Zakres egzaminu dyplomowego

Przedmioty obowiązkowe:

1. Współczesne architektury cyberbezpieczeństwa
2. Sposoby i narzędzia do monitorowania i detekcji zagrożeń.
3. Podatności aplikacji Web — najpopularniejsze podatności, metody wykrywania
4. Dowody incydentów bezpieczeństwa — gromadzenie, metody analizy i oceny jakości
5. Metody zacierania i fałszowania dowodów cyfrowych
6. System Zarządzania Bezpieczeństwem Informacji. Organizacja bezpieczeństwa informacji.

1. Blok A
   1.1. Zabezpieczenia systemów operacyjnych Windows i Linux
   1.2. Narzędzia monitorowania i detekcja zagrożeń w systemach chmurowych
2. Blok B
   2.1. Luki w bezpieczeństwie popularnych systemów bezprzewodowych, takich jak WiFi, Bluetooth, ZigBee oraz urządzeń mobilnych pracujących na systemach Android i Apple iOS
   2.2. Testy penetracyjne związane z technikami kryptograficznymi.
3. Blok C
   3.1. Metodyki inżynierii bezpieczeństwa systemu IT.
   3.2. Audyt infrastrul<tury sieciowej — etapy, sposób prowadzenia
4. Blok D
   4.1. Metody analizy sieci i analizy języka naturalnego w rozpoznawaniu wzorców behawioralnych
   4.2. Metody sztucznej inteligencji i uczenia maszynowego w modelowaniu i wykrywaniu zagrożeń systemów IT

s. Blok E
   5.1. Metody zapewniania bezpieczeństwa komunikacji w aplikacjach webowych
   5.2. Testowanie programów - testy jednostkowe, funkcjonalne, wydajnościowe, software quality assurance