1. Omów przykłady zastosowań wybranych działów matematyki (np. Statystyki, Metod numerycznych, Matematyki dyskretnej) w przygotowaniu i realizacji projektów informatycznych.   
2. Scharakteryzuj właściwości wybranych systemów CMS (zarządzania treścią) i określ podstawowe obszary ich zastosowań.   
3. Scharakteryzuj wybrane narzędzia automatyzacji testowania programów desktopowych i aplikacji webowych.   
4. Porównaj właściwości stosowanych narzędzi dla potrzeb grafiki komputerowej i przetwarzania obrazów.   
5. Omów podstawowe właściwości i zastosowania rozproszonych baz danych.   
6. Omów etapy konstrukcji modelu przypadków użycia w procesie projektowania oprogramowania systemu informatycznego (SI) oraz jego opis w dokumentacji projektu SI.   
7. Scharakteryzuj właściwości i przeznaczenie diagramów języka UML.   
8. Scharakteryzuj stosowane w praktyce metody i narzędzia zarządzaniem projektami (project managment).   
9. Scharakteryzuj właściwości i zastosowania systemów rozproszonych.   
10. Scharakteryzuj przykłady zastosowań sztucznej inteligencji w wybranych rozwiązaniach informatycznych (np. w robotyce).   
11. Scharakteryzuj kanały komunikacji elektronicznej i perspektywy ich zastosowań (rozwoju).   
12. Scharakteryzuj narzędzia, jakie należy stosować do zgodnego z prawem zarządzania obiegiem informacji w formie elektronicznej.   
13. Omów znaczenie technologii Cloud Computing na dostępność, skalowalność, bezpieczeństwo i optymalizację kosztów świadczonych usług.   
14. Omów modele usługowe przetwarzania w chmurze obliczeniowej (Cloud Computing): SaaS (Software-as-a-Service), IaaS (Infrastructure as a Service), PaaS (Platform as a Service).   
15. Porównaj obszary zastosowań i właściwości usług w modelu chmury prywatnej, publicznej i ieszanej.   
16. Scharakteryzuj koncepcję „Four V” w odniesieniu do bezpieczeństwa Big Data.   
17. Porównaj technologie: GSM, Bluetooth, Wi-Fi.   
18. Scharakteryzuj właściwości i obszary zastosowań systemów WiFi-HotSpot oraz uprawnienia ich właścicieli.   
19. Scharakteryzuj techniki stosowane w centrach przetwarzania danych w celu poprawy ich efektywności energetycznej (tzw. zielone centrum danych).   
20. Scharakteryzuj sieciowe technologie zabezpieczające (Systemy firewall i VPN).   
21. Scharakteryzuj właściwości stosowanych narzędzi zabezpieczania poczty elektronicznej (Secure Mail).   
22. Omów zagrożenia bezpieczeństwa w Internecie Rzeczy (IoT - Internet of Things).   
23. Scharakteryzuj narzędzia stosowane do zarządzania bezpieczeństwem aplikacji dla urządzeń mobilnych.   
24. Scharakteryzuj zasady polityki bezpieczeństwa stosowane w przedsiębiorstwach (firmach) różnej skali.   
25. Scharakteryzuj zasady planowania ciągłości działania IT w firmie (DRP - Disaster Recovery Plan).   
26. Omów zagrożenia bezpieczeństwa wiążące się z wykorzystywaniem prywatnych urządzeń mobilnych (BYOD: Bring Your Own Device) do celów służbowych w firmie.   
27. Omów obsługę operacyjną incydentów bezpieczeństwa komputerowego.   
28. Scharakteryzuj narzędzia dla przedsiębiorstw, które umożliwiają bezpieczną współpracę pracownikom z różnych działów.   
29. Scharakteryzuj narzędzia dla urządzeń przenośnych, które umożliwiają utrzymanie kontaktu i wydajną pracę w podróży dla pracowników z różnych działów przedsiębiorstwa.

30. Omów procedurę reagowania na incydenty bezpieczeństwa IT w firmie

31. Opisz algorytm drzew decyzyjnych i zastosowania tego algorytmu w rzeczywistych scenariuszach inżynierskich.

32. Jakie są metody oceny modeli uczenia maszynowego i dlaczego jest to ważne?

33. Wyjaśnij, jak algorytmy uczenia maszynowego są stosowane do analizy i przetwarzania języka naturalnego.

34. Wyjaśnij, jak działają systemy rekomendacyjne i jaki mają wpływ na decyzje biznesowe i inżynieryjne.

35. Podaj przykład zastosowania uczenia maszynowego w specyficznym projekcie inżynierskim, opisując zarówno cel, jak i wykorzystane metody.36. Omów wpływ normalizacji danych w modelach uczenia maszynowego, zwłaszcza w kontekście algorytmów opartych na odległości, takich jak kNearest-Neighbours.

37. Jakie są różnice pomiędzy uczeniem się nadzorowanym, bez nadzoru i wzmocnionym w kontekście uczenia maszynowego?38. Omów etapy uczenia głębokiej sieci neuronowej z algorytmem propagacji wstecznej.

39. Omów metody k-najbliższych sąsiadów, maszynę wektorów nośnych i losowy las.

40. Na czym polega operacja splotu w kontekście przetwarzania obrazu i splotowych sieci neuronowych?

41. Opisz mechanizm przeszukiwania drzew SLD

42. Wyjaśnij pojęcie sieci neuronowych Hopfielda i ich zastosowania

43. Wyjaśnij pojęcie algorytmu propagacji wstecznej

44. Jakie są elementy robota?

45. Jakie są różne typy czujników stosowanych w robotyce?

46. Co to jest mikrokontroler?1. Omów przykłady zastosowań wybranych działów matematyki (np. Statystyki, Metod numerycznych, Matematyki dyskretnej) w przygotowaniu i realizacji projektów informatycznych.  
 Statystyka jest niezbędna do analizy danych, identyfikacji wzorców i trendów. W projektach informatycznych może być wykorzystywana do oceny wydajności systemów, monitorowania użytkowania i analizy danych wejściowych/wyjściowych. Modele statystyczne mogą być używane do przewidywania zachowań użytkowników lub prognozowania obciążenia systemu.  
 Teoria prawdopodobieństwa jest używana w modelowaniu zjawisk losowych. Może obejmować modele probabilistyczne w systemach bezpieczeństwa czy w algorytmach sztucznej inteligencji. Teoria prawdopodobieństwa jest także istotna w dziedzinie kryptografii, gdzie algorytmy oparte na teorii prawdopodobieństwa są używane do zabezpieczania danych.  
 Matematyka dyskretna jest powszechnie stosowana do struktur danych, takich jak sieci komputerowe czy relacje między danymi w bazach danych. Jest ona podstawą dla projektowania i analizy algorytmów. Algorytmy sortowania, przeszukiwania czy te używane w sztucznej inteligencji.  
2. Scharakteryzuj właściwości wybranych systemów CMS (zarządzania treścią) i określ podstawowe obszary ich zastosowań.   
 Systemy CMS są narzędziami, które pomagają tworzyć czy też edytować treści na stronach internetowych bez większej wiedzy technicznej. Oczywiście wybór odpowiedniego systemu CMS zależy od konkretnych potrzeb projektu.  
 WordPress jest jednym z najpopularniejszych systemów CMS na świecie. Jest łatwy w użyciu, posiada ogromną społeczność oraz szeroką gamę dostępnych wtyczek i dodatków. Jest idealny do blogów, stron internetowych firm czy też sklepów internetowych. Jego elastyczność sprawia, że jest szeroko stosowany w różnych branżach.  
 Wix to platforma do tworzenia stron internetowych, oferująca prosty interfejs typu "przeciągnij i upuść". Nie jest tradycyjny CMS, ale umożliwia łatwe tworzenie stron. Jest idealny dla małych firm, stron osobistych. Bardzo łatwy w użyciu dla osób bez doświadczenia programistycznego.  
3. Scharakteryzuj wybrane narzędzia automatyzacji testowania programów desktopowych i aplikacji webowych.   
 WinAppDriver to otwarto źródłowe narzędzie dostarczane przez Microsoft, które umożliwia automatyzację testów dla aplikacji desktopowych na platformie Windows. Jest to narzędzie, które działa na bazie protokołu WebDriver, co sprawia, że jest kompatybilne z wieloma popularnymi narzędziami do automatyzacji testów. WinAppDriver obsługuje różne języki programowania, takie jak C#, Java, Python i pozwala deweloperom i testerom na pisanie testów automatycznych dla aplikacji Windows. Integruje się z Selenium, co pozwala na współdzielenie kodu między testami dla aplikacji desktopowych i webowych.  
 Selenium o którym przed chwilą wspomniałem jest stosowany do automatyzacji testów dla aplikacji webowych. Jest używany do testowania różnych przypadków użycia, weryfikacji funkcjonalności, testów jednostkowych i innych. Selenium jest szczególnie przydatne w projektach, gdzie istnieje potrzeba regularnego i powtarzalnego testowania interfejsu użytkownika na różnych przeglądarkach i platformach. Wspiera różne języki programowania, takie jak Java, Python, C#, Ruby, JavaScript, co pozwala programistom i testerom na pisanie skryptów w preferowanym przez nich języku.   
4. Porównaj właściwości stosowanych narzędzi dla potrzeb grafiki komputerowej i przetwarzania obrazów.  
 Narzędzia graficzne, skupiają się na edycji i tworzeniu grafiki dla celów artystycznych, projektowych i reklamowych, natomiast narzędzia do przetwarzania obrazów, są bardziej ukierunkowane na analizę obrazów medycznych, mikroskopowych czy satelitarnych lub detekcję obiektów. Adobe Photoshop jest przykładem narzędzia graficznego natomiast OPEN CV narzędzia do przetwarzania obrazów.  
5. Omów podstawowe właściwości i zastosowania rozproszonych baz danych.   
 Podstawowymi właściwościami są:  
 Rozproszenie Danych: Dane są rozproszone pomiędzy różne węzły a każdy węzeł może przechowywać część danych.  
 Rozproszony Zarząd Danych: Zarząd danych obejmuje dystrybucję danych, równoważenie obciążenia, strategie partycjonowania danych i replikację w celu zwiększenia dostępności i odporności na awarie.  
 Autonomiczność: Każdy węzeł jest autonomiczny i może działać niezależnie w przypadku awarii innych węzłów. To oznacza, że system jest elastyczny i odporny na pojedyncze punkty awarii.  
 Transakcje i Koordynacja: RBD muszą obsługiwać transakcje, czyli operacje bazodanowe, które są atomowe, spójne, izolowane i trwałe. Koordynacja transakcji pomiędzy różnymi węzłami jest kluczowym wyzwaniem.  
 Komunikacja Międzywęzłowa: Wymaga efektywnych mechanizmów komunikacji między węzłami w celu wymiany danych.  
 Co do zastosowania to rozproszone bazy danych są używane np. w dużych witrynach internetowych, gdzie różne elementy strony, są przechowywane na różnych węzłach. W sektorze finansowym, gdzie bezpieczeństwo i dostępność są kluczowe. W dziedzinie nauki i badań, gdzie dużo danych musi być przechowywane, analizowane i udostępniane wielu użytkownikom.  
6. Omów etapy konstrukcji modelu przypadków użycia w procesie projektowania oprogramowania systemu informatycznego (SI) oraz jego opis w dokumentacji projektu SI.   
 Model przypadków użycia stanowi istotny element analizy wymagań i pomaga zrozumieć, jak użytkownicy będą korzystać z systemu. Kolejno możemy wziąć pod uwagę etapy miedzy innymi takie jak   
 Identyfikacja aktorów - czyli osób, systemów zewnętrznych lub innych elementów, które będą oddziaływać z systemem.  
 Określenie Przypadków Użycia, stworzenie diagramu oraz jego opis – dla każdego aktora należy zidentyfikować jego zadania lub funkcje, które będzie pełnił w systemie. Stworzyć diagram przypadków użycia, który przedstawia aktorów i przypadki użycia, a także relacje między nimi. Przygotowanie szczegółowego opisu, który zawiera informacje na temat celu przypadku użycia, warunków wstępnych, kroków realizacji i warunków końcowych  
 Diagramy Sekwencji i Komunikacji - Dla kluczowych przypadków użycia istnieją diagramy sekwencji lub diagramy komunikacji, które pokazują interakcje między aktorami a systemem w czasie.  
 Weryfikacja i Akceptacja – Upewniamy się że model przypadków użycia spełnia oczekiwania użytkowników oraz jest zgodny z wymaganiami systemu.  
 Opis W Dokumentacji Projektu – model przypadków użycia powinien znajdować się w dokumentacji projektu. Umieszczamy diagramy przypadków użycia, opisy przypadków użycia, diagramy sekwencji i komunikacji oraz wszelkie inne istotne informacje. W miarę ewolucji projektu, aktualności są wprowadzane do dokumentacji.   
7. Scharakteryzuj właściwości i przeznaczenie diagramów języka UML.   
 Diagramy języka UML są używane do modelowania, projektowania i dokumentowania systemów informatycznych. UML to narzędzie komunikacji między zespołami programistycznymi i interesariuszami projektu. Pomagają w zrozumieniu, analizie i dokumentacji różnych aspektów systemu, co przyczynia się do skutecznego projektowania i wdrażania oprogramowania. Istnieje kilka rodzajów diagramów UML, z których każdy służy do przedstawiania różnych aspektów systemu.   
 Diagram przypadków użycia - Opisuje funkcjonalności systemu z perspektywy użytkownika. Pomaga zidentyfikować główne przypadki użycia systemu i relacje między aktorami a przypadkami użycia.  
8. Scharakteryzuj stosowane w praktyce metody i narzędzia zarządzaniem projektami (project managment).   
 Metody zarządzania projektami to procesy lub podejścia do planowania, realizacji i kontrolowania projektu, które pomagają w efektywnym zarządzaniu projektami poprzez zastosowanie określonych zasad i praktyk. Np. Metodyka kaskadowa - model, gdzie każda faza projektu musi być zakończona przed rozpoczęciem kolejnej. Prosta do zrozumienia i zastosowania, szczególnie w przypadku prostych projektów o dobrze zdefiniowanych wymaganiach.  
 Narzędzia zarządzania projektami to oprogramowanie lub technologie, które wspomagają zarządzanie projektami, ułatwiając planowanie, śledzenie postępu i komunikację w zespole projektowym. Mogą obejmować różnorodne funkcje, takie jak harmonogram zadań, śledzenie zasobów, zarządzanie ryzykiem. Np. Confluence - Narzędzie do tworzenia dokumentacji i współpracy zespołowej, integrujące się z Jira.  
9. Scharakteryzuj właściwości i zastosowania systemów rozproszonych.   
 Systemy rozproszone charakteryzują się miedzy innymi   
 Rozproszoną Architekturą - która składa się z wielu komponentów rozproszonych na różnych maszynach, co umożliwia lepsze wykorzystanie zasobów i skalowalność. Dzięki rozproszeniu, systemy te są bardziej odporne na awarie. Jeśli jedna część systemu ulegnie awarii, inne komponenty mogą nadal działać.  
 Komunikacją Międzyprocesową - komponenty systemu muszą komunikować się między sobą poprzez sieć co wymaga efektywnych mechanizmów komunikacyjnych.   
 Systemy rozproszone są szeroko stosowane w bazach danych, gdzie dane są przechowywane i zarządzane na wielu serwerach, co zwiększa dostępność i wydajność.   
 W Aplikacjach Internetowych wielu dostawców usług internetowych korzysta z systemów rozproszonych do obsługi dużej liczby użytkowników, zapewniając szybkość i skalowalność  
 Lub W grach komputerowych wieloosobowych systemy rozproszone umożliwiają interakcję wielu graczy na różnych urządzeniach.  
10. Scharakteryzuj przykłady zastosowań sztucznej inteligencji w wybranych rozwiązaniach informatycznych (np. w robotyce).   
 Medycyna – Stosuje się ją w analizie obrazów medycznych, takich jak tomografia komputerowa, w celu wspomagania diagnoz i identyfikacji zaburzeń. Systemy SI analizują dane kliniczne do oszacowania ryzyka wystąpienia chorób, co może pomóc w wczesnym rozpoznawaniu i leczeniu.  
 Mechanika samochodowa – w pojazdach sztuczna inteligencja jest kluczowa dla podejmowania decyzji na podstawie danych z czujników, identyfikacji tras, zarządzania ruchem oraz bezpiecznej nawigacji. Algorytmy uczenia maszynowego wspierają funkcje takie jak rozpoznawanie obiektów, klasyfikacja znaków drogowych i adaptacyjne sterowanie.  
 Robotyka - np. w robotyce przemysłowej sztuczna inteligencja jest wykorzystywana do programowania robotów do wykonywania zadań, takich jak precyzyjne montowanie produktów, spawanie czy pakowanie. Algorytmy uczenia maszynowego są używane do optymalizacji trajektorii ruchu robotów  
11. Scharakteryzuj kanały komunikacji elektronicznej i perspektywy ich zastosowań (rozwoju).   
 Kanały komunikacji elektronicznej to środki, za pomocą których odbywa się przekazywanie informacji w postaci elektronicznej. Współczesne technologie umożliwiają różnorodne formy komunikacji elektronicznej, takie jak  
 E-mail - to elektroniczna forma komunikacji, która umożliwia wysyłanie, odbieranie i przechowywanie wiadomości tekstowych, plików oraz innych danych. Stosowana najczęściej w Biznesie i Praca lub Osobiście.  
 Komunikatory Internetowe (Messenger) – te i inne podobne aplikacje umożliwiają natychmiastową komunikację tekstową, głosową i wideo między użytkownikami. Stosuje się również w Biznesie i pracy lub osobiście do rozmów, współpracy w grupie czy kontaktu z klientem.  
 Wideokonferencje (Zoom) - są to usługi umożliwiające prowadzenie spotkań online, konferencji wideo i audio. Najczęściej stosowane do pracy zdalnej lub edukacji.  
 Forum Internetowe - Strony internetowe, na których użytkownicy mogą wymieniać się informacjami i opiniami na określony temat. Wykorzystywane jest jako Wsparcie Techniczne lub Wymiana Wiedzy, gdzie Użytkownicy dzielą się doświadczeniem i rozwiązują problemy.  
12. Scharakteryzuj narzędzia, jakie należy stosować do zgodnego z prawem zarządzania obiegiem informacji w formie elektronicznej.   
 Narzędzia do zgodnego z prawem zarządzania obiegiem informacji w formie elektronicznej przede wszystkim powinny być zgodne z przepisami prawnymi, chronić dane osobowe oraz dokumenty, zarządzać bezpieczeństwem informacji oraz minimalizować ryzyko bezpieczeństwa. Do popularnych narzędzi należą:  
 System Zarządzania Dokumentami – który, umożliwia przechowywanie, zarządzanie i udostępnianie dokumentów elektronicznych w sposób zorganizowany. Zapewnia kontrolę dostępu, wersjonowanie dokumentów, a także funkcje śledzenia i audytu.   
 Elektroniczne Podpisy Cyfrowe - to metoda potwierdzania tożsamości i autentyczności dokumentów elektronicznych. Zapewniają bezpieczeństwo prawne i są równoważne podpisowi odręcznemu.  
13. Omów znaczenie technologii Cloud Computing na dostępność, skalowalność, bezpieczeństwo i optymalizację kosztów świadczonych usług.   
 Dostępność - Usługi chmurowe pozwalają na rozmieszczenie aplikacji i danych na wielu serwerach na całym świecie. To z kolei umożliwia dostępność usług na różnych kontynentach, minimalizując ryzyko przerw w dostępie. Umożliwia dostawcom usług skonfigurowanie infrastruktury w sposób elastyczny. Dzięki temu, jeśli jeden z serwerów ulegnie awarii, inne automatycznie przejmują obciążenie, co zapewnia ciągłość usług.  
 Skalowalność - W chmurze zasoby, takie jak moc obliczeniowa czy pamięć, mogą być łatwo skalowane w górę lub w dół w zależności od bieżących potrzeb, co jest szczególnie istotne w przypadku aplikacji o zmiennym obciążeniu, takich jak sklepy internetowe podczas okresów promocji.  
 Bezpieczeństwo - Dostawcy chmurowi oferują również szereg narzędzi i usług zabezpieczeń, takich jak firewall, systemy detekcji intruzów i szyfrowanie danych, co pomaga w ochronie przed atakami cybernetycznymi. Usługi chmurowe są często świadczone z użyciem profesjonalnych centrów danych, które spełniają najwyższe standardy bezpieczeństwa.  
 Optymalizacja Kosztów - Dzięki narzędziom do monitorowania i zarządzania zasobami w chmurze, firmy mogą kontrolować wydatki, ponieważ model rozliczeń w chmurze często opiera się na płatności za faktyczne zużycie zasobów. To pozwala unikać konieczności inwestowania w stałe zasoby, a klient płaci tylko za to, co faktycznie zużył.  
14. Omów modele usługowe przetwarzania w chmurze obliczeniowej (Cloud Computing): SaaS (Software-as-a-Service), IaaS (Infrastructure as a Service), PaaS (Platform as a Service).   
 SaaS (Software-as-a-Service) - Model SaaS dostarcza użytkownikom gotowe, skończone aplikacje lub usługi oprogramowania przez internet. Użytkownicy korzystają z aplikacji bez konieczności instalowania, konfigurowania czy zarządzania infrastrukturą. Odpowiada to zaawansowanym usługom, takim jak zarządzanie relacjami z klientami, systemy zarządzania treścią czy narzędzia do obsługi biura online.   
 IaaS (Infrastructure-as-a-Service) - Model IaaS dostarcza użytkownikom elastyczną infrastrukturę IT, obejmującą zasoby obliczeniowe, pamięć masową, sieci i inne zasoby, dostarczane jako usługi w chmurze. Użytkownicy mają pełną kontrolę nad systemem operacyjnym, aplikacjami i konfiguracją. Nie muszą martwić się o fizyczną infrastrukturę, która pozwala na elastyczne skalowanie zasobów.  
 PaaS (Platform-as-a-Service) - Model PaaS dostarcza platformę programistyczną, która obejmuje narzędzia, środowisko wykonawcze i usługi, które ułatwiają rozwijanie, testowanie i wdrażanie aplikacji. Użytkownicy skupiają się głównie na tworzeniu i wdrażaniu aplikacji, ponieważ większość zadań związanych z infrastrukturą, takich jak zarządzanie systemem operacyjnym czy bazami danych, jest obsługiwana przez platformę.  
15. Porównaj obszary zastosowań i właściwości usług w modelu chmury prywatnej, publicznej i mieszanej.   
 Chmura Prywatna - jest dedykowana jednej organizacji. Stworzona dla organizacje o wysokim stopniu regulacji, które wymagają pełnej kontroli nad infrastrukturą i bezpieczeństwem danych, takie jak instytucje finansowe czy służba zdrowia. Zapewnia wyższy poziom bezpieczeństwa, ponieważ infrastruktura jest zarządzana i kontrolowana wewnętrznie  
 Chmura Publiczna - jest dostępna dla ogółu użytkowników i współdzielona między różnymi organizacjami. Idealna dla firm, które potrzebują elastyczności i skalowalności w zakresie zasobów obliczeniowych w zależności od zmieniających się potrzeb. Jest korzystny dla organizacji, które chcą unikać inwestycji w infrastrukturę, ponieważ model oparty jest na opłatach za użycie.  
 Chmura Hybrydowa - Łączy elementy chmury prywatnej i publicznej, umożliwiając przenoszenie danych i aplikacji między nimi. Dla firm, które potrzebują zrównoważyć kontrolę nad danymi w chmurze prywatnej z elastycznością chmury publicznej. Zarządzanie zasobami i danymi jest zintegrowane, co pozwala na elastyczne korzystanie z różnych modeli w zależności od potrzeb.  
16. Scharakteryzuj koncepcję „Four V” w odniesieniu do bezpieczeństwa Big Data.   
 Jak sama nazwa wskazuje koncepcja ta obejmuje cztery kluczowe wyzwania związane z zbiorami danych.   
 Pierwsza z nich Volume (Objętość) - Odnosi się do ilości danych przechowywanych i przetwarzanych w środowisku Big Data. Bezpieczeństwo danych musi radzić sobie z ogromnymi ilościami informacji, co oznacza konieczność zastosowania odpowiednich mechanizmów ochrony przed utratą lub innymi zagrożeniami.  
 Velocity (Szybkość) - Odnosi się do tempa, z jakim dane są generowane, przesyłane i przetwarzane. Bezpieczeństwo musi być w stanie dostosowywać się do dynamicznego charakteru danych, aby zapewnić ochronę w czasie rzeczywistym.  
 Variety (Zróżnicowanie) - Odnosi się do różnorodności formatów danych, takich jak tekst, obrazy, dźwięki itp.  
Bezpieczeństwo musi obsługiwać różnorodność formatów danych, stosować odpowiednie metody szyfrowania i zabezpieczania dostępu.  
 Veracity (Wiarygodność) - Odnosi się do stopnia pewności i jakości danych, ze względu na ich pochodzenie, dokładność i spójność. Bezpieczeństwo musi uwzględniać kontrolę dostępu do danych, weryfikacją tożsamości użytkowników, aby utrzymać ich wiarygodność.  
17. Porównaj technologie: GSM, Bluetooth, Wi-Fi.   
 GSM (Global System for Mobile Communications) - Głównie używane do transmisji głosu i danych w sieciach telefonii komórkowej. Stosowany w systemach 2G, 3G i czasami 4G. Działa w sieci komórkowej o dużym zasięgu, obejmującej obszary krajowe i międzynarodowe. Przepustowość relatywnie niska w porównaniu do nowocześniejszych technologii. Zapewnia podstawowe mechanizmy bezpieczeństwa. Przeznaczony głównie do komunikacji głosowej  
 Bluetooth stworzony jest do krótkodystansowej komunikacji między urządzeniami, takimi jak słuchawki, klawiatury itp. Zasięg ma krótki, około kilku metrów. Średnia przepustowość, wystarczająca do przesyłania danych audio czy krótkich informacji. Zapewnia różne poziomy bezpieczeństwa, np. szyfrowanie danych lub mechanizmy uwierzytelniania. Idealny do zastosowań w domu i biurze.  
 Wi-Fi stworzono do lokalnej bezprzewodowej sieci komputerowej (LAN). Używany do dostępu do internetu w domach, biurach, kawiarniach, itp. Średni lub duży zasięgu, w zależności od standardu WiFi. Wysoka przepustowość, zwłaszcza w nowszych standardach Wi-Fi. Zapewnia różne protokoły bezpieczeństwa, aby zabezpieczyć transmisje danych.  
18. Scharakteryzuj właściwości i obszary zastosowań systemów WiFi-HotSpot oraz uprawnienia ich właścicieli.   
 Systemy WiFi-HotSpot umożliwiają bezprzewodowe połączenie z siecią internetową, umożliwiając użytkownikom korzystanie z sieci na urządzeniach takich jak smartfony, tablety czy laptopy. HotSpoty są łatwe w użyciu. W wielu przypadkach wystarczy jedno kliknięcie, aby połączyć się z dostępną siecią. Systemy HotSpot mogą być przenoszone, co sprawia, że są idealne dla miejsc, gdzie mobilność jest kluczowa, na przykład w kawiarniach, hotelach, czy miejscach publicznych. Nowoczesne systemy WiFi-HotSpot oferują wysoką przepustowość, co umożliwia użytkownikom szybki dostęp do zasobów internetowych.  
 Z zastosowaniem Wifi możemy się spotkać prawie wszędzie. W Kawiarniach i Restauracjach, wielu przedsiębiorców oferuje dostęp do darmowego WiFi, aby przyciągnąć klientów i zaoferować im wygodę korzystania z internetu. W Hotelach HotSpoty stają się standardowym wyposażeniem, umożliwiając gościom korzystanie z internetu w pokojach lub wybranych częściach obiektu. Miejsca o dużym natężeniu ruchu, takie jak lotniska czy dworce kolejowe często są wyposażone w HotSpoty pozwalające podróżnym na dostęp do informacji i rozrywki podczas oczekiwania. W miejscach pracy HotSpoty mogą być używane do umożliwienia pracownikom elastycznego dostępu do sieci.  
 Właściciele HotSpotów mają kontrolę nad tym, kto może uzyskać dostęp do ich sieci. Mogą wymagać uwierzytelniania. Mogą również zarządzać przepustowością sieci, oraz są odpowiedzialni za zapewnienie bezpieczeństwa, w tym np. stosowanie szyfrowania. Oprócz tego mogą też ustalać warunki korzystania z sieci, określając limity czasowe, ograniczenia prędkości, czy zakazywane treści.  
19. Scharakteryzuj techniki stosowane w centrach przetwarzania danych w celu poprawy ich efektywności   
energetycznej (tzw. zielone centrum danych).   
 Zielone centra danych to takie, które starają się zminimalizować negatywny wpływ na środowisko naturalne i jednocześnie maksymalizować efektywność energetyczną. Do takich technik zaliczamy między innymi:  
 Wirtualizację: która pozwala na uruchamianie wielu maszyn wirtualnych na jednym fizycznym serwerze. Dzięki temu można lepiej wykorzystać dostępne zasoby sprzętowe, co przekłada się na mniejsze zużycie energii.  
 Zarządzanie zasobami: Centra danych coraz częściej korzystają z systemów zarządzania zasobami, które umożliwiają dostosowywanie mocy obliczeniowej do bieżących potrzeb. Ta technika pozwala na automatyczne skalowanie zasobów w zależności od obciążenia.  
 Chłodzenie: Jednym z głównych obszarów zużycia energii w centrach danych jest chłodzenie. Dlatego stosuje się zaawansowane techniki chłodzenia, np. chłodzenie wodą. Te rozwiązania pozwalają utrzymać optymalną temperaturę wewnątrz centrum danych przy mniejszym zużyciu energii.  
 Zrównoważona energia: Centra danych starają się coraz częściej korzystać z odnawialnych źródeł energii, takich jak energia słoneczna czy wiatrowa. To pozwala na zmniejszenie śladu węglowego i minimalizację negatywnego wpływu na środowisko.  
 Energooszczędne sprzęty: Wybór sprzętu o niskim zużyciu energii to kluczowy element. Sami producenci sprzętu starają się tworzyć energooszczędne rozwiązania, zarówno w zakresie serwerów, jak i innych urządzeń.  
20. Scharakteryzuj sieciowe technologie zabezpieczające (Systemy firewall i VPN).   
 Firewall i VPN to elementy infrastruktury bezpieczeństwa sieciowej, które pomagają chronić dane i zasoby przed nieautoryzowanym dostępem.  
 Firewalle - są kluczowym narzędziem w ochronie sieci przed nieautoryzowanym dostępem. Są one projektowane do monitorowania i kontrolowania ruchu sieciowego, blokowania niebezpiecznych połączeń i chronienia zasobów sieciowych przed atakami. Maskuje adresy IP wewnętrznych urządzeń przed światem zewnętrznym. Możemy wyróżnić 3 rodzaje Firewall sieciowy ,Firewall hosta lub Firewall osobisty  
 VPN natomiast to technologia, która tworzy bezpieczne, zaszyfrowane połączenie między dwoma punktami końcowymi przez publiczną sieć. Zapewnia bezpieczeństwo na warstwie sieciowej wykorzystując technikę tunelowania do zapewnienia bezpiecznego przesyłania danych. Do 2 najpopularniejszych rodzajów należą, Remote Access VPN - Umożliwia zdalnym użytkownikom bezpieczny dostęp do sieci firmowej, oraz Site-to-Site VPN - łączy oddzielne sieci, na przykład siedzibę firmy z oddziałem, tworząc jedną wspólną sieć.  
21. Scharakteryzuj właściwości stosowanych narzędzi zabezpieczania poczty elektronicznej (Secure Mail).   
 Secure Mail to obszar bezpieczeństwa informatycznego skupiający się na ochronie poczty elektronicznej przed zagrożeniami, takimi jak phishing, malware czy utrata poufności informacji. Właściwości stosowanych narzędzi zabezpieczających pocztę elektroniczną obejmują różnorodne funkcje mające na celu minimalizowanie ryzyka i zapewnienie poufności komunikacji. Do takich funkcji należą  
 Filtrowanie Antyspamowe - Automatyczne wykrywa i blokuje niechciane maile, w tym spam i phishing.  
 Skanowanie Antywirusowe - Analizuje załączniki i treści wiadomości w poszukiwaniu wirusów i złośliwego oprogramowania.  
 Szyfrowanie Poczty - Zabezpiecza treści wiadomości przed nieautoryzowanym dostępem poprzez zastosowanie szyfrowania.  
 Autentykacja Dwuskładnikowa - Wymaga dodatkowego poziomu uwierzytelnienia poza standardowym hasłem, co zwiększa bezpieczeństwo konta pocztowego.  
 Zarządzanie Politykami Bezpieczeństwa i Filtrowanie Treści - Narzędzia umożliwiające definiowanie i egzekwowanie polityk bezpieczeństwa dla komunikacji e-mailowej. Monitorowanie treści wiadomości pod kątem naruszeń zasad bezpieczeństwa i polityk firmy  
22. Omów zagrożenia bezpieczeństwa w Internecie Rzeczy (IoT - Internet of Things).   
 Brak Standaryzacji Bezpieczeństwa - Wiele urządzeń IoT jest tworzonych przez różnych producentów, co prowadzi do braku jednolitego standardu bezpieczeństwa. To utrudnia utrzymanie spójnych praktyk bezpieczeństwa.  
 Słabe Hasła i Autentykacja - Wiele urządzeń korzysta ze słabych haseł lub nawet domyślnych ustawień, co ułatwia nieautoryzowany dostęp.   
 Ataki Hakerskie na Poziomie Fizycznym - Niektóre urządzenia IoT, zwłaszcza te związane z systemami przemysłowymi lub medycznymi, mogą być narażone na ataki fizyczne, takie jak próby, podmiany komponentów czy wstrzykiwanie fałszywych danych.  
 Brak Aktualizacji Oprogramowania - Wiele urządzeń może być trudno aktualizować ze względu na ograniczone zasoby sprzętowe lub brak interfejsów użytkownika. To sprawia, że urządzenia pozostają podatne na znane luki bezpieczeństwa.  
 Zagrożenia Związane z Przechwytywaniem Danych - Ponieważ urządzenia IoT często zbierają i przesyłają duże ilości danych, mogą stać się celem ataków mających na celu przechwycenie danych. To szczególnie ważne w przypadku danych wrażliwych, takich jak dane osobowe.  
23. Scharakteryzuj narzędzia stosowane do zarządzania bezpieczeństwem aplikacji dla urządzeń mobilnych.   
 Zarządzanie bezpieczeństwem aplikacji dla urządzeń mobilnych jest kluczowe, zwłaszcza w kontekście wzrostu przechowywania wrażliwych danych na urządzeniach przenośnych, jednak efektywne zarządzanie bezpieczeństwem aplikacji mobilnych wymaga często zastosowania wielu narzędzi. Do najpopularniejszych narzędzi należą:  
 Mobile Device Management - Narzędzie MDM umożliwia centralne zarządzanie urządzeniami mobilnymi w organizacji. Pozwala na zdalne konfigurowanie ustawień bezpieczeństwa, monitorowanie aktywności oraz usuwanie zdalne w razie utraty urządzenia. Zapewnia kontrolę nad urządzeniami mobilnymi w firmie, szczególnie w kontekście (Bring Your Own Device).  
 Mobile Application Management - podobnie jak MDM koncentruje się na zarządzaniu aplikacjami na urządzeniach mobilnych. Pozwala na kontrolę dostępu, konfigurację, aktualizacje i usuwanie aplikacji zdalnie.  
 App wrapping - to technika polegająca na dodawaniu warstwy zabezpieczającej do istniejącej aplikacji, dzięki czemu można zabezpieczyć istniejące aplikacje przed zagrożeniami bez potrzeby wprowadzania zmian w kodzie źródłowym.  
24. Scharakteryzuj zasady polityki bezpieczeństwa stosowane w przedsiębiorstwach (firmach) różnej skali.  
 Zasady polityki bezpieczeństwa, które obowiązują w większości firm o różnej skali to przede wszystkim.  
Zarządzanie Dostępem - Ograniczenie dostępów do zasobów tylko dla osób, które są do tego uprawnione.  
Szyfrowanie Danych - Wdrażanie technologii szyfrowania w celu ochrony ich podczas przesyłania i przechowywania.  
Aktualizacje - Regularne aktualizacje oprogramowania i stosowanie łatek bezpieczeństwa.  
Polityka Haseł - Wymuszanie silnych haseł i ich cykliczną zmianę.  
Zarządzanie Zdarzeniami Bezpieczeństwa - Efektywne monitorowanie i reagowanie na incydenty bezpieczeństwa.  
Polityka Prywatności - Ochrona prywatności danych klientów i pracowników.  
Szkolenie i Świadomość Bezpieczeństwa - Zapewnianie regularnych szkoleń pracowników w zakresie bezpieczeństwa.  
25. Scharakteryzuj zasady planowania ciągłości działania IT w firmie (DRP - Disaster Recovery Plan).   
 Zastosowanie zasad bezpieczeństwa w ramach planowania ciągłości działania IT pozwala firmom lepiej zabezpieczyć się przed incydentami i skutecznie odzyskać działalność w przypadku wystąpienia katastrofy. Do tych zasad należą:  
 Analiza ryzyka - przeprowadzenie analizy ryzyka, identyfikacja potencjalnych zagrożeń i ocena ich wpływu na firmę. Klasyfikacja systemów oraz danych pod względem ważności dla funkcjonowania firmy.  
 Określanie celów odzyskiwania - takich jak czas przywracania systemów, minimalne straty danych oraz minimalne zakłócenie działania firmy.  
 Plan działań awaryjnych - opracowanie planu działań awaryjnych na wypadek incydentu, obejmującego szybkie działania niezbędne do minimalizacji szkód.   
 Zabezpieczenia technologiczne - Wdrożenie odpowiednich zabezpieczeń technologicznych, takich jak kopie zapasowe czy systemy monitorowania i alarmowania, a także zabezpieczenia przed cyberzagrożeniami.  
 Testowanie i aktualizacja - testowanie planu odzyskiwania po katastrofie, aby upewnić się, że jest on skuteczny. Stała aktualizacja planu w odpowiedzi na zmiany w infrastrukturze IT.  
 Zaangażowanie personelu - szkolenie pracowników w zakresie procedur bezpieczeństwa. Zapewnienie, że personel jest świadomy roli, jaką pełni w przypadku wystąpienia incydentu.  
 26. Omów zagrożenia bezpieczeństwa wiążące się z wykorzystywaniem prywatnych urządzeń mobilnych (BYOD: Bring Your Own Device) do celów służbowych w firmie.   
 Wykorzystywanie prywatnych urządzeń mobilnych w celach służbowych w firmie niesie za sobą wiele korzyści, ale również stwarza potencjalne zagrożenia bezpieczeństwa takie jak:  
 Utrata lub kradzieżą urządzenia - Prywatne urządzenia mobilne są bardziej narażone na utratę lub kradzież niż urządzenia firmowe. Straty takiego urządzenia mogą prowadzić do utraty poufnych danych służbowych, a także dostępu do systemów firmy.  
 Ryzyko utraty danych - Użytkownicy mogą przechowywać na swoich urządzeniach dane, które są poufne i wrażliwe. Może to prowadzić do przypadkowego ujawnienia informacji osobą trzecim  
 Brak aktualizacji oprogramowania - Użytkownicy mogą nie być skłonni lub w stanie utrzymać aktualne oprogramowanie na swoich urządzeniach. Nieaktualne systemy operacyjne i aplikacje stanowią potencjalne ryzyko z punktu widzenia bezpieczeństwa.  
 Zagrożenia związane z zainstalowanymi aplikacjami - Prywatne aplikacje zainstalowane na urządzeniach mogą stanowić zagrożenie dla bezpieczeństwa, zwłaszcza jeśli nie są odpowiednio sprawdzone i zatwierdzone przez firmę. Niektóre aplikacje mogą zawierać złośliwe oprogramowanie lub naruszać zasady prywatności.  
 Ataki z wykorzystaniem publicznych sieci Wi-Fi - Użytkownicy często korzystają z różnych sieci Wi-Fi, w tym publicznych, co zwiększa ryzyko ataków.  
27. Omów obsługę operacyjną incydentów bezpieczeństwa komputerowego.   
 Kluczowe etapy obsługi operacyjnej incydentów bezpieczeństwa komputerowego to:  
 Wykrywanie incydentu - Implementacja systemów monitorowania i alarmowania w celu szybkiego wykrywania nieprawidłowości w sieciach, systemach czy aplikacjach.  
 Raportowanie incydentu - Ustalenie procedur zgłaszania podejrzanych sytuacji oraz incydentów bezpieczeństwa.  
 Analiza incydentu - Analiza i ocena sytuacji w celu zrozumienia zakresu incydentu.  
 Izolacja i ograniczenie szkód - Podjęcie natychmiastowych działań w celu izolacji zainfekowanych systemów lub ograniczenia szkód.  
 Zbieranie dowodów - Rozpoczęcie procesu zbierania informacji i dowodów związanych z incydentem.  
 Odzyskiwanie systemów - Przywracanie normalnego działania systemów i usług po upewnieniu się, że są one wolne od zagrożeń.  
 Analiza post-incydentalna - Szczegółowa analiza przyczyn incydentu w celu zidentyfikowania luk w bezpieczeństwie i ustalenia, jak można poprawić systemy i procedury.  
 Wdrażanie poprawek i ulepszeń - Wprowadzanie zmian w zabezpieczeniach, procedurach i systemach w celu poprawy odporności firmy na podobne incydenty w przyszłości.  
 Szkolenie i doskonalenie - Szkolenie zespołów odpowiedzialnych za obsługę incydentów oraz personelu.  
28. Scharakteryzuj narzędzia dla przedsiębiorstw, które umożliwiają bezpieczną współpracę pracownikom z różnych działów.   
 Istnieje wiele narzędzi przeznaczonych do bezpiecznej współpracy między pracownikami z różnych działów, te najpowszechniejsze to:  
 29. Scharakteryzuj narzędzia dla urządzeń przenośnych, które umożliwiają utrzymanie kontaktu i wydajną pracę w podróży dla pracowników z różnych działów przedsiębiorstwa.   
 Istnieje wiele narzędzi dla urządzeń przenośnych, które umożliwiają pracownikom utrzymanie kontaktu i wydajną pracę w podróży, do najpopularniejszych zaliczamy:  
 Microsoft 365 - Umożliwia współpracę w czasie rzeczywistym nad dokumentami, dzięki aplikacją jak Word, Excel, PowerPointa, a także korzystanie z poczty elektronicznej i wideokonferencji za pomocą Teams i Outlook.  
 OneDrive - Usługa przechowywania w chmurze od Microsoftu, umożliwia dostęp do plików z dowolnego urządzenia, oraz współpracę nad dokumentami i udostępnianie plików zespołowi.  
 Google Workspace - Oferuje narzędzia biurowe online, umożliwiające pracę na odległość. Integracja z chmurą Google Drive ułatwia przechowywanie i udostępnianie dokumentów.  
 Zoom - Aplikacja do wideokonferencji, umożliwiająca organizację spotkań online i komunikację w czasie rzeczywistym. Posiada funkcje udostępniania ekranu, nagrywania spotkań i integracji z kalendarzem.  
 VPN (Virtual Private Network) - Narzędzie zapewniające bezpieczne połączenie z firmową siecią, co umożliwia bezpieczny dostęp do zasobów firmy poza biurem.   
30. Omów procedurę reagowania na incydenty bezpieczeństwa IT w firmie.  
 Procedura reagowania na incydenty bezpieczeństwa IT w firmie to zbiór kroków i działań, które należy podjąć w przypadku wykrycia lub podejrzenia naruszenia bezpieczeństwa. Obejmuje ona zarówno szybkie działania w celu zminimalizowania szkód, jak i długofalowe środki mające na celu zrozumienie przyczyny incydentu i poprawę bezpieczeństwa. Ogólny zarys procedury reagowania wygląda następująco:  
 Wykrywanie incydentu - Implementacja systemów monitorowania i alarmowania w celu szybkiego wykrywania nieprawidłowości w sieciach, systemach czy aplikacjach.  
 Analiza incydentu - Szybka analiza i ocena sytuacji w celu zrozumienia zakresu incydentu.  
 Izolacja i ograniczenie szkód - Podjęcie natychmiastowych działań w celu izolacji zainfekowanych systemów lub ograniczenia szkód.  
 Zbieranie dowodów - Rozpoczęcie procesu zbierania informacji i dowodów związanych z incydentem.  
 Odzyskiwanie systemów - Przywracanie normalnego działania systemów i usług po upewnieniu się, że są one wolne od zagrożeń.  
 Analiza post-incydentalna - Szczegółowa analiza przyczyn incydentu w celu zidentyfikowania luk w bezpieczeństwie i ustalenia, jak można poprawić systemy i procedury.  
 Wdrażanie poprawek i ulepszeń - Wprowadzanie zmian w zabezpieczeniach, procedurach i systemach w celu poprawy odporności firmy na podobne incydenty w przyszłości.  
 Szkolenie i doskonalenie - Szkolenie zespołów odpowiedzialnych za obsługę incydentów oraz personelu.