# Szanse i zagrożenia związane z rozwojem informatyki i technologii – internet rzeczy

# Szanse i zagrożenia związane z rozwojem informatyki i technologii – internet rzeczy

Źródło: Nicolas Picard, dostępny w internecie: unsplash.com, domena publiczna.

Wygoda, bezpieczeństwo, funkcjonalność – takimi słowami moglibyśmy opisać nowoczesne, inteligentne domy, które dzięki podłączeniu do sieci wielu urządzeń oraz gadżetów zapewniają komfort lokatorom.

Internet rzeczy to jednak nie tylko ciekawostka, ale także potężne narzędzie, które może całkowicie przekształcić infrastrukturę miast, zamieniając je w bezpieczne, energooszczędne metropolie zarządzane przez systemy sztucznej inteligencji.

Czy internet rzeczy okaże się przyszłościowym rozwiązaniem, które wprowadzi nas do epoki powszechnej automatyzacji, czy też pozostanie na długo w cieniu sprawdzonych systemów?

Ciekawią cię inne aspekty szans i zagrożeń związanych z rozwojem informatyki? Omawiamy je w pozostałych e-materiałach z serii:

- Szanse i zagrożenia związane z rozwojem informatyki i technologii,
- Szanse i zagrożenia związane z rozwojem informatyki i technologii – dostępność usług,
- Szanse i zagrożenia związane z rozwojem informatyki i technologii – rozpraszanie danych,
- Szanse i zagrożenia związane z rozwojem informatyki i technologii – gromadzenie danych.

**Twoje cele**

- Wyjaśnisz, czym jest internet rzeczy.
- Wymienisz przykłady zastosowania internetu rzeczy w życiu codziennym.
- Scharakteryzujesz rolę, jaką może odegrać internet rzeczy, a także przeanalizujesz ewentualne zagrożenia z nim związane.

# Przeczytaj

## Internet rzeczy – definicja i funkcje

Często nawet nie zdajemy sobie sprawy z faktu, że codziennie korzystamy z urządzeń składających się na strukturę określaną mianem internetu rzeczy.

**Internet rzeczy** jest – w uproszczeniu – systemem urządzeń elektronicznych, które po podłączeniu do sieci mogą się ze sobą komunikować oraz przesyłać dane bez ingerencji człowieka (lub z jego bardzo małym udziałem).

Utworzone w ten sposób struktury mogą być **zarządzane za pomocą aplikacji lub asystenta głosowego**. Zadanie człowieka ogranicza się do użycia smartfona bądź asystenta i ustalenia odpowiednich parametrów systemu.

> **Ciekawostka**
>
> Termin internet rzeczy został po raz pierwszy użyty przez brytyjskiego przedsiębiorcę **Kevina Ashtona** w 1999 r. Zdefiniował on internet rzeczy jako „sieć połączonych ze sobą przedmiotów".
>
> Od tego czasu internet rzeczy rozrósł się do ogromnych rozmiarów; liczbę podłączonych do niego urządzeń szacuje się na **25 do 50 miliardów.**

## Inteligentny dom

Inteligentne domy mogą kojarzyć się ze szklanymi domami opisanymi w „Przedwiośniu" Stefana Żeromskiego, jednak budynki, w których wykorzystano zaawansowane technologie, pojawiają się coraz częściej.

Trzeba zdawać sobie sprawę z faktu, że **inteligentne systemy** są montowane na bieżąco wraz z budową domu. Najlepiej myśleć o nich zatem już na etapie projektu.

Jednym z udogodnień zapewnianych przez inteligentne domy jest **automatyczna regulacja oświetlenia** – system, który na podstawie danych z czujników oraz informacji pogodowych ocenia, czy ilość światła wpadającego przez okna jest wystarczająca, aby zapewnić komfort domownikom. W razie potrzeby odpowiednio korygowane jest ustawienie rolet lub natężenie światła sztucznego.

Inną funkcją jest **kontrola bezpieczeństwa**, realizowana zazwyczaj przez połączone układy monitoringu, oświetlenia, rolet antywłamaniowych oraz alarmu. Cały system można zaprogramować tak, aby automatycznie zamykał wszystkie rolety i włączał monitoring po

wyjściu domowników, a w przypadku włamania – informował ochronę i policję oraz wydawał głośne komunikaty odstraszające przestępcę.

> **Ciekawostka**
>
> Niektóre inteligentne domy można zaprogramować tak, aby sprawiały wrażenie, że ktoś stale w nich przebywa. System włącza co pewien czas oświetlenie, muzykę itd. Funkcja taka przydaje się na przykład podczas wyjazdu domowników na wakacje: zniechęca do działania potencjalnych włamywaczy.

Zaletą inteligentnych domów jest **wygoda w ich użytkowaniu.** Za pomocą jednego kliknięcia lub po wydaniu polecenia głosowego możemy sterować całym domem z dowolnego miejsca: włączać muzykę, zmieniać kolor oświetlenia, a ponadto zarządzać urządzeniami takimi jak piekarnik, pralka albo autonomiczny odkurzacz.

Dzięki monitoringowi podłączonemu do smartfona, możemy nawet na bieżąco obserwować, co robi nasz kot i czy na pewno doniczka stłukła się sama.

## Inteligentne miasta

Powstanie inteligentnych miast jest kwestią niedalekiej przyszłości. Przyczyni się do tego rozwój internetu rzeczy. **Im więcej urządzeń zostanie podłączonych do sieci, tym łatwiej będzie przeprowadzić optymalizację miejskiej infrastruktury.**

Pierwsze elementy inteligentnych miast możemy już obserwować. Jadąc samochodem i korzystając z popularnych map, jesteśmy informowani na bieżąco o zakorkowanych ulicach i proponowanych objazdach (wraz z oszacowaniem czasu, jaki zaoszczędzimy, wybierając wskazywaną drogę).

Jest to dopiero początek. Wraz z pojawianiem się w miastach coraz większej liczby odpowiednich czujników będzie można m.in. sterować oświetleniem, gromadzić informacje na temat wolnych miejsc parkingowych, automatycznie przekazywać właściwym służbom informacje o popełnieniu przestępstwa albo wykryciu sytuacji zagrażającej czyjemuś zdrowiu lub życiu.

Głównym celem wdrożenia koncepcji inteligentnych miast jest osiągnięcie **jak największej funkcjonalności przestrzeni publicznej**, a co za tym idzie – zmniejszenie kosztów utrzymania infrastruktury miejskiej.

## Internet rzeczy a służba zdrowia

**Inteligentne opaski**, monitorujące w sposób ciągły najważniejsze parametry organizmu, nie muszą być wyłącznie nowoczesnymi gadżetami. Mogą stać się częścią internetu rzeczy i wspierać służbę zdrowia.

Najbardziej oczywistym pomysłem wydaje się **zaopatrzenie w takie opaski ludzi starszych oraz osób należących do różnych grup ryzyka.** Często zdarza się, że cierpiący na ciężkie choroby ludzie nie są w stanie nawet zadzwonić po pomoc. Połączenie opasek monitorujących parametry organizmu pacjenta z centralnym systemem pozwoliłoby przekazać ratownikom medycznym **informacje o niepokojących zmianach tętna albo ciśnienia.**

Internet rzeczy może przyczynić się do **poprawy jakości życia osób z niepełnosprawnościami.** Specjalne czujniki oraz sensory ułatwią wykonywanie codziennych czynności osobom niewidomym lub niedosłyszącym. Co więcej, opiekunowie takich osób będą w stanie monitorować parametry życiowe podopiecznych nawet podczas krótkich nieobecności.

## Leczenie na odległość

**System teleporad oraz e-recept** może również zostać radykalnie zmieniony. Obecnie największym mankamentem teleporady jest fakt, że lekarz bazuje na opisie objawów choroby przekazanym mu przez pacjenta, a nie na osobistym sprawdzeniu stanu jego zdrowia. Zdalne dokonanie pomiarów temperatury, ciśnienia i innych parametrów życiowych przełoży się na postawienie precyzyjnej diagnozy.

W przypadku elektronicznych recept można np. posłużyć się aplikacją, dzięki której leki byłyby dostarczane wprost do domu pacjenta po przekazaniu przez lekarza listy potrzebnych środków oraz zweryfikowaniu tożsamości ich odbiorcy.

## Pozostałe zastosowania internetu rzeczy

### Przedsiębiorstwa i przemysł

Wyobrażenie o przyszłym zastosowaniu internetu rzeczy w przedsiębiorstwach da nam obserwacja firm działających już obecnie: za przykład niech posłuży system śledzenia przesyłek. W każdej chwili możemy sprawdzić, gdzie znajduje się przesyłka oraz kiedy dotrze do miejsca docelowego.

W przyszłości **sterowanie łańcuchami dostaw** będzie miało kluczowe znaczenie dla wydajności firmy. Co więcej, dzięki wbudowanym czujnikom system będzie w stanie określić jakość wyrobów i odpowiednio szybko zatrzymać produkcję w przypadku wykrycia wadliwej serii. Przełoży się to na zminimalizowanie strat.

### Systemy energetyczne

Głównym celem uruchomienia **inteligentnych systemów energetycznych** będzie zapewnienie wymiany danych między odrębnymi jednostkami wytwarzającymi energię elektryczną. Pozwoli to zaplanować przesyłanie energii do miejsc, w których jest ona w konkretnych momentach najbardziej potrzebna. W rezultacie uniknie się problemów związanych z magazynowaniem energii elektrycznej na skalę przemysłową.

Operatorzy współczesnych sieci energetycznych korzystają z przestarzałych, niedokładnych metod planowania dystrybucji energii: prognoza zapotrzebowania powstaje na bazie danych historycznych. Dodatkowym czynnikiem, który zaburza jej dokładność, jest zwiększenie się liczby odnawialnych źródeł energii. Ich wydajność zależy od warunków atmosferycznych, a te nigdy nie są całkowicie przewidywalne.

## Słownik

> **internet rzeczy**
>
> (ang. *Internet of Things*) system urządzeń elektronicznych, które po podłączeniu do sieci mogą się ze sobą komunikować bez udziału człowieka
> **inteligentny dom**
>
> określenie zaawansowanego technicznie budynku, do zarządzania którym wykorzystywana jest sieć komunikujących się ze sobą urządzeń

# Audiobook

> **Polecenie 1**
>
> Wysłuchaj audiobooka, a następnie zastanów się nad zagadnieniami cyberbezpieczeństwa w technologii internetu rzeczy. Przeprowadź dyskusję na temat zagrożeń omówionych w audiobooku.

Audiobook można wysłuchać pod adresem: https://zpe.gov.pl/b/POXi0dxoF

---

Idea internetu rzeczy realizuje się poprzez postępującą automatyzację i optymalizację procesów produkcyjnych. Wpływają one na życie codzienne, usprawniają szybkość, dokładność oraz efektywność wymiany informacji. Niestety, wraz z próbami wprowadzenia technologicznych zmian w istotnych gałęziach przemysłu lub infrastruktury, pojawiają się pierwsze poważne komplikacje.

Internet rzeczy jest bowiem strukturą szczególnie narażoną na ataki hakerskie. Wykradanie danych, ataki DDoS czy też złośliwe oprogramowanie (takie jak ransomware) są problemami, z którymi trzeba będzie się zmierzyć w najbliższej przyszłości.

Zapewnienie bezpieczeństwa urządzeń wchodzących w skład internetu rzeczy jest również istotne z tego powodu, że wkrótce staną się one podstawowymi narzędziami służącymi do obsługi autonomicznych pojazdów lub sprzętu medycznego.

Obecnie wiele z nich bazuje jednak na słabych zabezpieczeniach – przestarzałych protokołach Telnet lub FTP. Brakuje również szyfrowanej komunikacji między urządzeniami.

Jednocześnie cyberataki stają się coraz bardziej wyrafinowane oraz coraz trudniejsze do wykrycia. Główną przyczyną ich skuteczności jest – paradoksalnie – rozwój technologiczny.

Stare warianty złośliwego oprogramowania, z którymi jesteśmy w stanie się uporać, są zastępowane przez nowe odmiany – skuteczniejsze, a zarazem trudniejsze do wyeliminowania.

Od razu nasuwa się pytanie: Czy jesteśmy w stanie coś z tym zrobić? Albo raczej: Dlaczego MUSIMY coś z tym zrobić?

U progu rewolucji, która pozwoli nie tylko podnieść nasz standard życiowy, ale i zapewnić dużo lepszą ochronę zdrowia, ważne jest zadbanie o jak najlepsze bezpieczeństwo systemu.

Oprócz oczywistej konieczności zwiększania jakości zabezpieczeń przez producentów aplikacji i urządzeń, potrzebna jest świadomość zagrożenia wśród samych użytkowników – zadbanie o włączenie dwupoziomowej weryfikacji, unikatowe identyfikatory oraz hasła, czy też plan działania na wypadek cyberataku. Wszystko to, jeśli nie uniemożliwi, to przynajmniej utrudni dokonanie cyberprzestępstwa.

Co stanie się, gdy zaniecha się zabezpieczeń w internecie rzeczy?

Niestety, wizje są raczej ponure. Próby wymuszenia okupu w zamian za rezygnację z zamknięcia ofiary w mieszkaniu lub pojeździe, a nawet szantaż wspomagany groźbą wyłączenia rozrusznika serca lub innych urządzeń medycznych, to tylko kilka przykładów.

Tym bardziej projektanci powinni na pierwszym miejscu postawić bezpieczeństwo i ochronę systemu, nawet jeśli miałoby to odbyć się kosztem przesunięcia w czasie momentu wprowadzenia technologii do powszechnego użytku.

Pamiętajmy, że skutkiem zaniedbań na tym polu może być coś o wiele poważniejszego niż głupi kawał polegający na wydrukowaniu obrazka przez domową drukarkę czy złośliwe przełączanie piosenek odtwarzanych przez system głośników.

# Sprawdź się

Pokaż ćwiczenia:

### Ćwiczenie 1

### Ćwiczenie 2

Wskaż, kto jako pierwszy posłużył się terminem internet rzeczy.

- ◯ Gordon Moore
- ◯ Leonard Bosack
- ◯ Kevin Ashton

### Ćwiczenie 3

Zaznacz aplikacje, które wypełniają zadania asystentów głosowych.

- ☐ Google Home
- ☐ Microsoft Outlook
- ☐ Amazon Echo
- ☐ iCloud

### Ćwiczenie 4

Wskaż, czym jest inteligentny dom.

- ◯ Cyfrowym budynkiem osadzonym w chmurze.
- ◯ Wysoko zaawansowanym technicznie budynkiem wykorzystującym sieć połączonych ze sobą urządzeń.
- ◯ Budynkiem zaprojektowanym przez sztuczną inteligencję.

### Ćwiczenie 5

Uzupełnij tekst.

W obliczu coraz większego zagrożenia spowodowanego popularnością ataków hakerskich na urządzenia funkcjonujące w technologii internetu rzeczy – użytkownik powinien zadbać przede wszystkim o włączenie [ ] [ ], zaopatrzenie się w unikalne identyfikatory oraz [ ], a także przygotowanie planu działania na wypadek potencjalnego [ ].

weryfikacji | trzypoziomowej | dwupoziomowej | logowania | cyberataku | jednopoziomowej | wylogowania | aktualizacji | hasła

### Ćwiczenie 6

Podaj dwa przykłady możliwego wykorzystania internetu rzeczy w służbie zdrowia.

### Ćwiczenie 7

Podaj dwa przykłady wykorzystania internetu rzeczy w celu zoptymalizowania infrastruktury miejskiej.

### Ćwiczenie 8

Korzystając z dostępnych źródeł, podaj przykład wykorzystania internetu rzeczy w dowolnej dziedzinie, o której nie było mowy w e-materiale.

# Dla nauczyciela

**Autor:** Maurycy Gast
**Przedmiot:** Informatyka

**Temat: Szanse i zagrożenia związane z rozwojem informatyki i technologii – internet rzeczy**

**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

V. Przestrzeganie prawa i zasad bezpieczeństwa.

Zakres podstawowy. Uczeń:

1) postępuje zgodnie z zasadami netykiety oraz regulacjami prawnymi dotyczącymi: ochrony danych osobowych, ochrony informacji oraz prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji; jest świadomy konsekwencji łamania tych zasad;

2) respektuje obowiązujące prawo i normy etyczne dotyczące korzystania i rozpowszechniania oprogramowania komputerowego, aplikacji cudzych i własnych oraz dokumentów elektronicznych;

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.

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

1) objaśnia rolę technik uwierzytelniania, kryptografii i podpisu elektronicznego w ochronie i dostępie do informacji;

**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):**

- Wyjaśnisz, czym jest internet rzeczy.
- Wymienisz przykłady zastosowania internetu rzeczy w życiu codziennym.
- Scharakteryzujesz rolę, jaką może odegrać internet rzeczy, a także przeanalizujesz ewentualne zagrożenia z nim związane.

**Strategie nauczania:**

- konstruktywizm;
- konektywizm.

**Metody i techniki nauczania:**

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

**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. Uczniowie szukają interesujących przykładów rozwiązań należących do internetu rzeczy.

**Faza wstępna:**

1. Uczniowie prezentują przygotowane przykłady.
2. Nauczyciel wyświetla uczniom temat, wskazuje cele zajęć oraz ustala z uczestnikami zajęć kryteria sukcesu.

**Faza realizacyjna:**

1. Uczniowie zapoznają się z treścią e-materiału.
2. Nauczyciel inicjuje dyskusję na temat bezpieczeństwa internetu rzeczy. Uczniowie zastanawiają się, jakie zagrożenie może spowodować niedostateczne zabezpieczenie sprzętów należących do domowej sieci.
3. Uczniowie dzielą się swoim zdaniem nt. internetu rzeczy. Odpowiadają na pytanie o to, czy chcieliby zastosować takie rozwiązania w swoich domach.

**Faza podsumowująca:**

1. Uczniowie zastanawiają się nad przykładami zastosowania internetu rzeczy w popkulturze.
2. Uczniowie rozwiązują ćwiczenia wskazane przez nauczyciela.

**Praca domowa:**

1. Uczniowie rozwiązują pozostałe ćwiczenia z sekcji „Sprawdź się”.
2. Uczniowie realizują polecenie: Poszukaj przykładów złamania zabezpieczeń internetu rzeczy.

**Wskazówki metodyczne:**

- Audiobook może być zaproszeniem do dyskusji na temat tego, jak traktujemy swoją prywatność w sieci.