

Pytania egzaminacyjne

Cyberbezpieczeństwo II st.

Przedmioty obowiązkowe:

1. Współczesne architektury cyberbezpieczeństwa
2. Sposoby i narzędzia do monitorowania i detekcji zagrożeń.
3. Podatności aplikacji Web – najpopularniejsze podatności, metody wykrywania
4. Identyfikacja zasobów IT i analiza ryzyka
5. System Zarządzania Bezpieczeństwem Informacji. Organizacja bezpieczeństwa informacji.

Przedmioty wybieralne:

Blok A

1. Zabezpieczenia systemów operacyjnych Windows i Linux
2. Testy penetracyjne związane z technikami kryptograficznymi.
3. Metody zacierania i fałszowania dowodów cyfrowych
4. Dowody incydentów bezpieczeństwa – gromadzenie, metody analizy i oceny jakości
5. Metody sztucznej inteligencji i uczenia maszynowego w modelowaniu i wykrywaniu zagrożeń systemów IT

Blok B

6. Narzędzia monitorowania i detekcja zagrożeń w systemach chmurowych
7. Metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych
8. Audyt infrastruktury sieciowej – etapy, sposób prowadzenia