

Tradycja badań. Technologie przyszłości. Wiemy, jak to połączyć.

Misja

Badania naukowe, prace rozwojowe i wdrożeniowe w dziedzinie nauk inżynieryjno-technicznych, w szczególności w dyscyplinie informatyka techniczna i telekomunikacja oraz doskonalenie i poszerzanie specjalistycznych kompetencji służących społeczeństwu, administracji publicznej i przedsiębiorcom.

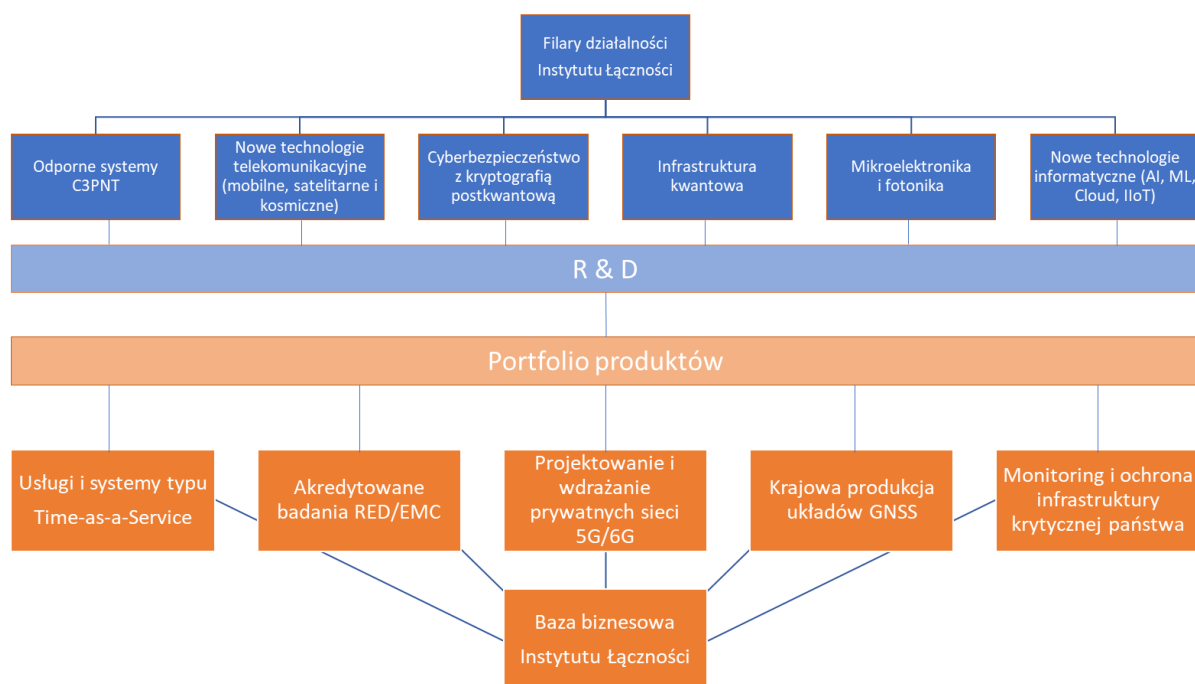
Wizja

Instytut Łączności – Państwowy Instytut Badawczy jako nowoczesna i wiarygodna instytucja badawczo-rozwojowa, atrakcyjna dla polskich i zagranicznych partnerów naukowych, biznesowych oraz dla administracji publicznej, dostarczająca wiedzę, rozwiązania i wsparcie w dziedzinie nauk inżynieryjno-technicznych.

Instytut Łączności – Państwowy Instytut Badawczy (IŁ-PIB) koncentruje się na sześciu synergicznych filarach: odporne systemy C3PNT (C3 – Communication, Command and Control, PNT – Positioning, Navigation, Timing), nowe technologie telekomunikacyjne (mobilne, satelitarne i kosmiczne), cyberbezpieczeństwo z kryptografią postkwantową, infrastruktura kwantowa, mikroelektronika i fotonika oraz nowe technologie informatyczne AI (Artificial Intelligence), ML (Machine Learning), HCC (Hybride Cloud Computing), IIoT (Industrial Internet of Things).

Tak zdefiniowany portfel produktów bezpośrednio odpowiada na priorytety regulacyjne NATO (BLR-6) i UE (NIS2, CER, Akt o Cyberbezpieczeństwie, CSA, Akt o Cyberodporności, (CRA), EU Chips Act), wzmacnia suwerenność cyfrową oraz bezpieczeństwo infrastruktury krytycznej państwa i otwiera potencjalne strumienie finansowania z Horizon Europe, EuroHPC oraz funduszy wewnętrznych. Jednocześnie tworzy solidną bazę biznesową, opartą na komercjalizacji usług typu Timing-as-a-Service, akredytowanych badaniach laboratoryjnych w obszarze dyrektyw RED oraz EMC, projektowaniu i wdrażaniu prywatnych sieci 5G/6G, krajowej produkcji układów GNSS (Global Navigation Satellite Systems) oraz usługach monitoringu i ochrony infrastruktury krytycznej państwa (rys. 1).

Strategia 2026–2030, ujęta w *Perspektywicznych kierunkach działalności* pozwoli Instytutowi łączności stać się wiodącym ośrodkiem R&D (Research and Development) w regionie, gwarantując interesariuszom pełne spektrum kompetencji – od laboratorium i certyfikacji, przez projekty pilotażowe, aż po wdrożenia w infrastrukturze krytycznej. Instytut łączności reaktywnie odpowiada na zapotrzebowanie cywilizacyjne związane z sytuacją geopolityczną i niekorzystnym oddziaływaniem na cyberprzestrzeń i pole elektromagnetyczne (PEM).



Rys. 1. Filary działalności Instytutu łączności i portfolio produktów

Strategiczne kierunki rozwoju

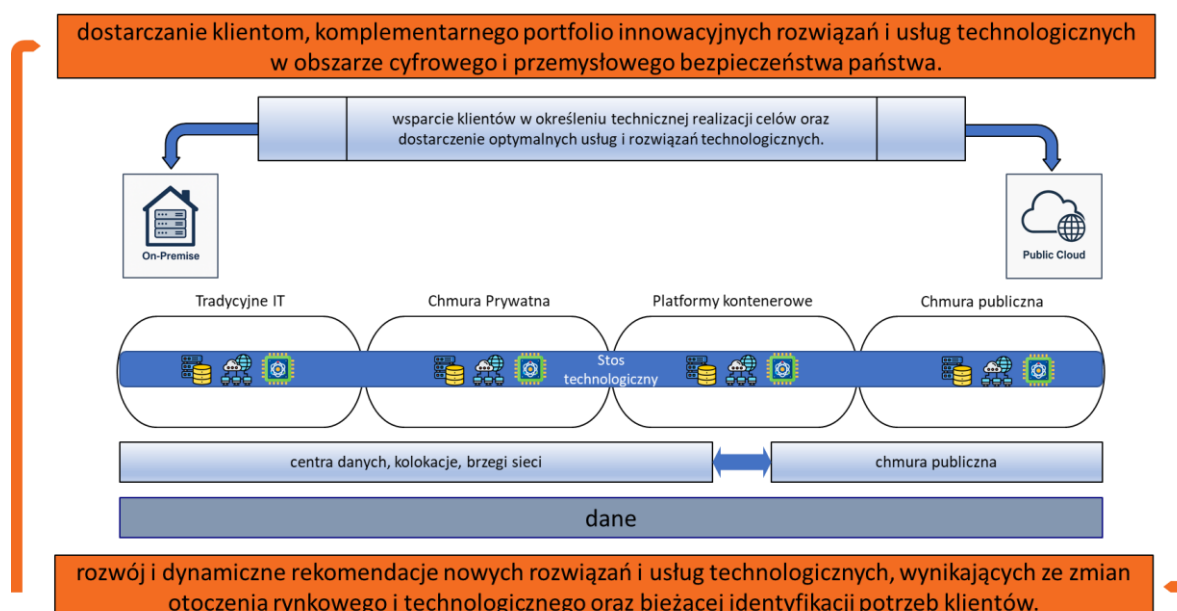
W latach 2026–2030 główne kierunki rozwoju naukowego Instytutu łączności, będą związane z budową potencjału wdrożeniowego w zakresie:

1. odpornych systemów łączności C3PNT (C3 – Communication, Command and Control, PNT – Positioning, Navigation, Timing);
2. nowych technologii telekomunikacyjnych, szczególnie mobilnych, satelitarnych i kosmicznych;
3. cyberbezpieczeństwa z kryptografią postkwantową;
4. infrastruktury kwantowej;
5. mikroelektroniki i fotoniki, w szczególności w dziedzinie projektowania i produkcji układów scalonych na potrzeby polskiego systemu bezpiecznych dokumentów tożsamości oraz innych zastosowań;

6. nowych technologii informatycznych wykorzystujących zaawansowane mechanizmy sztucznej inteligencji (Artificial Intelligence), systemów wspierania podejmowania decyzji, modelowania danych i uczenia maszynowego (Machine Learning) do przetwarzania dużych zbiorów danych i analityki (Big Data) w hybrydowej chmurze obliczeniowej (Hybrid Cloud Computing),

ze szczególnym uwzględnieniem zastosowań wszystkich wymienionych technologii i rozwiązań, w obszarze cyfrowego i przemysłowego bezpieczeństwa państwa.

Wyżej wymienione kierunki strategiczne, będą realizowane zarówno jako prace naukowe – podstawowe, prace badawczo-rozwojowe, środowiska edukacyjno-testowe oraz koncepcje i rozwiązania dla klientów biznesowych, obywateli i cyfrowego państwa (systemy informatyczne administracji publicznej, wojska i przemysłu), jak i wdrożenia biznesowe, rozwijane i oferowane w taki sposób, który zapewni interesariuszom i klientom Instytutu łączności, dostęp do szerokiego portfela innowacyjnych usług i rozwiązań technologicznych (rys. 2).



Rys. 2. Kompleksowy, elastyczny i ukierunkowany na potrzeby klienta model świadczenia usług technologicznych przez Instytut Łączności

Strategiczne kierunki rozwoju Instytutu Łączności, będą realizowane zarówno w ramach współpracy krajowej, jak i międzynarodowej, w zakresie:

1. współpracy naukowej z ośrodkami naukowymi w Polsce i zagranicą (uczelnie, instytuty badawcze);
2. udziału ekspertów IŁ-PIB w pracach krajowych i międzynarodowych organizacji normalizacyjnych i regulacyjnych (m.in. PKN, ISO, IEC, CEN, CENELEC, ETSI, ITU, IALA, IMO, CEPT, ITU);

3. wsparcia merytorycznego administracji państwowej reprezentującej Polskę na forum międzynarodowym (m.in. ESA, Komisja Europejska, ENISA);
4. udziału w międzynarodowych programach badawczych;
5. organizacji krajowych i międzynarodowych konferencji naukowych tematycznie związanych z telekomunikacją;
6. współpracy z przedsiębiorcami telekomunikacyjnymi.

Perspektywiczne kierunki działalności zostały opracowane na bazie ugruntowanego stanu wiedzy i doświadczeń oraz odpowiednio do prowadzonych w ubiegłych latach i kontynuowanych oraz nowych, odpowiadających trendom projektów. W razie potrzeby dokument będzie podlegał przeglądowi i dalszemu rozwinięciu.

Dzięki interdyscyplinarnym kompetencjom w obszarze radiokomunikacji, metrologii czasu, cyberbezpieczeństwa oraz analizy i przetwarzania danych, Instytut Łączności będzie oferował innowacyjne rozwiązania i usługi technologiczne o wysokiej wartości rynkowej i społecznej z zakresu:

1. Technologie telekomunikacyjne:

- a) ochrona systemów GNSS/GPS przed atakami, w tym ochrona przed desynchronizacją czasu;
- b) systemy łączności krytycznej np. LoRa, Meshtastic, 5G;
- c) interferometryczne lokalizatory źródeł zakłóceń widma radiowego np. w pasmach GPS/GNSS;
- d) interferometryczne systemy fazowania atomowych źródeł czasu;
- e) interferometryczne alternatywne systemy precyzyjnej nawigacji;
- f) interferometryczne dyskretne systemy wykrywania obiektów na niskich wysokościach;
- g) interferometryczne dyskretne systemy śledzenia efemeryd obiektów kosmicznych;
- h) systemy ochrony stealth przed zakłóceniami anten GNSS;
- i) alternatywne systemy GPS/GNSS dla obszarów morskich i lądowych;
- j) projektowanie i ocena cyberbezpieczeństwa prywatnych sieci 5G/6G przeznaczonych do budowy sieci rządowych, samorządowych oraz infrastruktury krytycznej;
- k) systemy łączności hybrydowej, bezpiecznej łączności państwowej oraz usług łączności satelitarnej na potrzeby jednostek prywatnych i publicznych;
- l) radiokomunikacja i telekomunikacja optyczna;
- m) sieci komórkowe (4G/5G/6G) i badania pola elektromagnetycznego (PEM);
- n) metrologia elektryczna;
- o) monitoring i ochrona infrastruktury krytycznej.

2. Technologie informatyczne:

- a) systemy wspierania podejmowania decyzji (Decision Support Systems), oparte na modelowaniu dużych zbiorów danych, z wykorzystaniem AI (Artificial Intelligence), Business Intelligence dla modeli decyzyjnych i systemów ekspertowych dla jednostek finansów publicznych jak eToll, ZPA i GigaFactory AI;
- b) modelowanie i predykcja cyberzagrożeń na potrzeby krajowego systemu cyberbezpieczeństwa;
- c) automatyzacja i zastosowania Przemysłowego Internetu Rzeczy (IIoT), rozszerzonej rzeczywistości (AR) oraz bliźniaków cyfrowych (Digital Twin) w celu optymalizacji procesów oraz predykcji zdarzeń do zastosowania IIoT w samorządowych sieciach prywatnych na potrzeby Smart City, asystencji technologicznej OzN, akwizycji danych z wielkoobszarowych pól sensorów IIoT (LoRaWAN, 5G), bliźniakach cyfrowych na potrzeby zarządzania procesami w przedsiębiorstwach infrastruktury krytycznej oraz monitoringu i ochrony infrastruktury krytycznej;
- d) systemy przetwarzania krawędziowego (Edge Computing).

3. Cyberbezpieczeństwo i kryptografia postkwantowa:

- a) badanie zgodności elementów ekosystemu e-tożsamości zapewnianej przez państwo, w tym portfela tożsamości cyfrowej (EUDI Wallet, środków identyfikacji elektronicznej i poświadczeń (atrybutów) z normami referencyjnymi w kontekście interoperacyjności na poziomie europejskim;
- b) badania zgodności produktów teleinformatycznych zgodnie z metodyką Common Criteria oraz innymi metodykami zawartymi zwłaszcza w normach europejskich;
- c) opracowywanie metod ataków na bezpieczeństwo urządzeń sprzętowych przez złożenie analiz parametrów fizycznych i zaawansowanych metod matematycznych (w tym analizy korelacji oraz metody formalne);
- d) ocena bezpieczeństwa rozwiązań z zakresu kryptografii postkwantowej;
- e) projektowanie rozwiązań systemów świadomości sytuacyjnej w cyberprzestrzeni np. centra świadomości, reagowania, oceny i zarządzania ryzykiem.

4. Infrastruktura kwantowa oraz systemy autonomiczne:

- a) budowa i utrzymanie otwartego komputera kwantowego na potrzeby świata nauki i biznesu oraz edukacji kadr w zakresie pułapek jonowych z funkcjami symulatora kwantowego;
- b) budowa systemu autonomicznego z wykorzystaniem dronów na potrzeby monitoringu i nadzoru procesów realizowanych przez jednostki państwowe i prywatne.

5. Mikroelektronika:

- a) projektowanie i produkcja polskich układów scalonych na potrzeby polskiego systemu bezpiecznych dokumentów tożsamości i innych zastosowań – uruchomienie krótkoseryjnej linii produkcyjnej;
- b) projektowanie i produkcja innych rozwiązań z zakresu mikroelektroniki na potrzeby sterowania przepływem energii i informacji;

- c) projektowanie czujników i systemów sensorów wideo do zastosowań IIoT;
- d) projektowanie elementów brzegu sieci zdolnych działać autonomicznie w długim okresie czasu;
- e) projektowanie układów odbiornika sygnałów GNSS w technologii nano-CMOS do precyzyjnego pozycjonowania obiektów mobilnych;
- f) projektowanie układów SDR w szczególności w oparciu o układy FPGA;
- g) projektowanie układów elektronicznych na potrzeby monitoringu środowiska elektromagnetycznego np. wielospektralnych obserwacji aktywności Słońca oraz przestrzeni kosmicznej w celu budowy systemów ochrony i systemów predykcji zakłóceń systemów telekomunikacyjnych.

Działania Instytutu łączności będą wspierane przez prace badawcze, badania laboratoryjne i ocenę zgodności oraz usługi prowadzone w:

1. Laboratoriach badawczych i wzorcujących;
2. Jednostkach potwierdzających zgodność z normami i wymaganiami odniesienia oraz certyfikujących lub przygotowujących do certyfikacji.

Planowany jest dalszy rozwój laboratoriów badawczych i wzorcujących:

1. Laboratorium Badań Urządzeń Telekomunikacyjnych (LBUT);
2. Laboratorium Badań EMC;
3. Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych (LOB);
4. Laboratorium Metrologii Elektrycznej, Elektronicznej i Optoelektronicznej (LMEEiO);
5. Laboratorium Aparatury Pomiarowej EMC;
6. Jednostki ds. Porównań Międzylaboratoryjnych.

W celu utrzymania i doskonalenia systemów jakości w laboratoriach planowane są następujące działania:

- a) ustawiczne podnoszenie jakości usług;
- b) wdrażanie metod badawczych i wzorcowania zgodnie z rozwojem techniki, wymagań normalizacyjnych i zapotrzebowaniem rynku;
- c) rozszerzanie zakresów akredytacji;
- d) utrzymywanie i doskonalenie systemów zarządzania akredytowanych jednostek;
- e) rozbudowa infrastruktury służącej pomiarom;
- f) podnoszenie kompetencji personelu.

Utworzenie i rozwój Jednostki Certyfikującej Wyroby:

Kontynuowanie prac mających na celu utworzenie Jednostki Certyfikującej Wyroby, prowadzącej ocenę zgodności wyrobów według modułu B – badanie typu UE, zgodnie z wymaganiami zasadniczymi:

- a) dyrektywy 2014/53/UE (tzw. RED) dotyczącej udostępniania na rynku urządzeń radiowych;
- b) dyrektywy 2014/30/UE (tzw. EMCD) dotyczącej kompatybilności elektromagnetycznej;
- c) rozporządzenia wykonawczego Komisji Europejskiej 2024/482 dotyczącego programu EUCC

Jednostka Certyfikująca Wyroby będzie pełniła funkcję jednostki oceny zgodności notyfikowanej w UE po uzyskaniu wszystkich wymaganych certyfikatów Polskiego Centrum Akredytacji (PCA) i uzyskaniu autoryzacji wydanej przez MC.

Wskaźniki realizacji perspektywicznych kierunków działalności i wdrożeniowej IŁ–PIB (2026–2030)

1. Rozwój badań i technologii telekomunikacyjnych

- Poziom gotowości technologicznej (TRL) opracowanych rozwiązań w obszarze sieci mobilnych, satelitarnych i krytycznych systemów łączności.
- Liczba zrealizowanych projektów i środowisk testowych dla technologii 5G/6G, GNSS, LoRa, Meshtastic.
- Stopień wykorzystania wyników badań w praktyce – np. wdrożenia w infrastrukturze krytycznej, sieciach rządowych i samorządowych.
- Jakość współpracy z przemysłem telekomunikacyjnym (ocena trwałości partnerstw, liczba wspólnych projektów wdrożeniowych).

2. Cyberbezpieczeństwo i kryptografia postkwantowa

- Poziom rozwoju kompetencji w zakresie oceny bezpieczeństwa systemów teleinformatycznych (zgodność z Common Criteria, EUCC).
- Liczba opracowanych lub przetestowanych rozwiązań postkwantowych.
- Skuteczność wdrożeń w krajowym systemie cyberbezpieczeństwa (np. narzędzia detekcji, centra świadomości sytuacyjnej).
- Zaufanie instytucji publicznych do wyników badań potwierdzone poprzez udział w projektach strategicznych lub rolę ekspercką w KE, ESA itp.

3. Infrastruktura kwantowa i systemy autonomiczne

- Stopień rozwoju krajowych kompetencji w zakresie technologii kwantowych (otwarty komputer kwantowy, pułapki jonowe, symulatory).
- Liczba projektów pilotażowych w zakresie systemów autonomicznych i dronowych dla administracji, biznesu i przemysłu.
- Poziom współpracy międzynarodowej w ramach programów Horizon Europe lub ESA.

4. Mikroelektronika i fotonika

- Stopień zaawansowania linii produkcyjnej układów scalonych (uruchomienie, stabilność, produkcja krótkoseryjna).
- Liczba opracowanych układów i czujników do zastosowań w infrastrukturze krytycznej, dokumentach tożsamości, energetyce, monitoringu środowiska.
- Jakość wdrożeń technologii fotonicznych i elektronicznych w polskich zastosowaniach przemysłowych.

5. Technologie informatyczne i sztuczna inteligencja

- Liczba opracowanych rozwiązań z zakresu AI/ML, systemów wspierania decyzji (DSS) i Digital Twin.

- Stopień wykorzystania narzędzi AI i Big Data w administracji publicznej, systemach finansów publicznych i przemyśle.
- Poziom integracji technologii IIoT i Edge Computing w środowiskach Smart City i infrastrukturze krytycznej.

6. Rozwój laboratoriów i infrastruktury badawczej

- Stopień modernizacji i rozbudowy laboratoriów badawczych i wzorcujących.
- Liczba nowych metod badawczych wdrożonych zgodnie z wymaganiami normalizacyjnymi UE.
- Poziom utrzymania i doskonalenia systemów jakości (akredytacje PCA, rozszerzenie zakresów).
- Utworzenie i uruchomienie Jednostki Certyfikującej Wyroby (RED, EMCD, EUCC).

7. Współpraca naukowa i międzynarodowa

- Jakość i trwałość partnerstw naukowych i przemysłowych – ocena ciągłości projektów, wspólnych publikacji i wdrożeń.
- Udział w projektach i sieciach badawczych UE (Horizon Europe, EuroHPC, ESA, ENISA).
- Udział ekspertów IŁ-PIB w organizacjach normalizacyjnych (ETSI, ITU, ISO, CENELEC).
- Rozpoznawalność Instytutu w międzynarodowym środowisku naukowym i technologicznym.

8. Efekty społeczne i gospodarcze

- Wpływ działalności Instytutu na wzrost suwerenności cyfrowej i bezpieczeństwa infrastruktury państwa.
- Stopień komercjalizacji wyników badań i rozwiązań technologicznych.
- Wkład Instytutu w rozwój krajowych kompetencji technologicznych (szkolenia, certyfikacje, publikacje).
- Pozycja Instytutu jako krajowego ośrodka referencyjnego w dziedzinie telekomunikacji i cyberbezpieczeństwa.

9. Zarządzanie strategiczne i rozwój organizacyjny

- Spójność działań z misją i wizją Instytutu określoną w strategii 2026–2030.
- Poziom realizacji celów strategicznych w poszczególnych filarach.
- Rozwój kultury innowacyjnej, otwartości na interdyscyplinarność i elastyczność organizacyjną.