton, po raz pierwszy, użył określenia „Internet rzeczy"), jesteśmy w stanie określić nasze położenie na osi „rozwoju technologicznego". Obecnie znajdujemy się pod koniec środkowej fazy. Faza ta charakteryzuje się, przede wszystkim, możliwością kontroli obiektów w czasie rzeczywistym. Pozwala to, chociażby, na przewidzenie natężenia ruchu w danym miejscu i czasie oraz na bieżące monitorowanie lokalizacji przedmiotu.

Funkcja ta wykorzystywana jest w wielu gałęziach Internetu rzeczy – począwszy od smart opasek, które potrafią określić przebyty dystans podczas aktywności fizycznej, po – wcześniej wspomniane – monitorowanie natężenia ruchu, dzięki któremu jesteśmy na bieżąco informowani o utrudnieniach na drodze oraz przewidywanym czasie przejazdu. Możemy także zawczasu sprawdzić, który obiekt sportowy jest najbardziej oblegany, gdy planujemy weekendowe rozgrywki ze znajomymi.

Etapem poprzedzającym pełną automatyzację sprzętów, działających w strukturze Internetu rzeczy, jest faza bezpośredniej komunikacji maszyn. Oznacza to, iż przy zaistnieniu pewnych czynników, urządzenia potrafią wpływać na siebie – bez ingerencji człowieka. Przykładem takiego rozwiązania jest inteligentny termostat, który – po zebraniu informacji na temat temperatury otoczenia – potrafi regulować ciepło wewnątrz budynku. Nadal jednak cały ten proces opiera się wyłącznie na

informacjach występujących w jednej strukturze (w tym przypadku w tak zwanym inteligentnym domu).

Przyszłość Internetu rzeczy zmierza natomiast w kierunku inteligentnego powiązania każdego aspektu naszej codziennej rutyny, w celu jej automatyzacji oraz optymalizacji. Począwszy od pobudki, która za sprawą inteligentnego budzika odbyłaby się kilka minut wcześniej niż zwykle, z uwagi na złe warunki pogodowe lub zaistniałe korki. Wszystkie kolejne czynności byłyby na bieżąco dostosowane pod kątem naszych preferencji oraz względnie niezależnych od nas rzeczy, takich jak: pogoda, utrudnienia na drodze czy inne zdarzenia losowe.

Wypadki w świecie Internetu rzeczy byłyby tym samym ograniczone do absolutnego minimum, choć trzeba mieć na uwadze, że ich wystąpienie mogłoby spowodować absolutny paraliż takiego systemu. Co więcej, wszelkiego typu awarie lub cyberataki miałyby niebagatelny wpływ na każdy aspekt życia codziennego, z powodu ich wzajemnego powiązania. W tak na pozór zoptymalizowanych do perfekcji inteligentnych miastach, uzyskalibyśmy więc nowoczesną odsłonę efektu motyla – wówczas mała awaria świateł na obrzeżach miasta, mogłaby spowodować paraliż w centrum, z uwagi na przekierowanie większej liczby samochodów na ten odcinek trasy.

Tym samym, jutrzejszy wymiar Internetu rzeczy to atrakcyjna sposobność do poprawienia jakości życia codziennego. Jednak z tą możliwością łączą się różne niebezpieczeństwa, niewiadome i konsekwencje, z których szacowaniem zmierzymy się w ciągu najbliższej dekady.

Sprawdź się

Pokaż ćwiczenia:

- Ćwiczenie 1
- Ćwiczenie 2
- Ćwiczenie 3
- Ćwiczenie 4
- Ćwiczenie 5
- Ćwiczenie 6
- Ćwiczenie 7
- Ćwiczenie 8

Dla nauczyciela

Autor: Maurycy Gast

Przedmiot: Informatyka

Temat: Rozwój informatyki: Internet rzeczy

Grupa docelowa:

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

Podstawa programowa:

Cele kształcenia – wymagania ogólne

> IV. Rozwijanie kompetencji społecznych, takich jak: komunikacja i współpraca w grupie, w tym w środowiskach wirtualnych, udział w projektach zespołowych oraz zarządzanie projektami.

Treści nauczania – wymagania szczegółowe

> IV. Rozwijanie kompetencji społecznych.
>
> Zakres podstawowy. Uczeń:
>
> 5) przedstawia trendy w historycznym rozwoju informatyki i technologii oraz ich wpływ na rozwój społeczeństw;

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):

- Dowiesz się, w jaki sposób rozwijała się technologia Internetu rzeczy na przestrzeni lat.
- Poznasz elementy stojące za nagłym rozwojem Internetu rzeczy.
- Przeanalizujesz skutki powszechnego zastosowania Internetu rzeczy oraz dowiesz się, w jakim kierunku rozwinie się on w przyszłości.

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: „Rozwój informatyki: Internet rzeczy". Nauczyciel prosi uczniów o zapoznanie się z treściami w sekcji „Przeczytaj".

Faza wstępna:

1. Nauczyciel wprowadza uczniów szczegółowo w temat lekcji i jej cele. Może posłużyć się wyświetloną na tablicy zawartością sekcji „Wprowadzenie".
2. **Rozpoznanie wiedzy uczniów.** Uczniowie tworzą pytania dotyczące tematu zajęć, na które odpowiedzą w trakcie lekcji.

Faza realizacyjna:

1. **Praca z tekstem.** Uczniowie przystępują do cichego czytania tekstu zawartego w sekcji „Przeczytaj", jeśli nauczyciel - na podstawie raportu na platformie - uważa, że przygotowanie uczniów jest wystarczające, może pominąć tę czynność.
2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Audiobook". Uczniowie wspólnie wysłuchują audiobooka i zastanawiają się nad przyszłością technologii Internetu rzeczy. następnie przeprowadzają dyskusję z kolegą lub koleżanką z ławki dotyczącą wyobrażeń na temat świata w pełni zautomatyzowanego za sprawą Internetu rzeczy.
3. **Ćwiczenie umiejętności.** Liga zadaniowa - uczniowie wykonują indywidualnie na czas ćwiczenia nr 1-6 z sekcji „Sprawdź się", a następnie omawiają zadania na forum.

Faza podsumowująca:

1. Nauczyciel ponownie wyświetla na tablicy temat i cele lekcji zawarte w sekcji „Wprowadzenie". W kontekście ich realizacji następuje omówienie ewentualnych problemów z rozwiązaniem ćwiczeń z sekcji „Sprawdź się".
2. Wybrany uczeń podsumowuje zajęcia, zwracając uwagę na nabyte umiejętności.

Praca domowa:

1. Uczniowie wykonują ćwiczenia 7 i 8 z sekcji „Sprawdź się".

Wskazówki metodyczne:

- Treści w sekcji „Audiobook" można wykorzystać na lekcji jako podsumowanie i utrwalenie wiedzy uczniów.