PROGRAMY

Bezpieczeństwo informacji (4 godz.)

- Polityka bezpieczeństwa informacji i zarządzanie bezpieczeństwem
- Źródła wycieku danych i najczęstsze błędy organizacji w zakresie ochrony informacji
- Bezprawna ingerencja wobec osób i obiektów
- Motywy przekazywania informacji i sposoby uzyskiwania wiedzy
- Narzędzia oddziaływania na postawy osób i funkcjonowanie organizacji
- Rola i zagrożenia ze strony *insider'a* w procesie pozyskiwania wiedzy

Polityka informacyjna w prewencji terrorystycznej (2-3 godz.)

- Kształtowanie odpowiedniej komunikacji w przeciwdziałaniu terroryzmowi
- Polityka informacyjna organizacji terrorystycznych
- Rodzaje narracji i treści o charakterze terrorystycznym on- i offline
- Rekomendowane reakcje na treści o charakterze terrorystycznym
- Komunikacja kryzysowa – prowadzenie działań komunikacyjnych przed, w trakcie i po wystąpieniu zdarzenia o charakterze terrorystycznym
- Analiza konkretnych przypadków

Cyberbezpieczeństwo (1 godz.)

- Czym jest Cyberbezpieczeństwo
- Omówienie zagrożeń (phishing, spoofing etc)
- Metody zabezpieczeń przed typowymi zagrożeniami
- Bezpieczna praca z klientem email, Word
- Zabezpieczenie danych przed nieautoryzowanym dostępem
- Bezpieczne korzystanie z internetu
- Zabezpieczenie smartphone
- Reagowanie w przypadku wystąpienia incydentu