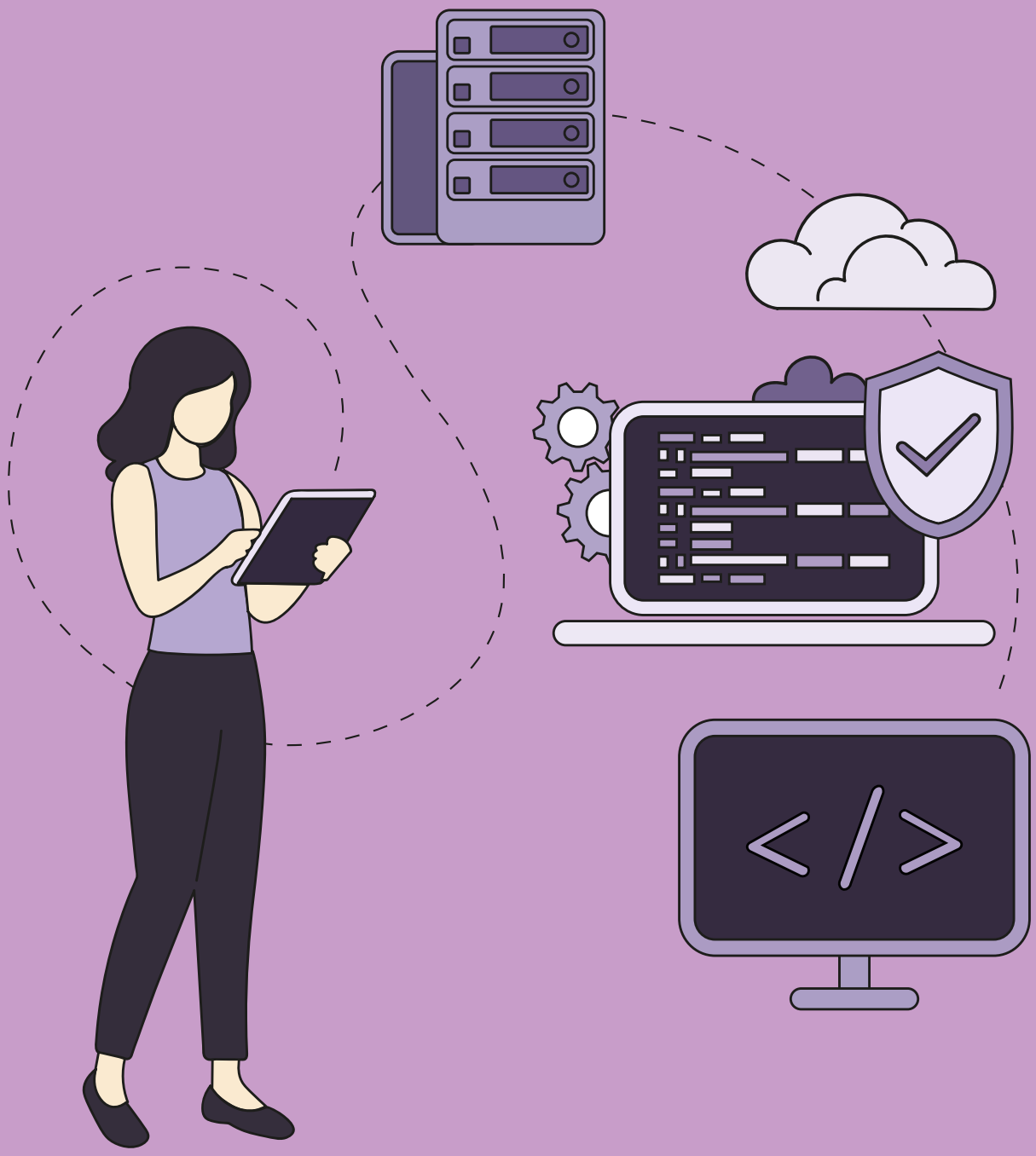
ZINTEGROWANY SYSTEM KWALIFIKACJI



ZAKTUALIZOWANA SEKTOROWA RAMA KWALIFIKACJI DLA INFORMATYKI (SRK IT)

Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
INSTYTUT BADAŃ EDUKACYJNYCH
Państwowy Instytut Badawczy

Autorzy rozdziałów wstępnych: Edyta Cieszkowska, Dawid Dymkowski, Michał Królikowski, Monika Lentacz, Mateusz Przywara, Urszula Wrońska

Autorzy zaktualizowanej SRK IT: Adam Białek, Edyta Cieszkowska, Witold Dobrzyński, Dawid Dymkowski, Rafał Kołodziejczyk, Monika Lentacz, Tadeusz Osowski, Damian Parol, Janusz Popielewski, Bartłomiej Przybyciel, Maciej Rakowski, Agnieszka Rogowska, Dominik Strzałka, Kamil Szostak, Urszula Wrońska, Jerzy Żemła

Redakcja językowa: Anna Herzog-Grzybowska
Projekt okładki: Zuzanna Gułaj
Skład: Wojciech Maciejczyk

ISBN: 978-83-68747-38-6

Wydawca:
Instytut Badań Edukacyjnych – Państwowy Instytut Badawczy
ul. Górczewska 8, 01-180 Warszawa
tel. (22) 241 71 00; www.ibe.edu.pl

Warszawa 2026

Wzór cytowania:
Białek, A., Cieszkowska, E., Dobrzyński, W., Dymkowski, D., Kołodziejczyk, R., Królikowski, M., Lentacz, M., Osowski, T., Parol, D., Popielewski, J., Przybyciel, B., Przywara, M., Rakowski, M., Rogowska, A., Strzałka, D., Szostak, K., Wrońska, U., Żemła, J. (2026). *Zaktualizowana Sektorowa Rama Kwalifikacji dla Informatyki (SRK IT)*. Instytut Badań Edukacyjnych – Państwowy Instytut Badawczy.

Publikacja powstała w ramach realizacji projektu systemowego „Wspieranie dalszego rozwoju Zintegrowanego Systemu Kwalifikacji w Polsce" (ZSK 6), współfinansowanego ze środków Unii Europejskiej w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021–2027 (FERS).

Egzemplarz bezpłatny

Spis treści

1. Definicja sektora

Sektor IT to obszar zajmujący się wszystkimi działaniami związanymi z przetwarzaniem, przechowywaniem, przesyłaniem i zarządzaniem informacją za pomocą technologii cyfrowych. W tym obszarze są podejmowane działania o różnym stopniu złożoności, takie jak: analiza wymagań, projektowanie, wytwarzanie, testowanie, zabezpieczenie i wdrażanie oprogramowania lub administrowanie konfiguracją i utrzymaniem w ruchu systemu informatycznego lub usług cyfrowych oraz niezbędne czynności związane z jego aktualizacją. Obszar ten obejmuje rozwój i zastosowanie sprzętu (hardware), oprogramowania (software), sieci komputerowych, baz danych, platform cyfrowych, a także świadczenie różnorodnych usług cyfrowych wykorzystujących systemy chmurowe i sztuczną inteligencję we współpracy z usługami dotyczącymi cyberbezpieczeństwa, zabezpieczającymi systemy IT (ICT) przed zagrożeniami i atakami hakerskimi.

Wyznaczniki sektorowe:

I. Infrastruktura IT
II. Technologie sieciowe
III. Inżynieria oprogramowania
IV. Aplikacje i usługi cyfrowe
V. Rozwiązania chmurowe
VI. Wsparcie IT
VII. Zarządzanie danymi i AI
VIII. Architektura rozwiązań IT
IX. Zarządzanie IT
X. Przełomowe technologie IT
XI. Green IT
XII. Komunikacja, współpraca, przywództwo
XIII. Orientacja na użytkownika
XIV. Odpowiedzialność i etyka
XV. Rozwój i innowacyjność

2. Możliwości wykorzystania Sektorowej Ramy Kwalifikacji dla Informatyki w praktyce

Sektorowa Rama Kwalifikacji dla Informatyki (SRK IT) to uniwersalne narzędzie do zarządzania kompetencjami w sektorze informatycznym. Dzięki temu, że budowa SRK IT nie narzuca określonych rozwiązań biznesowych, może być wykorzystywana w dowolny sposób przez wielu różnych odbiorców.

Pracodawcy

Za pomocą SRK IT pracodawcy mogą szerzej spojrzeć na kompetencje branżowe występujące w ich środowisku biznesowym, a dzięki temu efektywniej zarządzać zasobami ludzkimi i skuteczniej konkurować na rynku pracy. Do największych zalet wynikających z korzystania z tego narzędzia zalicza się wsparcie w procesach analizy luk kompetencyjnych branży czy firmy, planowania rozwoju zasobów ludzkich oraz siatki płacowej stanowisk, a także rekrutacji i doboru personelu.

Tabela kompetencji pozwoliła mi określić kryteria rekrutacji pracowników na podstawie kluczowych kompetencji w branży, a także przygotować opisy stanowisk pracy.

Szkoły i placówki oświatowe

Po zidentyfikowaniu głównych luk kompetencyjnych w branży rozpoczęliśmy program praktyk zawodowych, które mają za zadanie przygotować naszych uczniów do efektywnego wejścia na rynek pracy.

Na podstawie SRK IT szkoły i placówki oświatowe mogą dostosowywać realizowane programy nauczania do aktualnych i realnych potrzeb rynku pracy. Oznacza to, że tabela kompetencji wspiera te podmioty przy poszerzaniu i modyfikacji realizowanych programów nauczania oraz uzupełnianiu luk kompetencyjnych uczniów, np. dotyczących umiejętności praktycznych czy miękkich. Dodatkowo może być przydatna w doradztwie zawodowym dla uczniów czy monitorowaniu sukcesów absolwentów szkół.

Uczelnie wyższe

SRK IT jest narzędziem, które wspiera uczelnie wyższe w dopasowaniu programów kierunków studiów do bieżących trendów w rozwoju branży. Dzięki temu studenci mogą być lepiej przygotowani do wejścia na rynek pracy i osiągnięcia sukcesu zawodowego. Tabele kompetencji umożliwiają także monitorowanie postępów studentów oraz ocenę efektywności programów kierunków studiów.

SRK IT wykorzystaliśmy do analizy poziomu umiejętności studentów z zakresu informatyki oraz efektywności stosowanych przez nas programów.

Dzięki lepszemu dopasowaniu do potrzeb naszych klientów staliśmy się bardziej konkurencyjni na rynku firm szkoleniowych.

Firmy szkoleniowe

Firmy szkoleniowe korzystające z SRK IT mogą skutecznie projektować specjalistyczne szkolenia, dzięki czemu są w stanie przygotować ofertę szytą na miarę potrzeb konkretnej branży oraz oczekiwań swoich klientów. Za pomocą sektorowej ramy kwalifikacji mogą wybierać poszczególne kompetencje i dobierać je do efektów danego programu szkoleniowego. Mogą także przygotowywać egzaminy weryfikujące zdobytą wiedzę, umiejętności oraz kompetencje społeczne. Dzięki gradacji złożoności kompetencji w SRK IT łatwiej im również stworzyć ofertę szkoleniową z podziałem na różne poziomy zaawansowania.

Interesariusze ZSK

Spośród szerokiego grona odbiorców ZSK w największym stopniu mogą skorzystać na opracowanej SRK IT przede wszystkim organizacje branżowe oraz osoby opisujące kwalifikacje wolnorynkowe lub sektorowe. Zadaniem tych pierwszych jest m.in. nawiązywanie porozumień

edukacyjnych zacieśniających współpracę pomiędzy szkołami a pracodawcami oraz przekazywanie informacji na temat zapotrzebowania na kompetencje sektorowe instytucjom edukacyjnym lub instytucjom rynku pracy. Z kolei osoby opisujące kwalifikacje wolnorynkowe i sektorowe mogą korzystać z przygotowanego materiału w celu łatwiejszego definiowania zestawów efektów uczenia się.

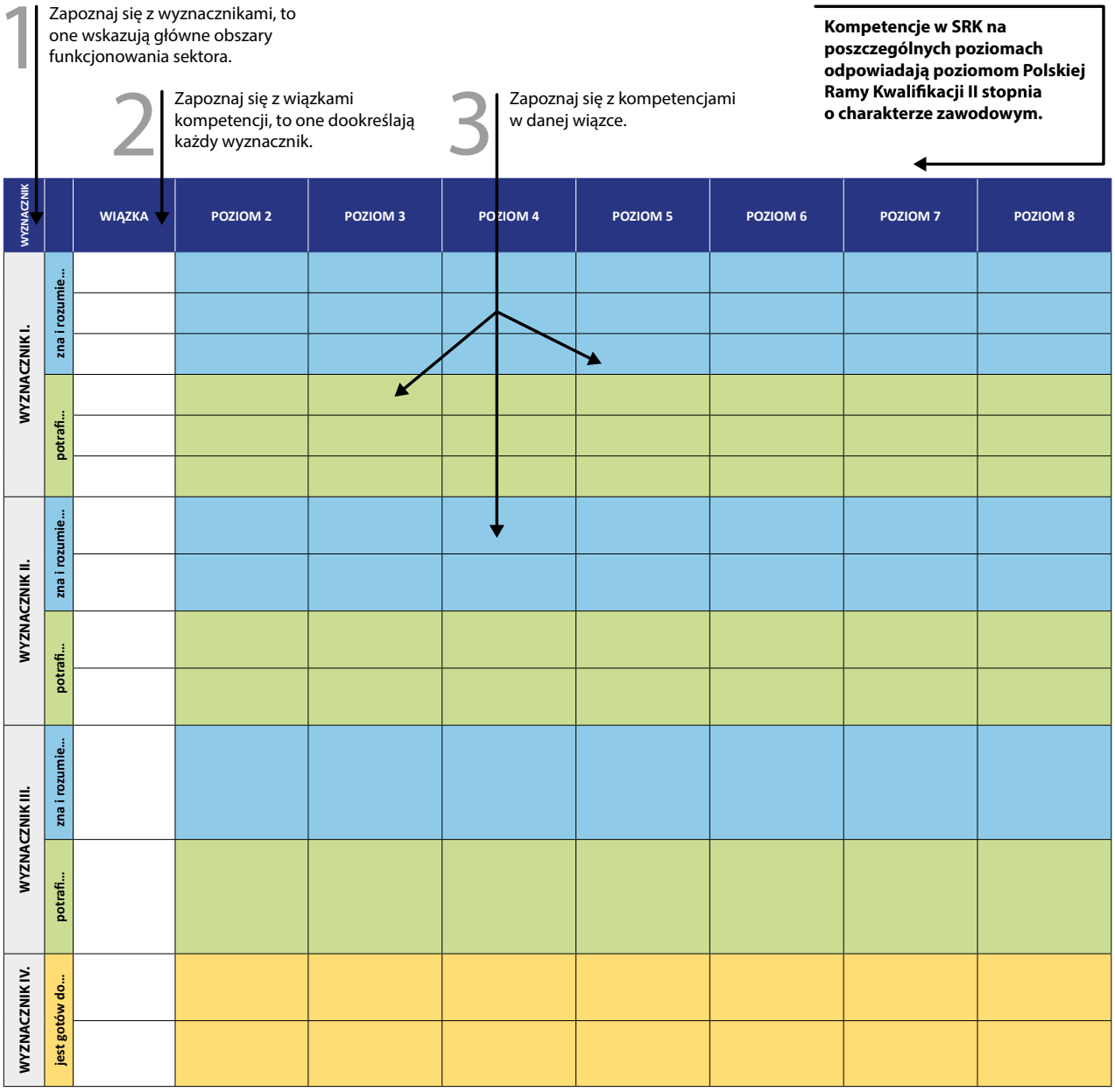
Inne podmioty

SRK IT może być wykorzystywana do wielu innych celów w zależności od aktualnych potrzeb branży. W przypadku sektora informatyki może to być narzędzie pomocnicze do przygotowania materiałów weryfikujących wiedzę pracowników w zakresie nowych technologii. Uwzględnienie w SRK IT takich obszarów jak sztuczna inteligencja, automatyzacja oraz zaawansowane usługi chmurowe może odpowiadać na zapotrzebowanie branżowego rynku pracy w tym zakresie. Na szczególną uwagę zasługuje również wyznacznik Green IT, w którym uwzględniono m.in. takie obszary jak zrównoważona infrastruktura sprzętowa.

Co więcej, aktualnie sektor informatyki boryka się z niedoborem wykwalifikowanych pracowników. Sektorowa Rama Kwalifikacji dla Informatyki może posłużyć do przekwalifikowania się i rozpoczęcia kariery zawodowej osób z bliskich merytorycznie sektorów.

Jako ekspert z branży IT staram się podążać za technicznymi nowinkami z branży. Analiza wyznacznika „Przełomowe technologie IT" pozwala mi skupić się na najważniejszych obszarach, które są istotne nie tylko w sektorze, ale i na rynku pracy.

3. Instrukcja korzystania z Sektorowej Ramy Kwalifikacji dla Informatyki



Kompetencje pogrupowane są w odpowiednie kategorie oznaczone kolorami:

wiedza (zna i rozumie…),

umiejętności (potrafi…)

kompetencje społeczne (jest gotów do…).

Pamiętaj!
Jeśli dana kompetencja jest pogrubiona i ma opis **ZK**, oznacza to, że jest to tak zwana **zielona kompetencja.**

Ważne!
Często dopiero połączenie wiązek z obszaru **wiedzy** oraz **umiejętności** pozwala w pełni opisać określony proces.

1. Zaktualizowana Sektorowa Rama Kwalifikacji dla Informatyki (SRK IT) ze wskazaniem zielonych kompetencji zidentyfikowanych w sektorze

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	zna i rozumie…	**Środowiska serwerowe**	podstawowe zagadnienia związane z sieciami komputerowymi oraz systemami operacyjnymi; budowę środowisk serwerowych	parametry i architekturę fizycznych serwerów, w tym procesorów wielordzeniowych; parametry interfejsów sieciowych i ich znaczenie; zasady administracji serwerowymi systemami operacyjnymi Windows Server i/lub Linux i/lub UNIX (np. Windows Server, Debian/ Ubuntu/RHEL, HP UX/AIX/ Solaris); warunki środowiskowe wpływające na pracę serwera (np. temperatura, wilgotność)	zasady konfiguracji serwerów i usług (m.in. www, plików, pocztowych, baz danych); zagadnienia klastrowe (tworzenie, zarządzanie); języki skryptowe i powłoki wiersza poleceń (np. Bash, PowerShell)	metody automatyzacji i orkiestracji środowisk serwerowych (np. IaC); mechanizmy wysokiej dostępności (HA); zasady konfiguracji sieci komunikacyjnych serwerów; zasady zarządzania środowiskami serwerowymi w modelu hybrydowym i rozproszonym	metody doboru rozwiązań dotyczących bezpieczeństwa dla środowisk serwerowych; metody projektowania skalowalnych i redundantnych środowisk serwerowych; zasady doboru technologii serwerowych pod kątem biznesowym i licencyjnym	
	potrafi…	**Środowiska serwerowe**	uruchamiać systemy operacyjne (Linux/Windows) z gotowych obrazów	dobierać i konfigurować parametry oraz architekturę fizycznych serwerów; nadać i skonfigurować interfejsy sieciowe (m.in. adres IP, maskę podsieci, bramę domyślną); dobierać parametry zasilania; dobierać rodzaj i parametry zasilania awaryjnego; zapewniać odpowiednie warunki środowiskowe pracy serwera	skonfigurować parametry serwera pod kątem usług; skonfigurować klaster serwerów; tworzyć/korzystać ze skryptów (automatyzujących) oraz posługiwać się powłokami wiersza poleceń	tworzyć i utrzymywać maszyny wirtualne i kontenery; zarządzać wysoką dostępnością środowisk serwerowych, w tym load balancingiem; automatyzować zarządzanie środowiskami serwerowymi (np. Ansible, Terraform, Puppet)	zabezpieczać środowiska serwerowe poprzez permanentne stosowanie tzw. hardeningu; budować, konfigurować i wdrażać środowiska serwerowe w infrastrukturze hybrydowej (własne DC i chmura)	
	zna i rozumie…	**Wirtualizacja**	podstawowe pojęcia wirtualizacji	zasady doboru infrastruktury pod rozwiązania wirtualne; cykl życia maszyny wirtualnej; podstawy sieci wirtualnej; różnicę pomiędzy snapshot a kopią zapasową	metody zarządzania sieciami zwirtualizowanymi; zasady tworzenia kopii zapasowych i retencji maszyn wirtualnych; zasady wirtualizacji pamięci masowych	metody zarządzania klastrami i mechanizmami HA oraz migracji na żywo (live migration)	metody migracji środowisk (wirtualne–fizyczne, wirtualne–wirtualne); ryzyka przy migracji środowisk P2V/V2V i metody powrotu (rollback)	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	potrafi…	**Wirtualizacja**	tworzyć maszyny wirtualne z szablonów oraz konfigurować ich podstawowe parametry	dobierać infrastrukturę pod wirtualizację; utworzyć snapshot dla maszyny wirtualnej; zmieniać parametry maszyn wirtualnych	konfigurować VLAN w wirtualnym przełączniku i przypisywać port-groups; konfigurować zadania backupu maszyn wirtualnych	konfigurować migrację na żywo oraz polityki HA dla kluczowych maszyn wirtualnych; tworzyć i zarządzać maszynami wirtualnymi w klastrze	opracowywać projekt architektury wirtualnej; planować i realizować migracje P2V/V2V z ewentualnym planem powrotu (rollback)	
	zna i rozumie…	**Konteneryzacja**		zasady stosowania konteneryzacji; podstawy działania kontenera; podstawy sieci kontenera (most/host) i trwałego zapisu (wolumen); podstawowe narzędzia do konteneryzacji (np. Docker, Podman) oraz standardy OCI	budowę obrazu warstwowego i działanie pamięci podręcznej; metody tworzenia sondy stanów aplikacji w kontenerze i zmiennych środowiskowych (np. health probe czy liveness probe); rolę prywatnego rejestru i zasady nadawania znaczników	metodę trwałości zapisu danych w kontenerze i jej znaczenie; orkiestratory i platformy kontenerowe (np. Kubernetes, OpenShift) oraz narzędzia do zarządzania klastrami (np. Rancher); zarządzanie cyklem życia kontenerów (od budowy obrazu po jego uruchomienie i monitorowanie)	wzorce przenoszenia aplikacji do kontenerów (modele migracji zasobów: Strategie 6R i 7R)	
	potrafi…	**Konteneryzacja**		zbudować obraz kontenera; uruchomić kontener z obrazu; zamontować wolumen; odczytać logi i stan kontenera	przygotować własny obraz kontenera; dodać health check i limity zasobów kontenera; przygotować plik kompozycji (Compose) dla zestawu usług z trwałym magazynem; zalogować się do rejestru prywatnego oraz wysłać i pobrać obrazy	wdrożyć lokalny rejestr obrazów z polityką retencji; zaprojektować środowisko wielousługowe z odseparowaną siecią, sekretami i trwałym zapisem	opracować plan migracji aplikacji do kontenerów; zaprojektować aktualizację etapową z health check i kryteriami powrotu	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	zna i rozumie…	**Monitorowanie infrastruktury IT**	podstawowe parametry systemowe (np. dostępność, obciążenie CPU, wykorzystanie pamięci, przestrzeń na dane, parametry środowiskowe); podstawowe parametry sieciowe (np. dostępność, przepustowość, opóźnienia, utrata pakietów, obciążenie interfejsów); podstawowe parametry aplikacyjne i usługowe (np. status usług i procesów, czas odpowiedzi, liczba połączeń)	parametry środowisk wirtualnych i chmurowych (np. obciążenie maszyn, status hostów i hypervisorów, dostępność zasobów w chmurze)	zasady analizy alertów narzędzi monitorujących; wpływ monitorowanych parametrów na dostępność systemów; narzędzia monitorujące (np. Zabbix, Grafana, Kibana)	metody korelacji zdarzeń	wpływ incydentów na SLA i KPI; strategie utrzymania infrastruktury IT	możliwości tworzenia i wykorzystania nowych algorytmów AI/ML do prognozowania awarii i automatyzacji reakcji
	potrafi…	**Monitorowanie infrastruktury IT**	odczytywać dane z narzędzi monitorujących infrastrukturę IT; rejestrować incydenty związane z monitorowanymi parametrami	konfigurować podstawowe parametry do monitorowania infrastruktury IT	konfigurować zaawansowane parametry do monitorowania infrastruktury IT; reagować na incydenty związane z monitorowanymi parametrami; analizować dzienniki zdarzeń systemu; oceniać wpływ monitorowanych parametrów na dostępność systemów	integrować monitoring z powiadomieniami; tworzyć dashboardy; proponować usprawnienia w infrastrukturze IT	projektować systemy monitoringu infrastruktury IT; raportować efektywność monitorowanych parametrów systemu; wspierać podejmowanie decyzji związanych z monitorowanymi komponentami; odpowiadać za SLA i KPI; tworzyć polityki monitoringu infrastruktury IT; nadzorować zgodność i efektywność operacyjną	wykorzystywać nowatorskie algorytmy AI/ML do prognozowania awarii i automatyzacji inicjowania działań prewencyjnych
	zna i rozumie…	**Technologie uwierzytelniania i autoryzacji**	podstawy uwierzytelniania; podstawy autoryzacji	różne technologie i systemy zarządzania tożsamością i dostępem (np. biometria)	w szerokim zakresie technologie i mechanizmy zarządzania tożsamością i dostępem w organizacji (np. MFA, SSO, PAM, PIM); metody kontroli dostępu (np. DAC, MAC, RBAC, ABAC, PBAC, Rule-Based Access Control); procedury organizacyjne i polityki związane z obsługą tożsamości i dostępu	złożone metody zarządzania tożsamością i dostępem nacechowane zwiększonym bezpieczeństwem, poprawą wydajności; systemy zarządzania tożsamością i dostępem; federację tożsamości; specjalistyczne metody zarządzania tożsamością i dostępem z wykorzystaniem automatyzacji	metody audytowania polityk bezpieczeństwa w zakresie zarządzania tożsamością i dostępem; zasady zarządzania strategią tożsamości i dostępów	badanie trendów rozwoju technologii Zero Trust i SASE

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	potrafi…	**Technologie uwierzytelniania i autoryzacji**	weryfikować tożsamość użytkownika podstawowymi metodami; wdrażać i obsługiwać technologie uwierzytelniania i autoryzacji	zgłaszać incydenty związane z tożsamością i dostępem; stosować różne technologie i systemy zarządzania tożsamością i dostępem (np. Active Directory, Microsoft Azure AD, SSO)	dobierać schemat nadawania i weryfikacji uprawnień w organizacji; określać optymalne metody zarządzania tożsamością i dostępem	administrować kontami użytkowników, rolami i dostępami, stosując zasady najmniejszych uprawnień i zgodności z politykami bezpieczeństwa; projektować złożone metody zarządzania tożsamością i dostępem; automatyzować procesy zarządzania dostępem (AD/IAM) i integrować uprawnienia	wdrażać i utrzymywać rozwiązania do uwierzytelniania, autoryzacji i audytu dostępu z wykorzystaniem narzędzi i skryptów automatyzujących zarządzanie tożsamościami i dostępem	
	zna i rozumie…	**Pamięci masowe i systemy plików**	rodzaje pamięci masowych i systemów plików	zasady dobierania pamięci masowych i systemów plików; zasady konfigurowania serwerów NAS	zasady kontroli i naprawy integralności systemów plików; zasady zabezpieczania danych; zasady konfigurowania macierzy z wykorzystaniem technologii RAID	zasady kontroli poprawności gromadzonych danych; polityki kopii bezpieczeństwa organizacji (w tym zagadnienia związane z retencją nośników/kopii, strategią wykonywania kopii, zasadami przechowywania kopii/nośników); zasady przydzielania zasobów macierzy do poszczególnych systemów operacyjnych	zasady konfigurowania klastrów macierzy; zasady replikacji danych; architekturę pamięci masowych dla organizacji	
	potrafi…	**Pamięci masowe i systemy plików**	wykorzystywać różne rodzaje pamięci masowych i sytemów plików	przygotować pamięci masowe do użytku (np. tworzyć partycje, wolumeny); konfigurować serwery NAS	kontrolować i naprawiać integralność systemów plików; konfigurować parametry zapewniające stabilność i bezpieczeństwo danych; konfigurować macierze z wykorzystaniem technologii RAID	kontrolować jakość danych; tworzyć polityki kopii bezpieczeństwa organizacji (z uwzględnieniem zagadnień związanych z retencją nośników/kopii, strategią wykonywania kopii, zasadami przechowywania kopii/nośników); zarządzać zasobami macierzy przydzielonymi do poszczególnych systemów operacyjnych	konfigurować klastry macierzy; konfigurować replikację danych; konfigurować architekturę pamięci masowych dla organizacji; tworzyć wirtualne sieci pamięci masowych (np. SDS)	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	zna i rozumie…	**Zarządzanie systemami operacyjnymi**	podstawowe typy systemów operacyjnych (np. serwerowe, desktopowe i mobilne); strukturę plików; podstawowe usługi systemowe; strukturę kont użytkowników, uprawnień i usług	różnice między systemami serwerowymi a desktopowymi; zasady zarządzania zasobami (np. RAM, CPU, dysk); zasady zarządzania użytkownikami i uprawnieniami w środowisku rozproszonym; podstawowe zasady działania usług katalogowych (np. LDAP/AD); typowe skrypty systemowe	zasady zarządzania wieloma systemami w środowisku rozproszonym; mechanizmy wirtualizacji, konteneryzacji i backupu; strukturę domen, OU, GPO i polityk bezpieczeństwa	architekturę systemów operacyjnych i ich wpływ na wydajność oraz dostępność; zależności między warstwą systemu operacyjnego a aplikacjami i sprzętem	metody projektowania zależności między systemami operacyjnymi w kontekście architektury IT, bezpieczeństwa, zgodności i automatyzacji	
	potrafi…	**Zarządzanie systemami operacyjnymi**	zainstalować system operacyjny; tworzyć konta użytkowników lokalnych; wykonywać podstawowe polecenia systemu operacyjnego	skonfigurować system operacyjny; monitorować działanie systemu i rozwiązywać typowe problemy związane z działaniem systemu operacyjnego; zarządzać atrybutami i uprawnieniami użytkowników lokalnych; wykonywać podstawowe operacje administracyjne i przeprowadzać podstawową konfigurację zabezpieczeń	projektować i wdrażać polityki bezpieczeństwa systemowego, zabezpieczać system oraz analizować logi systemu operacyjnego; zarządzać usługami systemowymi i sieciowymi (np. DNS, DHCP, NTP); administrować atrybutami kont użytkowników i grupami w LDAP/AD w systemach rozproszonych; konfigurować polityki haseł, uprawnień i dostępów; tworzyć skrypty systemowe	optymalizować konfiguracje systemu pod względem wydajności i zasobów; tworzyć procedury kopii bezpieczeństwa i odzyskiwania; zarządzać środowiskami rozproszonymi; zarządzać politykami bezpieczeństwa w środowisku rozproszonym	projektować złożone środowiska systemowe; dobierać technologie systemu operacyjnego zgodnie z wymaganiami biznesowymi; audytować i ocenić zgodność systemów operacyjnych oraz usług z normami i standardami IT; zarządzać systemami i politykami bezpieczeństwa w środowiskach wielodomenowych; integrować AD/LDAP z systemami chmurowymi	
	zna i rozumie…	**Zarządzanie usługami systemowymi środowiska**	podstawowe usługi systemowe (np. DNS, DHCP, NTP, usługi katalogowe, usługi drukowania)	rolę usług systemowych w przełożeniu na środowisko IT; sposoby monitorowania usług systemowych	zaawansowane usługi systemowe (np. SNMP, RDP, SSH, PKI, VPN, WSUS, syslog); zależności między usługami systemowymi a infrastrukturą IT; podstawy zarządzania usługami w modelu klient--serwer; wpływ synchronizacji czasu na bezpieczeństwo i zgodność	architekturę usług systemowych w środowiskach wielodomenowych; wpływ konfiguracji usług systemowych na bezpieczeństwo i wydajność środowiska IT; wpływ i zależności usług systemowych na ciągłość działania organizacji	zasady skalowania, redundancji i wysokiej dostępności usług systemowych; logi zbierane z poszczególnych usług systemowych i ich znaczenie dla bezpieczeństwa środowiska IT	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	potrafi…	**Zarządzanie usługami systemowymi środowiska**		uruchomić i skonfigurować podstawowe usługi systemowe na poziomie lokalnym; monitorować dostępność usług systemowych i zgłaszać związane z tym problemy	konfigurować i utrzymywać usługi systemowe (np. DNS, DHCP, SNMP, NTP, RDP, SSH, usługi katalogowe, usługi drukowania); diagnozować i rozwiązywać typowe problemy z działaniem usług systemowych; zapewnić synchronizację czasu między wszystkimi serwerami w środowisku organizacji; zarządzać certyfikatami cyfrowymi; zarządzać bezpiecznym dostępem zdalnym (np. VPN, RDP)	projektować i wdrażać usługi systemowe w środowiskach wielodomenowych; tworzyć dokumentację techniczną i procedury operacyjne w zakresie usług systemowych; integrować usługi systemowe z innymi komponentami infrastruktury; zarządzać aktualizacją środowiska i bezpieczeństwem systemów (np. WSUS, SCCM)	optymalizować konfigurację usług systemowych; projektować polityki zarządzania usługami zgodne z wymaganiami biznesowymi i regulacyjnymi; audytować i doskonalić procesy świadczenia usług systemowych; zarządzać centralnym zbieraniem logów; dobierać technologie i modele świadczenia usług (on-prem, edge, cloud native) do potrzeb biznesowych organizacji; oceniać ryzyko zaburzenia działania usług systemowych oraz ich zgodność z normami	
	zna i rozumie…	**Systemy wbudowane i czasu rzeczywistego**		podstawowe pojęcia i różnice dotyczące systemów wbudowanych i systemów czasu rzeczywistego; podstawy użytkowe środowiska uruchomieniowego	różnice między systemem ogólnego przeznaczenia a systemem wbudowanym; pojęcia bezpieczeństwa, niezawodności i odporności systemów czasu rzeczywistego i systemów krytycznych; architekturę systemów wbudowanych (np. mikrokontroler, pamięć, interfejsy, czujniki); podstawowe mechanizmy działania RTOS (np. zadania, priorytety, harmonogramowanie)	zasady projektowania i implementacji systemów czasu rzeczywistego z uwzględnieniem wymagań czasowych; wpływ ograniczeń sprzętowych na projektowanie oprogramowania	standardy i normy dla systemów krytycznych; modele komunikacji i synchronizacji zadań w RTOS	najnowsze metody projektowania systemów krytycznych czasu rzeczywistego i systemów wbudowanych o wysokiej niezawodności

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	potrafi…	**Systemy wbudowane i czasu rzeczywistego**		rozpoznać system wbudowany i jego główne komponenty; rozpoznać system czasu rzeczywistego; uruchomić prosty program sterujący mikrokontrolerem	tworzyć aplikacje dla mikrokontrolerów z wykorzystaniem podstawowych funkcji RTOS; implementować zadania z priorytetami i testować ich współbieżne działanie; analizować podstawowe błędy synchronizacji i blokady zasobów; korzystać z podstawowych narzędzi do programowania i debugowania urządzeń wbudowanych	tworzyć oprogramowanie dla systemów wbudowanych z ograniczonymi zasobami; integrować komponenty sprzętowe i programowe w systemach czasu rzeczywistego; analizować wydajność, opóźnienia i niezawodność systemu	prowadzić analizę ryzyka i bezpieczeństwa funkcjonalnego; wdrażać rozwiązania zapewniające deterministyczne działanie i zgodność z normami bezpieczeństwa	projektować nowoczesne systemy krytyczne czasu rzeczywistego i systemy wbudowane o wysokiej odporności na awarie
	zna i rozumie…	**Ciągłość działania, kopie zapasowe i odzyskiwanie danych po awarii**		rodzaje kopii zapasowych (pełne, różnicowe, przyrostowe); zasady i procedury tworzenia kopii zapasowych środowisk fizycznych i wirtualnych; narzędzia do tworzenia kopii zapasowych; technologie tworzenia kopii zapasowych środowisk fizycznych i wirtualnych	zasady i procedury odzyskiwania danych po awarii; narzędzia do odzyskiwania danych po awarii; procedury ciągłości działania infrastruktury IT w organizacji; strategię zapewnienia odporności biznesowej i ciągłości działania kluczowych procesów biznesowych podczas i po awarii, również w środowiskach hybrydowych	w szerokim zakresie zasady i standardy ciągłości działania w organizacji IT; zasady analizy ryzyka w organizacji w zakresie ciągłości działania systemów informatycznych	procedury tworzenia strategii ciągłości działania infrastruktury IT dla utrzymania kluczowych procesów w biznesie; trendy budowania odporności z wykorzystaniem modeli predykcyjnych; wykorzystanie AI, automatyzacji i rozwiązań chmurowych (np. DRaaS) w budowaniu ciągłości działania	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	potrafi…	**Ciągłość działania, kopie zapasowe i odzyskiwanie danych po awarii**		stosować standardowe procedury zapewnienia ciągłości działania infrastruktury IT w organizacji; tworzyć kopie zapasowe wg procedury; dokumentować tworzone kopie zapasowe	tworzyć procedury przywracania i odzyskiwania kopii zapasowych; precyzować i oceniać ryzyka wystąpienia awarii i utraty danych; dobierać rodzaj kopii zapasowych; testować kopie zapasowe i weryfikować ich poprawność; przywracać środowisko i/lub dane z kopii zapasowych (wg procedury); dokumentować proces odzyskiwania z kopii zapasowych; zgłaszać incydenty związane z naruszeniem ciągłości działania oraz kopiami zapasowymi	tworzyć procedury zapewnienia ciągłości działania infrastruktury IT; prowadzić analizę ryzyka w organizacji w zakresie ciągłości działania systemów informatycznych; administrować kopiami zapasowymi z użyciem złożonych narzędzi bezpieczeństwa i optymalizacji; stosować rozwiązania redundantne (np. klastry, wiele lokalizacji, rozwiązania chmurowe); planować i realizować działania naprawcze w sytuacjach kryzysowych w organizacji IT; stosować optymalne rozwiązania zapewniające szybkie wznowienie działania w celu minimalizowania strat; przeprowadzać testy odzyskiwania kopii zapasowych	korzystać z zaawansowanych metod i narzędzi monitorowania i przeciwdziałania (z użyciem przewidywania) awariom i atakom zakłócającym ciągłość działania systemów informatycznych; stosować automatyzację tworzenia kopii zapasowych, przywracania i weryfikacji poprawności odzyskiwania danych lub przywracania środowiska; tworzyć plany ciągłości działania systemów informatycznych	
	zna i rozumie…	**Integracja z rozwiązaniami chmurowymi**	podstawowe rozwiązania i aplikacje chmurowe	różnicę między środowiskiem lokalnym (on-prem) a środowiskiem chmurowym; podstawowe metody synchronizacji usług; metody zabezpieczeń środowisk chmurowych	zasady współpracy sieci lokalnej z chmurą; metody integracji zasobów i współpracy z chmurą; podstawowe wzorce integracji (np. punkt-punkt, wspólna baza, wymiana plików, API); metody ujednolicenia kont i ustawień między środowiskiem lokalnym a chmurowym	metody doboru odpowiednich aplikacji mobilnych do obsługi rozwiązań chmurowych; zasady projektowania połączeń hybrydowych; mechanizmy synchronizacji tożsamości i uprawnień; metody synchronizacji okresowej oraz zdarzeniowej	metody testowania i wdrażania odpowiednich standardów jakości integracji rozwiązań chmurowych; wzorce integracji środowisk hybrydowych i wielochmurowych (multi--cloud); metody zapewnienia spójności usług, w tym usług katalogowych	trendy w zakresie nowych rozwiązań cloud bursting, edge computing, service mesh

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
I. Infrastruktura IT	potrafi…	**Integracja z rozwiązaniami chmurowymi**	stosować aplikacje chmurowe	skorzystać z przygotowanego połączenia (np. VPN) i sprawdzić podstawową łączność; zgłosić brak dostępu do usługi po stronie chmury	zintegrować dane z chmurą; opisać wymagania sieciowe dla usługi w chmurze; wskazać cykl synchronizacji usług komunikujących się z chmurą; uruchomić aplikacje do wykorzystywania danych z chmury; wdrożyć zabezpieczenia małych środowisk chmurowych	przygotować opis integracji, w tym uwzględnić komunikację pomiędzy elementami infrastruktury lokalnej i chmurowej; przygotować synchronizację kont użytkowników; wdrożyć zabezpieczenia dużych środowisk chmurowych	testować, analizować i zapewniać bezpieczeństwo danych w chmurze; opracować jednolity opis rozwiązania hybrydowego, w tym dla systemów krytycznych; określić minimalny akceptowalny poziom niedostępności dla infrastruktury hybrydowej	tworzyć nowatorskie rozwiązania wykorzystujące cloud bursting, edge computing, service mesh
	zna i rozumie…	**Zarządzanie centrami danych**	podstawy infrastruktury IT; typy urządzeń w centrum danych; podstawowe zasady BHP i bezpieczeństwa fizycznego	zasady okablowania i konfiguracji prostych połączeń; zasady działania i doboru UPS oraz agregatów; podstawy chłodzenia serwerowni; zasady związane z wykrywaniem pożaru i gaszeniem w centrum danych; typowe zagrożenia infrastrukturalne w centrum danych	architekturę centrum danych; redundancję i dostępność (HA) urządzeń w centrum danych; standardy dokumentacji (np. TIA-942)	projektowanie topologii sieci w centrum danych (np. spine--leaf); projektowanie systemów zasilania redundantnego; monitorowanie zużycia energii i wskaźników efektywności; normy energetyczne i środowiskowe mające związek z funkcjonowaniem centrów danych; polityki bezpieczeństwa centrum danych	projektowanie i rozbudowa centrum danych zgodne z wymaganiami biznesowymi; zarządzanie ryzykiem i plany ciągłości działania centrum danych; standardy funkcjonowania centrum danych (np. ISO/IEC 22237, Uptime Institute Tier Standard); zasady współpracy z operatorami i dostawcami usług sieciowych	trendy w nowo projektowanym centrum danych (np. edge, green IT, DLC – direct liquid cooling); ocenę i technologię wdrażania nowatorskich, alternatywnych źródeł energii (np. fotowoltaika, SMR, magazyny energii)
	potrafi…	**Zarządzanie centrami danych**	wykonywać proste prace serwisowe związane z funkcjonowaniem centrum danych; obsługiwać podstawowe wskaźniki urządzeń zainstalowanych w centrum danych; zgłaszać incydenty związane z funkcjonowaniem centrum danych	monitorować środowisko (temperatura, wilgotność); diagnozować urządzenia zainstalowane w centrum danych; współpracować przy wdrożeniach infrastrukturalnych	zarządzać serwerami i sieciami; planować konserwacje i przeglądy w centrum danych; wdrażać backup (np. backup taśmowy, deduplikacja)	koordynować pracę zespołu technicznego skierowanego do centrum danych; projektować topologię sieci, systemy zasilania, systemy monitorowania; optymalizować zasoby centrum danych; tworzyć raporty (dostępności, środowiskowy, bezpieczeństwa, konserwacji i przeglądów, incydentów, zmian, zgodności z procedurami)	planować inwestycje w centrach danych; dobierać technologie i dostawców dla centrum danych; nadzorować zgodność funkcjonowania centrum danych z normami i standardami; wdrażać procedury BCP, DRP w centrum danych	tworzyć nowe strategie rozwoju centrum danych; oceniać wpływ nowych technologii wykorzystywanych w nowatorskim centrum danych na środowisko i zarządzać innowacjami IT

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
II. Technologie sieciowe	zna i rozumie…	**Sieci lokalne (LAN)**	podstawowe elementy sieci lokalnych (koncentratory, przełączniki, karty sieciowe); rodzaje okablowania (np. skrętka określonej kategorii, światłowody jedno- i wielomodowe); zasady dostępu do sieci lokalnych w organizacji; pojęcia związane z adresacją sieci IP; zasady fizycznej adresacji urządzeń sieciowych (MAC); podstawowe elementy infrastruktury sieci lokalnych; warstwy komunikacji (OSI, TCP/IP)	architekturę sieci lokalnych; podstawowe parametry i ograniczenia sieci lokalnych (np. długości segmentów sieci); podstawowe protokoły (np. Ethernet, ARP, DHCP); różnice między topologiami sieci (np. magistrala, gwiazda, pierścień, siatka, drzewo); różnice między rodzajami sieci przewodowych; narzędzia do zarządzania urządzeniami w sieci; narzędzia do aktualizacji urządzeń sieciowych, w tym aktualizacji firmware; zasady segmentacji sieci (VLAN) i bezpieczeństwa; zasady konfiguracji urządzeń do budowy sieci lokalnych (np. przełączniki)	zasady projektowania sieci LAN; zasady redundancji w projektowaniu sieci i łączeniu urządzeń; protokoły zarządzania (SNMP); metody konfiguracji jakości usług (QoS); zasady optymalizacji, audytów i standaryzacji konfiguracji w sieciach lokalnych; narzędzia do monitorowania wydajności i bezpieczeństwa sieci	zaawansowane mechanizmy sieci LAN (np. STP, RSTP, MSTP); działanie narzędzi bezpieczeństwa sieci (np. NAC, 802.1X, ACL); urządzenia do diagnozowania połączeń w sieciach; zasady integracji LAN z sieciami WAN i chmurą; narzędzia IaC do konfiguracji i zarządzania siecią	architekturę sieci LAN w dużych organizacjach; zasady wdrażania i zarządzania architekturą SDN z wykorzystaniem centralizacji płaszczyzny sterowania do optymalizacji przepływu danych i automatyzacji konfiguracji urządzeń; mechanizmy automatyzacji konfiguracji (np. Ansible, NetConf)	
	potrafi…	**Sieci lokalne (LAN)**	montować i konfigurować podstawowe elementy sieciowe; podłączyć urządzenia do sieci LAN; skonfigurować prostą adresację IP; skonfigurować dostęp do internetu przez różne technologie (DSL, kablowa, światłowodowa); sprawdzić połączenie sieci (ping)	konfigurować przełączniki sieciowe; konfigurować podstawowe sieci VLAN; diagnozować typowe problemy sieciowe; dokumentować konfigurację sieci lokalnej; wykorzystywać narzędzia do zarządzania urządzeniami sieciowymi; konfigurować i aktualizować urządzenia sieciowe	projektować i wdrażać sieci LAN w organizacji; konfigurować VLAN, trunking, podstawowe ACL; monitorować działanie sieci i reagować na incydenty; wykorzystywać narzędzia monitorujące sieci do zapewnienia wydajności i bezpieczeństwa sieci	optymalizować konfigurację sieci LAN; określać miejsce wystąpienia awarii w sieciach lokalnych; wdrażać polityki bezpieczeństwa w sieciach lokalnych; wdrażać polityki QoS	projektować strategię rozwoju sieci LAN w skali organizacji; korzystać z technologii SDN; dobierać technologie i modele zarządzania siecią zgodnie z wymaganiami biznesowymi i regulacyjnymi	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
II. Technologie sieciowe	zna i rozumie…	**Sieci bezprzewodowe (WLAN)**	podstawowe zasady wykorzystania sieci WLAN; standardy WLAN (802.11 a/b/g/n/ac/ax); podstawowe pojęcia sieci WLAN (np. AP, WiFi, SSID, hasło); podstawy bezpieczeństwa sieci WLAN (np. WEP, WPA, WPA2, WPA3); podstawowe urządzenia sieci bezprzewodowych (np. AP, kontroler, repeater)	różnice między siecią przewodową a bezprzewodową; wykorzystanie technologii PoE	podstawowe topologie WLAN (np. BSS, ESS, IBSS, mesh); standardy i przeznaczenie sieci bezprzewodowych IoT (LoRa, SIgfax, NB-IoT)	zasady projektowania WLAN; kanały radiowe i interferencje; zasady roamingu; mechanizmy uwierzytelniania (802.1X, RADIUS)	zaawansowane mechanizmy zarządzania WLAN (kontrolery, centralne zarządzanie, segmentacja SSID); zasady integracji WLAN z chmurą i 5G; normy regulacyjne w zakresie sieci bezprzewodowych (np. ograniczenia mocy); globalny system internetu satelitarnego i wersje mobilne	najnowsze technologie wykorzystujące AI w sieciach bezprzewodowych do diagnozowania i bezpieczeństwa
	potrafi…	**Sieci bezprzewodowe (WLAN)**	podłączyć urządzenie do sieci WLAN; konfigurować podstawowe ustawienia sieci bezprzewodowej (np. SSID, hasło)	konfigurować urządzenia sieciowe korzystające z technologii PoE; konfigurować proste punkty dostępowe sieci WLAN; ustawić zabezpieczenia sieci WLAN (np. WEP, WPA, WPA2, WPA3)	diagnozować podstawowe problemy z połączeniami sieci WLAN; podłączyć i skonfigurować czujnik do przesyłu danych w sieci IoT np. LoRa czy NB-IoT); konfigurować i integrować system satelitarny w miejscu wykonywania usługi	projektować i wdrażać rozbudowane sieci WLAN w organizacji; planować wykorzystanie kanałów radiowych i unikać zakłóceń; konfigurować kontrolery i polityki dostępu sieci WLAN; monitorować działanie sieci WLAN i reagować na incydenty	optymalizować konfiguracje WLAN; wdrażać polityki bezpieczeństwa i QoS dla sieci WLAN; audytować i doskonalić procesy zarządzania siecią WLAN	projektować i wdrażać zaawansowane sieci WLAN, wykorzystując najnowsze technologie, zwłaszcza AI
	zna i rozumie…	**Sieci rozległe (MAN/ WAN)**	model OSI; stos protokołów TCP/IP, IPV4/ IPV6; podstawowe protokoły (np. NAT, DHCP, DNS); elementy infrastruktury sieciowej (np. routery, modemy, przełączniki)	architekturę sieci WAN, MAN, LAN oraz ich wzajemnych zależności; reguły bezpieczeństwa w sieciach WAN; protokoły routingu (np. OSPF, BGP, RIP, EIGRP); protokoły routingu oraz standardy komunikacyjne stosowane w sieciach rozległych (WAN)	narzędzia do monitorowania sieci (np. Wireshark, SNMP, SolarWinds, Zabbix); architekturę sieci rozległych; segmentację sieci, klastry, szyfrowanie ruchu; automatyzację konfiguracji i funkcjonowania urządzeń sieciowych	zasady projektowania WAN/ MAN; sposoby diagnozowania opóźnień, strat pakietów, aberracji i problemów z trasowaniem; sieci rozproszone; wykorzystanie SD-WAN; zaawansowane mechanizmy sieciowe (np. MPLS, QoS); zasady optymalizacji, audytów i standaryzacji konfiguracji w sieciach rozległych	zaawansowane mechanizmy zarządzania WAN (routery, UTM, kontrolery, segmentacja WAN); polityki związane z bezpieczeństwem funkcjonowania sieci WAN; integrację sieci rozległych z chmurą	kierunki rozwoju i wykorzystania sieci kwantowych w komunikacji cyfrowej

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
II. Technologie sieciowe	potrafi…	**Sieci rozległe (MAN/ WAN)**	rozpoznawać typowe problemy związane z działaniem sieci; posługiwać się podstawowymi narzędziami diagnostycznymi (np. ping, traceroute)	wykorzystywać technologie sieciowe (np. VPN, IPsec, SSL VPN, BGP, OSPF, EIGRP); przeprowadzić proste prace konfiguracyjne	konfigurować zaawansowane funkcje routerów i przełączników, w tym automatyzować ich funkcjonowanie; wykorzystywać możliwości UTM; monitorować wydajność i dostępność sieci;	projektować oraz wdrażać rozległe sieci WAN; projektować i wdrażać procesy migracji sieci; tworzyć dokumentację techniczną i diagramy sieci; konfigurować komponenty sieciowe i polityki zarządzania WAN; monitorować działanie sieci WAN zgodne z politykami bezpieczeństwa i administracji sieci WAN (np. incydenty bezpieczeństwa lub ciągłości działania)	optymalizować i konfigurować WAN/MAN; zarządzać politykami bezpieczeństwa dla WAN/MAN; optymalizować oraz audytować procesy zarządzania siecią WAN; projektować architekturę sieci rozległych	
	zna i rozumie…	**Usługi internetowe**	podstawowe rodzaje usług internetowych (np. www, poczta, FTP); podstawowe zależności między kategoriami innych usług internetowych	zasady działania usług internetowych; działanie sieci i aplikacji webowych	zasady równoważenia obciążenia oraz wysokiej dostępności aplikacji; zastosowanie load balancingu w kontekście warstw L4 vs L7	zasady projektowania dostępności usług internetowych; algorytmy równoważenia obciążenia (np. Round Robin, Least Connections, Weighted RR, IP Hash); mechanizmy podtrzymywania sesji; metody zachowania wysokiej dostępności usług internetowych (tzw. High Availability); mechanizmy przełączania na zapasowy system (tzw. failover); technologie rozproszonych sieci dostarczania treści (CDN); narzędzia do load balancingu (np. HAProxy, NGINX, F5 BIG-IP, Traefik, Envoy)	zaawansowane mechanizmy zmniejszania obciążenia serwera aplikacji i zwiększania jego wydajności (np. TLS/SSL termination lub offloading); metody balancingu w chmurze (np. AWS, GCP, Azure); strategie ochrony przed przeciążeniem i atakami DoS i DDoS; metody automatycznego kontrolowania stanu systemu (tzw. health checks)	najnowsze technologie dotyczące optymalizacji ruchu sieciowego oraz dostępności usług z wykorzystaniem AI

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
II. Technologie sieciowe	potrafi…	**Usługi internetowe**	korzystać z podstawowych rodzajów usług internetowych	oceniać poprawność działania podstawowych narzędzi do świadczenia usług internetowych	diagnozować typowe problemy z dostępnością i wydajnością usług internetowych	projektować i wdrażać rozwiązania do równoważenia obciążenia i poprawy dostępności usług internetowych; stosować metody zachowania wysokiej dostępności usług internetowych; monitorować działanie usług internetowych i reagować na incydenty; korzystać z rozproszonych sieci dostarczania treści; posługiwać się narzędziami do load balancingu	optymalizować pracę serwerów aplikacji z wykorzystaniem zaawansowanych mechanizmów; stosować metody balancingu w chmurze; przewidywać i mitygować ryzyka przeciążenia oraz ataków DoS i DDoS; audytować pracę i monitoring usług internetowych; projektować rozproszone sieci dostarczania treści	projektować i wdrożyć szybkie usługi internetowe o wysokim stopniu niezawodności i bezpieczeństwa
	zna i rozumie…	**Monitorowanie i utrzymanie sieci**		zasady zapewnienia ciągłości działania sieci IT w stopniu podstawowym; metody analizy ruchu sieciowego (przepustowość, obciążenie, opóźnienie); podstawowe narzędzia do monitorowania sieci IT	typowe rodzaje awarii sieci IT; metody identyfikacji luk i problemów z wydajnością sieci IT; narzędzia do monitorowania wydajności sieci i analizy logów (np. NetFlow, sFlow, Nagios, Zabbix, PRTG)	narzędzia do analizy ruchu sieciowego; metody wykrywania nieautoryzowanych działań i potencjalnych zagrożeń bezpieczeństwa sieci IT; sposoby optymalizacji wykorzystania zasobów sieciowych	zasady polityki bezpieczeństwa i obowiązujące regulacje niezbędne do zapewnienia ciągłości działania sieci; trendy rozwoju i modernizacji sieci	
	potrafi…	**Monitorowanie i utrzymanie sieci**		zapewniać podstawową ciągłość działania sieci IT; diagnozować podstawowe problemy z utrzymaniem sieci IT (brak łączności, przeciążenia); wykonywać rutynowe czynności utrzymaniowe (np. restart urządzeń, aktualizacja)	wykrywać awarie sieci IT i im zapobiegać; rozpoznać wąskie gardła i problemy z wydajnością sieci IT; monitorować wydajność sieci IT; konfigurować systemy monitorujące i alertujące pracę sieci IT	rozpoznawać zagrożenia bezpieczeństwa IT (nieautoryzowane działania); zoptymalizować wykorzystanie zasobów sieciowych; zaplanować rozwój i modernizację sieci IT; tworzyć skrypty obsługujące urządzenia sieciowe; dobierać i wykorzystywać narzędzia do analizy ruchu sieciowego (np. Wireshark, Cloudshark)	zapewniać ciągłość działania sieci zgodnie z obowiązującymi politykami bezpieczeństwa i regulacjami	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
II. Technologie sieciowe	zna i rozumie…	**Bezpieczeństwo sieciowe i internetowe**	rodzaje zagrożeń sieciowych; podstawowe pojęcia bezpieczeństwa (np. NAT, DMZ, sieci gościnne)	rodzaje zapory sieciowej w zależności m.in. od wdrożenia czy technologii; rolę zapory sieciowej w ochronie stacji roboczej i małej sieci lokalnej; zasady filtracji ruchu sieciowego	zasady funkcjonowania zapór sieciowych nowej generacji (NGFW); podstawowe funkcje systemów IDS i IPS; sposoby analizowania incydentów bezpieczeństwa; metody klasyfikowania treści cyfrowych	architekturę bezpieczeństwa sieci z uwzględnieniem zapór sieciowych nowej generacji; zasady działania silników detekcji zagrożeń sieciowych; koncepcje zero trust, mikrosegmentacji i wielowarstwowej ochrony (defence in depth); wpływ konfiguracji zapór sieciowych na dostępność usług i wydajność sieci; metody ochrony przed atakami DDoS; narzędzia klasy SIEM, SOAR	modele zagrożeń i scenariusze ataku uwzględniające infrastrukturę lokalną i środowiska chmurowe; metody oceny skuteczności wdrożonych rozwiązań (FW/NGFW/IPS/IDS) na podstawie metryki, testów i audytów bezpieczeństwa; wpływ nowych technologii i trendów (np. SD-WAN, SASE, XDR) na kształt architektury bezpieczeństwa sieci; sposoby integracji narzędzi bezpieczeństwa (np. SIEM, SOAR, XDR, AV)	
	potrafi…	**Bezpieczeństwo sieciowe i internetowe**	rozpoznawać podstawowe rodzaje zagrożeń sieciowych	tworzyć proste reguły filtracji ruchu w urządzeniu brzegowym; interpretować wpisy w logach systemowych urządzeń sieciowych	skonfigurować reguły firewall; zaprojektować proste polityki firewall dla małej sieci; wdrożyć proste scenariusze IDS/IPS; interpretować wpisy w logach systemowych FW/IDS/IPS; wykorzystać metody klasyfikacji treści cyfrowych	zaprojektować polityki bezpieczeństwa sieciowego; skonfigurować zapory nowej generacji; dobrać i dostroić profile IDS/IPS do ochrony kluczowych usług; zintegrować FW/NGFW/IDS/IPS z systemami logowania i monitoringu; zastosować/tworzyć podstawowe listy kontroli dostępu (ACL); projektować architekturę odporną na ataki DDoS	zaprojektować integracje SIEM z systemami bezpieczeństwa; zaprojektować i wdrożyć schematy automatyzacji w SOAR dla incydentów sieciowych	
	zna i rozumie…	**Orkiestracja sieci**	elementy infrastruktury sieciowej (np. kontrolery SDN i płaszczyzny sterowania); pojęcie wirtualizacji sieci	zastosowanie architektury SDN (Application Plane, Control Plane, Data Plane); tablice przepływów (flow tables); zasady działania protokołów OpenFlow (na poziomie podstawowym)	zastosowanie różnych typów architektur SDN (np. Hybrydowa, Centralizowana); zasady działania API (np. REST, NETCONF, gRPC); architekturę wirtualizacji funkcji sieciowych (NFV); koncepcję SFC (Service Function Chaining)	zastosowanie protokołów wirtualizacji sieci (np. szczegóły OpenFlow, NETCONF, RESTCONF); zasady modelowania danych (np. YANG)	wpływ najnowszych rozwiązań w dziedzinie orkiestracji sieci (np. Intent-Based Networking); integrację modeli wysokiej dostępności i odporności (HA/DR) dla klastrów kontrolerów SDN; metody tworzenia polityki zarządzania pełnym cyklem życia usługi	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
II. Technologie sieciowe	potrafi…	**Orkiestracja sieci**	zalogować się do prostego interfejsu monitorującego SDN; zidentyfikować podstawowe elementy sieci (np. porty) w interfejsie; wykonać polecenie (np. sprawdzenie statusu usługi kontrolera)	skonfigurować prosty, wirtualny kontroler SDN (np. w Mininet); monitorować status i podstawowe metryki w interfejsie kontrolera; wdrożyć i zweryfikować działanie prostego, statycznego routingu	wykorzystywać API kontrolera do dynamicznej konfiguracji sieci; analizować i rozwiązywać problemy związane z przepływem danych (np. błędy w tablicach przepływów); wdrażać i zarządzać prostym łańcuchem usług NFV (Service Chain)	projektować i wdrożyć kompleksową architekturę SDN/NFV dla małej sieci; opracowywać i zaimplementować zaawansowane skrypty automatyzujące (np. do provisioningu); integrować rozwiązania SDN z systemami chmurowymi	projektować i ewaluować mechanizmy zapewniające wysoką dostępność i odporność kontrolerów SDN; przeprowadzać testy wydajnościowe i bezpieczeństwa (np. testy penetracyjne) systemów SDN; rekomendować optymalizacje SDN; opracowywać dokumentację standardów wdrożeniowych SDN; tworzyć polityki zarządzania pełnym cyklem życia usługi	
III. Inżynieria oprogramowania	zna i rozumie…	**Analiza wymagań**		podstawowe pojęcia dotyczące analizy wymagań; podstawy standardu UML; metody opracowywania diagramów przypadków użycia	metodykę analizy wymagań i modelowania systemu (UML, BPMN); metody opracowywania diagramów klas; wymagania niefunkcjonalne (NFR)	metody opracowywania diagramów behawioralnych, w tym metody przepływu obiektu	metody opracowywania diagramów implementacyjnych (komponentów i wdrożeniowe)	
	potrafi…	**Analiza wymagań**		zrozumieć kontekst tworzonego oprogramowania zgodnie z wymaganiami; definiować proste diagramy w UML	analizować zależności między wymaganiami poszczególnych klas obiektów; ustalić wymagania użytkownika i wymagania organizacyjne w kontekście tworzonego oprogramowania; modelować diagramy klas; interpretować diagramy BPMN; opisać zachowania, funkcje i operacje, które system musi wykonywać	tworzyć modele systemu informatycznego; modelować diagramy behawioralne; analizować zależności między oprogramowaniem a komponentami systemu informatycznego; tworzyć diagramy BPMN; zrozumieć potrzeby biznesowe w kontekście tworzonego oprogramowania	tworzyć diagramy implementacyjne (komponentów i wdrożeniowe)	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
III. Inżynieria oprogramowania	zna i rozumie…	**Projektowanie**	rolę projektowania w cyklu życia oprogramowania; znaczenie dokumentacji technicznej w projekcie IT	podstawowe wzorce projektowe; podstawowe modele danych	architekturę systemów informatycznych (np. trójwarstwowa, klient–serwer); metodyki projektowania; zależności między wymaganiami a projektem systemu	zaawansowane wzorce projektowe (np. MVC, Observer); wpływ decyzji projektowych na koszty, ryzyka i przyszły rozwój oprogramowania; projektowanie API i integracji systemów	projektowanie systemów rozproszonych i mikroserwisowych; zasady projektowania systemów IT o wysokiej dostępności, skalowalności i bezpieczeństwie	nowe trendy w projektowaniu systemów z możliwością wykorzystania AI; nowatorskie metody oceny innowacyjności rozwiązań
	potrafi…	**Projektowanie**	tworzyć proste diagramy blokowe; korzystać z dokumentacji projektowej	tworzyć proste diagramy UML; modelować proste systemy; tworzyć proste modele danych	projektować komponenty systemu zgodnie z wymaganiami; analizować ryzyka projektowe; tworzyć dokumentację projektową zgodną ze standardami; identyfikować funkcjonalne i niefunkcjonalne wymagania oprogramowania	zaprojektować komponenty i przepływy; rozwiązywać problemy projektowe o wysokiej złożoności; prowadzić przeglądy projektów systemów informatycznych	projektować systemy rozproszone i mikroserwisowe; projektować systemy IT o wysokiej dostępności, skalowalności i bezpieczeństwie	opracowywać nowe innowacyjne wzorce projektowe z możliwością wykorzystania AI; weryfikować wpływ nowych rozwiązań na dostępność, skalowalność i bezpieczeństwo
	zna i rozumie…	**Projektowanie UX/UI**	rolę projektowania UX/IU w wytwarzaniu oprogramowania	podstawowe pojęcia i zasady dotyczące UX (user experience) i UI (user interface)	proces projektowania doświadczenia użytkownika; zasady projektowania zorientowanego na użytkownika (UCD – User-Centered Design); zasady projektowania interakcji (user flow); narzędzia i programy wspierające projektowanie interfejsów	zasady dostępności cyfrowej i ergonomii interfejsów; narzędzia i programy wspierające budowę modeli-prototypów;	metody badawcze UX/UI na poprawę użyteczności oprogramowania	
	potrafi…	**Projektowanie UX/UI**		wykonać statyczny zarys struktury aplikacji/strony/programu/systemu (wireframe – model szkieletowy)	wykonać wizualizację wyglądu (mock-up – makieta); zapewnić spójność wizualną i funkcjonalną tworzonych rozwiązań	wykonać interaktywny prototyp z użyciem narzędzi UX/UI; wykonać audyt użyteczności UX wraz ze sprawdzeniem zasad dostępności; wykonać testy użyteczności	zastosować odpowiednie metody badawcze i rodzaje badań UX	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
III. Inżynieria oprogramowania	zna i rozumie…	**Programowanie**	podstawy algorytmów; podstawy kodowania; rodzaje języków programowania; narzędzia programistyczne IDE; znaczenie struktury i przydatności dokumentacji technicznej środowiska sprzętowego i oprogramowania	podstawy programowania strukturalnego i obiektowego; rodzaje bazy danych	środowisko typu GIT (kontrola wersji); frameworki i biblioteki (w tym open-source) wspierające rozwój aplikacji; cykl życia oprogramowania	wiele języków programowania i narzędzi wspierających tworzenie kodu i aplikacji; narzędzia i metody programowania w rozproszonych i chmurowych rozwiązaniach; programowanie zorientowane na mikroserwisy; możliwości wykorzystania AI, no-code, low-code dla wytwarzania oprogramowania; technologie sieciowe REST API i SOAP; zasadę idempotencji	metody programowania w chmurze; metody programowania wieloplatformowe	
	potrafi…	**Programowanie**	opracować schemat blokowy dla wymagania	korzystać z narzędzi programistycznych IDE; zaprogramować prosty proces z wykorzystaniem bazy danych; tworzyć kod w przynajmniej jednym języku programowania; tworzyć proste fragmenty kodu przy wsparciu asystentów AI; weryfikować poprawność składniową kodu generowanego przez AI	analizować prosty kod, w tym znajdować błędy logiczne i składniowe; korzystać z bibliotek i frameworków programistycznych; korzystać ze środowiska typu GIT (kontroli wersji); monitorować działanie kodu i wprowadzonych poprawek w aplikacji; przeprowadzać refaktoryzację i optymalizację kodu sugerowanego przez narzędzia GenAI; stosować zasady tworzenia czystego kodu (clean code); budować i implementować reprezentację programową modeli obiektowych systemów i procesów	programować w wielu językach programowania i ich ekosystemie; korzystać z platform no-code i low-code; wykorzystywać AI do tworzenia kodu i automatyzacji rutynowych zadań; integrować aplikacje na podstawie różnych metod i technologii sieciowych (API); zapewnić idempotencję operacji; przeprowadzać audyt bezpieczeństwa kodu generowanego przez AI (AI Code Review) pod kątem podatności i logiki biznesowej; integrować asystentów kodowania z potokiem CI/CD	programować w chmurze hybrydowej; programować wieloplatformowo	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
III. Inżynieria oprogramowania	zna i rozumie…	**Wdrożenie**		terminologię branżową wdrożenia; środowisko IT dotyczące wdrożenia; rodzaj i etapy wdrożenia; potrzeby biznesowe wdrożenia	technologie związane z przedmiotem wdrożenia; zasady planowania etapów wdrożenia (technicznych i związanych z implementacją); funkcjonowanie wdrażanego systemu; metody zarządzania projektem wdrożeniowym, w tym zarządzania zmianą; zasady bezpieczeństwa wdrożeniowego	metody analizy systemowej i zbierania wymagań użytkowników (analiza przedwdrożeniowa); metody testowania systemu; procedury migracji danych	zasady planowania harmonogramu wdrożenia; technologie wdrożeń (tradycyjna, CI/CD); zasady planowania migracji danych i konfiguracji systemu; metody analizy i optymalizacji kosztów wdrożenia; terminologię branżową wdrożenia i otoczenie prawne wdrożania	nowoczesne i innowacyjne metody wdrożenia i trendy, np. Blue-Green Deployment, Strangler Fig Pattern
	potrafi…	**Wdrożenie**		określić funkcjonalność systemu informatycznego; konfigurować podstawowe funkcje oprogramowania; instalować oprogramowanie oraz przenosić i migrować dane	zaplanować etapy wdrożenia systemu; weryfikować i dokumentować wdrażany projekt zgodnie z metodyką, w tym zarządzać zmianą; zaplanować i przeprowadzić proces szkolenia z wdrażanego systemu; konfigurować i parametryzować funkcje systemu	zarządzać projektem wdrożeniowym zgodnie z metodyką; stosować technologie optymalizujące proces wdrożenia; stosować metody do testowania; zaplanować proces migracji danych	uzgadniać szczegóły wdrożenia, podział pracy na etapy; analizować potrzeby zamawiającego (analiza przedwdrożeniowa); uwzględniać prawne aspekty wdrożania; planować wdrożenia i jego etapy (techniczne i związane z oprogramowaniem); zarządzać procesem migracji i weryfikacją danych; zarządzać procesem wdrożenia zgodnie z przyjętą koncepcją	stosować nowoczesne metody wdrożeniowe
	zna i rozumie…	**Testowanie**		cele testowania; podstawowe pojęcia związane z testowaniem (np. scenariusz testu, rodzaje testów); podział środowisk testowych; metodykę testów manualnych	pełny cykl testów, w tym strukturę zapytań do API; wartości brzegowe testowanych przypadków; zasady przygotowania danych do testów; metodykę testów akceptacyjnych; narzędzia do zarządzania testami; Testy Autonomiczne	dobór strategii do ryzyka testów; testy jednostkowe, integracyjne, systemowe; typy testów niefunkcjonalnych; metodykę definiowania metryk testów; strukturę testu automatycznego; testy eksploracyjne; metody testowania z izolacją zależności	metodykę łączenia różnych rodzajów testów; zasady integrowania procesu testowania z cyklem wytwórczym (np. DevOps); możliwości wykorzystywania AI w testowaniu systemów	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
III. Inżynieria oprogramowania	potrafi…	**Testowanie**		definiować przypadki testowe; sprawdzić przygotowany przypadek testowy; dokumentować rezultaty testów, a zwłaszcza zgłosić błąd z niezbędnymi warunkami do replikacji przypadku	zaplanować przypadki testowe dla wszystkich wymagań, w tym dla API; weryfikować scenariusze do testów akceptacyjnych; korzystać z narzędzi do zarządzania testami; wdrażać i nadzorować agentów autonomicznego testowania	zaprojektować i uruchomić testy jednostkowe; zaprojektować i przeprowadzić testy integracyjne; zaprojektować i przeprowadzić testy systemowe; zaprojektować testy automatyczne; projektować sesje eksploracyjne; zaprojektować testy wydajności, bezpieczeństwa, użyteczności, niezawodności	przygotować raport z gotowości rozwiązania do wdrożenia; zarządzać danymi testowymi i weryfikować pokrycie testami generowanymi automatycznie przez AI; formułować działania korygujące i zapobiegawcze dla błędów nawracających; aktualizować potoki w CI/CD, dodając testy automatyczne, oraz wykorzystywać AI do testowania systemów	
	zna i rozumie…	**Utrzymanie i rozwój**		metody utrzymania systemów informatycznych; metody rozwoju systemów informatycznych; różnice między metodami utrzymania i rozwoju systemów informatycznych wynikające ze sposobu funkcjonowania organizacji; metody obsługi zgłoszeń dotyczących funkcjonujących systemów informatycznych	metody zarządzania zmianami w funkcjonujących systemach informatycznych; metody monitorowania funkcjonujących systemów informatycznych	metody utrzymania ciągłości działania systemu informatycznego; metody rozwijania systemów informatycznych; zasady optymalizacji i automatyzacji w przyspieszeniu rozwoju oprogramowania; praktyki ciągłej integracji i rozwijania systemów (CI/CD, Dev/Ops) zgodnie z polityką bezpieczeństwa	metody implementacji nowych funkcjonalności systemu informatycznego; metody stosowania innowacyjnych rozwiązań w utrzymaniu i rozwoju systemów informatycznych; metody oceny efektywności systemów informatycznych, ich nadzoru i audytu	
	potrafi…	**Utrzymanie i rozwój**		kategoryzować zgłoszenie dotyczące funkcjonujących systemów informatycznych; obsługiwać zgłoszenie dotyczące funkcjonujących systemów informatycznych	dokonywać aktualizacji środowiska w związku z wprowadzaną zmianą; wykorzystywać narzędzia do monitorowania systemów informatycznych	utrzymywać i rozwijać systemy w środowisku Dev/Sec/Ops; tworzyć koncepcje modyfikacji i zmian systemów uwzględniające korekty, stabilizacje wersji, ulepszenia i modyfikacje; wykorzystywać narzędzia automatyzacji (w tym AI) do rozwoju i utrzymania systemu informatycznego	zarządzać polityką utrzymania i rozwoju systemów informatycznych; integrować aplikacje (w tym w czasie rzeczywistym); optymalizować koszty utrzymania i rozwoju systemów informatycznych; adaptować systemy informatyczne do zmian otoczenia (w tym technologicznych, prawnych i biznesowych)	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
III. Inżynieria oprogramowania	zna i rozumie…	**Dokumentacja**	podstawowe pojęcia i podstawy dokumentowania	różnice między rodzajami dokumentacji, np. użytkową a techniczną; platformy do współpracy zespołowej i zarządzania wiedzą typu Confluence, Jira, Miro	zasady wersjonowania dokumentacji, w tym cykl życia dokumentacji; standardy dokumentacji i zarządzania wiedzą, formaty dokumentacji (np. markdown, AsciiDoc); sposoby notacji modelowania diagramów i wizualizacji (UML, BPMN)	narzędzia do automatyzacji tworzenia dokumentacji (np. Swagger/Open API, Redocly, Doxygen, Sphinx, Javadoc)	trendy w zakresie rozwoju strategii zarządzania dokumentacją IT; optymalizację dokumentacji API przy wykorzystaniu możliwości AI	
	potrafi…	**Dokumentacja**	tworzyć prostą instrukcję użytkownika, np. README	tworzyć instrukcję użytkownika czy dokumentację użytkową; dokumentować modyfikacje w dzienniku zmian (changelog)	zarządzać wersjami dokumentacji IT; tworzyć dokumentację użytkową modułu/komponentu/systemu (np. manual, tutorial); dokumentować listę zadań, wymagań i funkcjonalności (np. Dev/Ops, backlog)	tworzyć dokumentację projektową systemu informatycznego; generować automatyczną dokumentację techniczną; tworzyć szablony dokumentacyjne; wdrażać repozytoria wiedzy	wyznaczać standardy tworzenia dokumentacji IT; zarządzać wiedzą i dokumentacją na podstawie najnowszych narzędzi do tworzenia dokumentacji	
	zna i rozumie…	**Organizacja zespołów wdrożeniowo-programistycznych**		podstawowe struktury zespołów wdrożeniowo-deweloperskich; zadania zespołów wdrożeniowych i programistycznych w zależności od struktury organizacyjnej; standardowe i aktualne metodologie wdrażenia systemów; wzorce projektowe i zasady tworzenia oprogramowania	zasady tworzenia i działania zespołów dev/ops i dev/ops/sec (ciągła: integracja/dostarczanie CI/CD); metodyki projektowe adekwatne do organizacji i przeznaczenia oprogramowania; znaczenie doboru odpowiednich narzędzi do zarządzania projektem, wytwarzania oprogramowania i wdrożenia; narzędzia do zarządzania zespołem wdrożeniowo-programistycznym i komunikacji w projekcie (np. Slack, Teams, Jira)	mikroserwisy jako transformację rozwoju oprogramowania i dekompozycji systemów monolitycznych; narzędzia automatyzacji procesów wytwarzania oprogramowania (np. Jenkins)	w szerokim zakresie technologiczną rożnorodność IT w wyborze środowiska pracy zespołów wdrożeniowo-programistycznych (np. framework); organizację specjalistycznych zespołów wdrożeniowo-programistycznych	konieczność budowania nowatorskich zespołów interdyscyplinarnych z programistami w celu realizacji innowacji cyfrowych; wykorzystanie różnych nowoczesnych metodyk projektowych i innowacji, w tym AI, w tworzeniu oprogramowania; znaczenie przywództwa w zespołach wdrożeniowo-programistycznych

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
III. Inżynieria oprogramowania	potrafi…	**Organizacja zespołów wdrożeniowo-programistycznych**		określić sposób działania zespołu; określić zakres działań programisty w danej organizacji; dokumentować pracę zgodnie ze standardem programowania; określić etapy wdrożenia systemu	stosować w praktyce rozwiązania takie jak np. programowanie wspomagane testami; wykorzystywać metodyki dla efektywnego procesu programowania (np. Agile, Scrum); korzystać z narzędzi do zespołowej edycji kodu (np. GitHub, GitLab);	implementować zadania programistyczne zgodnie z zaproponowaną architekturą oraz dobrymi zasadami programowania; określić warunki kontraktu usługi wdrożeniowo-programistycznej w środowisku dev/test/prod	zarządzać zespołami wdrożeniowo-programistycznymi; organizować samodzielną pracę nad projektem wdrożeniowo-programistycznym	dostarczyć, stworzyć i wdrożyć wiele innowacyjnych narzędzi i technik, które przyspieszają proces tworzenia oprogramowania, w tym AI; proponować innowacyjne rozwiązania zgodne z potrzebami zespołów wdrożeniowo-programistycznych; przewodzić zespołowi wdrożeniowo-programistycznemu i kierować procesem wytwarzania innowacyjnych rozwiązań
IV. Aplikacje i usługi cyfrowe	zna i rozumie…	**Cyfrowe platformy usługowe**	różnice między tradycyjną aplikacją a platformą usługową; zasady korzystania z rozwiązań oferowanych na platformie usługowej	podstawowe pojęcia dotyczące platform usługowych; podstawowe zasady bezpieczeństwa i autoryzacji w platformach; podstawowe pojęcia związane z wykorzystaniem wewnętrznych platform usługowych	rodzaje i zastosowanie cyfrowych platform usługowych; zasady udostępniania usług w formie API, modułów lub komponentów; typowe mechanizmy zabezpieczeń stosowane w platformach usługowych	zasady projektowania nowych usług z wykorzystaniem dostępnych modułów; zasady monitorowania, skalowalności, dostępności i bezpieczeństwa usług platformowych; zaawansowane metody integracji platform z systemami	zaawansowane modele bezpieczeństwa i zgodności regulacyjnej dla usług cyfrowych; trendy, kierunki rozwoju i integracji platform usługowych z systemami w organizacji	nowoczesne sposoby kreowania innowacyjnych usług na platformach cyfrowych
	potrafi…	**Cyfrowe platformy usługowe**	korzystać z katalogu usług; wywoływać poszczególne usługi	konfigurować prostą usługę na podstawie znanych parametrów; zgłaszać problemy i niezgodności działania platformy	konfigurować i uruchamiać usługi na platformie; przeprowadzać podstawowe testy funkcjonalne działania usług; zarządzać w aplikacjach uprawnieniami, rolami i przestrzeniami roboczymi	projektować nowe usługi lub moduły usługowe zgodnie ze standardami platformy; identyfikować wąskie gardła i problemy wydajnościowe, optymalizując działanie istniejących usług; przeprowadzać testy funkcjonalne działania usług i zabezpieczeń na platformie	ustanawiać standardy tworzenia i utrzymania usług, w tym zasady jakości, wydajności i bezpieczeństwa; nadzorować prace wdrożeniowe usług cyfrowych w organizacji; zarządzać portfelem usług cyfrowych i kierować ich rozwojem w organizacji	wyznaczać nowe trendy i kierunki rozwoju platform usługowych w globalnym ekosystemie cyfrowym

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IV. Aplikacje i usługi cyfrowe	zna i rozumie…	**Dostępność**	zasady dostępności cyfrowej, w tym WCAG	rolę dostępności w projektowaniu UX/UI; narzędzia wspomagające dostępność	zaawansowane metody projektowania dostępnych interfejsów; krajowe i unijne akty prawne i normy dotyczące dostępności; zasady projektowania treści i mediów dostępnych dla użytkowników	metody projektowania dostępnych rozwiązań dla urządzeń i systemów informatycznych; sposób integracji wymagań dostępności z procesami CI/CD; wpływ dostępności na biznes i doświadczenie użytkownika	strategię dostępności cyfrowej i polityki jakości; trendy i innowacje w zakresie dostępności	
	potrafi…	**Dostępność**	tworzyć materiały zgodne z WCAG	korzystać z narzędzi do testów dostępności; identyfikować i klasyfikować problemy dostępności; przeprowadzać audyt dostępności stron internetowych	wdrażać rozwiązania poprawiające dostępność w projektach; opracowywać wytyczne dla zespołów projektowych w zakresie dostępności; przeprowadzać audyt dostępności aplikacji i dokumentów elektronicznych	koordynować projekty dostępnościowe w całej organizacji; uwzględniać wymagania dostępności w całym procesie tworzenia oprogramowania, w tym dla urządzeń realizujących usługi cyfrowe; oceniać efektywność wprowadzonych rozwiązań dostępnościowych	tworzyć i nadzorować politykę dostępności w organizacji; analizować trendy i innowacje w zakresie dostępności	
	zna i rozumie…	**Zarządzanie cyklem życia aplikacji i usług**		etapy cyklu życia aplikacji (np. planowanie, wytworzenie, wdrożenie, utrzymanie, wycofanie); narzędzia zarządzania wersjami aplikacji	metody i standardy zarządzania cyklem życia aplikacji i usług cyfrowych; wytyczne zarządzania wersjami, wydaniami i wycofaniami w organizacji	złożone procesy zarządzania cyklem życia aplikacji i usług cyfrowych w organizacji wielousługowej	zarządzanie portfelem aplikacji i usług w ujęciu strategicznym	
	potrafi…	**Zarządzanie cyklem życia aplikacji i usług**		rejestrować i aktualizować informacje o wersjach aplikacji i usług cyfrowych; zgłaszać oraz dokumentować potrzebę wprowadzenia zmian lub wycofania aplikacji	planować wydania i aktualizacje aplikacji oraz usług cyfrowych w ramach ustalonego harmonogramu; koordynować działania utrzymaniowe aplikacji oraz testy przedwdrożeniowe z użytkownikami biznesowymi (praktyki CI/CD)	projektować i wdrażać zautomatyzowane procesy; zarządzać ryzykiem i ciągłością usług cyfrowych; monitorować stan projektu w całym cyklu życia aplikacji	definiować i wdrażać strategię zarządzania cyklem życia aplikacji i usług cyfrowych dla całej organizacji	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IV. Aplikacje i usługi cyfrowe	zna i rozumie…	**Monitoring**	podstawowe parametry aplikacyjne i usługowe; podstawy logowania zdarzeń w aplikacjach; podstawowe pojęcia analityki internetowej (web analytics)	narzędzia do monitoringu aplikacji i usług cyfrowych; proces monitorowania zachowań użytkownika	zasady tworzenia i zbierania metryk dla pomiaru wydajności aplikacji i usług cyfrowych w narzędziach monitorujących (np. Prometheus, Grafana); zasady analizy logów aplikacyjnych; wpływ monitorowanych parametrów na dostępność aplikacji i usług	zależności między warstwami aplikacji oraz sposób propagacji błędów; korelację metryk technicznych z metrykami biznesowymi	trendy i możliwości wykorzystania AI w analizie danych aplikacyjnych; zależności między monitoringiem a koncepcją Observability do analizy i optymalizacji infrastruktury IT, usług oraz blokowania podatności w czasie rzeczywistym	
	potrafi…	**Monitoring**	odczytywać dane z narzędzi monitorujących aplikacje i usługi cyfrowe; identyfikować podstawowe symptomy problemów użytkowników na podstawie prostych komunikatów o błędach i statusów usług; rejestrować incydenty związane z monitorowanymi parametrami aplikacji i usług cyfrowych	korzystać z gotowych dashboardów do monitoringu aplikacji; odczytywać podstawowe statystyki (np. z Google Analytics)	tworzyć i analizować podstawowe dashboardy aplikacji; rozpoznawać i opisywać typowe anomalie w działaniu aplikacji i usług cyfrowych; określać metryki i zależności wszystkich typów aplikacji i środowisk technologicznych w narzędziach monitorujących (np. Prometheus, Grafana)	analizować źródła problemów poprzez korelowanie statystyk z różnych komponentów aplikacji; wdrażać i rozwijać standardy monitoringu aplikacyjnego; współpracować z zespołami produktowymi przy definiowaniu wskaźników jakości usług (SLI/SLO) i progów alertowania		
	zna i rozumie…	**Modele udostępniania i monetyzacja**		podstawowe modele udostępniania usług cyfrowych; podstawowe warunki licencyjne i subskrypcyjne aplikacji	typy licencjonowania i monetyzacji; podstawowe różnice kosztowe, operacyjne i ryzyka biznesowe między modelami udostępniania	wpływ architektury aplikacji i usług na model udostępniania i monetyzację; ryzyka związane z monetyzacją usług cyfrowych	zarządzanie modelami monetyzacji w obrębie całej organizacji; ramy regulacyjne i ekonomiczne modeli subskrypcyjnych; bieżące uwarunkowania rynku w kontekście monetyzacji	
	potrafi…	**Modele udostępniania i monetyzacja**		rozróżniać rodzaje licencji i subskrypcji; utrzymywać model licencjonowania/subskrypcji dla danej aplikacji/usługi	analizować podstawowe dane wykorzystania aplikacji i nowej usługi cyfrowej; porównywać oferty licencyjne i subskrypcyjne różnych dostawców; wskazywać możliwości optymalizacji planów zakupowych licencji i subskrypcji	zaprojektować model udostępniania i monetyzacji dla nowej lub rozwijanej usługi; zaproponować koncepcję monetyzacji portfela usług i aplikacji cyfrowych; oceniać potencjalne ryzyko zaproponowach rozwiązań w zakresie monetyzacji usług cyfrowych	projektować i nadzorować wdrożenie złożonych, wielokanałowych modeli monetyzacji; tworzyć długoterminową strategię monetyzacji portfela usług i aplikacji cyfrowych; przeprowadzać analizę rynku w kontekście monetyzacji usług cyfrowych	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IV. Aplikacje i usługi cyfrowe	zna i rozumie…	**Integracja systemów**		podstawowe sposoby integracji systemów; podstawy i ograniczenia REST API	zaawansowane koncepcje API (np. uwierzytelnianie, ograniczenie liczby żądań); zasady projektowania API (np. RESTful); podstawowe zasady ESB jako centralnego punktu integracyjnego; wykorzystanie HTTP/REST i SOAP	mechanizmy zarządzania błędami podczas integracji systemów; wpływ integracji systemów na bezpieczeństwo i wydajność aplikacji; zaawansowane sposoby integracji systemów	podejścia hybrydowe w integracji systemów, szczególnie z użyciem API; strategię integracji systemów w organizacji	
	potrafi…	**Integracja systemów**		korzystać z gotowych narzędzi i skryptów do komunikacji z API; wykorzystać istniejące API do pobrania lub wysłania danych	projektować, implementować i dokumentować API; tworzyć klientów API, obsługując uwierzytelnianie i podstawowe błędy; korzystać z narzędzi szyny danych w celu integracji systemów	dobierać sposób integracji systemów w zależności od architektury; optymalizować wydajność integracji systemów; projektować i wdrażać złożone, odporne na błędy architektury integracyjne pomiędzy systemami	definiować standardy i dobre praktyki integracji systemów; projektować architekturę systemów rozproszonych, szczególnie z użyciem API; prognozować kierunki rozwoju i wyzwania integracyjne	
	zna i rozumie…	**Bezpieczeństwo aplikacji i usług cyfrowych**	podstawowe pojęcia dotyczące bezpieczeństwa aplikacji i usług cyfrowych (np. podatność, zagrożenie, incydent, poufność, dostępność usług, autoryzacja); znaczenie podstawowej „higieny cyfrowej" (np. silne hasła, ostrożność wobec linków i załączników)	podstawowe zagrożenia bezpieczeństwa cyfrowego (np. phishing, malware, przejęcie konta, wyciek danych, nieautoryzowany dostęp, DDos); środki ochrony przed zagrożeniami (np. MFA, szyfrowanie komunikacji, aktualizacje oprogramowania); zagrożenia związane z oszustwami i dezinformacją, w tym generowanie fałszywych treści (np. deepfake)	metody analizowania incydentów IT; mechanizmy wykorzystywane do naruszenia bezpieczeństwa aplikacji i usług cyfrowych; testy bezpieczeństwa aplikacji (np. testy penetracyjne, skanery podatności, testy bezpieczeństwa API, testy socjotechniczne, testy odporności na przeciążenia)	standardy projektowania i wdrażania bezpiecznych aplikacji i usług; metody zabezpieczania interfejsów API aplikacji	strategiczne zarządzanie bezpieczeństwem aplikacji i usług cyfrowych; wykorzystanie AI do wykrywania incydentów i nadużyć bezpieczeństwa aplikacji i usług cyfrowych	nowe globalne trendy w zakresie kształtowania bezpieczeństwa aplikacji i usług cyfrowych

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IV. Aplikacje i usługi cyfrowe	potrafi…	**Bezpieczeństwo aplikacji i usług cyfrowych**	uwzględniać podstawowe zasady „higieny cyfrowej”	używać podstawowych mechanizmów bezpieczeństwa w aplikacjach i usługach (np. MFA, polityki haseł, role i uprawnienia, szyfrowanie połączeń, podstawowe logowanie zdarzeń); dbać o bieżące aktualizacje oprogramowania; rozpoznać typowe symptomy incydentów bezpieczeństwa IT; zgłaszać incydenty bezpieczeństwa IT	analizować ryzyka bezpieczeństwa aplikacji; konfigurować mechanizmy bezpieczeństwa w aplikacjach i usługach cyfrowych; uczestniczyć w testach bezpieczeństwa aplikacji i usług cyfrowych	projektować i wdrażać rozwiązania bezpieczeństwa dla aplikacji i usług; planować i przeprowadzać audyty bezpieczeństwa aplikacji i usług cyfrowych; rekomendować i wdrażać mechanizmy naprawcze w aplikacjach i usługach cyfrowych w odpowiedzi na błędy i luki wykryte w wyniku przeprowadzanych testów	wdrażać polityki bezpieczeństwa aplikacji i usług; monitorować zgodność działań z przyjętymi politykami bezpieczeństwa; podejmować strategiczne decyzje dotyczące inwestycji w bezpieczeństwo	opracowywać i wdrażać nowatorskie metody w zakresie bezpieczeństwa aplikacji i usług cyfrowych
V. Rozwiązania chmurowe	zna i rozumie…	**Sposoby wdrożenia**		podstawowe rodzaje i sposób funkcjonowania chmur obliczeniowych (publicznej, prywatnej, hybrydowej, społecznościowej)	cechy chmury publicznej, prywatnej i hybrydowej w kontekście wdrażania aplikacji; modele środowisk (dev, test, pre-prod, prod); powiązanie pipeline CI/CD ze strategią wdrożeń (np. stopniowe, równoległe) oraz możliwością cofnięcia wdrożenia; metodykę Infrastructure as Code	podstawowe różnice organizacyjne i techniczne wdrożeń w środowisku hybrydowym; rolę środowisk pośrednich (test, pre-prod); metody wdrożeń w chmurze publicznej, prywatnej i hybrydowej; złożone problemy na poziomie użytkownika usługi chmurowej (np. brak synchronizacji usług)	wpływ sposobu wdrażania na dostępność systemu, ryzyko awarii; dostępne zaawansowane rozwiązania chmurowe (wielowarstwowa architektura); metodykę ciągłego wdrażania przy wykorzystaniu narzędzi CI/CD oraz IaC w wielu środowiskach, w tym multi-cloud	najnowsze rozwiązania chmurowe przyspieszające wdrażanie innowacji, skracanie czasu dostarczania usług i zwiększenia ich bezpieczeństwa

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
V. Rozwiązania chmurowe	potrafi…	**Sposoby wdrożenia**		skonfigurować i zabezpieczyć dostęp do prostych usług (np. udzielenie dostępu do plików) w zależności od rodzaju chmury	aktualizować komponenty aplikacji chmurowej; udokumentować wykonane aktualizacje komponentu aplikacji chmurowej; skorzystać z przygotowanych skryptów lub szablonów (w tym narzędzia IaC) do uruchomienia prostych zasobów; wskazać komponenty do wdrożenia odpornej usługi IT wykorzystującej chmurę	przygotować procedurę wdrożeniową rozwiązania chmurowego; wykonać wdrożenie aplikacji lub usługi w chmurze publicznej lub prywatnej; migrować usługi do środowiska chmurowego oraz pomiędzy środowiskami chmurowymi; diagnozować i rozwiązywać złożone problemy użytkownika usługi chmurowej; przeprowadzać ocenę ryzyka wdrożeniowego jako element decyzji o dopuszczeniu zmiany na środowisko produkcyjne	zastosować i zarządzać organizacją i infrastrukturą chmurową; dobrać odpowiednią strategię wdrożenia (np. stopniowe wdrażanie, równoległe uruchomienie) do charakteru systemu i wymagań biznesowych; koordynować wdrażanie zmian w środowisku hybrydowym; przygotować procedury awaryjne i scenariusze rollbacku oraz przeprowadzić testy odtworzeniowe wdrożeń	tworzyć nowe rozwiązania chmurowe na podstawie aktualnych potrzeb organizacji
	zna i rozumie…	**Modele wdrożeniowe**		techniczne podstawy modeli IaaS, PaaS, SaaS, FaaS; podstawowe mechanizmy wirtualizacji i izolacji zasobów w modelu IaaS	model współodpowiedzialności (shared responsibility) w IaaS, PaaS, SaaS, FaaS; różnice w konfiguracji, utrzymaniu i aktualizacjach między PaaS, SaaS i FaaS	mechanizmy automatycznego skalowania, równoważenia obciążenia i wysokiej dostępności w różnych modelach usług (IaaS, PaaS, FaaS); metodykę integracji narzędzi do monitoringu w różnych modelach chmurowych; metodykę zarządzania sekretami; wpływ wyboru modelu na skalowalność, koszty oraz odporność aplikacji i usług	metody projektowania aplikacji PaaS (np. mikroserwisy, architektury event-driven); metodykę wykorzystania FaaS w architekturach serverless i event-driven	
	potrafi…	**Modele wdrożeniowe**		wdrożyć elementy infrastruktury na platformie IaaS (uruchomić wirtualną maszynę); skonfigurować opcje SaaS w organizacji	skonfigurować prostą aplikację na platformie PaaS; skonfigurować podstawowe komponenty w architekturze chmurowej; optymalizować dobór rozwiązania do konkretnej infrastruktury IT	wdrożyć narzędzie do zarządzania sekretami; zaprojektować komponenty aplikacji dające możliwość skalowania aplikacji; wdrożyć narzędzie do monitoringu komponentów chmurowych	zaprojektować złożoną architekturę aplikacji cloud native opartą głównie na PaaS i FaaS; opracować standardy techniczne korzystania z PaaS/SaaS/FaaS w organizacji; projektować rozwiązania wykorzystujące FaaS jako element orkiestracji procesów technicznych i biznesowych	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
V. Rozwiązania chmurowe	zna i rozumie…	**Optymalizacja i zarządzanie kosztami chmury**			pojęcie rozliczania kosztów konsumpcji usług chmurowych (opłaty za wykorzystanie zasobów)	metody liczenia kosztów poszczególnych składowych projektu chmurowego; zasady doboru klas zasobów (rightsizing), autoskalowania oraz ustalania harmonogramów wyłączania zasobów w celu optymalizacji kosztów; mechanizmy budżetów i alertów kosztowych oferowanych przez dostawców chmury	wpływ architektury systemu (monolit vs mikroserwisy, serverless vs IaaS, różne klasy storage, cache) na profil kosztowy rozwiązania; metody optymalizacji kosztów w dużych środowiskach chmurowych (rezerwacje i plany oszczędnościowe, zobowiązania do użycia/ committed use, zasoby spot/ preemptible, wybór regionów i stref pod kątem kosztów); zasady FinOps oraz koncepcje showback/chargeback; metody estymacji kosztów związanych ze zmianą lub wdrożeniem nowych projektów w środowisku chmurowym	
	potrafi…	**Optymalizacja i zarządzanie kosztami chmury**				identyfikować główne kategorie kosztów i analizować rachunki oraz raporty kosztowe chmury; dobrać odpowiednie klasy zasobów dla wybranego komponentu chmurowego (np. rozmiar VM); skonfigurować budżety i alerty kosztowe z podsumowaniem kosztów dla projektu chmurowego; przygotować plan optymalizacji kosztów dla małego/średniego środowiska chmurowego, uwzględniając zmienność ruchu i automatyczne skalowanie	zaprojektować i wdrożyć proces optymalizacji kosztów chmury na poziomie poszczególnych systemów w organizacji; definiować i egzekwować standardy tagowania w rozwiązaniach chmurowych; dokumentować optymalizacje kosztowe związane z infrastrukturą chmurową; przygotować wycenę zmiany lub wdrożenia nowego projektu w infrastrukturze chmurowej	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
V. Rozwiązania chmurowe	zna i rozumie…	**Modele wielochmurowe**			pojęcia chmury multi-cloud i chmury cross-cloud; zależności między chmurami multi-cloud a cross-cloud; znaczenie chmury hybrydowej	metody integracji między chmurami; metody dystrybucji obciążeń między chmurami	wzorce architektoniczne multi--cloud (np. rozdział systemów między chmurami, aktywne--aktywne/aktywne-pasywne między chmurami); metodologie w modelach usług, sieci, bezpieczeństwa i tożsamości głównych dostawców chmury oraz ich wpływ na projekt systemów multi-cloud; metody tworzenia wspólnych warstw usług; metody tworzenia scenariuszy awarii i odtwarzania w modelach multi-cloud oraz cross-cloud	
	potrafi…	**Modele wielochmurowe**			dobrać właściwe rozwiązanie chmurowe w zależności od potrzeb	wskazać elementy systemu zależne od dostawcy chmury (vendor lockin) oraz określić możliwości ich minimalizacji; zrealizować proste scenariusze integracji multi-/cross-cloud; utrzymywać spójną konfigurację i standardy multi-/cross-cloud; analizować problemy wynikające z różnic między chmurami	projektować architekturę systemów multi-cloud oraz cross-cloud; wdrożyć zatwierdzony model multi-cloud; zaplanować i koordynować rozszerzanie systemu o kolejną chmurę oraz migrację między chmurami; projektować mechanizmy integracji cross-cloud; projektować wspólne standardy i szablony techniczne dla wszystkich chmur w organizacji; wdrażać warstwy usług wspólnych w chmurach	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
V. Rozwiązania chmurowe	zna i rozumie…	**Bezpieczeństwo w środowisku chmurowym**			różnicę między szyfrowaniem danych w spoczynku a szyfrowaniem danych w tranzycie w środowisku chmurowym; zasady stosowania protokołów szyfrowanych przy dostępie do usług w środowisku chmurowym	mechanizmy szyfrowania danych w spoczynku (np. certyfikaty dostawców, certyfikaty zarządzane przez klientów, KMS) oraz w tranzycie (np. TLS, certyfikaty, konfiguracja endpointów) w środowisku chmurowym; wymagania środowiska chmurowego dotyczące lokalizacji danych, retencji i usuwania w kontekście regulacji i polityk organizacji	strategie szyfrowania end-to-end w środowisku chmurowym; procesy modelu wyjścia z chmury; metody tworzenia raportu zgodności w środowisku chmurowym	
	potrafi…	**Bezpieczeństwo w środowisku chmurowym**			skonfigurować szyfrowanie w tranzycie w środowisku chmurowym; korzystać z usług chmurowych z włączonym szyfrowaniem danych w spoczynku; udokumentować podstawowe aspekty bezpieczeństwa wdrożonego rozwiązania w środowisku chmurowym	zaprojektować i skonfigurować szyfrowanie danych w spoczynku z użyciem certyfikatów zarządzanych przez dostawców w środowisku chmurowym; weryfikację poprawności konfiguracji szyfrowania oraz ocenę wpływu na wydajność usług; skonfigurować szyfrowanie danych w tranzycie między komponentami systemu w środowisku chmurowym; skonfigurować logowanie i audyt zdarzeń bezpieczeństwa w środowisku chmurowym	zaprojektować i wdrożyć model szyfrowania dla systemu w środowisku chmurowym; zaprojektować i opisać model wyjścia z chmury dla systemu, wraz z analizą ryzyka i planem zapewnienia ciągłości działania migrowanej usługi; zaplanować i wdrożyć polityki bezpieczeństwa i zgodności w środowisku chmurowym; analizować ryzyka bezpieczeństwa i zgodności w środowisku chmurowym; przygotować i przedstawić dokumentację bezpieczeństwa i zgodności dla systemu w środowisku chmurowym	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VI. Wsparcie IT	zna i rozumie…	**Obsługa użytkownika i zarządzanie zgłoszeniami**	podstawowe pojęcia i terminologię IT; systemy obsługi zgłoszeń; podstawowe pojęcia dotyczące zgłoszeń; zasady priorytetyzacji zgłoszeń	standardowe aplikacje używane w organizacji; typowe problemy zgłaszane przez użytkowników związane ze sprzętem i oprogramowaniem; procedury organizacyjne i polityki związane z obsługą użytkownika końcowego; pojęcia z zakresu eskalacji zgłoszenia incydentu, problemu oraz zmiany; znaczenie SLA i zasady kategoryzacji zgłoszeń; KPI, których wymaga organizacja	cykl życia zgłoszenia, incydentu, problemu oraz zmiany; strukturę środowiska IT w organizacji; dziedzinowe aplikacje używane w organizacji; systemy biznesowe używane w organizacji; środowisko sprzętowe i peryferyjne w organizacji	sposób obsługi incydentu, problemu oraz zmiany w organizacji; obsługę zgłoszeń w zespołach typu DevOps i DevSecOps; standardy zarządzania usługami, np. ITIL	poziom usług SLA i OLA; zasady tworzenia KPI; modele zarządzania usługami IT	
	potrafi…	**Obsługa użytkownika i zarządzanie zgłoszeniami**	rejestrować zgłoszenia; rozwiązywać najprostsze problemy według gotowych skryptów	kwalifikować zgłoszenia; priorytetyzować obsługę zgłoszeń; udzielać prostych instrukcji użytkownikowi końcowemu; diagnozować i rozwiązywać typowe problemy użytkownika końcowego; obsługiwać zdarzenia w systemie zgłoszeniowym; dokumentować sposób rozwiązywania problemu	walidować zgłoszenia; monitorować SLA i OLA; eskalować zgłoszenie incydentu, problemu oraz zmiany; rozwiązywać problemy związane z aplikacjami i systemami biznesowymi wynikłymi z błędów infrastruktury IT lub sieci	tworzyć procesy związane z obsługą incydentu, problemu oraz zmiany; analizować złożone problemy w organizacji dotyczące zarządzania usługami IT	zarządzać poziomem usług SLA i OLA; monitorować wykonanie i definiować poszczególne KPI; tworzyć modele zarządzania usługami IT	
	zna i rozumie…	**Instalacja i konfiguracja oprogramowania**	podstawowe zasady instalacji i konfiguracji oprogramowania	procedury i polityki dotyczące licencjonowania, instalacji, uprawnień i bezpieczeństwa IT; zasady wersjonowania oprogramowania i kompatybilności; oprogramowanie standardowo używane w organizacji oraz jego przeznaczenie	zasady instalacji i konfiguracji oprogramowania w rozproszonym środowisku (np. sieciowym); techniki diagnostyki błędów instalacji oraz logi instalacyjne	narzędzia automatyzacji instalacji i konfiguracji oprogramowania; zasady konfiguracji profili użytkowników, ustawień domyślnych i polityk grupowych	technologie pozwalające na automatyzację instalacji i aktualizacji oprogramowania w organizacji (np. WSUS)	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VI. Wsparcie IT	potrafi…	**Instalacja i konfiguracja oprogramowania**	analizować podstawowe logi instalacyjne; wykorzystać podstawowe narzędzia diagnostyczne do usuwania błędów konfiguracyjnych oprogramowania; instalować standardowe oprogramowanie	konfigurować standardowe oprogramowanie; rozwiązywać problemy kompatybilności wersji oprogramowania; weryfikować dostępność licencji na oprogramowanie w organizacji	instalować i konfigurować rozproszone oprogramowanie; testować poprawność oprogramowania; rozwiązywać błędy instalacji na podstawie analizy logów i diagnostyki systemu	wykorzystywać dostępne narzędzia do aktualizacji oprogramowania w organizacji	automatyzować proces instalacji i aktualizacji oprogramowania w organizacji; nadzorować poprawność automatyzacji aktualizacji oprogramowania	
	zna i rozumie…	**Zarządzanie sprzętem i zasobami IT**	podstawy sprzętu IT; cykl życia sprzętu IT w organizacji (zakup, używanie, wycofanie)	przeznaczenie sprzętu IT i zasady jego użytkowania; procedury wydawania sprzętu IT w organizacji	pełny cykl życia sprzętu IT; dokumentację techniczną IT i zasady jej prowadzenia	zasady zarządzania zasobami IT i zasady tworzenia bazy zasobów (CMDB); standardy bezpieczeństwa sprzętu IT (np. utylizacja dysków, zabezpieczanie sprzętu)	potrzeby w zakresie sprzętu i zasobów IT organizacji; trendy rynkowe w zakresie rozwiązań sprzętowych w IT	
	potrafi…	**Zarządzanie sprzętem i zasobami IT**	ewidencjonować zasoby sprzętowe; sprawdzić poprawność działania sprzętu komputerowego, podstawowych urządzeń sieciowych oraz urządzeń peryferyjnych (np. router, AP)	inwentaryzować sprzęt i zasoby IT; stosować procedury serwisowe i gwarancyjne	planować wymianę lub naprawę sprzętu i zasobów IT; przygotować specyfikację podstawowego sprzętu i zasobów IT	oceniać koszty w zakresie wykorzystywanego sprzętu i zasobów IT; planować budżet na sprzęt i zasoby IT	planować i optymalizować zasoby IT; podejmować decyzje zakupowe w zakresie zarządzanego sprzętu i zasobów IT; optymalizować koszty i wydatki w zakresie wykorzystywanego sprzętu i jego wydajności	
	zna i rozumie…	**Wsparcie zdalne dla sprzętu komputerowego i wirtualnego**	standardowe problemy sprzętowe i systemowe; politykę dostępu zdalnego; podstawowe komponenty komputera i systemu operacyjnego	działanie systemów IT w organizacji; zasady pracy z użytkownikiem zdalnym; typowe problemy użytkownika związane ze sprzętem komputerowym; narzędzia zdalnego wsparcia (np. RDP, VNC, TeamViewer)	rozwiązania wirtualne (np. VDI, terminal)	zasady zarządzania zasobami sprzętowymi i rozwiązaniami wirtualnymi (np. VDI, terminal; integrację z AD i chmurą	strategię utrzymania infrastruktury końcowej użytkownika; trendy dotyczące rozwiązań desktopowych	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VI. Wsparcie IT	potrafi…	**Wsparcie zdalne dla sprzętu komputerowego i wirtualnego**	zdalnie połączyć się z komputerem użytkownika i wykonać prostą diagnozę	zdalnie diagnozować i rozwiązywać problemy ze sprzętem komputerowym i z oprogramowaniem	planować zabezpieczenia dot. wsparcia zdalnego; diagnozować problemy maszyn wirtualnych; konfigurować aplikacje i usługi w środowiskach wirtualnych	projektować i wdrażać zabezpieczenia dot. wsparcia zdalnego; konfigurować narzędzia centralnego zarządzania	projektować i tworzyć strategię zarządzania środowiskami desktopowymi w organizacji	
	zna i rozumie…	**Wsparcie zdalne dla rozwiązań mobilnych**	podstawowe funkcje smartfonów i tabletów; zasady tworzenia kopii bezpieczeństwa, migrowania danych między urządzeniami	systemy Android i iOS; typowe problemy użytkownika związane z urządzeniami mobilnymi; rodzaje i funkcje podstawowych aplikacji mobilnych	narzędzia klasy MDM; polityki bezpieczeństwa i regulacje dotyczące mobilności w organizacji	zasady mobilnego zarządzania urządzeniami i integracji z AD i chmurą	strategię zarządzania mobilnością w organizacji; zasady dotyczące mobilności w tym BYOD	
	potrafi…	**Wsparcie zdalne dla rozwiązań mobilnych**	pomagać użytkownikowi zdalnie konfigurować urządzenie	wykonać kopie bezpieczeństwa danych i aplikacji; wspierać zdalną konfigurację aplikacji kont i połączeń; migrować dane i aplikacje między urządzeniami użytkownika	zdalnie zarządzać urządzeniami mobilnymi (np. resetować, blokować urządzenia); wykorzystywać system MDM do zarządzania urządzeniami mobilnymi	tworzyć i wdrażać polityki MDM; automatyzować procesy aktualizacji urządzeń	projektować i nadzorować procesy wsparcia mobilnego; tworzyć strategie mobilności i polityki bezpieczeństwa	
	zna i …	**Szkolenie i edukacja użytkowników rozwiązań IT**	zasady tworzenia prostych instrukcji z zakresu używania aplikacji	podstawy obsługi typowych aplikacji i urządzeń końcowych	metody dydaktyczne i komunikacyjne użyteczne w szkoleniu użytkowników	zasady projektowania szkoleń IT, w tym szkoleń e-learningowych i webinarów	trendy i potrzeby w edukacji IT	
	potrafi…	**Szkolenie i edukacja użytkowników rozwiązań IT**		objaśniać podstawowe opcje oraz przykłady stosowania rozwiązań IT; tworzyć proste w odbiorze instrukcje z zakresu używania aplikacji i wykorzystania urządzeń końcowych	prowadzić krótkie szkolenia IT; uzupełniać bazę wiedzy IT; tworzyć pełne szkolenia IT; dostosować język do poziomu wiedzy odbiorcy	tworzyć materiały edukacyjne i programy szkoleniowe w zakresie IT	zarządzać strategią szkoleń IT w organizacji; oceniać efekty szkoleń IT	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VI. Wsparcie IT	zna i rozumie…	**Zarządzanie tożsamością i dostępem**	zasady ochrony danych użytkowników; podstawowe pojęcia: konto użytkownika, hasło, logowanie, uprawnienie, rola; standardowy proces zakładania konta i nadawania prostych uprawnień; zasady bezpiecznego zarządzania hasłami; podstawowe ryzyka związane z niewłaściwymi uprawnieniami	zasady tworzenia kont i haseł; model ról użytkowników i schematy uprawnień w organizacji; procedury tworzenia, modyfikowania i usuwania kont	model nadawania i odbierania uprawnień IT w organizacji; proces weryfikowania uprawnień IT pracownika w organizacji	matryce uprawnień w organizacji; narzędzia do monitorowania dostępu i analizowania logów bezpieczeństwa	polityki dostępu; definiowanie i monitorowanie KPI dla zarządzania dostępem	
	potrafi…	**Zarządzanie tożsamością i dostępem**	realizować wnioski o dostęp według zatwierdzonych ścieżek	tworzyć i usuwać konta użytkowników	nadawać, odbierać oraz weryfikować uprawnienia zgodnie z rolami użytkowników i strukturą organizacji	monitorować dostęp, analizować logi bezpieczeństwa i identyfikować anomalie w dostępie i uprawnieniach; weryfikować matryce uprawnień i analizować związane z tym ryzyka	nadzorować politykę dostępu i prowadzić związane z tym audyty; definiować KPI i mierniki jakości zarządzania dostępami	
	zna i rozumie…	**Automatyzacja wsparcia IT**	podstawowe pojęcia związane z automatyzacją	podstawowe narzędzia helpdesk; typowe skrypty automatyzujące	metody tworzenia prostych skryptów automatyzujących (np. Powershell)	metody tworzenia zaawansowanych skryptów automatyzujących	technologie RPA i API	nowe modele rozwiązań w zakresie automatyzacji zadań IT, w tym z wykorzystaniem AI
	potrafi…	**Automatyzacja wsparcia IT**	korzystać z podstawowych, gotowych skryptów	wykorzystywać podstawowe skrypty automatyzujące	tworzyć podstawowe skrypty automatyzujące; automatyzować powtarzalne zadania helpdesk	tworzyć zaawansowane skrypty automatyzujące	tworzyć nowe rozwiązania automatyzacji zadań IT	tworzyć nowe, złożone modele automatyzacji zadań IT z możliwością wykorzystania AI

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VII. Zarządzanie danymi i AI	zna i rozumie…	**Bazy danych i platformy danych**		przykłady i zastosowanie podstawowych baz danych (np. Access, MySQL, SQL Server); relacyjne i nierelacyjne bazy danych (np. SQL, NoSQL); języki zapytań podstawowych baz danych (np. SQL); rodzaje i przykłady platform danych	w szerokim zakresie struktury danych (np. tabele, indeksy, widoki, procedury); zaawansowane składnie zapytań językiem bazy danych; zastosowanie chmurowych baz danych i platform danych; zastosowanie i przykłady magazynów danych (np. hurtownia danych, big data)	różnorakie metody analizy danych; różnorodne zasady i metody normalizacji, spójności i integracji danych (np. ETL, ELT); zasady modelowania danych i wykorzystania narzędzi wspomagających (np. modułów LLM); zasady działania złożonych architektur rozwiązań typu hurtownie danych i big data (np. Hadoop)	różnorodne zasady i metody strojenia baz danych i orkiestracji; zaawansowane zasady i metody skalowalności baz danych; złożone zasady i metody optymalizacji objętości, prędkości i wydajności baz danych; zasady bezpieczeństwa obsługi i wykorzystania baz danych; wykorzystanie AI i modułów LLM do zarządzania bazami danych	
	potrafi…	**Bazy danych i platformy danych**		tworzyć podstawowe bazy danych; korzystać z podstawowych baz danych; tworzyć typowe zapytania do bazy danych	tworzyć rozbudowane bazy danych (w tym z wykorzystaniem AI); w szerokim zakresie posługiwać się zaawansowanymi zapytaniami do baz danych; dobierać specjalnie do tego przeznaczone narzędzia do zarządzania bazami danych i korzystać z nich; korzystać z chmurowych platform danych (np. Azure, Google Cloud, AWS); monitorować aktywność i dostępy do bazy danych	projektować złożone bazy danych (np. Oracle, Hadoop, MS SQL); korzystać z narzędzi do analizy danych (np. BI); korzystać z narzędzi do przetwarzania danych (np. Apache Spark, Airflow, Kafka, Databricks); korzystać z narzędzi do modelowania danych; optymalizować przepływy danych i zapytania; projektować platformy, jeziora, potoki i siatki danych (np. lakehouse, data lake, data warehouse), w tym ich integracje	projektować optymalne i skalowalne przepływy danych; efektywnie analizować błędy i wydajność baz danych i platform danych; projektować i dokonywać orkiestracji; automatyzować administrację baz i platform danych; używać AI i narzędzi LLM do administrowania i korzystania z baz danych i platform danych	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VII. Zarządzanie danymi i AI	zna i rozumie…	**Przetwarzanie danych**	podstawowe zasady bezpieczeństwa i higieny cyfrowej przy pracy z danymi w rejestrach (ochrona kluczy, phishing); rolę adresu IP publicznego i prywatnego w identyfikacji danych; podstawowe aktywa cyfrowe i jednostki danych w systemach firmowych	różnice między środowiskiem testowym a produkcyjnym w kontekście wiarygodności danych; typy awarii węzłów sieciowych wpływające na dostępność danych	podstawy prawne przetwarzania danych osobowych na blockchainie; typy danych w smart kontraktach (np. mapping, struct) i ich ograniczenia pojemnościowe	techniki optymalizacji zapisu danych cyfrowych w celu redukcji kosztów transakcyjnych; sposoby zapewnienia spójności danych przy integracji blockchaina z systemami tradycyjnymi; mechanizmy indeksowania danych w systemach rozproszonych i ich wpływ na wydajność dApps	ryzyko związane z nielegalnymi praktykami w krytycznych cyfrowych procesach biznesowych; zaawansowane metody kryptograficzne ochrony prywatności danych cyfrowych; problemy interoperacyjności danych cyfrowych między różnymi standardami blockchaina	aktualne trendy badawcze w zakresie algorytmów konsensusu oraz skalowalności przetwarzania danych cyfrowych (np. Sharding); wpływ technologii kwantowych na bezpieczeństwo i trwałość danych cyfrowych w rejestrach blockchaina
	potrafi…	**Przetwarzanie danych**	tworzyć proste raporty historii operacji z poziomu interfejsu użytkownika (portfela lub dashboardu); odczytywać status transakcji (potwierdzona, oczekująca, odrzucona)	weryfikować statusy transakcji w publicznych i prywatnych eksploratorach w ramach obsługi zgłoszeń (ticketów); monitorować synchronizację lokalnego węzła z siecią i ciągłość przepływu danych	interpretować logi zdarzeń (event logs) generowane przez smart kontrakty w celu diagnozy błędów logicznych; tworzyć zestawienia analityczne dotyczące przepływów finansowych aktywów cyfrowych	tworzyć i wdrażać schematy baz danych i rozproszonych systemów plików (np. IPFS + blockchain); opracowywać rozwiązania typu big data do bezpiecznego dostarczania danych off-chain do smart kontraktów	projektować kompleksową architekturę przepływu danych w hybrydowych systemach enterprise blockchain; przeprowadzać audyty bezpieczeństwa logiki przetwarzania danych w smart kontraktach; opracowywać politykę zarządzania kluczami i dostępem do danych wrażliwych w systemach blockchain	tworzyć i wdrożyć nowe standardy protokołów wymiany i weryfikacji danych cyfrowych; prowadzić prace badawczo-rozwojowe nad nowymi algorytmami konsensusu lub strukturami baz danych cyfrowych
	zna i rozumie…	**Analityka danych i raportowanie**	zasady i metody tworzenia prostych raportów; podstawowe funkcje i narzędzia do tworzenia prostych raportów (np. arkusz kalkulacyjny Excel)	rodzaje raportów (np. tabelaryczne, graficzne); metody i narzędzia do tworzenia klasycznych raportów (np. Canva); narzędzia do raportowania w środowisku chmurowym (np. Google Sheets); typowe zagadnienia statystyki danych; podstawowe zadania analityki danych oraz data science	technologie i narzędzia do wyszukiwania, eksploracji i weryfikacji danych; technologie i narzędzia do modelowania i prognozowania danych; technologie i narzędzia do wizualizacji danych (np. wykresów, danych przestrzennych); w szerokim zakresie funkcje i narzędzia oraz sposoby tworzenia rozbudowanych raportów	specjalistyczne metody czyszczenia, profilowania i przygotowania danych (ETL); zaawansowane testy statystyczne i korelacje; złożone metody budowania świata obiektów na potrzeby raportowania (np. Digital Twin); profesjonalne narzędzia i ich funkcje do tworzenia skomplikowanych raportów i wizualizacji danych (np. systemy BI takie jak Power BI, Tableau); narzędzia do zarządzania i analizy dużych zbiorów danych (np. big data)	specjalistyczne procesy tworzenia metryk zapewniających spójność, dokładność i wiarygodność danych; metodykę modelowania predykcyjnego (w tym z wykorzystaniem AI) i kierunki jej rozwoju (np. Spark, Orange Data Mining); specjalne platformy do analizy danych, zarządzania jakością danych i raportowania; narzędzia do konsolidacji dużych zbiorów danych z różnych obszarów (np. IoT, przemysł, dane przestrzenne)	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VII. Zarządzanie danymi i AI	potrafi…	**Analityka danych i raportowanie**	tworzyć proste raporty (np. w arkuszu kalkulacyjnym Excel)	korzystać z typowych funkcji i szablonów narzędzi do tworzenia klasycznych raportów (np. Canva); tworzyć typowe raporty, także z wykorzystaniem narzędzi chmurowych; wyciągać podstawowe wnioski z danych na potrzeby analiz	korzystać z technologii i narzędzi do wyszukiwania, eksploracji i weryfikacji danych; korzystać z technologii i narzędzi do modelowania i prognozowania danych; korzystać z technologii i narzędzi do wizualizacji danych (w tym GIS); tworzyć rozbudowane raporty (w tym z wykorzystaniem AI); dokumentować analizy danych	procedować wydajne czyszczenie i przygotowanie danych (ETL); wyciągać wnioski z analizowanych danych (praktycznie tłumaczyć raporty); zamieniać dane na konkretne rekomendacje; tworzyć skomplikowane, interaktywne raporty i wizualizacje danych (tzw. dashboardy), np. na podstawie systemów BI takich jak Power BI, Tableau; tworzyć analizy dużych zbiorów danych i symulację zjawisk zachodzących w świecie realnym	identyfikować strategiczne KPI i budować metryki; wspierać zarządzanie projektami poprzez sprawne raportowanie; automatyzować raportowanie, w tym w czasie rzeczywistym oraz z wykorzystaniem AI; wykorzystywać narzędzia LLM do raportowania; wykorzystać analizy i raporty do podejmowania strategicznych decyzji biznesowych i zarządzania jakością danych	
	zna i rozumie…	**Strategia zarządzania danymi**	podstawowe definicje: dane, informacja, dane osobowe, dane nieustrukturyzowane oraz metadane; podstawowe zasady organizacji plików i dokumentów	klasyfikacje danych (np. jawne, poufne) w organizacjach; procedury dotyczące bezpieczeństwa i poufności danych w organizacjach	szczegółowe zasady ładu danych (Data Governance), w tym role, procesy i technologie w organizacjach; metody modelowania danych oraz architektury różnych baz i hurtowni danych; procedury naprawcze danych; zasady tworzenia metryk pomiaru jakości danych	modele architektur danych (np. Data Mesh, Data Lakehouse); strategiczne podejścia do monetyzacji i wartościowania aktywów danych; metody zarządzania ryzykiem związanym z danymi; zasady wdrożeń przy zastosowaniu polityki danych	zaawansowane teorie i modele zarządzania danymi; różne podejścia etyczne i filozoficzne do danych oraz prywatności; trendy badawcze w zakresie polityki danych i ich potencjalne implikacje strategiczne dla organizacji	aktualne globalne strategie, regulacje prawne i polityki danych z możliwością wykorzystania AI

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VII. Zarządzanie danymi i AI	potrafi…	**Strategia zarządzania danymi**	posługiwać się podstawowymi narzędziami informatycznymi do praktycznej realizacji polityki danych	weryfikować i walidować dane pod kątem jakości i kompletności zgodnie z polityką organizacji; przygotować raport lub zestawienie danych zgodnie z wewnętrznymi standardami raportowania	współtworzyć metryki pomiaru jakości danych; stosować procedury naprawcze przywracające integralność danych; analizować modele danych	projektować i implementować kompleksową architekturę ładu danych w dużej organizacji; opracować strategię zarządzania danymi w organizacji; podejmować decyzje dotyczące wykorzystania danych w nieprzewidywalnych kontekstach regulacyjnych	definiować długoterminową strategię danych dla całej organizacji; prowadzić audyty i doradztwo w zakresie zgodności regulacyjnej i strategicznego wykorzystania danych; zaproponować tworzenie nowych standardów, procedur i modeli zarządzania danymi w organizacji; audytować i oceniać zgodność procesów gromadzenia i przetwarzania danych z wewnętrznymi politykami organizacji	realizować i aktualizować wg potrzeb długoterminową strategię danych; efektywnie doradzać na poziomie strategicznym w zakresie zgodności regulacyjnej i polityki wykorzystania danych w tym AI
	zna i rozumie…	**Prywatność danych**		rodzaje uprawnień do przetwarzanych danych (dostępu, tworzenia, modyfikacji, usuwania); rodzaje gromadzonych danych, cel ich gromadzenia oraz długość okresu przechowywania; zasady i kryteria podziału danych wrażliwych (w szczególności tożsamość) podlegających ochronie prawnej; procedury reagowania na incydenty naruszenia prywatności danych; metody analizy i wizualizacji danych chronionych; zagrożenia wynikające z niewłaściwego działania AI dotyczącego prywatności danych	przepisy w zakresie prywatności danych (np. RODO, ustawy i przepisy, kodeks pracy, umowy powierzenia, klauzule poufności); standardowe metody i narzędzia do zarządzania dostępem do danych oraz zniszczeniem; standardowe metody i narzędzia do ochrony prywatności danych (w tym tożsamości, danych wrażliwych, aktywności online); standardowe metody i narzędzia do zarządzania cyklem życia danych prywatnych; zasady dokumentowania zarządzania danymi	złożone metody i narzędzia do szyfrowania, kontroli dostępu, anonimizacji, pseudonimizacji danych; zasady „privacy by design" i „privacy by default"; zasady analizy ryzyka zgodnie z RODO; zasady zabezpieczania prywatnych danych	kierunki rozwoju AI w ochronie prywatności danych; najnowsze metody i narzędzia ochrony danych z wykorzystaniem AI	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VII. Zarządzanie danymi i AI	potrafi…	**Prywatność danych**		wskazać dane podstawowe i szczególnie wrażliwe podlegające ochronie prawnej; wskazać użytkowników oraz ich uprawnienia do danych chronionych; reagować na incydenty naruszenia prywatności danych zgodnie z procedurami w tym zakresie	stosować przepisy w zakresie prywatności danych; korzystać z narzędzi do zarządzania dostępem do danych oraz zniszczeniem; stosować narzędzia do ochrony prywatności danych; zarządzać danymi zgodnie z ich przeznaczeniem i cyklem życia; dokumentować sposób zarządzania danymi i dostępem do nich	stosować złożone narzędzia do szyfrowania, kontroli dostępu, anonimizacji, pseudonimizacji danych; zapewniać zasady „privacy by design" i „privacy by default"; analizować ryzyko zgodnie z RODO; stosować zasady podwyższonego bezpieczeństwa dostępu do danych; zabezpieczać dane przed niewłaściwym działaniem AI	stosować najnowsze metody ochrony i narzędzia prywatności danych z wykorzystaniem AI; wykorzystać rozwiązania AI do podniesienia poziomu bezpieczeństwa danych	
	zna i rozumie…	**Sztuczna inteligencja**	podstawowe zagadnienia związane ze sztuczną inteligencją; podstawowe zastosowania AI w życiu codziennym i w pracy; podstawowe zasady odróżniania zadań wykonanych przez sztuczną inteligencję; podstawowe zasady bezpieczeństwa i ochrony danych podczas korzystania z narzędzi AI	rodzaje uczenia maszynowego (nadzorowane, nienadzorowane, ze wzmocnieniem); zależności między tradycyjnym oprogramowaniem a systemami uczącymi się; pojęcie autonomii AI i agenta AI	pełny cykl życia projektu ML; podstawowe i najpopularniejsze algorytmy ML; problemy związane z bias i halucynacjami AI	skalowanie modeli, obliczenia rozproszone i modele predykcyjne; regulacje europejskie (AI Act), kategorie ryzyka i bezpieczeństwo związane z użyciem AI/ML; działanie modeli LLM i DL (deep learning); metody konfiguracji i strojenia modelu AI; technikę RAG do rozbudowy modeli LLM; zasady nadzoru człowieka (human oversight) nad systemami AI zgodnie z AI Act; procedury oceny zgodności systemów AI wysokiego ryzyka oraz wymogi dotyczące dokumentacji technicznej według AI Act; wymogi AI Act dla modeli AI ogólnego przeznaczenia (GPAI), w tym obowiązki dostawców i kryteria ryzyka systemowego	najnowsze badania naukowe w dziedzinie AI i ML/LLM; najnowsze trendy w AI; metody explainable AI (XAI) i interpretowalność modeli; zaawansowane frameworki badawcze i obszary rozwojowe nowych algorytmów AI/ML; zaawansowane architektury AI, LLM i głębokiego uczenia (DL), np. systemy wieloagentowe; zasady monitorowania systemów AI po wprowadzeniu do obrotu oraz obowiązki raportowania poważnych incydentów; rolę i zasady funkcjonowania piaskownic regulacyjnych AI (AI regulatory sandboxes) w procesie wdrażania innowacji	aktualne oraz dominujące światowe strategie AI; najnowsze światowe kierunki rozwoju data science/AI

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VII. Zarządzanie danymi i AI	potrafi…	**Sztuczna inteligencja**	korzystać z gotowych narzędzi i aplikacji opartych na AI; stosować zasady rozpoznawania treści wygenerowanych przez AI; stosować podstawowe zasady bezpieczeństwa i ochrony danych podczas korzystania z narzędzi AI	dobrać proste zbiory danych do użycia w narzędziach AI/ML; uruchamiać gotowe modele ML w narzędziach no-code/low-code; interpretować podstawowe wyniki ocen modelu AI/ML; zastosować proste narzędzia AI w różnych zadaniach; uruchomić agenta AI	przeprowadzić wstępne przetwarzanie surowych danych wejściowych w bardziej efektywny zestaw i wybrać model; czyścić i dobierać zbiory danych do użycia w narzędziach AI/ML; samodzielnie zbudować i wytrenować model ML przy użyciu ogólnodostępnych bibliotek; wdrożyć prosty model AI/ML; rozpoznać halucynacje i bias AI; wykorzystywać API modeli językowych (LLM) do prostych zadań automatyzacji; stosować techniki Prompt Engineering w celu uzyskania powtarzalnych wyników	projektować i wdrażać kompleksowe rozwiązania AI/ML/RAG; rozpoznawać i ocenić bias, dryf i halucynacje modelu AI/ML; tworzyć dokumentację techniczną dla opracowanych rozwiązań AI/ML/RAG; realizować nadzór nad systemami AI zgodnie z AI Act; wdrożyć i zastosować procedury oceny zgodności systemów AI i dokumentacji technicznej według AI Act; zastosować wymogi AI Act dla modeli AI ogólnego przeznaczenia (GPAI)	samodzielnie prowadzić eksperymenty i badania w zakresie AI/ML (w tym optymalizacji kosztów obliczeniowych); projektować nowe architektury modeli LLM lub znacząco ulepszać istniejące, np. systemy wieloagentowe; zarządzać pełnym ciągiem optymalizacji i automatyzacji procesów MLOps; minimalizować bias, dryf i halucynacje modelu AI/ML oraz zapewnić zgodność z regulacjami etycznymi i prawnymi; stosować metody wyjaśnialności AI (XAI) w celu zapewnienia przejrzystości działania systemów AI zgodnie z wymogami AI Act	wskazywać bieżące trendy i kierunki rozwoju AI; tworzyć, dobierać i łączyć nowoczesne strategie AI pożądane przez biznes; opracowywać nowatorskie strategie AI dla organizacji zgodne z AI Act i innymi regulacjami, np. AI TRiSM
	zna i rozumie…	**Etyka AI**	pojęcie halucynacji AI i deepfake'a; zasady stosowania AI	kategorie ryzyka według AI Act (niedopuszczalne, wysokie, ograniczone, minimalne); podstawowe obowiązki prawne i etyczne dostawcy i użytkownika systemów IT w kontekście AI; zagrożenia i odpowiedzialności dotyczące stosowania agentów AI	szczegółowe wymagania AI Act dla systemów wysokiego ryzyka; metody wykrywania i ograniczania halucynacji AI; techniki tworzenia i wykrywania deepfake'ów; odpowiedzialność karną i cywilną za szkodliwe użycie generatywnego AI; mechanizmy powstawania halucynacji w modelach LLM i generatywnych	zaawansowane metody ataku i obrony w zakresie deepfake'ów i manipulacji multimediami; procedury oceny zgodności z AI Act pod kątem polityki wykrywania i reagowania na deepfaki, bias oraz halucynacje; globalne i europejskie standardy wykrywania syntetycznych treści; etyczne standardy wdrażania AI (w szczególności agentów AI)	najnowsze badania nad przyczynami i ograniczeniami halucynacji i bias w modelach AI; zaawansowane metody ataku na modele AI i ich implikacje etyczne oraz prawne	najnowsze światowe publikacje naukowe dotyczące bezpieczeństwa i wyrównania dużych modeli AI; potencjalnie długoterminowe ryzyka związane z niekontrolowanymi halucynacjami, bias i dezinformacją na skalę globalną

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VII. Zarządzanie danymi i AI	potrafi…	**Etyka AI**	rozpoznać oczywiste halucynacje i deepfaki w mediach; stosować zasady nierozpowszechniania podejrzanych treści wygenerowanych przez AI; weryfikować fakty podane przez AI; zgłosić niewłaściwe działania AI (np. podejrzane treści) odpowiednim służbom	ocenić, czy dane zastosowanie AI należy do kategorii wysokiego ryzyka; oznaczać treści generowane przez AI; weryfikować zgodność stosowania narzędzi z AI Act i RODO	stosować mechanizmy redukcji halucynacji w aplikacjach produkcyjnych; zastosować narzędzia do wykrywania deepfake'ów i syntetycznych mediów; stosować wymagania prawne i zasady oznaczenia oraz rejestracji systemów AI wysokiego ryzyka; wykrywać i ograniczać halucynacje w codziennej pracy z LLM	projektować systemy wykorzystujące AI (w tym agentów AI) zgodnie z etyką i kontekstem społecznym; wdrożyć system zarządzania ryzykiem AI; przeprowadzić audyt systemów AI pod kątem zgodności prawnej i etycznej; skutecznie reagować na deepfaki, bias oraz halucynacje	testować metody wykrywania i zapobiegania halucynacjom, bias oraz deepfake'om; projektować systemy certyfikacji i standardy bezpieczeństwa dla generatywnego AI; interpretować i weryfikować LLM i modele multimodalne w aspektach etycznych AI; stworzyć politykę wykrywania i reagowania na deepfaki oraz halucynacje	doradzać rządom i instytucjom międzynarodowym w zakresie tworzenia i aktualizacji polityki regulacyjnej dotyczącej ryzyk AI; opracowywać nowe metody wykrywania i zapobiegania halucynacjom, bias oraz deepfake'om
	zna i rozumie…	**Otwarte dane**	podstawową definicję danych otwartych i zasady ich udostępniania; pojęcie i przykłady metadanych; główne publiczne portale z danymi otwartymi; licencje umożliwiające ponowne wykorzystanie danych; typowe narzędzia do przetwarzania zbiorów danych	główne zasady i metody udostępniania danych otwartych; różnice między popularnymi formatami danych; podstawowe kategorie wyłączeń i ograniczeń w udostępnianiu danych	wspólne struktury i formaty danych, w tym danych przestrzennych; kluczowe platformy do udostępniania danych publicznych (np. CKAN, DKAN, GeoServer); platformy współpracujące w otwieraniu danych publicznych i komercyjnych (np. Sokrata, OpenDataSoft); szczegółowe wymogi prawne i techniczne dotyczące publikacji danych otwartych; metody oceny jakości i dojrzałości udostępnianych zbiorów danych; zaawansowane standardy metadanych	metody i narzędzia do tworzenia i zarządzania złożonymi systemami danych otwartych; rolę API w dostępie do danych i budowy aplikacji działających na danych w czasie rzeczywistym; politykę udostępniania danych z urządzeń IoT; rozwiązania techniczne do automatycznego i skalowalnego udostępniania danych; znaczenie czyszczenia otwartych danych dla projektów i innowacji (np. OpenRefine)	metodologie badawcze dotyczące oceny danych otwartych; trendy i technologie w zakresie interoperacyjności i wymiany danych otwartych; znaczenie budowania ekosystemu wspólnego otwierania danych publicznych i komercyjnych	wyzwania dotyczące przyszłości regulacji prawnych i technicznych dla danych otwartych; zasady etycznej strony przetwarzania otwartych danych (Data Ethics Canvas); najnowsze metodyki i trendy w ciągłej popularyzacji korzystania bezpośrednio z otwartych danych (np. data storytelling) z możliwością wykorzystania AI

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VII. Zarządzanie danymi i AI	potrafi…	**Otwarte dane**	znaleźć i pobrać typowe tabele danych z oficjalnego portalu danych otwartych; posługiwać się podstawowymi narzędziami do otwierania i wizualizacji zbiorów danych; rozpoznać, czy dany zbiór ma metadane i potrafi je odczytać	wyszukiwać i łączyć dane z różnych źródeł otwartych; posługiwać się narzędzami do wykonywania zapytań do publicznych zbiorów danych; prawidłowo powoływać się na licencje i przypisywać je do udostępnianych danych otwartych	opracować wewnętrzną procedurę publikacji danych; dokonać deidentyfikacji i anonimizacji danych; zarządzać i utrzymywać zbiory na platformie danych otwartych; dbać o aktualność danych otwartych i jakość metadanych; oceniać potencjalne ryzyka techniczne, prawne i etyczne związane z udostępnianiem danych otwartych	opracować procedurę publikacji danych otwartych dla organizacji lub sektora; wdrażać zaawansowane mechanizmy informatyczne do automatycznego i skalowalnego udostępniania danych	opracowywać modele udostępniania danych otwartych o wysokim stopniu złożoności; projektować złożone mechanizmy informatyczne do automatycznego i skalowalnego udostępniania danych; wdrażać wspólne platformy otwartych danych publicznych i komercyjnych	prowadzić badania i opracowywać innowacyjne modele udostępniania danych otwartych o wysokim stopniu złożoności; tworzyć nowe standardy i procedury na poziomie krajowym lub międzynarodowym w zakresie otwierania danych, w tym komercyjnych; współpracować w budowaniu innowacji w ciągłym procesie otwierania danych i budować społeczność wokół nich
VIII. Architektura rozwiązań IT	zna i rozumie…	**Wizja architektury IT**		podstawy architektury IT i analizy IT	rolę architektury rozwiązań IT w zależności od organizacji; podstawy architektury korporacyjnej i jej elementy (TOGAF, Open Agile Architecture); zależności między architekturą IT a analizą rozwiązań IT	metody i narzędzia projektowania architektury IT (na podstawie TOGAF); zasady tworzenia docelowej wizji architektury IT (TO-BE); zależności i zasady tworzenia warstw architektury IT (komponenty: architektura biznesowa, danych, aplikacji, technologii i systemów krytycznych)	znaczenie opisu stanu AS-IS i stanu TO-BE dla modelu architektonicznego organizacji; wagę i znaczenie pryncypiów architektonicznych dla organizacji w powiązaniu z jej strategią; znaczenie wizji dla realizacji projektów zgodnie ze standardami technologicznymi i interoperacyjnością systemów zawartymi w wizji	znacznie tworzenia rekomendacji nowatorskich zmian strategii rozwoju organizacji i wizji architektury IT; wpływ najnowszych technologii na rozwój organizacji z wykorzystaniem np. rozwiązań chmurowych i AI

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VIII. Architektura rozwiązań IT	potrafi…	**Wizja architektury IT**			zinwentaryzować stan bieżącej architektury IT (AS-IS); wskazać powiązania między głównymi komponentami w istniejącym środowisku IT	analizować i oceniać zależności między komponentami środowiska IT w architekturze TO-BE; tworzyć diagramy architektury IT (np. C4, ArchiMate); dobierać komponenty wizji dla realizacji projektów zgodnie ze standardami technologicznymi i interoperacyjnością systemów zawartymi w wizji	aktualizować stan architektury AS-IS i TO-BE; współtworzyć i wytyczać pryncypia architektoniczne dla IT; prowadzić strategiczny nadzór nad realizacją projektów zgodnie z wizją architektury IT; ograniczać Shadow IT zgodnie z zasadami wizji; zarządzać warstwami w repozytorium komponentów architektury IT (legislacyjną, organizacyjną, semantyczną, techniczną)	wskazywać i tworzyć nowatorskie technologie mające wpływ na rozwój organizacji z wykorzystaniem np. rozwiązań chmurowych i AI; tworzyć innowacyjne podejście do złożonych problemów i zależności komponentów nowoczesnej architektury IT
	zna i rozumie…	**Stos technologiczny i dobór technologii**				typowe komponenty stosu technologicznego (różnica między frameworkami, narzędziami a stosem); rodzaje stosów technologicznych przeznaczonych dla typowych zastosowań; znaczenie stosów technologicznych opartych na open source dla niezależności architektonicznej	znaczenie wyboru stosu technologicznego w natywnych technologiach chmurowych oraz we własnym środowisku IT i jego wpływu na architekturę IT; kluczowe wymagania i komponenty (w tym AI) stosu technologicznego dla rozwiązań chmurowych i ich bezpieczeństwa; wpływ stosu technologicznego i jego ujednolicenie na wydajność, skalowalność i bezpieczeństwo	trendy nowoczesnych stosów technologicznych dla nowatorskiej transformacji organizacji; potrzebę wykorzystania nowych elementów stosu technologicznego do budowania spójnych ekosystemów z narzędziami AI

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VIII. Architektura rozwiązań IT	potrafi…	**Stos technologiczny i dobór technologii**				wskazać komponenty stosu technologicznego w zależności od jego przeznaczenia; wybrać stos technologiczny na podstawie kluczowych aspektów (np. projekt, skalowalność, budżet, kompetencje zespołu, bezpieczeństwo); stosować wybrane komponenty ze stosu technologicznego do realizacji projektu, w tym wykorzystującego open source	skomponować i wdrożyć stos technologiczny dla środowisk chmurowych i hybrydowych w architekturze IT; wybrać i zastosować komponenty technologiczne do budowania i rozwijania własnego stosu technologicznego; przeprowadzić proces standaryzacji stosowania stosu technologicznego i opracować standardy oraz wytyczne użycia zaimplementowanych technologii; przeprowadzać analizę ryzyka związanego z wyborem stosu technologicznego	dokonywać modyfikacji w nowatorskim stosie technolgicznym architektury IT i migrować stworzone rozwiązania do funkcjonującej technologii; przeprowadzić za pomocą AI nowatoskie analizy i symulacje środowiskowe oraz funkcjonalne stosu technologicznego
	zna i rozumie…	**Wzorce architektoniczne i referencyjne**			podstawy architektury komponentowej i usługowej oraz style architektoniczne (np. SOA, warstwowa, mikroserwisy, zdarzeniowa EDA)	znaczenie wzorców architektonicznych i integracyjnych (np. REST API, SOAP, Kafka); znaczenie relacji między wzorcami a pryncypiami wizji architektury (np. mikroserwisy vs monolit) i ich zależności (np. pod względem skalowalności, niezawodności, wielkości projektu); zasady doboru wzorców architektonicznych realizujących pryncypia (np. time to market, wysoka dostępność, niezależność od dostawcy); znaczenie doboru wzorców dla obliczeniowej chmury hybrydowej (łączące własne DC, chmurę prywatną i chmury publiczne) pod kątem ciągłości działania biznesu	metody i zasady tworzenia oraz utrzymania architektur referencyjnych; metody i zasady utrzymania oraz aktualizacji wzorców odporności architektury IT; znaczenie i zależności wykorzystania wzorców opartych na open source lub na platformach komercyjnych; znaczenie wzorców architektonicznych z open source dla wdrażania rozwiązań chmurowych w modelu cloud agnostic lub cloud native; sposoby definiowania standardów integracyjnych	strategię i innowacyjne kierunki rozwoju wzorców architektonicznych, zwłaszcza z wykorzystaniem AI, w tworzeniu nowatorskich rozwiązań cyfrowych jako element budowania przewagi konkurencyjnej

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VIII. Architektura rozwiązań IT	potrafi…	**Wzorce architektoniczne i referencyjne**					dokonać wyboru wzorca projektowego i uzasadnić jego wybór w danym projekcie IT; tworzyć architektury referencyjne dla stosowanych wzorców oraz katalogi standardów, wytycznych i rekomendacji architektonicznych; dokumentować wykorzystanie wzorców projektowych i ich zgodność z pryncypiami; stosować i wykorzystywać open source w architekturach referencyjnych pod kątem optymalizacji kosztów i uniezależnienia się od dostawców; stosować zasady doboru rozwiązań chmurowych (cloud agnostic vs cloud native) w zależności od potrzeb i pryncypiów; identyfikować zagrożenia i opracowywać exit plan dla kluczowych lub obarczonych ryzykiem rozwiązań architektury IT	identyfikować nowoczesne systemy i usługi wymagające modyfikacji architektury ze względu na dług technologiczny; aktualizować, dobierać i tworzyć nowe wzorce architektury z uwzględnieniem rozwiązań chmurowych i AI; wykorzystać nowe wzorce (np. RAG) oparte na AI (łączenie modeli LLM z własnymi zasobami danych)

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
VIII. Architektura rozwiązań IT	zna i rozumie…	Nadzór i rozwój				znaczenie architektury IT jako wspierającej strategię biznesową i zapewniającej rozwój organizacji; zasady doboru architektury IT do zasobów organizacji (np. eliminacja vendor lock-in, eliminacja duplikacji systemów, technologii powtarzających się, lepsze wykorzystanie zasobów)	przywództwo technologiczne i rolę architektury IT w długofalowej strategii biznesowej organizacji; frameworki architektoniczne i standardy do zarządzania architekturą IT i dokumentowania wizji; znaczenie nadzoru nad wizją architektury IT pod względem długu technologicznego, bezpieczeństwa i zgodności; zasady tworzenia architektury IT do zarządzania pełnym spektrum możliwości biznesowych (IT, OT, IoT); podejście API First jako strategii nie tylko technologicznej, ale również biznesowej	trendy rozwojowe, w tym wykorzystanie AI do tworzenia nowatorskiej architektury w modelu Green IT; trendy rozwoju nowych platform automatyzujących i wspierających architekturę IT
	potrafi…	Nadzór i rozwój				samodzielnie zbudować prototyp systemu potwierdzający, że wizja architektury IT jest wykonalna; zweryfikować wybory architektoniczne pod względem zgodności z wizją (np. z wykorzystaniem open source); wykorzystywać szeroką wiedzę z zakresu bezpieczeństwa, infrastruktury IT, oprogramowania, danych, przetwarzania w chmurze do tworzenia architektury IT	wdrażać i modyfikować architekturę IT w sposób ewolucyjny, zapewniając bezpieczeństwo i zrównoważony rozwój organizacji; wykonywać przeglądy architektury IT i dokumentować decyzje architektoniczne; aktualizować architektury referencyjne w organizacji i nadzorować wykonywanie pryncypiów (w tym reużywalność komponentów, usług i kodu); wdrażać architekturę, stosując API Management jako pryncypium	poszukiwać i testować nowe technologie do wdrożenia i aktualizacji architektury IT; wykorzystywać AI w projektowaniu, modelowaniu i nadzorze nad nowatorską architekturą IT; wykorzystywać architekturę IT w celu stworzenia innowacyjnej przewagi technologicznej w ekosystemie cyfrowym

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IX. Zarządzanie IT	zna i rozumie…	**Strategia IT**				cele biznesowe i ich powiązania z planami IT; infrastrukturę IT i architekturę systemów IT	metody budowy strategii IT organizacji; zarządzanie portfelem projektów IT; trendy rozwoju technologii IT; wpływ AI na technologie IT i biznes	aktualne i globalne trendy technologiczne w IT; bieżące polityki sektorowe i wpływ IT na gospodarkę
	potrafi…	**Strategia IT**				analizować potrzeby organizacji i proponować odpowiednie rozwiązania IT; analizować posiadane zasoby IT i wykorzystywać je do realizacji celów biznesowych	tworzyć i wdrażać strategię IT zgodną ze strategią organizacji; proponować i łączyć technologie IT z procesami biznesowymi i środowiskowymi; budować struktury IT zgodnie z potrzebami organizacji	kształtować długofalową i nowatorską wizję rozwoju technologii IT w organizacji; wpływać na bieżącą strategię całej instytucji i polityki sektorowe
	zna i rozumie…	**Przywództwo technologiczne i cyfrowa transformacja biznesu**				zasady kierowania zespołem IT; podstawy transformacji cyfrowej	metody zarządzania zmianą w IT; metody zarządzania innowacjami IT i ich wpływ na organizację	nowatorskie modele przywództwa cyfrowego w zależności od wymogów rynkowych; aktualne metody komunikacji strategicznej i rolę ambasadora organizacji; platformy i ekosystemy cyfrowe
	potrafi…	**Przywództwo technologiczne i cyfrowa transformacja biznesu**				kierować zespołem IT; motywować zespoły IT i wspierać wdrażanie nowych technologii	zarządzać transformacją cyfrową; zarządzać długiem technologicznym; prowadzić programy innowacyjne w zakresie IT; budować interdyscyplinarne zespoły wspierające transformację cyfrową; przeprowadzić organizację przez transformację cyfrową	wyznaczać nowoczesne kierunki rozwoju cyfrowego; rozwijać organizację w ekosystemie cyfrowym; na bieżąco czynnie uczestniczyć w konferencjach branżowych z zakresu IT

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IX. Zarządzanie IT	zna i rozumie…	**Budżetowanie i finanse IT**				podstawy planowania budżetu i kontroli kosztów związanych z wydatkami na IT	metody analizy ROI, TCO i finansowania projektów IT; modele finansowania IT, budowanie konsorcjów i klastrów; budżet IT w organizacji; optymalizację kosztów IT	zarządzanie budżetem strategicznym IT; sposoby pozyskiwania funduszy na innowacje IT; wpływ inwestycji IT na całą organizację i gospodarkę
	potrafi…	**Budżetowanie i finanse IT**				planować i kontrolować budżet zespołu/działu/projektu IT	zarządzać budżetem IT w organizacji; optymalizować koszty funkcjonowania IT i biznesu w organizacji; wpływać na interesariuszy w zakresie budżetu IT	negocjować bieżące finansowanie i oceniać strategiczne inwestycje IT; pozyskiwać fundusze zewnętrzne na działania strategiczne i innowacyjne w obszarze IT
	zna i rozumie…	**Zarządzanie licencjami IT**			zasady licencjonowania open source; zasady licencjonowania komercyjnego; proces zarządzania cyklem życia licencji; narzędzia do inwentaryzacji oprogramowania	modele licencjonowania oprogramowania; systemy do zarządzania licencjami (np. SAM, SLM)	politykę zarządzania licencjami w organizacji	
	potrafi…	**Zarządzanie licencjami IT**			identyfikować rodzaje licencji; korzystać z różnych licencji; tworzyć i aktualizować rejestry licencji w organizacji; dokonywać analizy rynku dostawców licencji; weryfikować zgodność licencji z umowami i regulacjami; prowadzić inwentaryzację oprogramowania	identyfikować nadmiarowe i nieużywane licencje w organizacji; prowadzić audyty licencji oprogramowania	planować zakup licencji; optymalizować koszty wyboru i zakupu licencji; negocjować warunki licencyjne z dostawcami; zarządzać licencjami w organizacji	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IX. Zarządzanie IT	zna i rozumie…	**Zarządzanie usługami IT**				metodyki ITIL/COBIT; sposoby monitorowania OLA i SLA; metody zapewnienia ciągłości usług IT; zagrożenia związane z cyberbezpieczeństwem usług IT i sposoby przeciwdziałania im	metody i narzędzia projektowania katalogu usług IT; systemy zarządzania usługami IT	politykę usług IT na poziomie ekosystemu cyfrowego; aktualne sposoby integracji IT i biznesu z ekosystemem cyfrowym; sposoby stabilnego utrzymywania relacji z kluczowymi dostawcami i osobami w ekosystemie cyfrowym
	potrafi…	**Zarządzanie usługami IT**				korzystać z metodyk ITIL/COBIT; monitorować OLA i SLA; zapewniać ciągłość usług IT; identyfikować zagrożenia związane z cyberbezpieczeństwem usług IT i ich wpływ na organizację	projektować katalog usług IT; wykorzystywać metodyki ITIL/COBIT zgodnie z potrzebami organizacji; tworzyć metodyki zarządzania usługami IT w organizacji; wdrażać procesy zarządzania usługami IT; zapewnić jakość i dostępność usług IT	tworzyć politykę usług IT w ekosystemie cyfrowym; integrować IT i biznes z ekosystemem cyfrowym; podtrzymywać relacje z kluczowymi dostawcami i kluczowymi osobami w ekosystemie cyfrowym
	zna i rozumie…	**Zarządzanie projektami IT**				metodyki zarządzania projektami IT (np. Agile, Scrum, PRINCE2)	metody zarządzania portfelem projektów IT; metodyki hybrydowe w zarządzaniu projektami IT (np. Water-Scrum-Fall, Agile--Waterfall Hybrid, PRINCE2 Agile); metody zarządzania ryzykiem w projektach IT	kulturę projektową organizacji i jej wpływ na strategię IT
	potrafi…	**Zarządzanie projektami IT**				prowadzić projekty IT zgodnie z metodykami; monitorować harmonogram, budżet i zakres projektów IT; korzystać z metody design thinking w zarządzaniu projektami IT	kierować portfelem projektów IT; zarządzać ryzykiem projektów IT; wdrażać metody hybrydowe w zarządzaniu projektami IT	decydować o bieżących i strategicznych inicjatywach IT; reprezentować nowe projekty IT wobec kierownictwa organizacji i interesariuszy zewnętrznych

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IX. Zarządzanie IT	zna i rozumie…	**Zarządzanie zasobami ludzkimi i kompetencjami IT**				odpowiedzialność i obowiązki poszczególnych członków zespołu IT; metody monitorowania realizacji zadań przez członków zespołu IT (np. Kanban, sprinty, retrospektywy); metody prowadzenia rekrutacji do zespołów IT; sposoby oceniania kompetencji pracowników IT	politykę HR w IT; politykę szkoleniową dla członków działów IT; metody budowania struktur IT w organizacji; systemy motywacyjne i modele rozwoju kompetencji pracowników IT	strategię rozwoju talentów IT w organizacji; sposoby współpracy z uczelniami i instytucjami edukacyjnymi w zakresie pozyskiwania talentów IT; sposoby wpływu na rynek pracy IT
	potrafi…	**Zarządzanie zasobami ludzkimi i kompetencjami IT**				organizować pracę zespołu IT; wyznaczać zadania w zakresie IT i oceniać ich realizację; rekrutować pracowników do zespołu IT; oceniać kompetencje pracowników IT; monitorować realizację zadań przez członków zespołu IT	nadzorować pracę poszczególnych działów IT w organizacji; wyznaczać cele dla poszczególnych działów IT i oceniać ich realizację; planować rozwój kompetencji pracowników IT; opracowywać ścieżki kariery pracowników IT; rozwijać kompetencje członków poszczególnych działów IT; wdrażać systemy motywacyjne w IT; inicjować organizację praktyk i staży IT	tworzyć i aktualizować strategię rozwoju talentów IT w organizacji; współpracować z uczelniami i instytucjami edukacyjnymi w zakresie ciągłego pozyskiwania talentów IT; wpływać na bieżąco na rynek pracy IT
	zna i rozumie…	**Zarządzanie ryzykiem i zgodnością IT**				ryzyka operacyjne w zakresie usług IT i infrastruktury IT; procedury zgodności w zakresie IT (np. RODO, normy ISO)	metody zarządzania ryzykiem strategicznym IT; systemy kontroli i audytu w IT; regulacje krajowe i unijne w zakresie IT; zasady tworzenia procedur zgodności w zakresie IT	politykę bezpieczeństwa i zgodności IT w organizacji; sposoby współpracy z instytucjami i regulatorami mającymi wpływ na zgodność w IT

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IX. Zarządzanie IT	potrafi…	**Zarządzanie ryzykiem i zgodnością IT**				identyfikować ryzyka operacyjne w zakresie usług IT i infrastruktury IT; stosować procedury zgodności w zakresie IT (np. RODO, normy ISO)	zarządzać ryzykiem strategicznym IT; wdrażać metody kontroli i audytu w IT; stosować regulacje krajowe i unijne w zakresie IT; tworzyć procedury zgodności w zakresie IT	kształtować i aktualizować politykę bezpieczeństwa i zgodności IT w organizacji; na bieżąco współpracować z regulatorami i instytucjami międzynarodowymi w zakresie zgodności w IT
	zna i rozumie…	**Zarządzanie ciągłością działania IT**				plany awaryjne i odzyskiwania zasobów w zakresie IT	rozwiązania wysokiej dostępności i programy ciągłości działania w zakresie IT	strategię odporności organizacji w zakresie IT; zasady integracji planów organizacji z polityką bezpieczeństwa państwa w zakresie IT
	potrafi…	**Zarządzanie ciągłością działania IT**				opracować i testować plany awaryjne w zakresie IT; koordynować odzyskiwanie zasobów IT	zarządzać programami ciągłości działania i wdrażać odzyskiwanie zasobów w zakresie IT	tworzyć i stale aktualizować strategię odporności organizacji w zakresie IT; integrować na bieżąco plany organizacji z polityką bezpieczeństwa państwa w zakresie IT
	zna i rozumie…	**Zarządzanie jakością IT**				narzędzia kontroli jakości usług IT (np. diagramy procesów, arkusze kontrolne procesów, diagramy Ishikawy); wskaźniki związane z jakością usług IT; narzędzia kontroli jakości oprogramowania (np. testy funkcjonalne i niefunkcjonalne, analiza statyczna i dynamiczna kodu, automatyzacja testów z użyciem Selenium, JUnit); narzędzia do testów wydajnościowych (np. JMeter)	standardy ISO/ITIL i metody audytu jakości usług IT	kulturę jakości usług IT i jej wpływ na branżę IT

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
IX. Zarządzanie IT	potrafi…	**Zarządzanie jakością IT**				stosować narzędzia kontroli jakości usług IT, oprogramowania i monitorować ich wskaźniki	projektować systemy zarządzania jakością usług IT; prowadzić audyty usług IT	wdrażać i kształtować kulturę jakości usług IT; tworzyć aktualne normy i standardy w gremiach normalizacyjnych w zakresie IT
X. Przełomowe technologie IT	zna i rozumie…	**Technologie immersyjne**		zasady wykorzystania technologii immersyjnych (np. VR, AR, MR); różnice pomiędzy technologiami immersyjnymi; zasady działania technologii immersyjnych	aplikacje i narzędzia informatyczne niezbędne do wykorzystywania odpowiednich technologii immersyjnych; zasady działania i wykorzystania symulatorów różnego rodzaju (np. medycznych, lotniczych)	zasady konfiguracji urządzeń i oprogramowania niezbędnego do wykorzystania technologii immersyjnych	trendy dotyczące technologii immersyjnych; złożone rozwiązania technologii immersyjnych; nowe obszary zastosowań technologii immersyjnych	
	potrafi…	**Technologie immersyjne**		rozpoznać rodzaj technologii immersyjnej	dobrać rodzaj technologii immersyjnej do wykonywanego działania; stworzyć koncepcję immersyjnego rozwiązania informatycznego; zastosować symulator do szkolenia i wykorzystania w pracy	wdrożyć i uruchomić rozwiązania technologii immersyjnej; przeprowadzić testy działania technologii immersyjnej	stworzyć funkcjonalne aplikacje współpracujące z technologią immersyjną; doskonalić metody technologii immersyjnych; inicjować pracę interdyscyplinarnego zespołu do rozwoju technologii immersyjnych	
	zna i rozumie…	**Komputery kwantowe**			podstawowe pojęcia informatyki kwantowej; główne różnice między komputerem klasycznym a kwantowym	podstawowe możliwości praktycznego użycia rzeczywistych komputerów kwantowych i symulatorów; podstawowe algorytmy kwantowe i możliwości ich użycia; podstawy teoretyczne funkcjonowania komputerów kwantowych	zaawansowane zasady kwantowej teorii informacji, w tym mechanizmy korekcji błędów kwantowych i protokoły komunikacji kwantowej; szeroki zakres zaawansowanych algorytmów oraz ich ograniczenia; podstawy różnych architektur sprzętowych	najnowsze osiągnięcia naukowe i teorie w zakresie wiedzy na styku informatyki kwantowej z fizyką i inżynierią; aktualne wyzwania teoretyczne i praktyczne związane z potencjalnymi zastosowaniami informatyki kwantowej

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
X. Przełomowe technologie IT	potrafi…	**Komputery kwantowe**			zidentyfikować w gotowym interfejsie graficznym (GUI) lub schemacie elementy prostego obwodu kwantowego; uruchomić program kwantowy zgodnie z instrukcją i odczytać jego prosty wynik	wykorzystywać interfejs graficzny służący do konstruowania algorytmów kwantowych; używać oprogramowania narzędziowego algorytmów kwantowych; oszacować złożoność obliczeniową algorytmów kwantowych	analizować i praktycznie syntetyzować wiedzę na styku informatyki kwantowej z fizyką i inżynierią; projektować i modyfikować algorytmy kwantowe; używać emulatory komputerów kwantowych	prowadzić oryginalne badania naukowe i opracowywać nowe teorie lub protokoły kwantowe; definiować, proponować i wdrażać nowe, strategiczne projekty badawczo-rozwojowe (R & D) w informatyce kwantowej; propagować wiedzę w obszarze informatyki kwantowej
	zna i rozumie…	**Rozwiązania autonomiczne**		podstawowe typy systemów autonomicznych i humanoidalnych oraz ich główne komponenty (np. sensory, sterowniki, aktuatory); ogólne zasady działania prostych metod lokalizacji i nawigacji w typowych warunkach pracy; podstawy integracji systemów autonomicznych z infrastrukturą IT/OT z uwzględnieniem zasad bezpieczeństwa	budowę typowych systemów autonomicznych; podstawy przetwarzania danych sensorycznych pod kątem rozwiązań autonomicznych; typowe rozwiązania komunikacyjne w systemach autonomicznych oraz zasady stosowania wymagań i procedur eksploatacyjnych	działanie kluczowych komponentów systemów autonomicznych oraz ich zależności w ramach rozwiązania; zasady doboru i konfiguracji rozwiązań autonomicznych do wymagań procesu biznesowego lub technologicznego; etapy cyklu życia rozwiązań autonomicznych oraz zasady projektowania środków bezpieczeństwa wewnątrz systemu	zasady projektowania docelowych architektur systemów autonomicznych i humanoidalnych w skali organizacji lub ekosystemu cyfrowego; modele organizacyjne i procesowe dla eksploatacji stocków systemów autonomicznych; uwarunkowania prawne, etyczne i społeczne stosowania rozwiązań autonomicznych; zasady identyfikacji, oceny i zarządzania ryzykiem na poziomie organizacji w zakresie rozwiązań autonomicznych	w pogłębionym stopniu zasady percepcji, lokalizacji i sterowania w systemach autonomicznych; aktualne kierunki badań naukowych w obszarze systemów autonomicznych i humanoidalnych; zaawansowane metody analizy bezpieczeństwa, niezawodności i odporności systemów autonomicznych

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
X. Przełomowe technologie IT	potrafi…	**Rozwiązania autonomiczne**		przygotować do pracy urządzenia autonomiczne, w tym z wykorzystaniem metod lokalizacji i nawigacji; wykonywać podstawowe czynności obsługowe i kalibracyjne sensorów i aktuatorów; monitorować podstawowe parametry pracy urządzenia autonomicznego; reagować na typowe komunikaty i alarmy zgodnie z procedurami	sterować wybranym komponentem urządzenia autonomicznego; parametryzować i optymalizować działanie gotowych systemów autonomicznych pod kątem konkretnych zadań; analizować logi i dane telemetryczne w celu identyfikacji problemów; planować i realizować testy odbiorcze urządzeń opartych na systemach autonomicznych	dobierać i łączyć elementy systemów autonomicznych w spójne rozwiązania dla konkretnego procesu z wykorzystaniem dostępnych komponentów i infrastruktury IT/OT; planować i realizować złożone scenariusze wdrożenia, testów i walidacji systemów autonomicznych (np. testy regresyjne, scenariuszowe, bezpieczeństwa); modyfikować konfigurację i parametry działania zaawansowanych systemów autonomicznych oraz doradzać przy wyborze i adaptacji rozwiązań różnych dostawców	projektować docelowe architektury rozwiązań autonomicznych dla organizacji; projektować i doskonalić procesy operacyjne dla stocków autonomicznych; koordynować interdyscyplinarne zespoły projektowe i inwestycyjne w zakresie rozwiązań autonomicznych	projektować i rozwijać nowe algorytmy oraz nowatorskie modele dla systemów autonomicznych i humanoidalnych; planować i prowadzić złożone badania i prace rozwojowe w obszarze rozwijania systemów autonomicznych i humanoidalnych; współtworzyć standardy techniczne, regulacje i wytyczne sektorowe w zakresie systemów autonomicznych i humanoidalnych; budować środowiska eksperckie i współpracę nauki, biznesu i administracji w zakresie systemów autonomicznych i humanoidalnych
	zna i rozumie…	**Technologie biocyfrowe**			zagadnienia bioinformatyki; zasady działania biosensorów; zasady działania technologii ubieralnych; rodzaje biosensorów; rodzaje technologii ubieralnych	rodzaje i przykłady technologii biocyfrowych; metody cyfrowego modelowania i symulacji procesów biologicznych	zasady funkcjonowania interfejsów mózg–komputer (BCI); metody projektowania systemów sterowania mózg–komputer (np. narzędzia ML i AI); zastosowanie ML i AI do analizy materiału biologicznego; perspektywy wykorzystania biokomputerów; metody i narzędzia nawigacji komputerowej w implantologii; BCI, biokomputery	najnowsze kierunki wsparcia badań bioinformatyki i technologii biocyfrowych; aktualne metody informatyczne wspierania diagnostyki, leczenia chorób i rozwoju nowych leków

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
X. Przełomowe technologie IT	potrafi…	Technologie biocyfrowe			odczytywać i dekodować sygnały z biosensorów; stosować biosensory; stosować technologie ubieralne;	tworzyć oprogramowanie dla technologii biocyfrowych	projektować interfejsy i systemy komunikacji oraz sterowania mózg–komputer; stosować ML i AI do analizy materiału biologicznego; tworzyć algorytmy oraz projektować metody i narzędzia nawigacji w technologiach biocyfrowych	prowadzić nowatorskie eksperymenty w obszarze bioinformatyki i technologii biocyfrowych; tworzyć nowe metody informatyczne wspierania diagnostyki, leczenia chorób i rozwoju nowych leków; projektować nowe zastosowania dla biokomputerów; współtworzyć innowacyjne podzespoły dla biokomputerów
XI. Green IT	zna i rozumie…	Zrównoważona infrastruktura sprzętowa	**(ZK) ogólne zasady energooszczędnego użytkowania sprzętu IT**	**(ZK) podstawowe elementy infrastruktury sprzętowej IT oraz ich wpływ na zużycie energii;** **(ZK) podstawowe zasady postępowania ze zużytym sprzętem IT oraz znaczenie procedur wewnętrznych**	**(ZK) zapotrzebowanie na energię elektryczną elementów infrastruktury IT;** **(ZK) podstawy monitorowania zużycia energii elektrycznej elementów infrastruktury IT;** **(ZK) zasady zrównoważonego cyklu życia sprzętu IT**	**(ZK) zależności między architekturą infrastruktury IT a zużyciem energii i śladem węglowym;** **(ZK) metody i narzędzia pomiaru zużycia zasobów infrastruktury IT oraz raportowania jej wpływu na środowisko;** **(ZK) zasady planowania modernizacji i wymiany przestarzałej infrastruktury IT z możliwością wykorzystania AI**	**(ZK) zasady projektowania docelowych architektur infrastruktury IT z uwzględnieniem Green IT w skali organizacji (data center, chmura, sieć, środowisko pracy);** **(ZK) ramy i standardy zarządzania zrównoważoną infrastrukturą IT oraz ich powiązania z wymaganiami raportowania ESG;** **(ZK) ekologiczne podejście do modernizacji środowisk infrastrukturalnych z możliwością wykorzystania AI**	**(ZK) zaawansowane technologie i najnowsze kierunki badań w obszarze zrównoważonej infrastruktury IT, z możliwością wykorzystania AI;** **(ZK) rozwijanie i projektowanie zrównoważonych modeli globalnych architektur infrastruktury IT w ekosystemie cyfrowym**

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
	potrafi…	Zrównoważona infrastruktura sprzętowa	(ZK) stosować ustawienia oszczędzania energii dla prostych urządzeń IT	(ZK) eksploatować sprzęt IT zgodnie z zasadami energooszczędności; (ZK) przekazywać zużyty sprzęt IT do właściwych punktów	(ZK) analizować podstawowe dane o zużyciu energii elektrycznej elementów infrastruktury IT; (ZK) stosować standardowe rozwiązania energooszczędne w infrastrukturze sprzętowej IT; (ZK) wskazywać najbardziej energochłonne elementy infrastruktury IT do wymiany lub optymalizacji	(ZK) projektować i wdrażać ekologiczne usprawnienia w infrastrukturze sprzętowej IT (np. chmura, wirtualizacja serwerów, optymalizacja zasilania i chłodzenia); (ZK) dobierać i wdrażać narzędzia monitoringu energetycznego w celu optymalizacji infrastruktury IT; (ZK) planować i koordynować modernizację nieefektywnej energetycznie infrastruktury IT z możliwością wykorzystania AI	(ZK) projektować zrównoważoną architekturę IT w skali organizacji; (ZK) definiować i nadzorować polityki, procesy oraz KPI dotyczące zrównoważonego rozwoju w obszarze infrastruktury IT; (ZK) koordynować programy modernizacji infrastruktury IT z możliwością wykorzystania AI	(ZK) projektować nowe modele, metody i narzędzia dla zrównoważonej infrastruktury IT z możliwością wykorzystania AI; (ZK) prowadzić nowatorskie projekty badawczo-rozwojowe dotyczące zrównoważonego rozwoju w infrastrukturze IT oraz wdrażać ich wyniki w postaci rozwiązań referencyjnych; (ZK) współtworzyć standardy, wytyczne i polityki dotyczące Green IT
	zna i rozumie…	Oprogramowanie w Green IT	(ZK) podstawowe zasady efektywnego korzystania z aplikacji pod kątem zrównoważonego rozwoju	(ZK) podstawowy wpływ oprogramowania na zużycie zasobów i energii elektrycznej; (ZK) podstawy cyklu życia oprogramowania oraz jego znaczenie dla trwałości środowiska IT	(ZK) podstawowe zasady programowania zorientowanego na ekologiczne wykorzystanie zasobów; (ZK) praktyki ograniczające wykorzystanie zasobów przez oprogramowanie; (ZK) wpływ przestarzałego oprogramowania na środowisko	(ZK) wpływ architektury oprogramowania na zużycie zasobów i efektywność energetyczną; (ZK) metody pomiaru i monitorowania zużycia zasobów przez oprogramowanie; (ZK) zasady reinżynierii przestarzałych systemów IT, w tym możliwości wykorzystania AI, w celu zmniejszenia niekorzystnego wpływu na środowisko	(ZK) zasady projektowania docelowych architektur aplikacyjnych z uwzględnieniem celów zrównoważonego rozwoju w skali organizacji; (ZK) zaawansowane podejścia do modernizacji i reinżynierii przestarzałych systemów IT w celu ochrony środowiska oraz rolę AI w tym procesie; (ZK) ekonomiczne i ekologiczne aspekty decyzji dotyczących architektury i rozwoju oprogramowania	(ZK) najnowsze podejścia, w tym AI, w automatycznej analizie, generowaniu i modernizacji oprogramowania pod kątem zrównoważonego rozwoju; (ZK) wpływ aktualnych regulacji, standardów oraz wymagań rynkowych na rozwój metod i narzędzi zrównoważonego wytwarzania oprogramowania

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
	potrafi…	Oprogramowanie w Green IT		(ZK) używać i konfigurować aplikacje w sposób ograniczający zużycie zasobów; (ZK) stosować zasady zrównoważonego rozwoju w korzystaniu z oprogramowania (np. optymalne korzystanie z usług w chmurze); (ZK) rozpoznać podstawowe problemy wydajnościowe i nadmierne zużycie zasobów przez oprogramowanie	(ZK) analizować proste aplikacje lub usługi pod kątem zużycia zasobów mających wpływ na środowisko; (ZK) stosować podstawowe praktyki Green Coding w rozwijanym oprogramowaniu; (ZK) uczestniczyć w zadaniach optymalizacyjnych, proponując zmiany konfiguracji lub funkcjonalności zmniejszające zużycie zasobów	(ZK) projektować i implementować komponenty architektury oprogramowania z uwzględnieniem wymagań zrównoważonego rozwoju; (ZK) konfigurować i wykorzystywać narzędzia monitoringu aplikacyjnego do identyfikacji oprogramowania wymagającego optymalizacji pod kątem zrównoważonego rozwoju; (ZK) uczestniczyć w reinżynierii przestarzałych systemów IT z możliwością wykorzystania AI, w celu zmniejszenia niekorzystnego wpływu na środowisko	(ZK) projektować architektury oprogramowania i aplikacje z uwzględnieniem efektywności zasobowej oraz celów zrównoważonego rozwoju; (ZK) prowadzić programy optymalizacji i modernizacji oprogramowania, w tym inicjatywy reinżynierii przestarzałych systemów IT z możliwością wykorzystania AI, w celu zmniejszenia niekorzystnego wpływu na środowisko; (ZK) definiować metryki i mechanizmy zarządcze oraz integrować je z procesami wytwarzania i utrzymania oprogramowania dla zrównoważonego rozwoju	(ZK) projektować i prowadzić nowatorskie badania oraz programy rozwojowe dotyczące zrównoważonego wytwarzania i ekologicznej eksploatacji oprogramowania; (ZK) współtworzyć nowe wzorce, standardy, wytyczne i polityki dotyczące zrównoważonego oprogramowania oraz aktywnie budować środowiska eksperckie i sieci współpracy w obszarze ekosystemów cyfrowych

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
XII. Komunikacja, współpraca, przywództwo	jest gotów do…	**Komunikacja i współpraca w zespole IT**	stosowania ustalonych zasad komunikacji w zespole IT; współpracy z innymi członkami zespołu IT pod nadzorem osoby bardziej doświadczonej; informowania przełożonego/ członków zespołu IT o napotkanych problemach technicznych	jasnego przekazywania informacji do członków zespołu IT o postępach prac oraz doprecyzowywania zakresu swoich zadań; rzetelnego i terminowego informowania zespołu o stanie działania usług informatycznych; korzystania z podstawowej anglojęzycznej dokumentacji technicznej i narzędzi IT	pomocy innym członkom zespołu IT w realizacji zadań oraz rozwiązywaniu problemów technicznych; prowadzenia komunikacji technicznej po angielsku w międzynarodowym zespole informatycznym	angażowania członków zespołu IT w powierzone im zadania; uczestniczenia w budowaniu skutecznej komunikacji w zespołach IT; **(ZK) współpracy z użytkownikami i zespołami w zakresie wdrażania zasad Green IT**	wdrażania standardów komunikacji oraz współpracy zespołowej IT w organizacji; radzenia sobie z konfliktami, eskalacjami oraz rozbieżnymi oczekiwaniami w zespołach IT oraz w relacjach z użytkownikami i klientami; reprezentowania i promowania zespołu IT wewnątrz organizacji; **(ZK) promowania ekologicznych praktyk IT wewnątrz organizacji**	kształtowania nowatorskich standardów komunikacji oraz wielozespołowej współpracy w ramach ekosystemu cyfrowego
		Komunikacja w IT z użytkownikami i klientami	uprzejmego i rzeczowego kontaktu z użytkownikami i klientami w kontekście zgłoszeń dotyczących systemów i usług IT (pierwszy kontakt); przekazywania zgłoszeń/ problemów do odpowiednich osób lub zespołów IT	przekazywania informacji zwrotnych dotyczących statusu zgłoszeń, zmian lub rozwiązań IT; samodzielnego komunikowania się z użytkownikami i klientami w celu wyjaśniania podstawowych rozwiązań IT	opisywania wymagań użytkowników i klientów wobec systemów oraz usług IT w sposób jednoznaczny i zrozumiały dla zespołów technicznych; pośredniczenia w komunikacji pomiędzy użytkownikami a zespołami IT; komunikowania się z dostawcami i podwykonawcami rozwiązań informatycznych	budowania i utrzymywania długofalowych relacji z kluczowymi użytkownikami i klientami korzystającymi z rozwiązań IT; weryfikacji wymagań funkcjonalnych rozwiązań informatycznych; prowadzenia anglojęzycznych prezentacji i negocjacji technicznych z klientami/ partnerami	reprezentowania jednostki IT w relacjach z zewnętrznymi podmiotami; wdrażania strategii komunikacji z użytkownikami i klientami w obszarze rozwiązań informatycznych; przejmowania odpowiedzialności za komunikację z użytkownikami i klientami w sytuacjach kryzysowych dotyczących systemów i usług IT	kreowania nowych strategii komunikacji z zewnętrznymi podmiotami w obszarze rozwiązań informatycznych; bieżącej współpracy z akcjonariuszami oraz kluczowymi jednostkami biznesowymi w celu planowania i aktualizacji architektur IT; reprezentowania organizacji w obszarze ekosystemów cyfrowych
		Dzielenie się wiedzą IT, mentoring i przywództwo zespołowe		aktywnego uczestniczenia w regularnych spotkaniach wymiany wiedzy zespołu IT; dzielenia się wiedzą dotyczącą stosowanych rozwiązań informatycznych; dokumentowania swojej pracy w sposób przyjęty w organizacji IT, umożliwiający jej wykorzystanie przez innych członków zespołu	inicjowania spotkań mających na celu wymianę wiedzy zespołu IT; zachęcania współpracowników w zespołach IT do dzielenia się wiedzą i doświadczeniem	prowadzenia szkoleń i warsztatów technicznych IT; precyzyjnego delegowania zadań w zespołach IT	pełnienia funkcji lidera zespołu IT z dostosowaniem stylu przywództwa i komunikacji; mentoringu i promowania dobrych praktyk w zakresie IT w organizacji	pełnienia funkcji autorytetu w obszarze rozwoju nowych kompetencji technicznych, mentoringu i przywództwa w sektorze IT; koordynowania aktualnych międzynarodowych form wymiany wiedzy w ekosystemach cyfrowych

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
XIII. Orientacja na użytkownika	jest gotów do…	**Obsługa użytkownika przez IT**	okazywania empatii, cierpliwości, uprzejmości i kultury osobistej w kontakcie z użytkownikiem, także w sytuacjach stresu, presji czasu lub frustracji po stronie użytkownika systemu IT	aktywnego słuchania użytkownika systemu IT i dopytywania, tak aby dobrze zrozumieć jego sytuację i realną potrzebę; dostosowywania stylu komunikacji i formy wsparcia IT do zróżnicowanych potrzeb użytkowników (np. mniej sprawnych pod względem technicznym, starszych, pracujących pod dużą presją czasu)	traktowania użytkowników systemów IT jako partnerów, bez obwiniania ich o błędy, pomyłki czy brak wiedzy technicznej	asertywnego reagowania na niewłaściwe zachowania lub nierealistyczne oczekiwania użytkowników systemów IT, przy zachowaniu szacunku i profesjonalnego tonu; wspierania użytkowników w nauce korzystania z systemów i usług cyfrowych w cierpliwy, życzliwy i niewywyższający się sposób	budowania i utrzymywania relacji z użytkownikami systemów IT opartych na zaufaniu i współpracy; tłumaczenia użytkownikom systemów IT celów wprowadzanych zmian w kontekście korzyści dla organizacji	
		Analiza potrzeb i dbałość o doświadczenie użytkownika systemów IT		angażowania się w poznawanie potrzeb, oczekiwań i ograniczeń użytkowników systemów IT, z uwzględnieniem osób z niepełnosprawnością i wykluczonych cyfrowo	uwzględniania perspektywy użytkownika systemu IT przy planowaniu i realizacji działań; przyjmowania opinii i krytyki użytkowników systemów IT jako źródła informacji służącego do poprawy doświadczenia użytkownika	współpracy z innymi osobami i zespołami w celu poprawy doświadczenia użytkownika systemu IT; dostrzegania zróżnicowania użytkowników i dążenia do ograniczania barier w korzystaniu z rozwiązań IT	budowania zaufania dla rozwiązań informatycznych poprzez uwzględnianie potrzeb użytkowników systemów IT w kontekście potrzeb organizacji	
XIV. Odpowiedzialność i etyka		**Etyka cyfrowa i odpowiedzialne wykorzystanie technologii**	postępowania zgodnie z regulacjami wewnętrznymi organizacji w zakresie IT; zgłaszania nieetycznych zachowań i nadużyć w środowisku cyfrowym, z zachowaniem zasad poufności i ochrony osób zgłaszających	postępowania zgodnie z regulacjami prawnymi dotyczącymi IT	uwzględniania perspektywy różnych grup użytkowników, w tym narażonych na wykluczenie cyfrowe; odpowiedzialnego i zgodnego z przeznaczeniem wykorzystania technologii IT; **(ZK) uwzględniania wpływu rozwiązań cyfrowych na środowisko i zrównoważony rozwój**	współpracy z innymi osobami i zespołami IT w celu identyfikowania ryzyk etycznych oraz wypracowywania odpowiedzialnych rozwiązań technologicznych; promowania kultury odpowiedzialnego korzystania z technologii IT w swoim środowisku pracy	stawiania etycznych granic przy wykorzystaniu technologii IT, także w sytuacjach presji biznesowej; zaangażowania się w działania edukacyjne i informacyjne dotyczące etyki cyfrowej; **(ZK) podejmowania działań i dobierania technologii IT ograniczających negatywny wpływ na środowisko**	podejmowania nowatorskich działań w zakresie ochrony społeczeństwa przed nieetycznymi skutkami wykorzystania technologii IT
		Dbałość o bezpieczeństwo informacji		dbania o bezpieczeństwo informacji, a w szczególności jej integralność, poufność i dostępność w systemach IT; poszanowania prywatności użytkowników systemów IT	uwzględniania aspektów bezpieczeństwa informacji i prywatności przy podejmowaniu codziennych decyzji w środowisku cyfrowym; uwzględniania potrzeb osób szczególnie narażonych na naruszenia prywatności w środowisku cyfrowym	współpracy w środowisku cyfrowym w celu eliminowania ryzyk związanych z bezpieczeństwem informacji, ochroną danych i prywatności	przyjmowania odpowiedzialności za przyczyny i skutki niewłaściwego wykorzystania informacji i danych cyfrowych	

WYZNACZNIK		WIĄZKA	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
XIV. Odpowiedzialność…	jest gotów do…	**Samodzielność i odpowiedzialność za realizację zadań**	korzystania z wiedzy doświadczonych specjalistów IT; przestrzegania ustalonych instrukcji i procedur IT przy wykonywaniu zadań	samodzielnego planowania i realizacji własnych zadań zgodnych z ustalonym zakresem w środowisku cyfrowym	przyjmowania odpowiedzialności za realizację własnych zadań lub projektów IT	przyjmowania odpowiedzialności za realizację zadań zespołowych oraz jakość dostarczanych rozwiązań IT	ponoszenia odpowiedzialności za skutki podejmowanych decyzji w obszarze systemów i usług IT	ponoszenia odpowiedzialności za aktualne i długoterminowe skutki strategicznych decyzji dotyczących systemów i usług IT
XV. Rozwój i innowacyjność		**Rozwój własny i adaptacja do zmian technologicznych**	przyjmowania prostych wskazówek dotyczących usprawnienia swojej pracy w środowisku IT	przyjmowania informacji zwrotnej na temat swojej pracy i wykorzystywania jej do rozwoju kompetencji IT; uczenia się na błędach oraz otwartego mówienia o nich w sposób sprzyjający wyciąganiu wniosków w środowisku cyfrowym	otwartego komunikowania swoich potrzeb rozwojowych w zakresie IT; zachowania elastyczności w obliczu zmian organizacyjnych, procesowych i technologicznych w środowisku cyfrowym	aktywnego poszukiwania nowych rozwiązań, narzędzi i praktyk w środowisku IT oraz umiejętnego ich selekcjonowania i oceniania przydatności; wychodzenia poza swoją strefę komfortu i podejmowania się nowych zadań związanych z różnorodnymi technologiami IT	tworzenia kierunków adaptacji współpracowników do zmian technologicznych w środowisku cyfrowym; dzielenia się sposobami uczenia się i doświadczeniami z pracy z nowymi technologiami IT	inicjowania nowatorskich działań sprzyjających ciągłemu rozwojowi i eksperymentowaniu z nowymi technologiami w ekosystemie cyfrowym
		Tworzenie i wspieranie innowacji cyfrowych		współpracy przy testowaniu usprawnień w systemach IT	zgłaszania pomysłów na usprawnienia procesów wykorzystujących systemy IT; zachęcania współpracowników do eksperymentowania z nowymi rozwiązaniami i narzędziami IT	aktywnego uczestnictwa w inicjatywach na usprawnienia procesów wykorzystujących systemy IT; **(ZK) wspierania inicjatyw zrównoważonego rozwoju w organizacji**	wspierania cyfrowej kultury organizacji opartej na ciągłym doskonaleniu, eksperymentowaniu i uczeniu się; współpracy w interdyscyplinarnym zespole wspierającym innowacje cyfrowe; **(ZK) rekomendowania innowacyjnych rozwiązań IT z uwzględnieniem aspektów środowiskowych**	wspierania i pełnienia funkcji lidera w nowatorskich transformacjach w skali ekosystemu cyfrowego; tworzenia interdyscyplinarnych zespołów wspierających innowacje cyfrowe

5. Słownik pojęć stosowanych w Sektorowej Ramie Kwalifikacji dla Informatyki (SRK IT)

POJĘCIE	DEFINICJA
ABAC (ang. *attribute-based access control*) – model kontroli dostępu oparty na atrybutach	Model kontroli dostępu oparty na atrybutach, w którym decyzje o przyznaniu dostępu podejmowane są na podstawie zestawu cech opisujących: użytkownika, zasób, środowisko, działanie. System ABAC analizuje te atrybuty w czasie rzeczywistym i stosuje zdefiniowane polityki, aby określić, czy dany dostęp jest dozwolony.
ACL (ang. *access control list*) – lista kontroli dostępu	Mechanizm definiowania, kto i do czego ma prawo dostępu w systemie lub sieci. Lista reguł, które określają, jakie operacje (np. odczyt, zapis, połączenie sieciowe z danego adresu) są dozwolone lub blokowane dla określonych użytkowników, grup, adresów czy usług. W praktyce stosowana m.in. w systemach operacyjnych, na zaporach sieciowych i przełącznikach do egzekwowania polityk bezpieczeństwa.
AD (ang. *active directory*)	Usługi katalogowe Microsoft do centralnego zarządzania użytkownikami, komputerami i zasobami w sieciach opartych na Windows (odpowiednik LDAP).
Administracja IT (ang. *IT administration*)	Praktyczny i operacyjny aspekt zarządzania technologią w organizacji. Polega na bieżącym utrzymaniu, konfiguracji, monitorowaniu i zarządzaniu infrastrukturą IT w celu zapewnienia jej stabilnego, bezpiecznego i efektywnego działania.
Agent AI (ang. *artificial intelligence agent*) – agent sztucznej inteligencji	Komponent systemu informatycznego wykorzystujący metody sztucznej inteligencji do samodzielnego realizowania celu poprzez planowanie kroków, podejmowanie decyzji i wykonywanie akcji w środowisku (np. wywoływanie narzędzi, korzystanie z interfejsów API, uruchamianie procedur). Agent AI może utrzymywać kontekst zadania (stan), stosować reguły bezpieczeństwa i kontrolę uprawnień oraz realizować zadania w sposób częściowo autonomiczny pod nadzorem człowieka.

Agile	Zbiór zasad i praktyk zarządzania wytwarzaniem oprogramowania oraz rozwojem produktów oparty na iteracyjnym dostarczaniu przyrostów, ścisłej współpracy z interesariuszami i szybkim reagowaniu na zmiany wymagań. Agile kładzie nacisk na krótkie cykle planowania i realizacji, ciągłą inspekcję i adaptację oraz budowanie wartości biznesowej małymi krokami o dużej częstotliwości.
Agile Waterfall Hybrid	Sposób prowadzenia przedsięwzięcia, w którym część zakresu lub strumieni prac jest realizowana w metodykach zwinnych (np. Scrum, Kanban), a część w podejściu kaskadowym, z koordynacją na poziomie wspólnego planu i punktów integracyjnych. Wymaga zdefiniowanych interfejsów między zespołami, uzgodnienia sposobu raportowania postępu oraz spójnego zarządzania ryzykiem i zakresem w obu stylach pracy.
AI TRiSM (ang. *AI trust, risk and security management*) – zarządzanie zaufaniem, ryzykiem i bezpieczeństwem AI	IT TRiSM oznacza systemy AI, które są odporne na awarie (bezpieczeństwo), działają zgodnie z prawem (zgodność) i pozwalają na pełną kontrolę ich decyzji (audytowalność).
Aktualizacje oprogramowania	Proces wprowadzania uaktualnień (ang. *update*), poprawek (ang. *patch*) lub ulepszeń (ang. *upgrade*) do istniejącego programu, systemu operacyjnego lub aplikacji. Celem jest naprawa błędów, zwiększenie bezpieczeństwa, poprawa wydajności lub dodanie nowych funkcji. Brak regularnych aktualizacji sprawia, że oprogramowanie staje się podatne na ataki hakerskie i niefunkcjonalne.
Aktuatory (ang. *actuators*) – elementy wykonawcze	Urządzenia wykonawcze przekształcające sygnał sterujący z układu sterownika na działanie fizyczne w obiekcie, np. otwarcie/zamknięcie zaworu, zmianę położenia siłownika, uruchomienie napędu. Aktuatory są końcowym elementem toru sterowania – realizują zmiany w procesie technologicznym zgodnie z decyzjami układu sterowania.

Aktywa cyfrowe (ang. *digital assets*)	Zasoby mające wartość dla organizacji lub osoby, istniejące wyłącznie w postaci elektronicznej. Obejmują m.in. pliki danych, bazy danych, oprogramowanie, konta w usługach, klucze kryptograficzne, tokeny w rozproszonych rejestrach oraz inne zapisy, które mogą być przedmiotem obrotu, licencjonowania lub wymagają ochrony. W zarządzaniu bezpieczeństwem traktuje się je jako aktywa, dla których określa się właściciela, wartość, wymagany poziom ochrony i cykl życia.
Ansible	Narzędzie do automatyzacji i orkiestracji konfiguracji infrastruktury oraz wdrażania aplikacji, rozwijane przez Red Hat. Pozwala deklaratywnie opisywać pożądany stan systemów (serwerów, usług, kontenerów, urządzeń sieciowych) w plikach tekstowych oraz masowo konfigurować je za pomocą zadań wykonywanych z serwera sterującego. Szeroko stosowane w zarządzaniu konfiguracją, powtarzalnych wdrożeniach i podejściu „infrastruktura jako kod". Zmniejsza liczbę ręcznych operacji i ryzyko błędów konfiguracyjnych.
Antywzorce projektowe/ architektoniczne (ang. *antipatterns*)	W architekturze IT lub inżynierii oprogramowania pojęcie opisujące rozwiązania powtarzalne, nieskuteczne lub nieproduktywne, które na pozór wydają się sensowne, ale w praktyce prowadzą do złych rezultatów, wysokiego długu technicznego i trudności w utrzymaniu systemu. Antywzorce opisują typowe błędy podczas podejmowania decyzji architektonicznych (np. nadmierne sprzężenie komponentów systemu, brak separacji odpowiedzialności w kodzie oprogramowania, skupianie zbyt wielu funkcji systemu przez pojedynczą klasę lub moduł, uzależnienie od dostawcy czy kod oprogramowania o chaotycznej strukturze) oraz konsekwencje tych decyzji i sposoby ich unikania lub eliminowania.
AP (ang. *access point*) – punkt dostępowy sieci bezprzewodowej	Urządzenie sieciowe, które łączy sieć przewodową z siecią bezprzewodową i umożliwia urządzeniom Wi-Fi dołączanie do sieci lokalnej. Punkt dostępowy realizuje funkcje nadawania i odbioru sygnału radiowego, uwierzytelniania użytkowników oraz egzekwowania podstawowych polityk bezpieczeństwa i jakości obsługi dla ruchu bezprzewodowego.

API (ang. *application programming interface*) – interfejs programowania aplikacji	Zbiór zasad i specyfikacji umożliwiających komunikację i wymianę danych między różnymi aplikacjami lub systemami. Pełni funkcję pośrednika, pozwalając na wymianę danych między różnymi systemami i platformami, bez konieczności ich bezpośredniej integracji. Dzięki API można budować nowe aplikacje, korzystając z już istniejących usług i danych.
API first (ang. *API-first approach*) – podejście „najpierw API"	Podejście do wytwarzania systemów, w którym punkt wyjścia stanowi interfejs API (zakres operacji, formaty danych, błędy, wersjonowanie i zasady bezpieczeństwa), a dopiero potem implementuje się usługi i integracje. Celem jest spójność integracji, możliwość równoległej pracy zespołów (backend, frontend, integracje) oraz lepsza kontrola zmian poprzez formalne zarządzanie cyklem życia API.
API management – zarządzanie interfejsami API	Zestaw procesów, narzędzi i komponentów służących do projektowania, publikowania, zabezpieczania, wersjonowania, monitorowania i rozliczania użycia interfejsów API. Obejmuje m.in. bramy API, katalogi API, mechanizmy uwierzytelniania i autoryzacji, limity wywołań, analitykę ruchu oraz cykl życia API (od projektowania do wycofania), tak aby integracje między systemami były kontrolowane, bezpieczne i mierzalne.
Aplikacja cloud native	Oprogramowanie zaprojektowane i zbudowane od podstaw z myślą o wykorzystaniu elastyczności, skalowalności i dynamiczności środowiska chmurowego. Działa z wykorzystaniem mikrousług, konteneryzacji i orkiestracji do tworzenia odpornych, automatycznie skalujących się systemów, które szybko dostarczają wartość biznesową.
Application Plane – płaszczyzna aplikacji	Warstwa logiki aplikacyjnej, w której działają programy korzystające z sieci (np. aplikacje zarządzające, systemy orkiestracji, systemy bezpieczeństwa) i opisujące „intencję" – co sieć ma robić. Płaszczyzna aplikacji komunikuje się z płaszczyzną sterowania za pomocą interfejsów (np. API), przekazując polityki i wymagania biznesowe, natomiast nie zajmuje się fizycznym przełączaniem pakietów.

AR (ang. *augmented reality*) – rzeczywistość rozszerzona	Technologia polegająca na nakładaniu cyfrowych informacji (np. grafiki, tekstu, modeli 3D, wskazówek kontekstowych) na obraz świata rzeczywistego postrzegany przez użytkownika, w czasie rzeczywistym. AR wykorzystuje sensory i algorytmy pozycjonowania oraz rozpoznawania otoczenia, aby osadzić elementy wirtualne w odpowiednim miejscu i skali, wspierając m.in. szkolenia, serwis, nawigację i wizualizację danych w środowisku fizycznym.
ArchiMate	Otwarty, niezależny język modelowania stworzony do opisywania, analizowania i wizualizowania architektury korporacyjnej. Łączy w spójny sposób domeny: biznesową, danych, aplikacji i technologii, wspierając zarządzanie złożonymi zmianami w przedsiębiorstwie na różnych poziomach szczegółowości.
Architektura aplikacji (ang. *application architecture*)	Struktura logiczna systemu określająca sposób, w jaki są zorganizowane jego komponenty, jak ze sobą współdziałają i jak wspierają cele biznesowe poprzez zapewnienie skalowalności, łatwości utrzymania oraz wydajności. Definiuje podział na warstwy (np. prezentacji, logiki biznesowej, danych) i wzorce integracji. Ułatwia rozwój, testowanie i zarządzanie systemem.
Architektura biznesowa (ang. *business architecture*)	Kompleksowe podejście do opisu organizacji definiujące jej strategiczne cele, procesy, strukturę, zdolności oraz przepływy wartości. Tworzy spójny plan dopasowujący operacje do strategii, umożliwiając lepsze zarządzanie, planowanie i wdrażanie zmian. Łączy biznes z technologią, zapewniając efektywne funkcjonowanie przedsiębiorstwa.
Architektura danych (ang. *data architecture*)	Ogólny plan i model definiujący sposób gromadzenia, przechowywania, integrowania, zarządzania i wykorzystywania danych w organizacji. Tworzy spójny system wspierający cele biznesowe, zapewniając spójność i dostępność informacji, a także zarządzając cyklem życia danych.
Architektura IT	Zestaw zasad, struktur i komponentów technologicznych (sprzęt, oprogramowanie, dane) definiujących sposób działania i współdziałania systemów informatycznych w organizacji. Prawidłowa architektura IT zapewnia spójność na wszystkich poziomach i wsparcie realizacji celów biznesowych. Jest to całościowy projekt systemu obejmujący jego organizację, relacje między elementami, środowisko i reguły rozwoju zapewniające bezpieczne, skalowalne oraz efektywne fundamenty dla technologii.

Architektura korporacyjna (ang. *enterprise architecture*)	Formalny opis struktury i funkcji organizacji, obejmujący biznes, dane, aplikacje i technologię. Jego celem jest zapewnienie spójności, efektywności i wsparcia realizacji celów strategicznych poprzez mapowanie powiązań, ustalanie wytycznych i zarządzanie zmianami w złożonym środowisku. Jest pomostem pomiędzy biznesem a IT pomagającym unikać błędów i podejmować lepsze decyzje technologiczne.
Architektura technologii i systemów krytycznych	Strategiczny plan i struktura opisująca współpracę systemów, danych, sprzętu, oprogramowania i procesów w organizacji z uwzględnianiem systemów krytycznych niezbędnych do pracy organizacji. Jest kluczowa dla stabilnej pracy oraz zarządzania złożonością i skalowalnością systemów IT.
Architektury serverless	Architektury bezserwerowe (model chmurowy), w których deweloperzy piszą kod aplikacji, a dostawca chmury zajmuje się infrastrukturą serwerową, automatycznym skalowaniem i zarządzaniem. Klient płaci tylko za rzeczywiste użycie funkcji.
Arkusze kontrolne procesów (ang. *process control sheets*)	Strukturyzowane formularze lub szablony zawierające listy pytań, kryteriów i punktów kontrolnych służących do oceny, czy dany proces jest wykonywany zgodnie z przyjętymi procedurami, wymaganiami jakościowymi i regulacyjnymi. Wykorzystywane w audytach, przeglądach i monitoringu procesów do systematycznego dokumentowania wyników kontroli oraz identyfikowania niezgodności i obszarów do usprawnień.
ARP (ang. *address resolution protocol*) – protokół odwzorowania adresów	Mechanizm sieciowy służący do ustalania, jaki adres sprzętowy interfejsu sieciowego (adres fizyczny karty sieciowej) odpowiada danemu adresowi IP w sieci lokalnej. Umożliwia urządzeniom komunikację poprzez znalezienie adresu sprzętowego karty sieciowej jedynie na podstawie jej adresu IP, co jest niezbędne do przesyłania ramek do właściwego odbiorcy w tej samej sieci.
AS-IS	Model analizy procesów biznesowych opisujący stan istniejący komponentów i ich relacji, „wąskie gardła" (stan wyjściowy projektu).

AV (ang. *autonomous vehicle*) – pojazd autonomiczny	Pojazd wyposażony w systemy percepcji, lokalizacji i podejmowania decyzji, zdolny do samodzielnego wykonywania zadań polegających na prowadzeniu w określonych warunkach ruchu. Wykorzystuje dane z sensorów (np. kamery, radar, lidar) oraz algorytmy sterowania do utrzymania toru jazdy, rozpoznawania przeszkód i planowania manewrów, przy ograniczonym lub zerowym udziale kierowcy, zależnie od poziomu autonomii.
AWS (ang. *Amazon Web Services*) – platforma usług chmurowych firmy Amazon	Udostępnia zasoby obliczeniowe, pamięć masową, bazy danych, usługi sieciowe, bezpieczeństwa i analityki. Umożliwia budowanie i uruchamianie systemów IT bez konieczności zakupu własnej infrastruktury, na podstawie modelu usług rozliczanych za wykorzystane zasoby.
Azure (ang. *Microsoft Azure*) – platforma usług chmurowych firmy Microsoft	Udostępnia zasoby obliczeniowe, przestrzeń dyskową, bazy danych, usługi integracyjne oraz rozwiązania z zakresu bezpieczeństwa i zarządzania tożsamością. Często wykorzystywana do uruchamiania aplikacji biznesowych oraz integracji z produktami z rodziny Microsoft (np. Windows Server, Active Directory, usługi biurowe).
Bash (ang. *bourne again shell*)	Powłoka systemowa używana głównie w systemach z rodziny Unix (Linux, macOS). Umożliwia interaktywne wykonywanie poleceń oraz automatyzację zadań za pomocą skryptów powłoki (np. instalacja oprogramowania, przetwarzanie plików, operacje na systemie). Jest *de facto* standardową powłoką w większości dystrybucji Linuksa i podstawowym narzędziem administratorów oraz inżynierów DevOps.
BCI (ang. *brain--computer interface*) – interfejs mózg–komputer	Technologia umożliwiająca komunikację pomiędzy aktywnością układu nerwowego a systemem komputerowym, w której sygnały biologiczne (np. elektryczna aktywność mózgu) są rejestrowane, przetwarzane i tłumaczone na komendy sterujące urządzeniami lub aplikacjami. BCI może działać w trybie nieinwazyjnym lub inwazyjnym i jest wykorzystywany m.in. w rehabilitacji, wspomaganiu osób z niepełnosprawnościami oraz w systemach sterowania i interakcji człowiek–maszyna.

BCP (ang. *business continuity plan*) – plan ciągłości działania	Dokument mający znaczenie strategiczne, określający procedury i instrukcje pozwalające organizacji kontynuować lub szybko wznowić krytyczne funkcje biznesowe w przypadku poważnych zakłóceń. Plan BCP wykracza poza zwykłe reagowanie na incydenty, stanowiąc usystematyzowane podejście do budowania odporności organizacyjnej na różnorodne zagrożenia i sytuacje kryzysowe. BCP koncentruje się na utrzymaniu ciągłości operacyjnej całej organizacji, a nie tylko systemów IT czy pojedynczych procesów.
BGP (ang. *border gateway protocol*) – protokół bramy granicznej	Protokół bramy granicznej jest używany do wymiany informacji o trasach pomiędzy systemami autonomicznymi w Internecie. BGP umożliwia wybór ścieżek na podstawie polityk routingu (np. preferencji operatora), a nie wyłącznie metryk technicznych, dzięki czemu wspiera kontrolę przepływu ruchu, redundancję połączeń oraz zapewnianie dostępności usług w skali globalnej.
BHP – Bezpieczeństwo i Higiena Pracy	Zbiór zasad, procedur i wymagań organizacyjno-technicznych służących do zapewnienia bezpiecznych warunków pracy oraz ograniczania ryzyka wypadków i chorób zawodowych. BHP obejmuje m.in. identyfikację zagrożeń, ocenę ryzyka, stosowanie środków ochrony, szkolenia, instrukcje stanowiskowe oraz nadzór nad przestrzeganiem przepisów i standardów bezpieczeństwa pracy.
BI (ang. *business intelligence*) – analityka biznesowa/ inteligencja biznesowa	Zestaw metod, procesów i narzędzi służących do przekształcania danych operacyjnych w informacje wykorzystywane do podejmowania decyzji w organizacji. Obejmuje m.in. hurtownie danych, procesy integracji i przetwarzania danych, raportowanie, kokpity menedżerskie oraz analizy wielowymiarowe zorientowane na wsparcie zarządzania i kontroli realizacji celów.
Bias	Stronniczość danych lub modelu polegająca na systematycznym, powtarzalnym odchyleniu w danych, modelu lub procedurze analitycznej, prowadzącym do zniekształconych wyników, np. faworyzowania lub dyskryminowania określonych grup, błędnego szacowania ryzyka albo jakości. Bias może wynikać m.in. z niepełnych lub nierównomiernych danych treningowych, sposobu etykietowania, doboru cech, konstrukcji algorytmu lub samego procesu zbierania danych i jest kluczowym zagadnieniem przy projektowaniu i ocenie systemów opartych na danych i sztucznej inteligencji.

Big data – dane masowe	Zbiory danych o tak dużej skali, szybkości napływu i różnorodności, że ich przetwarzanie klasycznymi narzędziami bazodanowymi jest nieefektywne lub niemożliwe. Obejmują dane strukturalne, częściowo strukturalne i niestrukturalne, wymagają rozproszonych platform przetwarzania, specjalistycznych narzędzi analitycznych oraz zautomatyzowanych procesów przetwarzania w celu wydobycia wartości biznesowej.
Blockchain – łańcuch bloków	Model rozproszonego rejestru, w którym zdarzenia (np. transakcje) są grupowane w bloki powiązane ze sobą kryptograficznie w uporządkowany łańcuch. Kopie rejestru są utrzymywane przez wiele węzłów sieci, a spójność danych zapewnia mechanizm konsensusu. Cechą blockchaina jest odporność na nieautoryzowane modyfikacje historycznych zapisów oraz możliwość weryfikacji stanu rejestru przez wszystkich uczestników zgodnie z przyjętymi regułami protokołu.
BPMN (ang. *business process model and notation*) – notacja modelowania procesów biznesowych	Standardowa notacja graficzna służąca do modelowania procesów biznesowych w postaci diagramów opisujących kroki procesu, zdarzenia, decyzje, role i przepływy pracy. Zapewnia wspólny język opisu procesów dla biznesu i IT, wykorzystywany do analizy, optymalizacji oraz automatyzacji procesów w organizacji.
BSS (ang. *basic service set*) – podstawowy zestaw usług sieci bezprzewodowej	Najprostsza logiczna jednostka sieci Wi-Fi; pojedynczy punkt dostępowy oraz podłączone do niego urządzenia klienckie współdzielące tę samą przestrzeń radiową. Taki zestaw tworzy jedną komórkę sieci bezprzewodowej, w obrębie której realizowana jest komunikacja.
BYOD (ang. *bring your own device*)	Polityka firmowa, która pozwala pracownikom na używanie własnych prywatnych urządzeń (smartfonów, tabletów, laptopów) do celów służbowych, takich jak dostęp do firmowych e-maili, danych i aplikacji, zamiast polegania wyłącznie na sprzęcie dostarczonym przez pracodawcę. Wymaga wdrożenia ścisłych zasad bezpieczeństwa (polityka BYOD) i oddzielenia przestrzeni prywatnej od służbowej.

C4	Metoda wizualizacji architektury oprogramowania systemu na czterech poziomach: ▪ Context (kontekst) – użytkownicy i systemy, ▪ Containers (kontenery) – aplikacje, bazy danych, serwisy, ▪ Components (komponenty) – logiczne grupy kodu wewnątrz kontenera, ▪ Code (kod) – implementacja, klasy, interfejsy.
Cache (ang. *cache memory*) – pamięć podręczna	Bardzo szybka tymczasowa pamięć w urządzeniach elektronicznych lub oprogramowaniu, która przechowuje często używane dane. Pozwala to na ich wykorzystywanie bez konieczności każdorazowego pobierania, co znacząco przyspiesza ładowanie stron i ogólne działanie systemu.
Canva	Platforma do projektowania grafiki w chmurze, dostępna przez przeglądarkę lub aplikację, służąca do tworzenia prostych projektów graficznych, takich jak: prezentacje, materiały marketingowe, grafiki do mediów społecznościowych czy proste infografiki. Udostępnia gotowe szablony, bibliotekę elementów graficznych oraz mechanizmy współpracy zespołowej ukierunkowane na użytkowników nietechnicznych.
Carbon Aware Computing – przetwarzanie uwzględniające ślad węglowy	Podejście do projektowania i eksploatacji systemów IT, w którym planowanie i uruchamianie obciążeń obliczeniowych uwzględnia aktualną lub prognozowaną emisyjność energii elektrycznej. Polega na sterowaniu czasem i miejscem wykonywania zadań (np. przesuwanie wsadów obliczeniowych, dobór regionu centrum danych, priorytetyzacja zadań) w celu ograniczenia emisji przy zachowaniu wymaganych parametrów jakości usług.
CDN (ang. *content delivery network*) – sieć dostarczania treści	Rozproszona geograficznie sieć serwerów pośredniczących, która przechowuje kopie treści (np. pliki statyczne, wideo, zasoby stron www) bliżej użytkowników końcowych. Minimalizuje opóźnienia i obciążenie serwerów źródłowych, zwiększa dostępność usług oraz umożliwia stosowanie dodatkowych mechanizmów bezpieczeństwa na brzegu sieci.

Certyfikacja dostawców	Proces potwierdzania przez niezależną zewnętrzną stronę, że dany dostawca spełnia określone normy, standardy (np. jakości, bezpieczeństwa) lub wymagania prawne. Daje to kupującym pewność co do jego wiarygodności, kompetencji i tego, że działa zgodnie z przepisami, upraszczając jednocześnie weryfikację i wybór partnerów biznesowych.
Chmura	Zasoby IT (moc obliczeniowa, pamięć masowa, usługi sieciowe, bazy danych itp.) dostarczane zdalnie przez zewnętrznego dostawcę za pośrednictwem sieci, bez konieczności posiadania i utrzymywania własnej fizycznej infrastruktury.
Chmura hybrydowa (ang. *hybrid cloud*)	Model usług chmurowych, który integruje prywatną infrastrukturę chmurową z chmurą publiczną, tworząc jedno środowisko. Pozwala na elastyczne przenoszenie danych i aplikacji między chmurami i wykorzystanie zalet obu rozwiązań – elastyczności i skalowalności chmury publicznej oraz bezpieczeństwa i kontroli nad danymi chmury prywatnej.
Chmura prywatna (ang. *private cloud*)	Model usług chmurowych przeznaczonych wyłącznie dla jednej organizacji, zapewniający jej pełną kontrolę nad infrastrukturą, wysoką izolację danych i większe bezpieczeństwo w porównaniu do chmury publicznej. Prywatna chmura może być hostowana w lokalnym centrum danych lub przez zewnętrznego dostawcę.
Chmura publiczna (ang. *public cloud*)	Model usług chmurowych, w którym zewnętrzny dostawca udostępnia przez internet zasoby wielu klientom korzystającym ze współdzielonej infrastruktury. Główną cechą tego rozwiązania jest to, że to dostawca zarządza infrastrukturą i ją utrzymuje, a użytkownik płaci tylko za zużyte zasoby, które może elastycznie skalować.
CI/CD (ang. *continuous integration/ continuous delivery* lub *deployment*) – procedury i narzędzia usprawniające tworzenie oprogramowania	Automatyzują procesy budowania, testowania i wdrażania kodu, co umożliwia szybsze i bardziej niezawodne dostarczanie aktualizacji do użytkowników, eliminując ręczne etapy i błędy. CI (Continuous Integration) dotyczy częstej integracji zmian i ich testowania, CD (Continuous Delivery/Deployment) automatyzuje dostarczanie (Delivery) lub automatyczne wdrażanie (Deployment).

CKAN (ang. *comprehensive knowledge archive network*) – platforma katalogowania i publikacji danych	Oprogramowanie służące do budowy portali danych, w których publikuje się zbiory danych wraz z opisami, metadanymi, wersjami, licencjami i mechanizmami wyszukiwania. Ułatwia zarządzanie katalogiem danych (w tym otwartych), udostępnianie plików lub interfejsów dostępu oraz kontrolę jakości i spójności informacji o zbiorach danych.
Cloud bursting – „wybijanie" do chmury w szczycie obciążenia	Wzorzec wykorzystania chmury, w którym podstawowe obciążenie jest obsługiwane przez infrastrukturę własną lub podstawową, a w momentach szczytowego zapotrzebowania część zadań jest tymczasowo przenoszona do chmury publicznej. Pozwala to zwiększyć dostępną moc obliczeniową tylko na czas wzmożonego ruchu, bez stałego utrzymywania przewymiarowanej infrastruktury.
Cloud native – architektura natywna dla chmury	Podejście do projektowania i budowy aplikacji, które w pełni wykorzystuje zalety modelu obliczeń w chmurze, w przeciwieństwie do przenoszenia tradycyjnych aplikacji do chmury. Kluczowe filary podejścia cloud native to: mikrousługi (aplikacja podzielona jest na małe, niezależne moduły, które komunikują się ze sobą), konteneryzacja (pakowanie aplikacji wraz z jej środowiskiem uruchomieniowym), usługi zarządzane (korzystanie z gotowych usług bazy danych, kolejek czy pamięci podręcznej dostarczanych przez dostawcę chmury), automatyzacja (wdrażanie i aktualizacje odbywają się automatycznie) i skalowalność (aplikacja automatycznie dostosowuje zasoby do aktualnego ruchu). Zalety tego podejścia to wysoka dostępność (ang. *high availability*), odporność na awarie (ang. *resilience*), elastyczność i szybkość wdrożeń.
CMDB (ang. *configuration management database*) – baza danych zarządzania konfiguracją	Przechowuje szczegółowe informacje o zasobach IT organizacji, takich jak: sprzęt, oprogramowanie i usługi, a także definicje relacji między nimi. Stanowi kluczowe repozytorium wiedzy o elementach konfiguracji (ang. *configuration item*, CI).

COBIT (ang. *control objectives for information and related technologies*) – ramy ładu i zarządzania IT	Zestaw zasad, procesów i modeli odniesienia służących do projektowania i oceny ładu korporacyjnego oraz zarządzania obszarem IT w organizacji. COBIT pomaga powiązać cele biznesowe z celami IT, zdefiniować odpowiedzialności, mierniki, mechanizmy kontroli oraz wymagania dotyczące zgodności, tak aby technologie informacyjne wspierały strategię organizacji w sposób kontrolowany i audytowalny.
Control Plane – płaszczyzna sterowania	Warstwa odpowiedzialna za podejmowanie decyzji dotyczącej tego, jak powinien być kierowany ruch w sieci. Uruchamiane są w niej protokoły i mechanizmy budujące obraz topologii oraz wyznaczające trasy (np. protokoły trasowania), a następnie instalujące odpowiednie reguły w płaszczyźnie danych. W architekturach z centralnym sterowaniem płaszczyzna sterowania może być wyniesiona z urządzeń do zewnętrznego kontrolera, który zarządza wieloma przełącznikami jednocześnie.
CPU (ang. *central processing unit*) – jednostka centralna komputera (nazywana też procesorem)	Główny element komputera odpowiedzialny za wykonywanie instrukcji programów oraz przetwarzanie danych.
Cross-cloud – rozwiązania międzychmurowe	Model architektury i eksploatacji systemów, w którym jedna aplikacja lub usługa jest projektowana do równoczesnej pracy w więcej niż jednej chmurze różnych dostawców, z aktywną integracją pomiędzy tymi środowiskami. Obejmuje spójne zarządzanie ruchem, tożsamością, konfiguracją bezpieczeństwa oraz danymi w wielu chmurach, tak aby możliwe było kontrolowane przenoszenie obciążeń, redundancja usług i utrzymanie jednolitych polityk na poziomie całego środowiska.
Cyberbezpieczeństwo	Działania, polityki i procedury mające na celu utrzymanie ciągłości działania organizacji poprzez ochronę systemów, sieci, danych, ich użytkowników oraz innych podmiotów przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem oraz zdolności do odzyskiwania ciągłości działania po incydencie.

DAC (ang. *discretionary access control*) – uznaniowa kontrola dostępu	Model kontroli dostępu, w którym właściciel zasobu (np. pliku, katalogu, obiektu w systemie) może samodzielnie nadawać i odbierać uprawnienia innym użytkownikom lub grupom. Decyzje o dostępie wynikają z uprawnień ustawionych przez właściciela oraz mechanizmu dziedziczenia i list uprawnień w systemie, a nie z centralnie narzuconej polityki bezpieczeństwa.
dApps (ang. *decentralized applications*) – aplikacje zdecentralizowane	Aplikacje, których logika biznesowa jest oparta na infrastrukturze rozproszonego rejestru (np. blockchain), a część funkcji realizowana jest przez smart kontrakty. dApp wykorzystuje sieć węzłów do wykonywania operacji i przechowywania stanu, dzięki czemu nie jest zależna od pojedynczego, centralnego serwera, a reguły działania wynikają z kodu i protokołu sieci.
Dashboard – kokpit, tablica rozdzielcza	Narzędzie do wizualizacji danych w formie panelu lub interaktywnej strony. Prezentuje zagregowane dane kluczowe, metryki oraz wskaźniki wydajności z różnych źródeł w jednym miejscu, umożliwiając wygodne monitorowanie stanu, analizę trendów i podejmowanie decyzji.
Data Center – centrum danych	Wyspecjalizowany obiekt i infrastruktura techniczna przeznaczone do utrzymania systemów IT i usług cyfrowych, obejmujące m.in. serwery, sieć, pamięć masową oraz środowisko zapewniające ciągłość działania (zasilanie podstawowe i awaryjne, chłodzenie, monitoring, zabezpieczenia fizyczne). Centrum danych realizuje wymagania dostępności, pojemności i odporności na awarie, a także stanowi element architektury bezpieczeństwa organizacji (kontrola dostępu, segmentacja, rejestrowanie zdarzeń, procedury operacyjne).
Data Ethics Canvas – kanwa etyki danych	Ustrukturyzowany szablon analityczny służący do identyfikacji i oceny ryzyk etycznych związanych z pozyskiwaniem, przetwarzaniem i wykorzystywaniem danych oraz modeli analitycznych. Porządkuje analizę m.in. w obszarach: interesariusze i wpływ, źródła i jakość danych, uprzedzenia i nierówne skutki, przejrzystość, zgody i podstawy przetwarzania, bezpieczeństwo, odpowiedzialność oraz działania ograniczające ryzyka.

Data lake – jezioro danych	Centralne repozytorium, w którym gromadzi się duże ilości danych w postaci surowej – zarówno ustrukturyzowanych (tabele), częściowo ustrukturyzowanych (logi), jak i nieustrukturyzowanych (pliki, multimedia). Dane są zapisywane bez uprzedniego narzucania jednolitego schematu; sposób ich strukturyzacji i model danych definiuje się dopiero na etapie odczytu, na potrzeby konkretnej analizy, raportowania lub modelowania.
Data lakehouse – platforma łącząca jezioro danych i hurtownię danych	Architektura i platforma danych, która łączy sposób przechowywania danych typowy dla jeziora danych (magazyn surowych i półprzetworzonych danych w skalowalnej pamięci masowej) z mechanizmami charakterystycznymi dla hurtowni danych (warstwa tabel z gwarancjami transakcyjnymi, zarządzanie schematem, obsługa SQL i pracy analitycznej). Umożliwia wykonywanie analiz i modeli na wspólnej warstwie danych, bez konieczności budowania osobnych, zdublowanych magazynów.
Data Mesh – siatka domen danych	Model organizacji i architektury danych, w którym odpowiedzialność za dane jest rozproszona pomiędzy domeny biznesowe, a każda domena publikuje własne „produkty danych" zgodne z uzgodnionymi standardami. Zamiast jednej centralnej hurtowni lub jeziora danych stosuje się federacyjny model zarządzania, wspólną infrastrukturę współdzieloną i zestaw reguł jakości, bezpieczeństwa oraz interoperacyjności, egzekwowanych na poziomie całego środowiska danych.
Data Plane – płaszczyzna danych/ przełączania	Część urządzenia sieciowego odpowiedzialna za faktyczne przetwarzanie i przekazywanie pakietów zgodnie z już zainstalowanymi regułami. W płaszczyźnie danych wykonywane są operacje, takie jak: przekazanie na określony port, oznaczanie, filtrowanie czy kolejkowanie ruchu – bez podejmowania decyzji routingowych „od zera" dla każdego pakietu.
Data science – nauka o danych	Obszar nauki łączący metody statystyczne, uczenie maszynowe, programowanie i inżynierię danych w celu wydobywania wiedzy z danych oraz budowy modeli wspierających decyzje biznesowe lub techniczne. Obejmuje pełny cykl pracy z danymi: pozyskiwanie, przygotowanie, eksplorację, budowę i walidację modeli, a następnie wdrażanie ich do środowisk operacyjnych.

DDoS (ang. *distributed denial of service*) – rozproszony atak odmowy usługi	Rodzaj cyberataku, w którym bardzo duża liczba zainfekowanych urządzeń jednocześnie wysyła ruch do wybranej usługi lub systemu, przeciążając jego zasoby. Prowadzi to do niedostępności usługi dla uprawnionych użytkowników, często z wykorzystaniem sieci zainfekowanych urządzeń (botnetu).
Debian	Dystrybucja systemu operacyjnego z rodziny Linux, rozwijana jako projekt społecznościowy, znana z dużej stabilności i konserwatywnego podejścia do aktualizacji. Często wykorzystywana jako baza dla innych dystrybucji oraz w serwerowych środowiskach produkcyjnych.
Deduplikacja (ang. *deduplication* lub *data deduplication*)	Technologia eliminacji nadmiarowych powielonych kopii danych w systemie pamięci masowej. Używana szczególnie w systemach backupu i archiwizacji. Prowadzi do oszczędności miejsca na dysku oraz czasu transferu danych. Działa przez identyfikację unikalnych bloków lub fragmentów danych i przechowywanie tylko jednej ich kopii.
Deepfake – zaawansowana lub głęboka podróbka	Technologia wykorzystująca zaawansowane formy sztucznej inteligencji, która łączy głębokie uczenie (ang. *deep learning*) z fałszowaniem treści, umożliwiając tworzenie niezwykle realistycznych, lecz nieprawdziwych materiałów wideo, audio i zdjęć. Pozwala to na tworzenie iluzji w celu dezinformacji, oszustwa, ale czasami także rozrywki (np. tworzenie fałszywych wypowiedzi polityków, celebrytów, efekty specjalne w filmach). Technologia ta zaciera granicę między prawdą a fałszem, co utrudnia weryfikację informacji i może niszczyć reputację osób prywatnych.
Design thinking	Iteracyjne podejście do rozwiązywania problemów i projektowania produktów lub usług, oparte na dogłębnym zrozumieniu potrzeb użytkowników, generowaniu wielu koncepcji, szybkim prototypowaniu i testowaniu rozwiązań. Łączy perspektywę użytkownika, wykonalność techniczną i opłacalność biznesową w ramach uporządkowanych etapów pracy zespołu.
Dev/Ops	Połączenie angielskich słów Development (rozwój) i Operations (operacje) oznaczające zarówno kulturę organizacyjną i metodologię, jak i zestaw praktyk i narzędzi, których celem jest automatyzacja i integracja procesów między zespołami rozwoju oprogramowania i zespołami infrastruktury IT. Stosowanie DevOps ma na celu skrócenie cyklu rozwoju systemu, poprawia czas dostarczania, jakość i niezawodność tworzonego oprogramowania.

DevSecOps (ang. *Dev* (*development*) + *Sec* (*security*) + *Ops* (*operations*)	Ewolucja DevOps włączająca bezpieczeństwo (ang. *security*) jako integralny element w każdym etapie cyklu życia oprogramowania (ang. *software development life cycle*). Wprowadza zasadę „shift left" (przesuń w lewo), czyli działania związane z bezpieczeństwem muszą być zintegrowane jak najwcześniej – w fazie projektowania, kodowania i testowania – co pozwala wykrywać i usuwać nieprawidłowości, zanim spowodują powstawanie kosztów.
DHCP (ang. *dynamic host configuration protocol*) – protokół dynamicznej konfiguracji hosta	Protokół sieciowy służący do automatycznego przydzielania urządzeniom w sieci parametrów konfiguracyjnych, takich jak: adres IP, maska sieci, brama domyślna, adresy serwerów DNS oraz inne opcje. Centralizuje zarządzanie adresacją i ogranicza błędy ręcznej konfiguracji.
Diagramy Ishikawy (ang. *Ishikawa diagrams*) – diagramy przyczynowo-skutkowe	Diagramy analityczne w formie „szkieletu ryby", używane do identyfikacji i grupowania potencjalnych przyczyn wybranego problemu lub zjawiska. Główna „oś" reprezentuje problem, a „gałęzie" – grupy przyczyn (np. ludzie, metody, maszyny, materiały, środowisko, pomiary), co pozwala zespołom systematycznie analizować źródła nieprawidłowości i planować działania korygujące w procesach.
Diagramy procesów (ang. *process diagrams*)	Graficzne modele przedstawiające przebieg procesu biznesowego lub technicznego: kolejność czynności, decyzje, wejścia/wyjścia, role oraz przepływ informacji lub materiałów. Wykorzystywane do analizy, projektowania i optymalizacji procesów, często oparte na ustalonej notacji (np. notacji modelowania procesów biznesowych), co ułatwia komunikację między biznesem a IT.
Digital Twin – bliźniak cyfrowy	Cyfrowa reprezentacja obiektu fizycznego, systemu lub procesu, utrzymywana i aktualizowana na podstawie danych eksploatacyjnych (np. pomiarów, logów, telemetrii). Bliźniak cyfrowy umożliwia monitorowanie stanu, analizę zachowania w czasie, symulowanie scenariuszy zmian oraz prognozowanie skutków awarii i działań utrzymaniowych w sposób odzwierciedlający realne środowisko działania.

DKAN – platforma portalu danych otwartych	Oprogramowanie do budowy portalu danych otwartych, umożliwiające katalogowanie i publikowanie zbiorów danych wraz z metadanymi oraz interfejsami dostępu. DKAN jest rozwijany jako open source i jest dystrybuowany bez opłat licencyjnych (model „bez licencji/subskrypcji" dotyczy oprogramowania, nie danych).
DL (ang. *deep learning*) – uczenie głębokie	Podobszar uczenia maszynowego oparty na wielowarstwowych sieciach neuronowych, które automatycznie uczą się reprezentacji cech z danych wejściowych. Uczenie głębokie jest wykorzystywane m.in. w rozpoznawaniu obrazów i mowy, przetwarzaniu języka naturalnego oraz analizie sekwencji i sygnałów, zwykle przy dużych zbiorach danych i wysokim zapotrzebowaniu na moc obliczeniową.
DLC (ang. *direct liquid cooling*) – bezpośrednie chłodzenie cieczą	Technika odprowadzania ciepła z komponentów IT (np. procesorów, układów GPU) przy użyciu cieczy chłodzącej doprowadzonej bezpośrednio do elementów generujących ciepło, np. poprzez bloki chłodzące lub zanurzenie w dielektrycznej cieczy. Pozwala uzyskać większą gęstość mocy i lepszą efektywność energetyczną niż klasyczne chłodzenie powietrzem, co jest istotne zwłaszcza w nowoczesnych centrach danych o wysokiej gęstości upakowania sprzętu.
Dług technologiczny (ang. *technical debt*)	Termin z zakresu inżynierii oprogramowania będący metaforą opisującą negatywne skutki podejmowania w IT krótkoterminowych, mniej efektywnych decyzji (np. skrócenia testowania). W przyszłości decyzje takie generują dodatkowe koszty, pracę i utrudniają rozwój (analogicznie do długu finansowego, który wymaga spłaty odsetek).
DMZ (ang. *demilitarized zone*) – strefa zdemilitaryzowana	Wydzielony segment sieci umieszczany pomiędzy siecią publiczną a siecią wewnętrzną organizacji, przeznaczony do udostępniania usług dostępnych z zewnątrz (np. serwery www, bramy pocztowe). DMZ jest odseparowana regułami filtracji ruchu, tak aby ograniczyć możliwość bezpośredniego dostępu do zasobów wewnętrznych oraz zmniejszyć skutki ewentualnego kompromitowania usług wystawionych do internetu.
DNS (ang. *domain name system*) – system nazw domenowych	Hierarchiczny, rozproszony system usług sieciowych, który mapuje nazwy domenowe (np. google.com) na odpowiadające im adresy IP oraz inne rekordy (np. MX, TXT, SRV). Umożliwia użytkownikom i aplikacjom korzystanie z przyjaznych nazw zamiast adresów liczbowych. Stanowi krytyczny element infrastruktury internetu i częsty wektor ataków (np. *spoofing*, *cache poisoning*).

Docker	Platforma do tworzenia, pakowania i uruchamiania aplikacji w postaci kontenerów. Ujednolica środowisko uruchomieniowe (zależności, biblioteki, konfiguracje), co ułatwia przenoszenie aplikacji między systemami i automatyzację wdrożeń.
DoS (ang. *denial of service*) – atak odmowy usługi	Rodzaj cyberataku, którego celem jest uniemożliwienie prawidłowego działania usługi lub systemu poprzez przeciążenie go nadmierną liczbą żądań albo wykorzystanie błędów w oprogramowaniu. Skutkiem ataku jest niedostępność usługi dla uprawnionych użytkowników – system działa bardzo wolno, przestaje odpowiadać lub całkowicie odmawia obsługi kolejnych połączeń.
DR (ang. *disaster recovery*) – odzyskiwane po awarii	Kluczowa strategia IT zapewniające ciągłość działania biznesu. DR (odzyskiwanie po awarii) koncentruje się na szybkim przywróceniu usług po poważnej katastrofie (np. po pożarze, powodzi) za pomocą kopii zapasowych i systemów w odrębnej lokalizacji.
DRaaS (ang. *disaster recovery as a service*)	Usługa odzyskiwania danych i infrastruktury po awarii świadczona w modelu chmurowym. Pozwala firmie na szybkie wznowienie działania systemów IT w przypadku klęski żywiołowej, ataku hakerskiego czy poważnej awarii sprzętowej. W odróżnieniu od kopii (ang. *backup*) DRaaS zabezpiecza nie tylko dane, ale całą infrastrukturę gotową do uruchomienia „od ręki", co pozwala na powrót do pracy w ciągu minut lub sekund.
DRP (ang. *disaster recovery plan*)	Szczegółowy, udokumentowany zbiór procedur i instrukcji, które określają, w jaki sposób organizacja ma przywrócić swoje krytyczne funkcje, systemy informatyczne i dane po wystąpieniu poważnej awarii.
DSL (ang. *digital subscriber line*) – cyfrowa linia abonencka	Technologia dostępu szerokopasmowego, która wykorzystuje istniejące miedziane linie telefoniczne do transmisji danych z dużo większą przepustowością niż tradycyjna telefonia analogowa. Wykorzystuje podział pasma częstotliwości w taki sposób, aby możliwa była równoległa transmisja danych i jednoczesne korzystanie z usług telefonicznych, często w wariantach dostosowanych do potrzeb użytkowników domowych i biznesowych.
EDA (ang. *exploratory data analysis*) – eksploracyjna analiza danych	Etap analizy danych polegający na wstępnym badaniu zbioru danych w celu zrozumienia jego struktury, rozkładów, zależności i jakości. EDA obejmuje m.in. identyfikację braków danych, wartości odstających, niespójności, korelacji oraz weryfikację założeń, co wspiera dobór metod przetwarzania, budowę cech i dalsze modelowanie.

EDA (ang. *event-driven architecture*) – architektura sterowana zdarzeniami	Styl architektury systemów, w którym komunikacja i uruchamianie logiki biznesowej są oparte na zdarzeniach opisujących fakt zajścia określonej zmiany stanu. Zdarzenia są publikowane przez komponenty źródłowe i asynchronicznie konsumowane przez inne usługi, co umożliwia luźne powiązanie systemów, skalowanie przetwarzania oraz budowę przepływów w czasie bliskim rzeczywistemu.
Edge computing – przetwarzanie brzegowe	Model architektury, w którym część przetwarzania danych przenosi się z centralnych centrów danych bliżej miejsca ich powstawania, np. do lokalnych węzłów w zakładzie czy oddziale, sieci operatora czy urządzenia. Pozwala to na szybszą reakcję (mniejsze opóźnienia), wstępną filtrację lub agregację danych oraz odciążenie łączy do centralnych systemów, co jest istotne w systemach czasu bliskiego rzeczywistego i środowiskach rozproszonych.
EIGRP (ang. *enhanced interior gateway routing protocol*) – rozszerzony wewnętrzny protokół routingu bram	Protokół routingu stosowany wewnątrz domeny administracyjnej, umożliwiający dynamiczne wyznaczanie tras pomiędzy podsieciami. EIGRP wykorzystuje algorytm doboru najlepszej ścieżki na podstawie złożonej metryki (np. opóźnienie i przepustowość), zapewnia szybkie przeliczanie tras po awarii oraz ogranicza rozgłaszanie zmian do niezbędnego minimum, co poprawia skalowalność w sieciach przedsiębiorstw.
Ekosystem cyfrowy	Zintegrowana sieć powiązanych technologii, danych, aplikacji, usług i użytkowników współdziałających poprzez określone interfejsy i przepływy informacji tworzących wartość dla organizacji i jej otoczenia. Obejmuje komponenty techniczne, procesy organizacyjne, modele współpracy oraz mechanizmy bezpieczeństwa traktowane jako jedno spójne środowisko usług cyfrowych.
ELT (ang. *extract, load, transform*) – ekstrakcja, ładowanie, transformacja danych	Proces integracji danych, w którym dane są najpierw pobierane ze źródeł, następnie ładowane do systemu docelowego (np. hurtowni danych lub platformy analitycznej), a dopiero potem transformowane wewnątrz tego systemu. ELT wykorzystuje moc obliczeniową platformy docelowej do przekształceń i jest często stosowane w środowiskach chmurowych oraz przy pracy na dużych wolumenach danych.

Emulator komputerów kwantowych (ang. *quantum computer emulator*)	Oprogramowanie uruchamiane na klasycznych systemach obliczeniowych, które odwzorowuje działanie komputera kwantowego na poziomie logiki obwodów i stanów kwantowych. Umożliwia testowanie, debugowanie i porównywanie algorytmów kwantowych bez dostępu do fizycznego komputera kwantowego kosztem istotnie większych wymagań obliczeniowych wraz ze wzrostem liczby kubitów.
Enterpise blockchain – blockchain korporacyjny/dla przedsiębiorstw	Zaawansowana technologia blockchain w środowiskach organizacyjnych i konsorcjach (ang. *permissioned blockchains*) jako odpowiedź na potrzeby biznesu, który wymaga bezpieczeństwa rozproszonego rejestru, ale bez pełnej anonimowości i otwartości publicznych sieci takich jak Bitcoin. Tego typu rozwiązania charakteryzują się kontrolą tożsamości uczestników, wysokim poziomem zgodności z przepisami (ang. *compliance*) oraz integracją z istniejącymi systemami IT.
ESB (ang. *enterprise service bus*) – szyna usług przedsiębiorstwa	Centralny komponent architektury integracyjnej, przez który realizowana jest wymiana komunikatów między systemami informatycznymi. ESB stanowi wspólny punkt integracji, zapewniając standaryzację komunikacji, trasowanie komunikatów, transformację formatów danych oraz mediację protokołów, a także centralne egzekwowanie polityk bezpieczeństwa i niezawodności komunikacji (obsługa błędów, ponawianie, kolejkowanie) w ramach integracji systemów.
ESG (ang. *environmental, social, governance*) – środowisko, społeczeństwo, ład korporacyjny	Kompleksowy zestaw kryteriów oceny i raportowania sposobu zarządzania organizacją w trzech wymiarach: wpływu na środowisko (np. emisje, zużycie energii i zasobów), odpowiedzialności społecznej (np. warunki pracy, wpływ na interesariuszy) oraz ładu korporacyjnego (np. nadzór, zgodność, transparentność). W sektorze IT oraz w cyberbezpieczeństwie ESG jest wykorzystywane do zarządzania ryzykiem niefinansowym, zapewnienia stabilności operacyjnej, budowania zaufania interesariuszy oraz odpowiedzialnego wykorzystania technologii (m.in. mierzenie śladu środowiskowego usług cyfrowych).
ESS (ang. *extended service set*) – rozszerzony zestaw usług sieci bezprzewodowej	Grupa kilku powiązanych ze sobą zestawów BSS, połączonych wspólną infrastrukturą przewodową i zwykle działających pod tą samą nazwą sieci. Tworzy jedną logiczną sieć Wi-Fi obejmującą większy obszar i umożliwia użytkownikom płynne przemieszczanie się między punktami dostępowymi bez utraty połączenia.

Ethernet	Rodzina przewodowych technologii sieciowych używanych głównie w sieciach lokalnych. Określa sposób kodowania danych na medium transmisyjnym, format ramek i zasady dostępu do medium, tak aby wiele urządzeń mogło współdzielić jedną sieć fizyczną. Obejmuje zarówno warstwę fizyczną (rodzaj przewodu, złącza), jak i warstwę łącza danych (adresy MAC, ramki, podstawowe mechanizmy wykrywania kolizji), w kolejnych wersjach rozwijana do coraz wyższych przepływności.
ETL (ang. *extract, transform, load*) – ekstrakcja, transformacja, ładowanie danych	Klasyczny proces przetwarzania danych polegający na: ekstrakcji danych ze źródeł (systemy operacyjne, pliki, bazy); transformacji – czyszczeniu, łączeniu, przeliczaniu oraz dopasowaniu do docelowego modelu; ładowaniu do hurtowni danych, magazynu analitycznego lub innego systemu docelowego.
Event-driven	Model architektoniczny i programistyczny, w którym komponenty systemu komunikują się i reagują na zdarzenia zamiast bezpośredniego wywoływania funkcji. Umożliwia to tworzenie elastycznych, skalowalnych i decentralizowanych systemów stosowanych powszechnie w mikrousługach i nowoczesnych aplikacjach, gdzie producenci emitują zdarzenia, a konsumenci je odbierają i przetwarzają za pomocą np. brokerów wiadomości.
Exit plan – plan wyjścia	Plan działań i wymagań techniczno-organizacyjnych zapewniających możliwość zakończenia korzystania z usługi, platformy lub dostawcy i przejścia do innego rozwiązania. Obejmuje w szczególności zasady przenoszenia danych i konfiguracji, utrzymania ciągłości działania, harmonogram odłączenia, wymagania dotyczące archiwizacji oraz kontrolowanego usunięcia danych i dostępów po migracji.
FaaS (ang. *function as a service*) – funkcja jako usługa	Model chmury bezserwerowej, który pozwala deweloperom uruchamiać kod w odpowiedzi na zdarzenia, bez zarządzania infrastrukturą. Opłata dotyczy tylko wykonania kodu, co przyspiesza rozwiązanie problemu i obniża koszty. Czasami usługa może oznaczać testowanie odporności systemów (ang. *failure as a service*, FaaS) na awarie.

FDDI (ang. *fiber distributed data interface*) – światłowodowy interfejs sieci rozproszonej	Technologia budowy sieci lokalnej oparta na światłowodzie i podwójnym pierścieniu logicznym. Zapewnia wysoką niezawodność; w przypadku przerwania jednego pierścienia ruch jest automatycznie przełączany na drugą drogę. Historycznie stosowana głównie w krytycznych sieciach kampusowych i centrach danych jako szybka (jak na swoje czasy) sieć szkieletowa, obecnie wyparta przez nowsze odmiany Ethernetu.
Federacja tożsamości (ang. *identity federation*)	W IT to system, który pozwala użytkownikom logować się do wielu różnych aplikacji i usług w różnych organizacjach (domenach) za pomocą jednego zestawu danych logowania, poprzez ustanowienie między nimi relacji zaufania. Działa z wykorzystaniem dostawców tożsamości (ang. *identity providers*, IdP) i dostawców usług (ang. *service providers*, SP), eliminując potrzebę żonglowania wieloma hasłami, co poprawia bezpieczeństwo i wygodę, szczególnie w środowiskach chmurowych i hybrydowych.
FinOps (ang. *cloud financial operations*) – operacje finansowe w chmurze	Podejście łączące zespoły techniczne, finansowe i biznesowe w celu maksymalizacji wartości biznesowej chmury przez optymalizację kosztów, zwiększenie przejrzystości wydatków i wspólną odpowiedzialność za finanse. Polega na wprowadzeniu kultury współpracy i dyscypliny finansowej w dynamicznym środowisku chmury, co pozwala podejmować świadome decyzje dotyczące wydatków i innowacji.
Framework – szkielet/ramy programistyczne lub procesowe	Ustrukturyzowany zbiór komponentów, reguł i wzorców, który wyznacza sposób budowy i organizacji rozwiązania – technicznego lub organizacyjnego. W obszarze oprogramowania framework to środowisko dostarczające gotowe mechanizmy (np. obsługa żądań, warstwa dostępu do danych, moduły bezpieczeństwa), w które wbudowuje się logikę biznesową aplikacji. W szerszym ujęciu framework może oznaczać również uporządkowany zbiór zasad i praktyk służących do realizacji określonego typu procesów (np. zarządzania usługami lub bezpieczeństwem).
FTP (ang. *file transfer protocol*) – protokół przesyłania plików	Protokół komunikacyjny warstwy aplikacji służący do przesyłania plików między klientem a serwerem w sieciach TCP/IP. Umożliwia listowanie katalogów, pobieranie i wysyłanie plików oraz zarządzanie nimi z poziomu klienta, historycznie często używany w administracji serwerami i do publikacji treści.

FW (ang. *firewall*) – zapora sieciowa	Mechanizm bezpieczeństwa (urządzenie lub oprogramowanie) kontrolujący ruch sieciowy pomiędzy segmentami sieci na podstawie zdefiniowanych reguł. Zapora filtruje połączenia, dopuszczając lub blokując ruch zgodnie z polityką bezpieczeństwa, a w zależności od funkcjonalności może uwzględniać adresy, porty, stan połączenia oraz cechy komunikacji na poziomie aplikacji.
GCP (ang. *Google Cloud Platform*) – platforma usług chmurowych firmy Google	Obejmuje usługi obliczeniowe, magazynowanie danych, bazy danych, usługi uczenia maszynowego, analityki oraz integracji. Platforma jest wykorzystywana do budowy aplikacji i systemów przetwarzających duże zbiory danych, często integrowanych z innymi usługami ekosystemu Google.
GeoServer – serwer danych	Serwer do udostępniania danych przestrzennych (GIS) w standardowych usługach sieciowych, wspierający publikację warstw i usług mapowych wykorzystywanych m.in. w portalach danych otwartych. GeoServer jest wolnym oprogramowaniem (ang. *open source*), dystrybuowanym na licencji GNU GPL v2.
GIS (ang. *geographic information system*) – system informacji geograficznej	System informatyczny służący do gromadzenia, przechowywania, przetwarzania, analizy i prezentacji danych przestrzennych powiązanych z lokalizacją. GIS integruje dane mapowe z danymi opisowymi, umożliwia wykonywanie analiz przestrzennych (np. odległości, zasięgi, nakładanie warstw) oraz wspiera planowanie i podejmowanie decyzji w obszarach takich jak: administracja, infrastruktura, środowisko i logistyka.
GPO (ang. *group policy object*)	Element Windows Server będący zbiorem reguł i ustawień, który umożliwia administratorom scentralizowane zarządzanie i egzekwowanie konfiguracji, bezpieczeństwa i oprogramowania dla użytkowników i komputerów w domenie Active Directory.
Grafana	Platforma do wizualizacji danych i ich monitoringu. Umożliwia tworzenie dynamicznych, interaktywnych pulpitów nawigacyjnych (dashboardów), wskaźników w czasie rzeczywistym oraz szybkie identyfikowanie nieprawidłowości w działaniu systemów IT. Wykorzystywana do analizy różnych źródeł danych, logów oraz śledzenia wydajności systemów.

Green coding – zrównoważone wytwarzanie oprogramowania	Podejście do projektowania i implementacji oprogramowania ukierunkowane na ograniczanie zużycia zasobów obliczeniowych (CPU/GPU), pamięci, operacji dyskowych i transferu sieciowego, a w konsekwencji także zużycia energii. Obejmuje dobór algorytmów i struktur danych, profilowanie wydajności, redukcję zbędnych obliczeń, optymalizację zapytań i operacji wejścia/wyjścia oraz świadome zarządzanie cyklem życia aplikacji (kompilacja, wdrożenie, konfiguracja i eksploatacja) pod kątem efektywności.
Green IT – zielone IT	Podejście do projektowania, eksploatacji i wycofywania infrastruktury IT z uwzględnieniem minimalizacji wpływu na środowisko. Obejmuje m.in. ograniczanie zużycia energii w centrach danych i na stacjach roboczych, wydłużanie cyklu życia sprzętu, odpowiedzialną utylizację, a także projektowanie rozwiązań programowych zmniejszających zapotrzebowanie na zasoby obliczeniowe.
gRPC (ang. *Google Remote Procedure Call*) – framework zdalnego wywoływania procedur	Nowoczesny, wysokowydajny framework do komunikacji między aplikacjami. Pozwala jednemu programowi wywołać funkcję na innym komputerze, tak jakby była ona lokalna, niezależnie od języka programowania, w jakim oba programy napisano.
HA (ang. *high availability*) – wysoka dostępność	Cecha systemu, która zapewnia ciągłość działania i minimalizuje czas przestoju (ang. *downtime*), nawet w przypadku awarii pojedynczych komponentów, serwisów czy całych serwerów. Systemy HA dążą do osiągnięcia stanu utrzymania usługi w pełnej funkcjonalności przez cały czas działania.
Halucynacje	Niewiarygodne zachowania modelu językowego generującego fikcyjne odpowiedzi. W kontekście modeli generatywnych sytuacja, w której system generuje odpowiedzi brzmiące poprawnie i przekonująco, ale niezgodne z rzeczywistością lub niepoparte danymi źródłowymi. Halucynacje wynikają z probabilistycznego charakteru działania modelu, ograniczeń danych treningowych i braku wbudowanej weryfikacji faktów; stanowią istotne ryzyko przy wykorzystaniu takich systemów w zadaniach wymagających wysokiej wiarygodności informacji.

Hardening – utwardzanie systemu	Proces wzmacniania bezpieczeństwa systemu, aplikacji lub urządzenia poprzez ograniczenie powierzchni ataku. Obejmuje m.in. wyłączanie zbędnych usług, zaostrzanie konfiguracji, stosowanie silnych mechanizmów uwierzytelniania, aktualizowanie oprogramowania oraz wdrażanie zasad minimalnych uprawnień.
Healthcheck – kontrola stanu usługi/systemu	Automatyczny test wykonywany cyklicznie w celu sprawdzenia, czy usługa, aplikacja lub komponent infrastruktury działa poprawnie i reaguje w oczekiwany sposób. Wynik kontroli stanu jest wykorzystywany m.in. przez równoważniki obciążenia i systemy orkiestracji do wyłączania z ruchu instancji, które działają nieprawidłowo.
Host	Urządzenie z adresem IP w sieci (komputer, serwer, maszyna wirtualna) udostępniające zasoby.
HP-UX (Hewlett-Packard Unix) – system HP-UX	System operacyjny typu Unix rozwijany przez firmę Hewlett-Packard, przeznaczony głównie dla serwerów klasy enterprise. Wykorzystywany w krytycznych środowiskach biznesowych, w których wymaga się wysokiej niezawodności, skalowalności i zaawansowanych mechanizmów zarządzania zasobami.
Hurtownia danych (ang. *data warehouse*)	Centralne zintegrowane repozytorium danych, zaprojektowane do długoterminowego przechowywania informacji pochodzących z wielu systemów źródłowych na potrzeby raportowania i analiz. Dane w hurtowni są zwykle oczyszczone, ujednolicone, zorganizowane tematycznie oraz historyczne, a struktura i mechanizmy dostępu są zoptymalizowane pod kątem zapytań analitycznych, a nie bieżącej obsługi transakcji.
IaaS (ang. *infrastructure as a service*) – infrastruktura jako usługa	Jeden z modeli usługi przetwarzania, w którym zasoby obliczeniowe są hostowane w chmurze. Dostawca usługi hostuje fizyczną infrastrukturę, oprogramowanie oraz sieć o określonej przepustowości.
IaC (ang. *infrastructure as code*) – infrastruktura jako kod	Podejście do zarządzania infrastrukturą (serwerami, sieciami, usługami, konfiguracją bezpieczeństwa) poprzez opisywanie jej w postaci kodu lub deklaratywnych plików konfiguracyjnych, przechowywanych w repozytorium i wersjonowanych jak oprogramowanie. Umożliwia automatyczne, powtarzalne odtwarzanie i modyfikowanie środowisk oraz pełną kontrolę zmian konfiguracji w cyklu życia systemu.

IBSS (ang. *independent basic service set*) – niezależny podstawowy zestaw usług	Tryb pracy sieci bezprzewodowej, w którym urządzenia komunikują się bezpośrednio między sobą, bez użycia punktu dostępowego. Tworzy sieć *ad hoc*, w której każde urządzenie pełni funkcję zarówno klienta, jak i przekaźnika ruchu.
Idempotencja operacji	Oznacza, że wielokrotnie wykonanie operacji daje dokładnie taki sam rezultat, jak wykonanie jej tylko raz. Zmiany stanu systemu zachodzą tylko raz, niezależnie od liczby powtórzeń żądania.
IDP (ang. *internal developer platform*) – wewnętrzna platforma deweloperska	Wewnętrzna platforma organizacji dostarczająca zespołom wytwórczym ustandaryzowane narzędzia, usługi i szablony do budowy, wdrażania i utrzymania aplikacji. IDP integruje elementy cyklu życia oprogramowania (np. repozytoria, automatyzację budowania i wdrożeń, środowiska uruchomieniowe, katalog usług, zarządzanie konfiguracją i sekretami, obserwowalność) w spójny zestaw, aby skrócić czas dostarczenia, zwiększyć powtarzalność wdrożeń i ułatwić zgodność z politykami bezpieczeństwa oraz standardami organizacji.
IEEE 802.11be – standard Wi-Fi 7	Standard sieci bezprzewodowych kolejnej generacji z rodziny Wi-Fi zaprojektowany do zapewnienia bardzo wysokich przepustowości, niskich opóźnień i lepszego wykorzystania pasma radiowego w porównaniu z wcześniejszymi wersjami. Określa m.in. sposób pracy w szerszych kanałach radiowych oraz równoległe wykorzystanie wielu pasm częstotliwości, co ma wspierać wymagające aplikacje, takie jak wideo w wysokiej rozdzielczości czy gry i systemy czasu quasirzeczywistego.
IEEE 802.1X – portowa kontrola dostępu do sieci	Standard kontroli dostępu do sieci przewodowych i bezprzewodowych, który wymaga uwierzytelnienia urządzenia lub użytkownika przed dopuszczeniem ruchu przez port sieciowy. Wykorzystuje mechanizm pośredniczący między klientem a serwerem uwierzytelniającym, umożliwiając centralne egzekwowanie polityk dostępu.
Incydent	Nieplanowane przerwanie lub pogorszenie jakości usługi IT lub zdarzenie, którego nieusunięcie może zakłócić lub obniżyć jakość działania systemów informatycznych, usług IT lub procesów biznesowych. Incydent wymaga reakcji w celu przywrócenia normalnego funkcjonowania i ograniczenia lub zminimalizowania negatywnego wpływu na organizację.

Intent-Based Networking – zaawansowane podejście do zarządzania siecią	Pozwala administratorom opisywać pożądane cele biznesowe w języku naturalnym, zamiast ręcznie konfigurować poszczególne urządzenia. System automatycznie tłumaczy te cele na polityki i konfiguracje, a następnie monitoruje i dostosowuje sieć, by zapewnić ich realizację.
Interfejs	Punkt styku lub mechanizm, który umożliwia komunikację i współpracę pomiędzy dwoma systemami, urządzeniami (np. port USB) lub człowiekiem a maszyną.
InVision	Nazwa popularnej platformy do projektowania i prototypowania interfejsów użytkownika (UI/UX) oraz współpracy zespołowej.
IOS	Mobilny system operacyjny firmy Apple Inc., który jest przeznaczony dla urządzeń mobilnych tej firmy.
IoT (ang. *internet of things*) – internet rzeczy	Sieć zbudowana z obiektów („rzeczy") wyposażonych w czujniki (sensory), które umożliwiają im zbieranie i wymianę danych przez internet z innymi urządzeniami, systemami lub użytkownikami; mogą tworzyć systemy automatyzujące procesy, np. inteligentne domy, miasta, przemysł.
IP Hash	IP Hash to metoda równoważenia obciążenia (load balancing), w której adres IP klienta jest używany jako klucz do wyznaczenia konkretnego serwera mającego obsłużyć dane zapytanie. Dzięki temu dany użytkownik zawsze trafia do tego samego serwera.
IPFS (ang. *interplanetary file system*) – rozproszony system plików	Protokół i system przechowywania plików oparty na rozproszonej sieci węzłów, w którym dostęp do danych odbywa się na podstawie ich kryptograficznego identyfikatora (adresowanie treści), a nie lokalizacji serwera. Pliki są dzielone na bloki, replikowane w sieci i mogą być udostępniane bez centralnego serwera, co sprzyja odporności na awarie oraz utrudnia cenzurowanie treści.

ISO/IEC (ang. *International Organization for Standardization*/ *International Electrotechnical Commission*) – Międzynarodowa Organizacja Normalizacyjna/ Międzynarodowa Komisja Elektrotechniczna	Dwie międzynarodowe organizacje normalizacyjne, które wspólnie opracowują standardy i serie norm z obszaru technologii informacyjnych i telekomunikacji. W kontekście IT odniesienie do ISO/IEC zwykle oznacza powołanie się na uznane, formalne normy dotyczące zarządzania bezpieczeństwem informacji, jakości usług IT czy inżynierii oprogramowania.
ITIL (ang. *information technology infrastructure library*)	Uznawany na całym świecie zbiór najlepszych praktyk (framework) w zakresie zarządzania usługami IT (ang. *information technology service management*, ITSM). Jego celem jest dostosowanie usług informatycznych do potrzeb i celów biznesowych i maksymalizacja wartości z inwestycji w IT. ITIL nie jest sztywną normą ani metodyką, lecz zbiorem elastycznych wytycznych, które można dostosować do specyfiki każdej firmy, niezależnie od jej wielkości czy branży.
Kafka (ang. *Apache Kafka*) – platforma strumieniowania zdarzeń	Rozproszona platforma do niezawodnej wymiany i przetwarzania strumieni zdarzeń (np. logów, komunikatów aplikacyjnych) pomiędzy systemami. Umożliwia publikowanie zdarzeń do logicznych kanałów tematycznych oraz ich równoległy odbiór przez wiele usług, z zachowaniem trwałości danych i możliwości ponownego odczytu. Stosowana do integracji systemów, budowy architektur zdarzeniowych oraz buforowania obciążenia między producentami i konsumentami danych.
Kibana	Oprogramowanie służące do wizualizacji, eksploracji i analizy danych przechowywanych w klastrach Elasticsearch. Umożliwia budowę dashboardów, raportów i wykresów, przeszukiwanie oraz filtrowanie logów i metryk, a także definiowanie wizualnych paneli do monitoringu systemów oraz detekcji zdarzeń i anomalii w danych operacyjnych.

Klasy storage	Predefiniowane kategorie danych w chmurze lub systemach IT, które określają, jak dane są przechowywane, jakie mają koszty dostępu i jak szybko są dostępne. Umożliwiają optymalizację pod kątem wydajności i ceny.
KMS (ang. *key management service*) – usługa zarządzania kluczami	System bezpiecznego zarządzania kluczami szyfrującymi. Stosowany w chmurze i lokalnie, aby kontrolować dostęp do danych i spełniać wymogi bezpieczeństwa i zgodności.
Koncepcje showback/ chargeback	Systemy rozliczania kosztów w obszarze IT i chmury. Showback to raportowanie kosztów zespołom, aby zwiększyć świadomość ich wykorzystania, a chargeback to działanie obciążające działy za zużyte zasoby, co wymusza odpowiedzialność i efektywność.
Konfiguracja endpointów	Proces dostosowywania i zabezpieczania punktów końcowych urządzeń oraz definiowania parametrów komunikacji dla API (interfejsów). Obejmuje ustawianie zasad bezpieczeństwa, zarządzanie dostępem i definiowanie sposobów wymiany danych między aplikacjami i systemami.
Konteneryzacja	Proces pakowania aplikacji wraz z jej komponentami (bibliotekami, plikami konfiguracyjnymi) w izolowane, przenośne środowisko zwane kontenerem, co umożliwia uruchomienie aplikacji na dowolnej infrastrukturze. Jest to alternatywa dla maszyn wirtualnych – kontenery współdzielą jądro systemu operacyjnego hosta, zamiast emulować cały system.
KPI (ang. *key performance indicators*) – kluczowe wskaźniki efektywności	Mierniki wartości skuteczności działania firmy lub działu. Analizują stany i postępy realizacji celów strategicznych i operacyjnych. Dostarczają obiektywne dane do podejmowania decyzji i optymalizacji działań.
Kubernetes	System orkiestracji kontenerów służący do uruchamiania i zarządzania aplikacjami kontenerowymi w środowisku rozproszonym. Automatyzuje m.in. wdrażanie, skalowanie, równoważenie obciążenia, aktualizacje oraz odtwarzanie usług po awariach.

LAN (ang. *local area network*) – lokalna sieć komputerowa	Logicznie wydzielona sieć łącząca urządzenia (komputery, serwery, drukarki, przełączniki) na ograniczonym obszarze, np. w biurze, hali produkcyjnej, kampusie. Zapewnia wysoką przepustowość i małe opóźnienia, zwykle jest zarządzana przez jedną organizację i stanowi podstawową infrastrukturę komunikacyjną wewnątrz firmy lub instytucji.
LB (ang. *load balancing*) – równoważenie obciążenia	Mechanizm rozkładania ruchu sieciowego lub zapytań aplikacyjnych na wiele serwerów, instancji usług lub łączy w taki sposób, aby uniknąć przeciążenia pojedynczego węzła. Równoważenie obciążenia poprawia dostępność, skalowalność i wydajność systemu, a w połączeniu z monitorowaniem stanu zasobów umożliwia automatyczne wyłączanie z ruchu elementów, które działają nieprawidłowo.
LDAP (ang. *lightweight directory access protocol*) – otwarty protokół komunikacyjny	Umożliwia dostęp i zarządzanie usługami katalogowymi, które przechowują informacje o użytkownikach, zasobach i urządzeniach w sieci, działając na protokole TCP/IP. Pozwala na centralne uwierzytelnianie i autoryzację użytkowników.
Least Connections – algorytm najmniej połączeń	Strategia rozdzielania ruchu, w której nowe połączenie kierowane jest do serwera mającego w danej chwili najmniejszą liczbę aktywnych połączeń. Pozwala lepiej wykorzystać zasoby niż proste podejście Round Robin, szczególnie przy nierównych czasach obsługi żądań lub różnej wydajności serwerów.
LLM (ang. *large language model*) – duży model językowy	Model uczenia głębokiego wyspecjalizowany w przetwarzaniu języka naturalnego, wytrenowany na bardzo dużych zbiorach tekstów. Umożliwia generowanie i parafrazę tekstu, odpowiadanie na pytania, streszczanie, tłumaczenie, analizę treści oraz inne zadania językowe, wykorzystując reprezentację statystycznych zależności między słowami i zdaniami.
Logi zdarzeń (ang. *event logs*) – dzienniki zdarzeń	Zbiory zapisów opisujących zdarzenia zachodzące w systemach, aplikacjach, urządzeniach sieciowych lub usługach. Każdy wpis logu zawiera typ zdarzenia, znacznik czasu oraz dodatkowy kontekst (np. identyfikator użytkownika, adres IP, kod błędu). Logi zdarzeń są podstawowym źródłem informacji do monitoringu, analizy incydentów, audytu oraz rekonstrukcji przebiegu zdarzeń w środowisku IT/OT.

Low-code – niskokodowe platformy programistyczne	Wizualne podejście do tworzenia oprogramowania, które wymaga minimalnej ilości ręcznego pisania kodu. Dzięki interfejsowi graficznemu i gotowym modułom pozwala szybko budować zaawansowane aplikacje, dając jednocześnie swobodę programistom na dodawanie własnych, niestandardowych funkcji tam, gdzie jest to konieczne.
MAC (ang. *media access control address*) – adres MAC, adres fizyczny karty sieciowej	Stały, najczęściej 48-bitowy identyfikator przypisany do interfejsu sieciowego (np. karty Ethernet lub modułu Wi-Fi), zapisywany w postaci liczb szesnastkowych oddzielonych dwukropkami lub myślnikami. Służy do jednoznacznego rozróżniania urządzeń w sieci na poziomie warstwy łącza danych. Wykorzystywany m.in. przez przełączniki sieciowe do przekazywania ramek do właściwego portu.
MAC (ang. *mandatory access control*) – obowiązkowa kontrola dostępu	Model kontroli dostępu, w którym decyzje o dostępie do zasobów są wymuszane przez centralnie zdefiniowaną politykę bezpieczeństwa, a nie przez właściciela zasobu. Uprawnienia wynikają z przypisanych etykiet lub poziomów klasyfikacji (np. tajności) dla użytkowników, procesów i obiektów, a użytkownik nie może samodzielnie zmieniać tych reguł ani przekazywać uprawnień innym podmiotom.
Malware – złośliwe oprogramowanie	Określenie programów komputerowych stworzonych do wyrządzania szkody użytkownikowi, kradzieży jego danych, uszkadzania urządzeń lub przejmowania nad nimi kontroli. Obejmuje m.in. wirusy, trojany, ransomware, programy szpiegujące. Działa potajemnie na komputerach, telefonach lub tabletach w celu wyłudzenia informacji, wyświetlania reklam lub blokowania systemu.
Mapping	Struktura danych stosowana w językach programowania smart kontraktów, reprezentująca odwzorowanie typu „klucz–wartość". Umożliwia powiązanie unikalnego klucza (np. adresu uczestnika, identyfikatora zasobu) z odpowiadającą mu wartością (np. saldem, strukturą danych, zestawem uprawnień) przechowywaną w stanie kontraktu. Mapping jest wykorzystywany do wydajnego zarządzania danymi w rozproszonym rejestrze bez konieczności iterowania po pełnych kolekcjach.

MDM (ang. *mobile device management*) – zarządzanie urządzeniami mobilnymi	System IT umożliwiający zdalne zarządzanie, monitorowanie i zabezpieczanie urządzeń mobilnych używanych w firmie (np. smartfony, tablety, laptopy). Systemy MDM pozwalają na egzekwowanie polityk bezpieczeństwa, konfigurowanie aplikacji i sieci, a także zdalne blokowanie lub czyszczenie urządzenia w przypadku zgubienia lub kradzieży.
Media syntetyczne (ang. *synthetic media*)	Treści tekstowe, graficzne, dźwiękowe lub wideo, które zostały wytworzone albo w istotny sposób przekształcone automatycznie przez algorytmy generatywne, a nie wyłącznie zarejestrowane z rzeczywistego świata. Obejmują m.in. generowane obrazy, nagrania głosu, awatary i filmy, co rodzi dodatkowe wymagania w zakresie oznaczania pochodzenia treści, weryfikacji autentyczności oraz ochrony przed dezinformacją.
Mesh – sieć mesh/ sieć kratowa	Architektura sieci, w której wiele węzłów jest połączonych ze sobą w sposób wielokrotny, a ruch może być przekazywany różnymi ścieżkami. W sieciach bezprzewodowych pozwala to na automatyczne omijanie uszkodzonych węzłów, rozszerzanie zasięgu oraz zwiększenie odporności na awarie pojedynczych punktów.
Metadane (ang. *metadata*)	Informacje opisujące inne dane, ułatwiające ich interpretację, wyszukiwanie, klasyfikację i kontrolę dostępu. Metadane mogą obejmować m.in. datę utworzenia, autora, format, lokalizację, wersję, poziom poufności, słowa kluczowe oraz powiązania z innymi zasobami. Odgrywają kluczową rolę w zarządzaniu cyklem życia informacji, audycie i bezpieczeństwie danych.
Metody kompensacyjne	W inżynierii systemów IT i w obszarze technicznym „kompensacja" odnosi się do technik reagowania na błędy (ang. *error compensation* lub *fault tolerance*) zapewniających niezawodność i stabilność działania systemów. IT kompensacja (odporność na błędy) oznacza zestaw technik, które minimalizują skutki opóźnień, utraty danych lub awarii, dzięki czemu system działa płynnie mimo niedoskonałości środowiska.

Metodyka zarządzania sekretami (ang. *secrets management*)	Proces bezpiecznego przechowywania, dystrybucji, rotacji i odwoływania poufnych informacji (hasła, klucze API, certyfikaty), kluczowy w DevOps i IT, który ma chronić krytyczne zasoby przed nieautoryzowanym dostępem. Wykorzystuje specjalistyczne narzędzia (np. Vault, AWS Secrets Manager) do dynamicznego dostarczania tymczasowych poświadczeń zamiast przechowywania ich w kodzie czy plikach konfiguracyjnych.
MFA (ang. *multi-factor authentication*) – uwierzytelnianie wieloskładnikowe	Metoda zwiększania bezpieczeństwa logowania, która wymaga podania co najmniej dwóch różnych form potwierdzenia tożsamości (np. poza samym hasłem), zanim zostanie uzyskany dostęp do konta, systemu lub aplikacji.
Mikroserwisy/ mikrousługi (ang. *microservices*)	Rodzaj architektury oprogramowania polegający na budowaniu aplikacji jako zestawu małych, niezależnych i luźno powiązanych usług. Każda z nich odpowiada za jedną, konkretną funkcjonalność biznesową. Usługi komunikują się ze sobą przez API i mogą być rozwijane, testowane i wdrażane niezależnie. Zwiększa to elastyczność, skalowalność i odporność systemu – awaria jednego serwisu nie paraliżuje całości.
ML (ang. *machine learning*) – uczenie maszynowe	Uczenie maszynowe to gałąź sztucznej inteligencji (AI) i informatyki, która skupia się na wykorzystaniu danych i algorytmów do naśladowania sposobu, w jaki uczą się ludzie – stopniowo zwiększając swoją dokładność. Jest ważnym elementem rozwijającej się dziedziny nauki o danych. Dzięki zastosowaniu metod statystycznych algorytmy są „szkolone" w celu klasyfikowania, przewidywania i odkrywania kluczowych zależności w projektach opartych na przetwarzaniu danych, pozwalając systemom na podejmowanie decyzji bez bezpośredniej interwencji człowieka po zakończeniu procesu szkolenia.
MLOps (ang. *machine learning operations*) – operacjonalizacja uczenia maszynowego	Zestaw praktyk, procesów i narzędzi służących do zarządzania pełnym cyklem życia modeli uczenia maszynowego – od eksperymentów, wersjonowania danych i modeli, przez wdrażanie do środowisk testowych i produkcyjnych, po monitoring jakości, ponowne trenowanie i wycofywanie modeli. Łączy podejście inżynierii danych, uczenia maszynowego i DevOps, aby zapewnić powtarzalność, skalowalność i kontrolę nad zmianami modeli w systemach produkcyjnych.

Mock-up	Termin używany w projektowaniu graficznym i webdesignie, określa realistyczny model lub wizualną reprezentację produktu, strony internetowej, aplikacji czy interfejsu użytkownika. Mock-upy są przydatne w procesie tworzenia i pozwalają na wizualizację końcowego efektu przed jego faktyczną realizacją. Dzięki nim można łatwiej zidentyfikować i poprawić ewentualne błędy oraz lepiej zrozumieć, jak dany projekt będzie wyglądał i funkcjonował w rzeczywistości.
Modele multimodalne/ wielomodalne (ang. *multimodal models*)	Modele sztucznej inteligencji zdolne do jednoczesnego przetwarzania i łączenia danych w różnych postaciach, np. tekstu, obrazu, dźwięku, wideo czy danych tabelarycznych. Umożliwiają budowę systemów, które jako wejście przyjmują wiele typów danych i generują wynik w jednej lub kilku modalnościach, np. opis słowny na podstawie obrazu i tekstowego kontekstu.
Monetyzacja	Proces przekształcania produktu, usługi lub zasobu (np. aplikacji, platformy, danych, ruchu sieciowego) w źródło przychodu. Obejmuje wybór i wdrożenie modelu zarabiania (np. opłat abonamentowych, opłat za wykorzystanie zasobów, sprzedaży danych, reklam lub funkcji premium) oraz mierzenie efektów biznesowych tych działań.
Monolit	Tradycyjna architektura oprogramowania zawierająca zintegrowane wszystkie funkcje w jednej, niepodzielonej jednostce, działające w ramach jednej bazy danych. Jest łatwy do wdrożenia i zarządzania, ale trudny do skalowania i modyfikacji, bo każda zmiana wymaga ponownego wdrożenia całości. Jest przeciwieństwem mikroserwisów.
Multi-cloud – środowisko wielochmurowe	Sposób wykorzystania więcej niż jednego dostawcy chmury w tej samej organizacji, np. osobne systemy w różnych chmurach lub podział usług między wielu dostawców. Nie zakłada automatycznie ścisłej integracji między chmurami – kluczowe jest to, że organizacja świadomie korzysta z wielu platform chmurowych (np. z powodów kosztowych, funkcjonalnych, regulacyjnych lub dla zmniejszenia zależności od jednego dostawcy).
NAS (ang. *network attached storage*) – sieciowa pamięć masowa	Urządzenie do przechowywania i udostępniania danych w sieci (domowej lub firmowej), działające jak prosty komputer z dyskami i dostępem przez sieć, do której jest dołączony.

NETCONF (ang. *network configuration protocol*) – protokół konfiguracji sieci	Standardowy protokół służący do zdalnego odczytu i zmiany konfiguracji urządzeń sieciowych w sposób ustrukturyzowany. Wykorzystuje modele danych opisujące konfigurację i stan urządzeń oraz zapewnia mechanizmy transakcyjnego wprowadzania zmian, dzięki czemu można spójnie i automatycznie zarządzać większą liczbą elementów sieci.
Neuromorficzne przetwarzanie (ang. *neuromorphic computing*)	Podejście do budowy systemów obliczeniowych, w którym architektura sprzętowa i model przetwarzania informacji są inspirowane działaniem układu nerwowego. Neuromorficzne przetwarzanie wykorzystuje wyspecjalizowane układy oraz modele przetwarzania zdarzeniowego i silnie równoległego (np. sieci neuronów impulsowych) w celu uzyskania wysokiej efektywności energetycznej. Stosowane jest m.in. do analizy strumieni danych z sensorów, rozpoznawania wzorców oraz przetwarzania na brzegu sieci w środowiskach o ograniczonych zasobach.
NFR (ang. *non--functional requirements*)	Wymagania określające właściwości jakościowe systemu oraz ograniczenia jego działania, a nie konkretne funkcje biznesowe. Opisują m.in. poziom bezpieczeństwa, dostępność, niezawodność, wydajność, skalowalność, odporność na awarie, zgodność regulacyjną, utrzymywalność, obserwowalność oraz użyteczność. W praktyce stanowią kryteria akceptacji i projektowe „parametry brzegowe", które determinują architekturę i sposób wdrożenia rozwiązania.
NFV (ang. *network functions virtualization*) – wirtualizacja funkcji sieciowych	Podejście, w którym tradycyjne funkcje realizowane przez specjalnie przeznaczone do tego urządzenia sieciowe (np. zapory, routery, równoważniki obciążenia) są uruchamiane jako oprogramowanie na standardowych serwerach i maszynach wirtualnych. Umożliwia to elastyczne skalowanie, szybkie wdrażanie nowych funkcji sieciowych oraz automatyzację ich cyklu życia z wykorzystaniem platform wirtualizacyjnych lub chmurowych.
NGFW (ang. *next-generation firewall*) – zapora sieciowa nowej generacji	Zapora sieciowa rozszerzająca klasyczne filtrowanie ruchu o analizę na poziomie aplikacji, identyfikację użytkowników, inspekcję zaszyfrowanego ruchu oraz wykrywanie zagrożeń na podstawie sygnatur i analizy behawioralnej. Umożliwia egzekwowanie złożonych polityk bezpieczeństwa, obejmujących nie tylko adresy i porty, ale także konkretne aplikacje, usługi i kategorie treści.

Nieautoryzowany dostęp	Uzyskanie dostępu do systemów, danych lub zasobów informatycznych bez zezwolenia właściciela lub operatora. Jest to naruszenie polityki bezpieczeństwa obejmujące m.in. próby logowania, uzyskania dostępu do plików czy korzystania z urządzeń bez uprawnień.
No-code – bez kodu	Narzędzia umożliwiające użytkownikom generowanie aplikacji, stron internetowych i automatyzacji procesów przy użyciu interfejsów za pomocą techniki „przeciągnij i upuść" lub gotowych komponentów, co eliminuje potrzebę ręcznego pisania kodu programu.
NTP (ang. *network time protocol*) – protokół synchronizacji czasu w sieci	Protokół używany do precyzyjnej synchronizacji zegarów systemowych urządzeń w sieciach IP z zaufanymi źródłami czasu. Działa hierarchicznie i zazwyczaj wykorzystuje UDP. Spójny czas jest kluczowy m.in. dla poprawności logów, ważności certyfikatów, działania mechanizmów kryptograficznych i analizy incydentów bezpieczeństwa.
Obserwowalność (ang. *observability*)	Właściwość systemu polegająca na tym, że o jego stanie wewnętrznym można wiarygodnie wnioskować na podstawie danych generowanych podczas działania. W praktyce opiera się na spójnej rejestracji i korelacji danych operacyjnych, takich jak: logi, metryki oraz śledzenie przepływu żądań między usługami, aby szybciej diagnozować przyczyny problemów i oceniać wpływ zmian.
OLA (ang. *operating level agreement*) – umowa na poziomie operacyjnym	Wewnętrzny dokument używany w organizacji, który może być powiązany z dokumentem SLA (ang. *service level agreement*) jako umowa zawierana między różnymi wewnętrznymi działami wewnątrz tej samej organizacji, które wspólnie świadczą usługę klientowi biznesowemu.
On-prem (ang. *on-premises*) – środowisko (oprogramowanie) lokalne	Model utrzymywania systemów IT, w którym infrastruktura (serwery, pamięć masowa, sieć) znajduje się fizycznie w siedzibie organizacji lub w jej własnym centrum danych i jest przez nią bezpośrednio zarządzana. Przeciwstawiany modelom chmurowym – organizacja samodzielnie odpowiada za zakup, utrzymanie, skalowanie i zabezpieczenie tej infrastruktury.

OpenDataSoft	Platforma do publikowania i udostępniania danych (często w formule open data portal) z katalogiem, metadanymi, wyszukiwaniem i wizualizacjami oraz API. Jest klasyfikowana jako rozwiązanie komercyjne; wspiera udostępnianie danych otwartych, natomiast model licencjonowania platformy jest niezależny od licencji danych publikowanych w portalu.
OpenFlow	Otwarty protokół sterowania urządzeniami sieciowymi, umożliwiający zewnętrznemu kontrolerowi programowe zarządzanie sposobem przełączania ruchu w przełącznikach i routerach. Oddziela logikę sterowania od samego przełączania pakietów, pozwalając kontrolerowi instalować, modyfikować i usuwać reguły w tablicach przepływów w urządzeniach sieciowych.
OpenRefine	Oprogramowanie do interaktywnego porządkowania danych, wykrywania niespójności, czyszczenia wartości, transformacji pól oraz ujednolicania formatów w zbiorach danych. Umożliwia m.in. masowe korekty, reguły przekształceń i łączenie danych z różnych źródeł w celu przygotowania ich do analiz, raportowania lub migracji.
Openshift	Platforma kontenerowa klasy enterprise oparta o Kubernetes, dostarczająca gotowe mechanizmy budowania, wdrażania i utrzymania aplikacji. Integruje elementy zarządzania cyklem życia aplikacji, bezpieczeństwa i polityk dostępu oraz ułatwia standaryzację środowisk wielozespołowych.
Open source – otwarte oprogramowanie lub otwarty kod źródłowy	Oprogramowanie, którego kod źródłowy jest publicznie dostępny. Pozwala to użytkownikom na jego legalne używanie, modyfikowanie i rozpowszechnianie na warunkach określonych w licencji.
Orkiestracja	Skoordynowane sterowanie wieloma narzędziami, systemami i procesami z jednego, centralnego miejsca w taki sposób, aby tworzyły spójny przepływ pracy. Polega na zintegrowaniu różnych systemów, przekazywaniu między nimi danych i wyników oraz uruchamianiu właściwych akcji w określonej kolejności, często jako podstawa do automatyzacji. W obszarze bezpieczeństwa dotyczy m.in. spinania platform monitoringu, analizy zagrożeń i systemów reakcji na incydenty w jedno zdolne do szybkiej, skoordynowanej odpowiedzi środowisko.

Orkiestracja sieci (w tym SDN) (ang. *software defined networking*)	Proces automatyzacji i centralnego zarządzania złożonymi procesami, przepływami (ang. *workflows*), domenami i elementami sieci, gdzie tradycyjne, rozproszone funkcje (np. routing, przełączanie) są oddzielone od sprzętu (warstwa infrastruktury) i zarządzane centralnie przez inteligentny kontroler (warstwa sterowania). Umożliwia to programowe definiowanie polityk, a zwłaszcza dynamiczne kierowanie ruchem oraz efektywne koordynowanie środowiska sieciowego przez API (zamiast konfigurowania każdego urządzenia osobno).
OSI (ang. *open systems interconnection*) – model odniesienia otwartych systemów komunikacji	Standard opisujący komunikację w sieciach teleinformatycznych w podziale na siedem warstw: fizyczną, łącza danych, sieciową, transportową, sesji, prezentacji i aplikacji. Każda warstwa ma zdefiniowany zakres odpowiedzialności i standardowe usługi, co umożliwia projektowanie, analizę i porównywanie protokołów sieciowych oraz architektur sieci.
OT (ang. *operational technology*) – technologie operacyjne	Zbiór urządzeń i systemów wykorzystywanych do sterowania, monitorowania i nadzorowania procesów produkcyjnych oraz infrastruktury fizycznej. Obejmuje rozwiązania sprzętowe i programowe pracujące bezpośrednio na procesie technologicznym.
OU (ang. *organizational unit*)	Jednostka organizacyjna w informatyce (zwłaszcza w Microsoft Active Directory) służąca do grupowania obiektów (użytkowników, komputerów).
PaaS (ang. *platform as a service*) – platforma jako usługa	Jeden z modeli usługi przetwarzania, w którym dostawca udostępnia platformę programistyczną lub developerską.

PAM (ang. *privileged access management*) – zarządzanie dostępem uprzywilejowanym do zabezpieczania, kontrolowania oraz monitorowania dostępu do krytycznych informacji i zasobów organizacji	Jest to połączenie rozwiązań i technologii IT używanych do zabezpieczania, kontrolowania oraz monitorowania dostępu do krytycznych informacji i zasobów organizacji. Chroni organizację przed cyberzagrożeniami, minimalizuje ryzyko nadużyć i zapewnia zgodność z regulacjami (wewnętrznymi i aktami prawnymi). Technologia PAM obejmuje szereg narzędzi, takich jak: zarządzanie hasłami, sesjami uprzywilejowanymi, kontrola urządzeń służbowych oraz przyznawanie dostępu do aplikacji.
PBAC (ang. *policy-based access control*) – kontrola dostępu oparta na politykach	Model kontroli dostępu, w którym decyzja o przyznaniu lub odmowie dostępu jest podejmowana na podstawie zestawu polityk (reguł) opisujących warunki dostępu. Polityki mogą uwzględniać kontekst żądania, np. tożsamość i rolę użytkownika, typ zasobu, wykonywaną operację, czas, lokalizację, poziom ryzyka oraz stan urządzenia. PBAC umożliwia centralne definiowanie i egzekwowanie reguł dostępu w wielu systemach, bez ręcznego przypisywania uprawnień do każdego zasobu.
Phishing	Popularna metoda oszustwa internetowego wykorzystująca inżynierię społeczną, polegająca na podszywaniu się pod zaufane instytucje w celu wyłudzenia poufnych danych (np. loginy, hasła, numery kart płatniczych, dane osobowe). Cyberprzestępcy wysyłają fałszywe e-maile, SMS-y lub wiadomości zawierające linki do fałszywych stron internetowych w celu nakłonienia ofiary do wprowadzenia danych lub zainfekowania komputera złośliwym oprogramowaniem.

Piaskownica regulacyjna dla systemów sztucznej inteligencji (ang. *regulatory sandbox for AI*)	Kontrolowane środowisko testowe, w którym organizacje mogą projektować, trenować, walidować i pilotażowo uruchamiać systemy sztucznej inteligencji pod nadzorem instytucji regulacyjnych lub w ramach ustalonych zasad zgodności. Celem jest bezpieczne sprawdzenie działania systemu w warunkach zbliżonych do rzeczywistych, w tym ocena ryzyk (np. dla prywatności, bezpieczeństwa, równego traktowania), weryfikacja wymagań prawnych i organizacyjnych oraz dopracowanie dokumentacji i mechanizmów kontroli przed wdrożeniem produkcyjnym.
PIM (ang. *privileged identity management*)	Procedura pozwalająca na prowadzenie nadzoru nad aktywnością użytkowników uprzywilejowanych. Uniemożliwia dostęp do kluczowych danych niewłaściwym użytkownikom oraz ogranicza możliwość nadużyć wynikających z szerokiego zakresu uprawnień.
PKI (ang. *public key infrastructure*) – infrastruktura klucza publicznego	Zbiór mechanizmów technicznych, organizacyjnych i proceduralnych służących do generowania, dystrybucji, przechowywania oraz unieważniania kluczy kryptograficznych i certyfikatów. Umożliwia stosowanie kryptografii klucza publicznego do uwierzytelniania, szyfrowania i podpisu elektronicznego w sposób zaufany, oparty na hierarchii urzędów certyfikacji.
Platforma	Termin oznaczający system, środowisko lub infrastrukturę, która umożliwia działanie aplikacji, usług i interakcji cyfrowych. Działa jako baza (fundament), która umożliwia interakcję między różnymi użytkownikami i systemami.
PoE (ang. *power over Ethernet*) – zasilanie przez przewód Ethernet	Technika umożliwiająca jednoczesne przesyłanie danych i energii elektrycznej tym samym kablem sieciowym Ethernet. Pozwala zasilać urządzenia takie jak punkty dostępowe czy kamery IP bez osobnych zasilaczy, upraszczając okablowanie i umożliwiając centralne zasilanie oraz awaryjne podtrzymanie pracy tych urządzeń.
PowerShell	Powłoka systemowa i język skryptowy firmy Microsoft, dostępny na Windows, Linux i macOS. Łączy interaktywne środowisko wiersza poleceń z obiektowym językiem skryptowym, co umożliwia zaawansowaną automatyzację administracji systemami, usługami katalogowymi, platformami chmurowymi i aplikacjami. Operuje na obiektach (a nie na samym tekście), co ułatwia filtrowanie, łączenie i przetwarzanie wyników poleceń w złożonych scenariuszach administratorskich.

PQC (ang. *post-quantum cryptography*) – kryptografia postkwantowa	Zestaw algorytmów kryptograficznych projektowanych w taki sposób, aby pozostały bezpieczne również w warunkach dostępności komputerów kwantowych zdolnych do łamania części obecnie stosowanych schematów kryptografii klucza publicznego. PQC obejmuje m.in. mechanizmy uzgadniania kluczy i podpisu cyfrowego oparte na problemach obliczeniowych uznawanych za odporne na znane algorytmy kwantowe i służy do planowania migracji kryptograficznej w systemach o długim horyzoncie ochrony danych.
PRINCE2 Agile	Rozszerzenie metodyki PRINCE2, łączące klasyczne procesowe zarządzanie projektem z praktykami podejść zwinnych. Określa, jak utrzymać strukturę ról, produktów zarządczych i etapów PRINCE2, prowadząc jednocześnie realizację zakresu w iteracjach, z wykorzystaniem backlogu, przyrostowego dostarczania i zwinnego planowania po stronie zespołów wykonawczych.
PRINCE2 (ang. *projects in controlled environments 2*) – metodyka PRINCE2	Metodyka zarządzania projektami oparta na zdefiniowanych rolach, produktach (rezultatach), etapach i zasadach sterowania projektem. Koncentruje się na uzasadnieniu biznesowym, zarządzaniu ryzykiem, podziale odpowiedzialności oraz kontroli postępu poprzez formalne punkty decyzyjne w cyklu życia projektu.
Privacy by default – ochrona prywatności w ustawieniach domyślnych	Zasada, zgodnie z którą domyślne ustawienia systemu lub usługi zapewniają wysoki poziom ochrony prywatności, bez konieczności dodatkowej konfiguracji przez użytkownika. Oznacza to m.in. zbieranie wyłącznie niezbędnych danych, wyłączanie niekoniecznych funkcji śledzących i profilujących oraz udostępnianie danych osobowych innym podmiotom tylko wtedy, gdy użytkownik wyrazi na to wyraźną, świadomą zgodę.
Privacy by design – ochrona prywatności w fazie projektowania	Podejście do projektowania systemów, procesów i usług, w którym wymagania dotyczące ochrony danych osobowych oraz prywatności są uwzględniane od najwcześniejszych etapów cyklu życia rozwiązania (analiza, projekt, implementacja, utrzymanie). Obejmuje m.in. minimalizację zakresu danych, ograniczanie dostępu, pseudonimizację, szyfrowanie oraz projektowanie architektury w taki sposób, aby ryzyka dla prywatności były identyfikowane, oceniane i redukowane już na etapie koncepcji, a nie dopiero po wdrożeniu.

Prometheus	Otwartoźródłowy system monitoringu metryk i alertowania. Oprogramowanie typu open source do zbierania i przechowywania metryk czasowych oraz generowania alertów na podstawie reguł. W praktyce służy do monitorowania usług i infrastruktury poprzez cykliczne pobieranie metryk z endpointów i analizę ich zmian w czasie.
Provisioning – przygotowanie i udostępnianie zasobów	Proces przygotowania, konfiguracji i udostępnienia zasobów IT (np. kont użytkowników, maszyn wirtualnych, baz danych, usług sieciowych czy licencji) zgodnie z określonym szablonem lub polityką. Obejmuje zarówno utworzenie obiektu (np. konta, instancji), jak i nadanie mu odpowiednich parametrów technicznych oraz uprawnień, często realizowane automatycznie w ramach systemów zarządzania tożsamością lub platform chmurowych.
Pryncypia technologiczne (ang. *technology principles*)	Zestaw podstawowych, trwałych zasad oraz wytycznych używanych przy procesach podejmowania wszystkich decyzji dotyczących architektury, technologii, rozwoju i zarządzania systemami informatycznymi (w ramach organizacji). Definiują podstawowe relacje między strategią biznesową a architekturą IT, zapewniając spójność technologiczną i wielodziedzinową efektywność przy realizacji celów biznesowych.
Przejęcie konta (ang. *account takeover*)	Cyberatak, który ma umożliwić uzyskanie dostępu do profilu ofiary, np. w celu wyłudzenia danych, rozsyłania spamu czy oszukania znajomych. Najczęstsze metody ataku to: phishing, malware czy kradzież haseł. Ochroną jest np. częsta zmiana haseł czy uwierzytelnianie dwuskładnikowe.
Przetwarzanie w chmurze (ang. *cloud computing*)	Model dostarczania zasobów IT (mocy obliczeniowej, pamięci masowej, usług sieciowych, baz danych itp.) przez zewnętrznego dostawcę za pośrednictwem sieci, zwykle w rozliczeniu za faktyczne wykorzystanie. Użytkownik korzysta z zasobów udostępnianych zdalnie, bez konieczności posiadania i utrzymywania własnej fizycznej infrastruktury.
PQC (ang. *post-quantum cryptography*) – kryptografia postkwantowa	Zestaw algorytmów kryptograficznych projektowanych w taki sposób, aby pozostały bezpieczne również w warunkach dostępności komputerów kwantowych zdolnych do łamania części obecnie stosowanych schematów kryptografii klucza publicznego. PQC obejmuje m.in. mechanizmy uzgadniania kluczy i podpisu cyfrowego oparte na problemach obliczeniowych uznawanych za odporne na znane algorytmy kwantowe i służy do planowania migracji kryptograficznej w systemach o długim horyzoncie ochrony danych.

Puppet	System do zarządzania konfiguracją i automatyzacji, działający najczęściej w modelu serwer–agent. Umożliwia opis pożądanego stanu systemów (np. pakiety, usługi, pliki konfiguracyjne), a następnie egzekwuje ten stan na wielu serwerach, zmniejszając liczbę ręcznych zmian i ryzyko rozbieżności konfiguracji.
QoS (ang. *quality of service*) – jakość obsługi w sieci	Zestaw mechanizmów w infrastrukturze sieciowej, które pozwalają sterować sposobem traktowania ruchu, np. nadawać priorytety wybranym typom transmisji, rezerwować pasmo, ograniczać opóźnienia i wahania opóźnień oraz kontrolować poziom strat pakietów. W praktyce QoS służy do zapewnienia przewidywalnej jakości działania usług wrażliwych na opóźnienia (np. głos, wideo, systemy sterowania) przy współdzieleniu tej samej sieci z innymi rodzajami ruchu.
RADIUS (ang. *remote authentication dial-in user service*) – zdalna usługa uwierzytelniania, autoryzacji i rozliczania	Protokół sieciowy używany do centralnej obsługi uwierzytelniania użytkowników, nadawania im uprawnień oraz rejestrowania wykorzystania usług sieciowych. Zwykle współpracuje z urządzeniami dostępowymi (np. przełącznikami, punktami dostępowymi, koncentratorami VPN), które przekazują żądania logowania do serwera RADIUS, a następnie egzekwują decyzje o przyznaniu lub odmowie dostępu.
RAG (ang. *retrieval-augmented generation*) – generowanie wspomagane wyszukiwaniem	Architektura systemów opartych na dużych modelach językowych, w której przed wygenerowaniem odpowiedzi model wyszukuje relewantne fragmenty informacji w zewnętrznej bazie wiedzy (np. dokumentach organizacji), a następnie wykorzystuje je jako kontekst do generowania wyniku. Celem RAG jest zwiększenie trafności i aktualności odpowiedzi oraz ograniczenie generowania treści niepopartych danymi, przy zachowaniu kontroli nad źródłem informacji wykorzystywanym w odpowiedzi.

RAID (ang. *redundant array of independent disks*) – nadmiarowa macierz niezależnych dysków	Technologia organizacji i wirtualizacji pamięci masowej, która łączy wiele fizycznych komponentów pamięci masowej w jedną lub więcej jednostek logicznych w celu redundancji danych oraz poprawy wydajności. Jest to sposób wykorzystania w systemie komputerowym dwóch lub większej liczby dysków twardych, które współpracują pomiędzy sobą. Stwarza się w ten sposób szereg różnorodnych możliwości nieosiągalnych przy użyciu zarówno pojedynczego dysku, jak i kilku dysków podłączonych jako oddzielne jednostki.
Rancher	Platforma do centralnego zarządzania klastrami Kubernetes (często wieloma, w różnych środowiskach). Zapewnia ujednolicone zarządzanie konfiguracją, kontrolą dostępu, politykami oraz obserwowalnością, upraszczając operacje w środowiskach wieloklastrowych.
RBAC (ang. *role-based access control* – kontrola dostępu oparta na rolach	Model kontroli dostępu, w którym uprawnienia w systemie są przypisywane do ról, a użytkownik uzyskuje dostęp poprzez przypisanie mu jednej lub wielu ról. Role odzwierciedlają funkcje organizacyjne i zakres obowiązków, co upraszcza zarządzanie uprawnieniami, wspiera zasadę minimalnych uprawnień oraz ułatwia audyt i utrzymanie spójności polityk dostępu.
RDP (ang. *remote desktop protocol*) – protokół zdalnego pulpitu	Protokół komunikacyjny firmy Microsoft umożliwiający zdalne, interaktywne korzystanie z pulpitu systemu operacyjnego przez sieć. Pozwala przesyłać obraz, dźwięk, dane klawiatury i myszy między klientem a serwerem, dzięki czemu administrator lub użytkownik może pracować na zdalnej maszynie jak lokalnie, z zachowaniem mechanizmów uwierzytelniania i szyfrowania.
RedHat (Red Hat Enterprise Linux)	Komercyjna dystrybucja systemu Linux rozwijana przez firmę Red Hat, ukierunkowana na zastosowania serwerowe i korporacyjne. Oferuje długi cykl wsparcia, certyfikacje dla środowisk biznesowych oraz ekosystem narzędzi do zarządzania infrastrukturą i wsparcia technicznego.
Replikacja danych	Tworzenie i utrzymywanie kopii danych na wielu serwerach (replikach), co zapewnia ich dostępność, odporność na awarie, lepszą wydajność i skalowalność poprzez rozkładanie obciążenia. Pozwala na szybkie przełączenie na kopię w razie problemów. Jest to rozwiązanie ograniczające czas przestojów (podstawa strategii ciągłości działania i *disaster recovery*).

REST (ang. *representational state transfer*) – architektury REST	Styl architektury projektowania usług sieciowych, w którym aplikacje udostępniają zasoby przez jednolity interfejs, zwykle na podstawie protokołu HTTP. Komunikacja opiera się na prostych operacjach na zasobach (np. odczyt, modyfikacja, usunięcie), a serwer nie utrzymuje stanu sesji klienta, co upraszcza skalowanie i integrację różnych systemów.
REST API (ang. *representational state transfer api*) – model architektoniczny budowania usług internetowych	Używa standardowych żądań HTTP do komunikacji między systemami, traktując dane jako zasoby, którymi można zarządzać za pomocą metod takich jak: GET, POST, PUT i DELETE, zwykle wymieniając dane w formacie JSON (ang. *JavaScript Object Notation*).
RESTCONF (ang. *representational state transfer configuration*) – protokół interfejsu programistycznego)	Umożliwia dostęp do danych zdefiniowanych w YANG za pośrednictwem REST API. Jest protokołem bezstanowym wykorzystującym protokół HTTPS do przesyłania konfiguracji, stanów oraz procedur RPC. Ma zastosowanie przy prostych zmianach konfiguracji realizowanych sekwencyjnie jedna po drugiej, przy odpytywaniu o stan oraz zbieraniu danych statystycznych.
ROI (ang. *return on investment*) – zwrot z inwestycji	Wskaźnik opisujący relację pomiędzy zyskiem osiągniętym z inwestycji a poniesionymi nakładami, wyrażany zazwyczaj w procentach. W obszarze IT i projektów cyfrowych służy do oceny opłacalności przedsięwzięć, porównywania wariantów rozwiązań oraz uzasadniania biznesowego wydatków na infrastrukturę, oprogramowanie i usługi.
Round Robin – algorytm Round Robin, „rotacyjne" przydzielanie	Sposób rozdzielania zadań lub ruchu sieciowego, w którym kolejne żądania kierowane są po kolei do każdego serwera z puli, w stałej, cyklicznej kolejności. Zapewnia prosty, równomierny rozkład obciążenia, ale nie uwzględnia aktualnego stanu ani wydajności poszczególnych serwerów.

RPA (ang. *robotic process automation*) – robotyczna automatyzacja procesów	Technologia automatyzacji powtarzalnych czynności wykonywanych w aplikacjach poprzez „roboty programowe", które naśladują działania użytkownika (np. odczyt i wprowadzanie danych, obsługa formularzy, generowanie dokumentów, realizacja kroków w kilku systemach). RPA działa na poziomie interfejsów aplikacji i reguł procesowych, dzięki czemu umożliwia automatyzację bez głębokiej przebudowy systemów, przy zachowaniu kontroli dostępu, rejestrowania działań i zasad nadzoru operacyjnego.
RTOS (ang. *real-time operating system*) – system operacyjny czasu rzeczywistego	System operacyjny zaprojektowany do uruchamiania zadań z gwarantowanymi ograniczeniami czasowymi, tak aby reakcja na zdarzenia następowała w przewidywalnym czasie. RTOS zapewnia deterministyczne planowanie zadań (priorytety, przerwania), kontrolę opóźnień oraz mechanizmy synchronizacji i komunikacji między zadaniami, co jest istotne w systemach wbudowanych, automatyce i rozwiązaniach krytycznych, gdzie przekroczenie czasu reakcji traktuje się jako błąd działania.
SaaS (ang. *software as a service*) – oprogramowanie jako usługa	Jeden z modeli usługi przetwarzania w chmurze, w którym dostawca usługi hostuje oprogramowanie klienta.
Saga – wzorzec saga	Sekwencja transakcji lokalnych, w których każda usługa wykonuje operację i inicjuje następny krok za pośrednictwem zdarzeń lub komunikatów. Jeśli krok w sekwencji zakończy się niepowodzeniem, saga wykonuje transakcje wyrównywujące, aby cofnąć ukończone kroki. Takie podejście pomaga zachować spójność danych.
SAM (ang. *software asset management*)	Infrastruktura i procesy niezbędne do sprawnego zarządzania, kontroli i ochrony zasobów programowych organizacji na wszystkich etapach ich cyklu życia (od zakupu aż do wycofania oprogramowania). SAM jest częścią szerszej dziedziny IT Asset Management (ITAM) – skupia się tylko na oprogramowaniu.

SASE (ang. *secure access service edge*) – brzeg usługi bezpiecznego dostępu	Architektura łącząca funkcje sieciowe i funkcje bezpieczeństwa w jedną usługę dostarczaną z chmury, jak najbliżej użytkownika lub urządzenia. Umożliwia bezpieczne, kontrolowane połączenie z aplikacjami i danymi (w chmurze i w centrach danych) niezależnie od lokalizacji użytkownika, upraszczając infrastrukturę i centralizując egzekwowanie polityk bezpieczeństwa.
SCCM (ang. *system center configuration manager*) – platforma zarządzania konfiguracją stacji roboczych i serwerów	Oprogramowanie firmy Microsoft do centralnego zarządzania komputerami i serwerami w organizacji. Służy m.in. do inwentaryzacji sprzętu i oprogramowania, zdalnej instalacji systemów i aplikacji, dystrybucji aktualizacji oraz egzekwowania wybranych polityk konfiguracyjnych.
SCI (ang. *software carbon intensity*) – intensywność węglowa oprogramowania	Wskaźnik opisujący wielkość emisji gazów cieplarnianych przypisywaną działaniu oprogramowania w odniesieniu do zdefiniowanej jednostki funkcjonalnej (np. transakcji, żądania, użytkownika, godziny działania). SCI uwzględnia emisje wynikające ze zużycia energii przez zasoby obliczeniowe, pamięć masową i transmisję danych oraz emisyjność energii elektrycznej w danym środowisku uruchomieniowym, dzięki czemu wspiera porównywanie wariantów architektury i optymalizację pod kątem śladu węglowego.
Scrum	Framework pracy zespołowej należący do rodziny podejść Agile, definiujący role (np. właściciel produktu, zespół deweloperski, osoba odpowiedzialna za proces), artefakty (np. backlog produktu, backlog sprintu) oraz zdarzenia (np. sprint, planowanie, przegląd, retrospektywa). Scrum organizuje pracę w stałych iteracjach (sprintach), w których zespół dostarcza potencjalnie gotowy do użycia przyrost produktu, utrzymując przejrzystość postępu i regularnie dostosowując sposób pracy.
SDS (ang. *software-defined storage*) – pamięć masowa definiowana programowo	Zasób, który oddziela oprogramowanie zarządzające pamięcią od fizycznego sprzętu. Umożliwia wirtualizację i centralne zarządzanie zasobami dyskowymi (np. od różnych dostawców) jako jednolitą pulą. Zapewnia to większą elastyczność, skalowalność i wydajność dzięki niezależności od konkretnego sprzętu.

Sensory/czujniki (ang. *sensors*)	Urządzenia lub moduły pomiarowe, które rejestrują wielkości fizyczne lub środowiskowe (np. temperatura, ciśnienie, ruch, pozycja, natężenie światła) i przekształcają je na sygnały cyfrowe wykorzystywane przez systemy informatyczne. W kontekście IT/OT i IoT sensory są źródłem danych dla systemów monitoringu, automatyki, analityki oraz systemów autonomicznych, a ich parametry (dokładność, częstotliwość próbkowania, kalibracja) wpływają bezpośrednio na jakość pozyskiwanych danych.
Service mesh – sieć usług/warstwa siatki usług	Warstwa infrastruktury w architekturach opartych na usługach (np. mikroserwisach), która przejmuje odpowiedzialność za komunikację między usługami. Dostarcza funkcje takie jak: trasowanie i równoważenie ruchu między instancjami, szyfrowanie połączeń, obserwowalność (metryki, logi, śledzenie zapytań) oraz egzekwowanie polityk bezpieczeństwa – bez konieczności implementowania tego w kodzie każdej usługi.
SFC (ang. *service function chaining*) – łańcuchowanie funkcji usługowych	Mechanizm budowy logicznej ścieżki, którą przechodzi ruch sieciowy przez kolejne funkcje usługowe, takie jak: zapora, system wykrywania włamań, optymalizator WAN, równoważnik obciążenia czy proxy. Zamiast sztywnego trasowania przez fizyczne urządzenia łańcuch funkcji jest opisany programowo i może dynamicznie kierować ruch przez wybrane funkcje w określonej kolejności.
Shadow IT	Wykorzystanie nieautoryzowanych narzędzi, systemów, aplikacji, urządzeń lub usług IT przez organizację.
Sharding – podział danych na partycje logiczne	Technika skalowania systemów przechowywania lub przetwarzania danych polegająca na podziale zbioru danych na niezależne logiczne fragmenty (shardy), rozproszone pomiędzy wiele węzłów lub instancji. Każdy fragment obsługuje tylko część danych i zapytań, co zmniejsza obciążenie pojedynczego węzła oraz umożliwia poziome skalowanie baz danych lub rejestrów rozproszonych.
Skanery podatności	Zautomatyzowane narzędzia (oprogramowanie) służące do identyfikacji, analizy i raportowania luk w zabezpieczeniach sieci, systemów i aplikacji. Działanie polega na porównaniu analizowanego obiektu z bazami znanych zagrożeń. Skanery pomagają wykryć przestarzałe oprogramowanie, otwarte porty, niepoprawne konfiguracje i tym samym uchronić przed cyberprzestępcami.

Sketch	Edytor grafiki wektorowej, przeznaczony głównie do projektowania interfejsów użytkownika (UI/UX) aplikacji mobilnych i stron internetowych.
SLA dla IT (ang. *service level agreement*) – umowa o gwarantowanym poziomie usług	Formalny dokument, który określa gwarantowany poziom dostępności, wydajności i jakości usług informatycznych świadczonych przez dostawcę na rzecz klienta (czas reakcji, czas usunięcia problemu, obowiązki obu stron, procedury naprawcze, kary umowne itd.)
SLM (ang. *software license management*)	Proces zarządzania, kontrolowania i optymalizacji licencji oprogramowania w organizacji na przestrzeni całego ich cyklu życia. Zapewnia zgodność z prawem oraz optymalizację kosztów poprzez identyfikację nieużywanego oprogramowania oraz minimalizację ryzyka operacyjnego.
Smart kontrakty (ang. *smart contracts*) – inteligentne umowy	Programy uruchamiane w infrastrukturze rozproszonego rejestru (np. blockchain), które automatycznie egzekwują zdefiniowane w nich reguły po spełnieniu określonych warunków. Smart kontrakt łączy zapis logiki biznesowej z przechowywaniem stanu w rejestrze, a wykonanie jego kodu prowadzi np. do przeniesienia aktywów cyfrowych, aktualizacji danych lub wywołania innych funkcji w sposób deterministyczny i rejestrowany w łańcuchu bloków.
Snapshot – migawka systemu/ danych	Zapis stanu systemu, maszyny wirtualnej, wolumenu dyskowego lub bazy danych w konkretnym momencie czasu. Migawka pozwala szybko przywrócić system do tego stanu (np. przed aktualizacją lub zmianą konfiguracji), bez pełnego odtwarzania z kopii zapasowej.
SNMP (ang. *simple network management protocol*) – prosty protokół zarządzania siecią	Protokół używany do monitorowania i zdalnego zarządzania urządzeniami sieciowymi, takimi jak: przełączniki, routery, zapory, serwery czy drukarki sieciowe. Umożliwia odczyt parametrów pracy, odbieranie pułapek alarmowych oraz wprowadzanie wybranych zmian konfiguracyjnych z systemów nadzorczych.
SOAP (ang. *simple object access protocol*)	Protokół komunikacyjny oparty na XML. Umożliwia wymianę strukturalnych informacji w zdecentralizowanym i rozproszonym środowisku.

SOC (ang. *security operations center*) – centrum operacji bezpieczeństwa/ centrum monitorowania bezpieczeństwa	Wyspecjalizowana jednostka organizacyjna łącząca zespół, procesy i narzędzia, odpowiedzialna za ciągły monitoring środowiska IT/OT, zbieranie i korelację zdarzeń bezpieczeństwa, wykrywanie anomalii, nadawanie priorytetów zgłoszeń – triaż (ang. *triage*) i obsługę incydentów. SOC wdraża i rozwija reguły detekcji, współpracuje z zespołami reagowania, utrzymuje widoczność stanu bezpieczeństwa organizacji i wspiera podejmowanie decyzji w czasie rzeczywistym.
SoC (ang. *system on a chip*) – system na układzie scalonym	Zintegrowany układ scalony, który łączy w jednym chipie kluczowe komponenty systemu komputerowego, takie jak: jednostka obliczeniowa, kontrolery pamięci, interfejsy wejścia/wyjścia oraz moduły komunikacyjne. SoC jest stosowany w urządzeniach wbudowanych i mobilnych, gdzie liczą się ograniczenia przestrzeni, poboru mocy i kosztu, a wysoki poziom integracji upraszcza konstrukcję sprzętu i umożliwia budowę kompaktowych systemów.
Sokrata (ang. *Socrata*)	Platforma do publikowania i udostępniania danych (często publicznych) w formie katalogów danych oraz interfejsów API, używana przez organizacje do zwiększania dostępności i wykorzystania oraz publikacji danych otwartych.
Spine-leaf – architektura spine-leaf	Topologia sieci centrów danych, w której przełączniki rdzeniowe (spine) łączą się w sposób pełnej lub prawie pełnej siatki z przełącznikami dostępowymi (leaf). Każdy przełącznik dostępu ma połączenia do wielu przełączników rdzeniowych, co zapewnia przewidywalną liczbę skoków, dużą przepustowość w poziomie i łatwe skalowanie poprzez dodawanie kolejnych przełączników leaf i spine.
SSH (ang. *secure shell*) – bezpieczna powłoka zdalna	Szyfrowany protokół sieciowy służący do zdalnego logowania na systemy, wykonywania poleceń oraz bezpiecznego przesyłania plików. Zapewnia poufność i integralność danych dzięki szyfrowaniu komunikacji oraz umożliwia silne uwierzytelnianie (np. klucze kryptograficzne zamiast haseł).
SSID (ang. *service set identifier*) – identyfikator/ nazwa sieci bezprzewodowej	Nazwa nadawana sieci Wi-Fi, wyświetlana użytkownikowi przy wyborze sieci do połączenia. SSID służy do logicznego rozróżniania wielu sieci pracujących w tym samym obszarze radiowym; jedno urządzenie może nadawać kilka różnych identyfikatorów SSID, aby wydzielić różne grupy użytkowników lub usługi (np. sieć firmową i gościnną).

SSO (ang. *single sign-on*) – logowanie jednokrotne	Mechanizm uwierzytelniania, który umożliwia dostęp do wielu aplikacji lub systemów za pomocą jednorazowego logowania.
Sterowniki/układy sterujące (ang. *drivers*, *controllers*)	Urządzenia lub moduły logiczne przetwarzające sygnały z sensorów i generujące sygnały sterujące dla aktuatorów, zgodnie z zaprogramowanymi algorytmami sterowania. W środowiskach przemysłowych są to najczęściej sterowniki programowalne (np. PLC), realizujące logikę procesu, nadzór, zabezpieczenia oraz komunikację z systemami nadrzędnymi.
Stos technologiczny (ang. *technology stack*)	Zestaw technologii używanych do budowy i utrzymania rozwiązania IT, który obejmuje: języki programowania, frameworki, biblioteki, systemy baz danych, narzędzia integracyjne, komponenty front-end i back-end, elementy infrastruktury oraz usługi chmurowe. Opis stosu technologicznego pokazuje, na jakich komponentach technicznych opiera się dany system lub cała architektura.
Struct (ang. *structure*) – struktura danych	Złożony typ danych używany w językach programowania (w tym w językach smart kontraktów) do grupowania kilku powiązanych pól w jedną logiczną całość. Struktura definiuje zestaw nazwanych atrybutów (np. identyfikator, właściciel, saldo), które są przechowywane i przetwarzane jako jeden obiekt, co ułatwia modelowanie bardziej złożonych encji w kodzie i w stanie kontraktu.
Syslog (ang. *system logging protocol*) – protokół logowania systemowego	Protokół i format komunikatów używany do przesyłania logów z systemów, aplikacji i urządzeń sieciowych na serwer zbierający logi. Umożliwia centralne gromadzenie, filtrowanie i analizę zdarzeń (np. błędów, ostrzeżeń, logowań) z wielu źródeł, co jest podstawą monitoringu i budowy systemów detekcji incydentów.
System czasu rzeczywistego (ang. *real-time system*)	System informatyczny, w którym poprawność działania zależy nie tylko od wyniku obliczeń, ale także od reagowania na zdarzenia w określonym czasie. System czasu rzeczywistego zapewnia przewidywalność opóźnień i terminową realizację zadań sterujących lub przetwarzających dane, co jest kluczowe m.in. w automatyce, systemach wbudowanych i rozwiązaniach krytycznych.

System krytyczny	System, którego zakłócenie działania lub awaria mogą spowodować poważne konsekwencje dla bezpieczeństwa ludzi, ciągłości działania organizacji, środowiska lub infrastruktury. Wymaga podwyższonych wymagań w zakresie niezawodności, dostępności, bezpieczeństwa (w tym cyberbezpieczeństwa), nadmiarowości oraz ścisłej kontroli zmian w całym cyklu życia.
System wbudowany (ang. *embedded system*)	Wyspecjalizowany system komputerowy będący częścią większego urządzenia lub instalacji, zaprojektowany do realizacji określonych funkcji sterowania, pomiaru lub komunikacji. System wbudowany działa zwykle na ograniczonych zasobach sprzętowych, pracuje w sposób ciągły lub w trybie czasu rzeczywistego i jest ściśle powiązany z elementami fizycznymi urządzenia, np. czujniki zbierające dane z otoczenia, sterujące urządzeniem na podstawie oprogramowania układowego, tzw. firmware (np. lodówka, czujnik temperatury, rozrusznik serca).
Sztuczna inteligencja (ang. *Artificial Intelligence*, AI)	Sztuczna inteligencja to dziedzina informatyki, która tworzy systemy zdolne do autonomicznego osiągania swoich celów, uczące się na podstawie własnych doświadczeń i adaptujące się do nowych danych. Sztuczna inteligencja może być wdrażana przy użyciu różnych technik, takich jak: uczenie maszynowe, uczenie głębokie, systemy eksperckie, algorytmy genetyczne, sieci neuronowe i przetwarzanie języka naturalnego.
Szyfrowanie komunikacji	Proces konwersji danych na kod znany tylko przez upoważnionych odbiorców. Dzięki odpowiednim kluczom chroni dane przed podsłuchem i nieautoryzowanym dostępem. Zabezpiecza dane w spoczynku i podczas przesyłania, a jego implementacja jest często wymogiem regulacyjnym.
Środowisko aplikacyjne	Określony zbiór zasobów sprzętowych, programowych i sieciowych, który hostuje aplikację i umożliwia jej prawidłowe funkcjonowanie. Takie środowisko zawiera wszystko, co jest potrzebne do uruchamiania, zarządzania, testowania i rozwijania aplikacji.
Środowisko deweloperskie (ang. *development environment*)	Specjalnie skonfigurowane środowisko, w którym programiści tworzą, testują i rozwijają oprogramowanie. Zapewnia niezbędne narzędzia, biblioteki, środowisko wykonawcze i inne zasoby potrzebne do pisania, debugowania i testowania kodu.

Środowisko GIT (ang. *distributed version control system*, DVCS),	Rozproszony system kontroli wersji, który pozwala na śledzenie zmian w plikach (zazwyczaj kodu źródłowego), efektywną współpracę nad projektem w zespole i łatwe przywracanie poprzednich wersji, dzięki czemu wielu osób może efektywnie współpracować nad tym samym kodem. Działa lokalnie, ale jest często używany z platformami chmurowymi (jak GitHub lub GitLab) do hostowania repozytoriów i koordynacji pracy zespołowej.
Środowisko pre-prod/ przedprodukcyjne (ang. *pre-production environment*)	Kluczowy etap w cyklu tworzenia oprogramowania, będący niemal kopią środowiska produkcyjnego (prod). Jego celem jest testowanie najnowszych wersji aplikacji i aktualizacji w warunkach jak najbardziej zbliżonych do realnych, ale bez ryzyka wpływu na działającą produkcję, poprzez używanie danych zanonimizowanych lub syntetycznych, jednak z prawdziwymi danymi uwierzytelniającymi, by wychwycić ewentualne błędy przed wdrożeniem produkcyjnym.
Środowisko prod (ang. *production environment*) – środowisko produkcyjne	Rzeczywiste, finalne środowisko, w którym wdrożone oprogramowanie jest udostępniane końcowym użytkownikom do wykonywania zadań biznesowych. Różni się od środowisk deweloperskich (dev) czy testowych (test) i charakteryzuje się najwyższym priorytetem stabilności, bezpieczeństwa, wydajności i dostępności.
Środowisko sieciowe (ang. *network environment*)	Termin odnoszący się do infrastruktury, technologii i zasobów, które umożliwiają urządzeniom elektronicznym łączenie się i komunikację ze sobą. Obejmuje to zarówno sprzęt fizyczny (Ethernet, światłowody, fale radiowe), jak i oprogramowanie (programy i protokoły), które zarządzają ruchem danych, bezpieczeństwem i funkcjonalnością sieci.
Środowisko sprzętowe (ang. *hardware environment*)	Zbiór wszystkich fizycznych komponentów i urządzeń, które składają się na system komputerowy lub infrastrukturę IT. Komponenty te stanowią platformę, na której działa oprogramowanie.
Środowisko testowe (ang. *test environment*)	Odizolowana, kontrolowana przestrzeń symulująca produkcyjne warunki, służąca do sprawdzania, czy nowa wersja oprogramowania działa poprawnie, zanim zostanie wdrożona. Obejmuje zazwyczaj bazę danych, serwery i infrastrukturę i zapewnia bezpieczeństwo systemom.

Tablice przepływów/ tablice reguł przepływu ruchu (ang. *flow tables*)	Struktury danych w urządzeniach sieciowych lub warstwie wirtualnej, które zawierają reguły opisujące postępowanie z określonym ruchem sieciowym. Każdy wpis w tablicy definiuje warunki dopasowania (np. adresy, porty, typ protokołu) oraz akcje (np. przekazanie na wskazany port, modyfikację nagłówków, odrzucenie, przekazanie do modułu analizy), co pozwala sterować przepływami ruchu w sposób precyzyjny i programowalny.
Tagowanie projektów	Proces przypisywania etykiet, słów kluczowych lub metadanych do elementów projektu, aby móc je organizować, kategoryzować i ułatwić wyszukiwanie oraz zarządzanie nimi. Polega na dodawaniu opisowych tagów do cyfrowych zasobów, co pozwala na szybkie filtrowanie i odnajdywanie powiązanych informacji w ramach platformy do zarządzania projektami.
TCO (ang. *total cost of ownership*) – całkowity koszt posiadania	Szacunkowy, całkowity koszt zasobu IT (np. systemu, aplikacji, infrastruktury) liczony w całym cyklu życia, obejmujący nie tylko zakup, ale także koszty wdrożenia, utrzymania, licencji, szkoleń, rozwoju, wsparcia, energii oraz wycofania rozwiązania z eksploatacji. TCO służy do porównywania wariantów technicznych pod kątem ich rzeczywistej długoterminowej opłacalności.
TCP/IP (ang. *transmission control protocol/ internet protocol*) – rodzina protokołów komunikacyjnych TCP/IP	Zestaw protokołów komunikacyjnych używanych w internecie i sieciach IP. Obejmuje warstwę odpowiedzialną za adresowanie i przekazywanie pakietów między sieciami oraz warstwę zapewniającą niezawodne dostarczenie strumieni danych między aplikacjami (kontrola połączenia, kolejności i integralności danych).
TeamViewer	Oprogramowanie do zdalnego dostępu (ang. *remote access*), zdalnego sterowania (ang. *remote control*) i zdalnego wsparcia technicznego (ang. *remote support*). Zapewnia nawiązanie bezpiecznego, zaszyfrowanego połączenia między dwoma komputerami lub urządzeniami mobilnymi przez internet.

Terraform	Narzędzie typu „infrastruktura jako kod" służące do deklaratywnego opisu i automatycznego tworzenia oraz modyfikowania infrastruktury (chmurowej i lokalnej). Pozwala definiować zasoby w plikach konfiguracyjnych i utrzymywać ich stan w sposób wersjonowany, tak aby odtwarzanie i zmiany środowisk były powtarzalne i kontrolowane.
Testy bezpieczeństwa API	Proces wykrywania luk i podatności w interfejsach programowania aplikacji. Test symuluje atak hakerów, co pozwala na wyłapywanie słabych punktów i ochronę danych przed nieautoryzowanym dostępem, modyfikacją czy kradzieżą. Proces analizy danych obejmuje testy uwierzytelniania, autoryzacji, walidacji, szyfrowania i odporności na ataki, z wykorzystaniem metod manualnych i automatycznych.
Testy penetracyjne (ang. *penetration tests, pentests*)	Testy bezpieczeństwa systemu informatycznego mające na celu wykrycie podatności (słabości) systemu poprzez próbę odwzorowania działań, które mogą wystąpić podczas ataku hakerskiego. Testy mogą być prowadzone ręcznie przez testera lub w sposób częściowo zautomatyzowany poprzez wykorzystanie gotowych exploitów, tj. schematów zawierających przykłady podatności systemów komputerowych. Celem testów penetracyjnych jest nie tylko wyszukiwanie podatności, ale również próba ich wykorzystania jako miejsce „włamania" do systemu. Testy penetracyjne obejmują działania w postaci testów bezpieczeństwa fizycznego i socjotechnicznego.
Testy socjotechniczne	Proces symulacji ataków hakerskich badający odporność pracowników i procedur bezpieczeństwa na manipulację psychologiczną. Testy polegają na podszywaniu się pod zaufane osoby lub instytucje albo wykorzystywaniu fizycznych słabości (np. pozostawiony pendrive) w celu wyłudzenia poufnych danych, haseł czy uzyskania nieautoryzowanego dostępu. Głównym celem testów jest identyfikacja luk w zabezpieczeniach wynikających z czynnika ludzkiego i podniesienie świadomości pracowników, którzy najczęściej są najsłabszym ogniwem w procesie zabezpieczania danych.

TLS/SSL termination (ang. *transport layer security/secure sockets layer termination*) – terminacja TLS/SSL	Mechanizm, w którym szyfrowane połączenie oparte na protokołach TLS/SSL jest zakończone na urządzeniu pośredniczącym (np. równoważniku obciążenia, serwerze pośredniczącym). Urządzenie odszyfrowuje ruch przychodzący od klienta, a następnie przekazuje go dalej do serwerów aplikacyjnych w postaci odszyfrowanej lub ponownie szyfrowanej, upraszczając zarządzanie certyfikatami i odciążając serwery.
TO-BE	Model analizy procesów biznesowych opisujący stan oczekiwany (docelowy), pozbawiony mankamentów i ograniczeń opisanych w stanie początkowym (AS-IS).
TOGAF (ang. *the open group architecture framework*)	Otwarty standard i kompleksowa metodologia projektowania, planowania, wdrażania oraz zarządzania architekturą korporacyjną (ang. *enterprise architecture*, EA). Pomaga organizacjom powiązać cele biznesowe z infrastrukturą IT, zapewnia ujednolicenie zarządzania złożonymi systemami i wspiera transformację cyfrową. Kluczowym elementem TOGAF jest metoda rozwoju architektury (ang. *architecture development method*, ADM), czyli sekwencyjny proces tworzenia architektury obejmujący cztery domeny: biznes, aplikacje, dane i technologię.
Token Ring	Technologia budowy sieci lokalnych oparta na logicznej topologii pierścienia, w której prawo do nadawania danych otrzymuje kolejno każde urządzenie poprzez tzw. token (specjalną ramkę krążącą w sieci). Zapewnia deterministyczny dostęp do medium (łatwo przewidzieć, kiedy urządzenie będzie mogło nadawać). Historycznie stosowana głównie w sieciach firmowych, dziś praktycznie wyparta przez Ethernet.
UCD (ang. *user-centered design*) – projektowanie zorientowane na użytkownika	Podejście, w którym potrzeby, wymagania i ograniczenia końcowego użytkownika są stawiane w centrum całego procesu tworzenia produktu lub usługi, aby zapewnić maksymalną użyteczność, intuicyjność i satysfakcję z użytkowania. Polega na szczegółowym badaniu docelowej grupy użytkowników i angażowaniu ich na każdym etapie projektowania.
UI (ang. *user interface*)	W IT to wszystko, co użytkownik widzi i z czym wchodzi w interakcję w aplikacjach, systemach czy na stronach www – przyciski, menu, kolory, układy, ikony itp.

UML (ang. *unified modeling language*)	Zunifikowany język modelowania służący do modelowania problemów (specyfikacji, konstruowania i dokumentowania funkcjonowania różnego rodzaju systemów). Jest to zbiór różnych elementów, które pomagają zrozumieć strukturę i zachowanie systemu przed, w trakcie i po jego zbudowaniu. UML jest przeważnie używany wraz ze swoją reprezentacją graficzną (jego elementom przypisane są odpowiednie symbole i relacje modelujące). UML jest oficjalnie zdefiniowany przez Object Management Group (OMG).
UPS (ang. *uninterruptible power supply*)	Urządzenie lub system, którego funkcją jest dostarczanie zasilania na wypadek przerw w dostawach energii elektrycznej w sieciach energetycznych.
Uptime Institute Tier Standard	Zestaw kryteriów klasyfikacji centrów danych do czterech poziomów (Tier I–IV) wg ich odporności na awarie i zapewnianej dostępności usług. Standard opisuje m.in. wymagania dotyczące redundancji zasilania i chłodzenia, możliwości prowadzenia prac serwisowych bez przerw oraz odporności na pojedyncze uszkodzenia, co pozwala porównywać niezawodność różnych obiektów.
User flow	Wizualna reprezentacja ścieżki, jaką użytkownik pokonuje w produkcie cyfrowym (stronie, aplikacji), aby osiągnąć określony cel, np. dokonać zakupu, zarejestrować się, znaleźć informację. Jest to kluczowe narzędzie w projektowaniu UX, mapujące kolejne kroki, interakcje (kliknięcia, wpisywanie danych) i decyzje użytkownika oraz pomagające tworzyć najbardziej intuicyjną, płynną i efektywną ścieżkę.
Usługa cyfrowa	Interaktywne rozwiązanie online, które umożliwia użytkownikom tworzenie, przetwarzanie, przechowywanie lub dostęp do danych w formie cyfrowej. Podstawowe przykłady obejmują platformy mediów społecznościowych, usługi finansowe, serwisy streamingowe, wyszukiwarki internetowe, aplikacje mobilne, itp.
UX	Całościowe doświadczenie użytkownika związane z korzystaniem i interakcją z produktem cyfrowym, obejmujące jego użyteczność, dostępność, emocje oraz poziom satysfakcji.
UXPin	Zaawansowane narzędzie (oprogramowanie) do projektowania interfejsów użytkownika (UI) i doświadczeń użytkownika (UX), które pozwala tworzyć interaktywne prototypy, makiety stron i aplikacji oraz umożliwia zespołom wspólną pracę nad produktami oraz ich testowanie.

VDI (ang. *virtual desktop infrastructure*)	Technologia wirtualizacji pozwalająca na hostowanie środowisk desktopowych (systemów operacyjnych i aplikacji) na centralnym serwerze lub klastrze serwerów w centrum danych lub w chmurze w celu dostarczania zdalnie usług użytkownikom końcowym.
Vendor lock-in	Stan, w którym klient uzależnia się od produktów lub usług jednego dostawcy (np. oprogramowania, platformy chmurowej). Następstwem tego jest sytuacja, w której przejście na konkurencyjne rozwiązanie staje się zbyt trudne, technicznie skomplikowane lub nieopłacalne finansowo. Wynika to z zastosowania specjalistycznych technologii, formatów danych czy długoterminowych umów ograniczających elastyczność i zdolność negocjacji.
VLAN (ang. *virtual local area network*)	Logiczne wydzielenie kilku odrębnych sieci w ramach jednej fizycznej infrastruktury przełączników. Umożliwia odseparowanie ruchu (np. dział finansów, goście) bez konieczności budowy osobnych kabli czy przełączników. Identyfikacja odbywa się poprzez znacznik VLAN w ramce (tagowanie portów lub ruchu), dzięki czemu administrator kontroluje, które urządzenia „widzą się" wzajemnie w tej samej domenie rozgłoszeniowej.
VM (ang. *virtual machine*)	Odizolowane środowisko uruchomieniowe, w którym system operacyjny i aplikacje działają jak na oddzielnym komputerze, choć współdzielą fizyczny sprzęt z innymi maszynami wirtualnymi. Maszyny wirtualne są tworzone i zarządzane przez oprogramowanie wirtualizacyjne, co pozwala elastycznie dzielić zasoby sprzętowe oraz łatwo przenosić i odtwarzać całe środowiska.
VNC (ang. *virtual network computing)*	System umożliwiający zdalne graficzne sterowanie pulpitem innego komputera. W odróżnieniu od RDP jest protokołem otwartym i wieloplatformowym.
VPN (ang. *virtual private network*)	Technologia, która tworzy bezpieczne i zaszyfrowane połączenie między urządzeniem a siecią (np. internetem lub firmową siecią lokalną). Działa jak tunel, który chroni dane przed podglądaniem, przechwyceniem i manipulacją. Informacje wewnątrz tunelu są zaszyfrowane.

Water Scrum Fall	Model organizacji projektu, w którym fazy analizy i wysokopoziomowego planowania są prowadzone w sposób kaskadowy, implementacja realizowana jest iteracyjnie z wykorzystaniem Scrum, a końcowe testy i wdrożenie odbywają się ponownie w układzie zbliżonym do podejścia kaskadowego. Model ten integruje pracę zwinnych zespołów z tradycyjnym otoczeniem organizacyjnym, które stosuje klasyczne procesy projektowe.
WCAG (ang. *web content accessibility guidelines*)	Międzynarodowy standard, zbiór wytycznych opublikowany przez World Wide Web Consortium (W3C), definiujący zasady tworzenia treści internetowych (strony www, aplikacje mobilne i inne zasoby cyfrowe) w sposób dostępny dla jak najszerszego grona użytkowników, a zwłaszcza osób z niepełnosprawnościami.
Weighted RR (ang. *weighted round robin*)	Odmiana algorytmu Round Robin, w której każdemu serwerowi przypisana jest waga odzwierciedlająca jego moc obliczeniową lub preferowany udział w obsłudze ruchu. Serwer o większej wadze otrzymuje proporcjonalnie więcej żądań, co umożliwia efektywniejsze wykorzystanie zróżnicowanej puli serwerów.
WEP (ang. *wired equivalent privacy*)	Mechanizm szyfrowania i uwierzytelniania w sieciach bezprzewodowych, wprowadzony jako pierwsza metoda ochrony Wi-Fi. Opiera się na stałym kluczu i prostym szyfrowaniu. Obecnie jest uważany za przestarzały i skrajnie niebezpieczny ze względu na liczne podatności i luki w bezpieczeństwie, które umożliwiają złamanie zabezpieczeń w ciągu kilku minut.
Wireframe	Uproszczony, schematyczny szkic interfejsu strony internetowej lub aplikacji, który koncentruje się na strukturze, układzie elementów (nagłówki, przyciski, pola tekstowe) i funkcjonalności, pomijając kolory, grafikę i stylizację. Służy do planowania logiki nawigacji i przepływu użytkownika (ang. *user flow*), ułatwiając wykrywanie problemów na wczesnym etapie projektowania.
WPA (ang. *Wi-Fi protected access*)	Rodzina mechanizmów ochrony sieci bezprzewodowych, która zastąpiła WEP, wprowadzając silniejsze szyfrowanie i dynamiczną wymianę kluczy. WPA umożliwia pracę z hasłem współdzielonym lub z centralnym serwerem uwierzytelniającym i jest standardowym sposobem zabezpieczania sieci Wi-Fi w organizacjach i w domu.

WSUS (ang. *windows server update services*)	Rola serwerowa systemów Microsoft Windows Server, która umożliwia centralne pobieranie, zatwierdzanie i dystrybucję aktualizacji systemów operacyjnych Windows oraz wybranych produktów Microsoft w środowisku sieci firmowych. Pozwala kontrolować, które poprawki i kiedy są instalowane na stacjach roboczych i serwerach, zmniejsza obciążenie łącza oraz umożliwia zgodność z polityką aktualizacji organizacji.
Wyciek danych (ang. *data leak*)	Nieautoryzowane ujawnienie poufnych, wrażliwych lub osobistych informacji (np. loginy, hasła, dane kart kredytowych, PESEL) podmiotom nieuprawnionym. Dane takie często są wykorzystywane do oszustw, kradzieży tożsamości czy włamań na konta. Wyciek może nastąpić na skutek celowych ataków hakerskich, błędów ludzkich lub luk w systemach informatycznych.
Wzorce architektury systemów (ang. *architectural patterns*)	Uogólnione, sprawdzone w praktyce schematy budowy systemów informatycznych opisujące podział na komponenty, warstwy i ich odpowiedzialności oraz sposób komunikacji między nimi. Wzorce architektoniczne (np. architektura warstwowa, mikroserwisy, architektura zdarzeniowa, architektura klient–serwer) stanowią punkt odniesienia przy projektowaniu rozwiązań, ułatwiając podejmowanie spójnych decyzji projektowych i komunikację między architektami a zespołami deweloperskimi.
YANG (ang. *yet another next generation*)	Język modelowania danych używany do formalnego opisu struktury konfiguracji i stanu urządzeń sieciowych oraz usług. Modele YANG definiują, jakie parametry są dostępne, jakie mają typy, zależności i ograniczenia, dzięki czemu narzędzia zarządzania (np. oparte na NETCONF czy RESTCONF) mogą w sposób spójny odczytywać i modyfikować konfiguracje wielu różnych urządzeń zgodnych z tym modelem.

Zabbix	Oprogramowanie (open source) klasy Enterprise służące do monitorowania sieci, serwerów, maszyn wirtualnych, kontenerów i usług w chmurze w czasie rzeczywistym. Służy do zbierania danych (metryk), monitorowania wydajności i generowania powiadomień o zdarzeniach. Umożliwia śledzenie wydajności i dostępności serwerów, maszyn wirtualnych, urządzeń sieciowych, baz danych oraz aplikacji i tworzy szczegółowe raporty oraz wykresy. Używa agentów lub protokołów takich jak SNMP, IPMI czy JMX do zbierania informacji i przedstawia je w panelu użytkownika.
Zarządzanie IT (ang. *IT management*)	Kompleksowy proces nadzorowania, administrowania i optymalizowania zasobów technologii informacyjnej w organizacji. Zarządzanie IT obejmuje szereg obszarów, w tym: sprzęt, oprogramowanie, sieci, dane, ludzi. Zarządzanie IT ma na celu wspieranie potrzeb biznesowych poprzez dostarczanie efektywnych i bezpiecznych usługi IT z uwzględnieniem zarządzania ryzykami.
Zero Trust	Model bezpieczeństwa zakładający brak domyślnego zaufania do jakiegokolwiek użytkownika, urządzenia czy usługi, niezależnie od tego, czy znajdują się „wewnątrz", czy „na zewnątrz" sieci organizacji. Dostęp do zasobów jest przyznawany wyłącznie na podstawie bieżącej weryfikacji tożsamości, kontekstu i stanu urządzenia, z minimalnymi niezbędnymi uprawnieniami oraz z silną segmentacją środowiska.
Zmiana (ang. *change*)	Dodanie, modyfikacja lub usunięcie czegokolwiek, co mogłoby mieć bezpośredni lub pośredni wpływ na usługi IT. Zmiany muszą być zarządzane w taki sposób, aby zminimalizować ryzyko incydentów powodujących zakłócenia osiągania celów biznesowych.