2020/2021

PYTANIA NA EGZAMIN DYPLOMOWY INŻYNIERSKI

Studia: I-stopnia stacjonarne

Kierunek: Cyberbezpieczeństwo

Specjalność: Bezpieczeństwo danych - CBD

PYTANIA KIERUNKOWE

1. Podstawowe techniki kryptograficzne
2. Koncepcja programowania obiektowego
3. Kodowe zabezpieczenie sygnału przed błędami transmisji
4. Charakterystyka systemów operacyjnych
5. Charakterystyki mediów transmisyjnych
6. Sieci komputerowe: struktura, protokoły, model warstwowy
7. Modulacje analogowe i cyfrowe
8. Metody zabezpieczania urządzeń sieciowych: uwierzytelnianie, autoryzacja, zapory
9. Zarządzanie bezpieczeństwem informacji: założenia, struktura
10. Rodzaje możliwych zagrożeń elektromagnetycznych dla systemów i sieci oraz metody techniczne i organizacyjne stosowane w celu ich zmniejszenia

PYTANIA SPECJALNOŚCIOWE

1. Pozyskiwanie danych z urządzeń: zasady, metody, narzędzia
2. Sieci bezprzewodowe WLAN (802.11xx): zasada działania, parametry interfejsu radiowego, techniki transmisji
3. Bazy danych: rodzaje, modele bezpieczeństwa dla różnych typów baz
4. Modele logiczne danych stosowane w przetwarzaniu dużych zbiorów danych oraz infrastruktura pamięci masowych
5. Wirtualizacja, klastry, gridy oraz infrastruktura chmur obliczeniowych w centrach przetwarzania danych
6. Bezpieczeństwo zasobów i danych w systemach rozproszonych
7. Prawne i etyczne problemy dotyczące biometrii
8. Metody oraz dobre praktyki zabezpieczania usług internetowych
9. Metodyka audytu technicznego
10. Zarządzanie usługami i ruchem sieciowym

PYTANIA NA EGZAMIN DYPLOMOWY INŻYNIERSKI

Studia: I-stopnia stacjonarne

Kierunek: Cyberbezpieczeństwo

Specjalność: Bezpieczeństwo sieci teleinformatycznych - CBS

PYTANIA KIERUNKOWE

1. Podstawowe techniki kryptograficzne
2. Koncepcja programowania obiektowego
3. Kodowe zabezpieczenie sygnału przed błędami transmisji
4. Charakterystyka systemów operacyjnych
5. Charakterystyki mediów transmisyjnych
6. Sieci komputerowe: struktura, protokoły, model warstwowy
7. Modulacje analogowe i cyfrowe
8. Metody zabezpieczania urządzeń sieciowych: uwierzytelnianie, autoryzacja, zapory
9. Zarządzanie bezpieczeństwem informacji: założenia, struktura
10. Rodzaje możliwych zagrożeń elektromagnetycznych dla systemów i sieci oraz metody techniczne i organizacyjne stosowane w celu ich zmniejszenia

PYTANIA SPECJALNOŚCIOWE

1. Sieci komórkowe 2G – 5G (rodzaje, architektury, interfejs radiowy, techniki transmisyjne) oraz sieci komunikacji krytycznej
2. Chmury obliczeniowe: modele, usługi, cechy charakterystyczne
3. Elementy systemu biometrycznego (jedno- i wielomodalnego)
4. Technologie wąskopasmowe LPWAN dla Internetu Rzeczu: LoRa oraz NB-IoT
5. Metody zdalnego dostępu do urządzeń i usług oraz ich zabezpieczanie
6. Jakość usług w sieciach transmisji danych, metody oceny i parametry QoS
7. Kompresja różnicowa w kodekach sygnałów mowy (ADPCM) oraz obrazów ruchomych (MPEG2, MPEG4)
8. Sieci bezprzewodowe WLAN (802.11xx) oraz WPAN (zasada działania, parametry interfejsu radiowego, techniki transmisji)
9. Narzędzia audytorskie, normy bezpieczeństwa ISO
10. Zarządzanie bezpieczeństwem sieci: zagrożenia, ochrona, narzędzia

PYTANIA NA EGZAMIN DYPLOMOWY INŻYNIERSKI

Studia: I-stopnia stacjonarne

Kierunek: Cyberbezpieczeństwo

Specjalność: Bezpieczeństwo w energetyce - CEN

PYTANIA KIERUNKOWE

1. Podstawowe techniki kryptograficzne
2. Koncepcja programowania obiektowego
3. Kodowe zabezpieczenie sygnału przed błędami transmisji
4. Charakterystyka systemów operacyjnych
5. Charakterystyki mediów transmisyjnych
6. Sieci komputerowe: struktura, protokoły, model warstwowy
7. Modulacje analogowe i cyfrowe
8. Metody zabezpieczania urządzeń sieciowych: uwierzytelnianie, autoryzacja, zapory
9. Zarządzanie bezpieczeństwem informacji: założenia, struktura
10. Rodzaje możliwych zagrożeń elektromagnetycznych dla systemów i sieci oraz metody techniczne i organizacyjne stosowane w celu ich zmniejszenia

PYTANIA SPECJALNOŚCIOWE

1. Komunikacja sieciowa w rozproszonych systemach automatyki. Zadania i sposoby realizacji.
2. Zagrożenia bezpieczeństwa pracy stacji elektroenergetycznej oraz sposoby i środki przeciwdziałania lub ograniczania tych zagrożeń
3. Ochrona systemu elektroenergetycznego przed jego destabilizacją wskutek nieuprawnionej ingerencji i zakłócaniem transmisji danych
4. Komunikacja w inteligentnych systemach pomiarowych (stosowane rozwiązania, technologia, konfiguracja połączeń)
5. Projektowanie bezpiecznych aplikacji sieciowych klient-serwer wspomagających działania kontrolno-regulacyjne w elektroenergetyce
6. Elementy i urządzenia ochrony przeciwprzepięciowej - budowa, zasada działania, parametry i zastosowanie
7. Klasyfikacja zaburzeń jakości energii elektrycznej, podstawowe źródła zaburzeń oraz wybrane sposoby poprawy jakości energii elektrycznej