

Pytania na egzamin magisterski (studia II stopnia)

Moduły specjalnościowe: Specjalność „inżynieria systemów bezpieczeństwa komputerowego”

Systemy kryptograficzne

1. Jakie jest zastosowanie algorytmu RSA. Omów działanie algorytmu.
2. Jakie jest zastosowanie algorytmu IDEA. Omów działanie algorytmu.
3. Jakie jest zastosowanie algorytmu AES lub DES. Wymień jego odmiany i omów działanie algorytmu.
4. Jakie jest zastosowanie algorytmu RC5. Omów działanie algorytmu.
5. Jakie jest zastosowanie algorytmu SEAL. Omów działanie algorytmu.

Systemy wykrywania włamań

1. Na czym polega metoda wykrywania włamań Misuse Detection ?
2. Na czym polega metoda wykrywania włamań Anomaly Detection ?
3. Opisz architekturę systemów wykrywania włamań.
4. Opisz wybraną metodę wykrywania włamań wykorzystującą algorytmy sztucznej inteligencji.
5. Scharakteryzuj oprogramowanie typu "Pułapki"

Technologie i systemy bezpieczeństwa komputerowego

1. Omów metody zarządzania kluczami kryptograficznymi. W jaki sposób takie klucze dystrybuuje się w środowisku, w którym nie jest zapewniona poufność danych?
2. Objasnij sposoby uwierzytelniania przy użyciu kryptografii symetrycznej oraz asymetrycznej.
3. Przedstaw problematykę bezpieczeństwa aplikacji webowych w obecnych systemach komputerowych. Jakie najważniejsze ataki obecnie wymierzone są w aplikacje webowe?
4. Omów metodykę zabezpieczania obecnych mobilnych systemów operacyjnych na przykładzie systemu Android.
5. Przedstaw sposoby kontroli dostępu w systemie operacyjnym w oparciu o obowiązkową kontrolę dostępu na przykładzie systemu SELinux. Wyjaśnij pojęcie kontekstu bezpieczeństwa.

Bezpieczeństwo aplikacji w środowisku sieciowym

1. Omów protokół HTTP w aspekcie bezpieczeństwa wymiany danych.
2. Przedstaw ataki związane z sesją HTTP. Jak można chronić aplikację przed tym typem ataków?
3. Wskaż główne podatności występujące w kodzie źródłowym aplikacji. Omów na przykładzie jedną z podatności.

4. Omów metodę uwierzytelniania z wykorzystaniem kluczy publicznych. Jakie problemy są związane z bezpieczeństwem uwierzytelniania?
5. Na czym polega eksploatowanie aplikacji? Omów techniki ataków i rodzaje exploitów.

Projektowanie aplikacji i systemów bezpieczeństwa komputerowego

1. W jaki sposób specyfikuje się zabezpieczenia na etapie projektowania funkcjonalności aplikacji?
2. W jaki sposób projektuje się bezpieczne aplikacje w aspekcie środowiska pracy aplikacji?
3. Przedstaw techniki wykorzystywania zagrożeń spowodowanych nieoczekiwanymi danymi wejściowymi.
4. Omów zautomatyzowane badanie systemów zabezpieczeń w aplikacjach.
5. Przedstaw sposoby zabezpieczeń przed złośliwym oprogramowaniem.

Zarządzanie bezpieczeństwem systemów komputerowych

1. Czym jest polityka bezpieczeństwa i jakie elementy wchodzi w skład polityki bezpieczeństwa?
2. Przedstaw standardy zasad bezpieczeństwa.
3. Omów zarządzanie ciągłością działania systemu komputerowego. W jaki sposób identyfikuje się krytyczne informacje i usługi?
4. Jak przeprowadza się audyt bezpieczeństwa? Co składa się na audyt bezpieczeństwa?
5. W jaki sposób opracowuje się i wdraża plan odtwarzania? Kopia bezpieczeństwa, rodzaje i przeznaczenie.