Załącznik nr 1

Do zapytania ofertowego nr OSU-VI.2610.2.1.2018

Minimalny zakres zagadnień szczegółowych szkolenia e-learningowego „Metodyki prowadzenia postępowań dotyczących przestępstw popełnianych przy użyciu internetu i systemów informatycznych”

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Proponowana nazwa modułu:** | **Proponowana nazwa lekcji:** | **Proponowany zakres:** |
| 1. | Podstawy prawne penalizacji i ścigania cyberprzestęp-czości | 1. Podstawy prawne penalizacji cyberprzestępczości. | Wskazanie regulacji kodeksu karnego i innych aktów w zakresie cyberprzestępczości. |
| 2. Podstawy prawne zwalczania cyberprzestępczości. | Omówienie podstaw prawnych zawartych w: kpk, ustawie o policji, ustawie antyterrorystycznej, regulacjach dotyczących telekomunikacji i ochrony danych osobowych. |
| 3. Współpraca z operatorami i dostawcami usług w zakresie pozyskiwania danych retencyjnych. | Praktyczne omówienie zasad pozyskiwania danych retencyjnych  i uzyskiwania informacji od operatorów i dostawców usług w prowadzonych postępowaniach dotyczących cyberprzestępczości. |
| 4. Współpraca międzynarodowa w zakresie zwalczania cyberprzestępczości. | Analiza regulacji i praktyczne wykorzystanie:   * konwencji o cyberprzestępczości, * pomocy prawnej, * europejskiego nakazu dochodzeniowego. |
| 2. | Wybrane rodzaje przestępstw/ ataków z uwzględnieniem metodyki prowadzenia postępowań oraz dowodów elektronicznych i ich zabezpieczania | 1. Ataki DDoS.  *(w tym naruszenie integralności danych, zakłócenie dostępu do danych, sabotaż komputerowy, zakłócenie pracy systemu lub sieci teleinformatycznej)* | * Opis i definicja przestępstwa/ataku. * Typy i rodzaje przestępstwa/ataku wraz z przykładami. * Analiza zawiadomienia lub materiału inicjującego postępowanie. * Rozpoznanie typu ataku, potencjalnego zasięgu i dokonanie ustalenie ustaleń co do celowości ataku * Analiza wykorzystania elementów socjotechnicznych przy popełnieniu przestępstwa. * Wyznaczenie kierunku postępowania i wstępnej kwalifikacji prawnej. * Zakres działań zleconych w ramach czynności sprawdzających lub wstępnych czynności śledztwa. * Praktyczne aspekty gromadzenie kompletnego materiału dowodowego i jego ocena w tym: wykorzystanie dowodów elektronicznych i ich zabezpieczanie, ustalanie użytkowników adresów IP, analiza komputerów, analiza informatycznych nośników danych, wykorzystanie techniki triage i live forensic, powołanie i zakres czynności do wykonania przez biegłego. |
| 2. Ransomware. | * Opis i definicja przestępstw/ataków. * Typy i rodzaje przestępstw/ataków wraz z przykładami. * Analiza zawiadomienia lub materiału inicjującego postępowanie. * Rozpoznanie typu ataku, potencjalnego zasięgu i dokonanie ustalenie ustaleń co do celowości ataku * Analiza wykorzystania elementów socjotechnicznych przy popełnieniu przestępstwa. * Wyznaczenie kierunku postępowania i wstępnej kwalifikacji prawnej. * Zakres działań zleconych w ramach czynności sprawdzających lub wstępnych czynności śledztwa. * Praktyczne aspekty gromadzenie kompletnego materiału dowodowego i jego ocena w tym: wykorzystanie dowodów elektronicznych i ich zabezpieczanie, ustalanie użytkowników adresów IP, analiza komputerów, analiza informatycznych nośników danych, wykorzystanie techniki triage i live forensic, powołanie i zakres czynności do wykonania przez biegłego. |
| 3. Hacking. | * Opis i definicja przestępstw/ataków. * Typy i rodzaje przestępstw wraz z przykładami. * Analiza zawiadomienia lub materiału inicjującego postępowanie. * Rozpoznanie typu ataku, potencjalnego zasięgu i dokonanie ustalenie ustaleń co do celowości ataku * Analiza wykorzystania elementów socjotechnicznych przy popełnieniu przestępstwa. * Wyznaczenie kierunku postępowania i wstępnej kwalifikacji prawnej. * Zakres działań zleconych w ramach czynności sprawdzających lub wstępnych czynności śledztwa. * Praktyczne aspekty gromadzenie kompletnego materiału dowodowego i jego ocena w tym: wykorzystanie dowodów elektronicznych i ich zabezpieczanie, ustalanie użytkowników adresów IP, analiza komputerów, analiza informatycznych nośników danych, wykorzystanie techniki triage i live forensic, powołanie i zakres czynności do wykonania przez biegłego. |
| 4. Ataki typu phishing (w tym spear phishing i whaling) | * Opis i definicja przestępstw/ataków. * Typy i rodzaje przestępstw/ataków wraz z przykładami. * Analiza zawiadomienia lub materiału inicjującego postępowanie. * Rozpoznanie typu ataku, potencjalnego zasięgu i dokonanie ustalenie ustaleń co do celowości ataku * Analiza aspektu naruszenia ochrony danych osobowych, tajemnicy służbowej i zawodowej przy popełnieniu przestępstwa. * Analiza wykorzystania elementów socjotechnicznych przy popełnieniu przestępstwa. * Wyznaczenie kierunku postępowania i wstępnej kwalifikacji prawnej. * Zakres działań zleconych w ramach czynności sprawdzających lub wstępnych czynności śledztwa. * Praktyczne aspekty gromadzenie kompletnego materiału dowodowego i jego ocena w tym: wykorzystanie dowodów elektronicznych i ich zabezpieczanie, ustalanie użytkowników adresów IP, analiza komputerów, analiza informatycznych nośników danych, wykorzystanie techniki triage i live forensic, powołanie i zakres czynności do wykonania przez biegłego. |
| 5. Mowa nienawiści w Internecie. | * Opis i definicja przestępstw/ataków. * Typy i rodzaje przestępstw/ataków wraz z przykładami. * Analiza zawiadomienia lub materiału inicjującego postępowanie. * Rozpoznanie typu ataku, potencjalnego zasięgu i dokonanie ustalenie ustaleń co do celowości ataku * Analiza wykorzystania elementów socjotechnicznych przy popełnieniu przestępstwa. * Wyznaczenie kierunku postępowania i wstępnej kwalifikacji prawnej. * Zakres działań zleconych w ramach czynności sprawdzających lub wstępnych czynności śledztwa. * Praktyczne aspekty gromadzenie kompletnego materiału dowodowego i jego ocena w tym: wykorzystanie dowodów elektronicznych i ich zabezpieczanie, ustalanie użytkowników adresów IP, analiza komputerów, analiza informatycznych nośników danych, wykorzystanie techniki triage i live forensic, powołanie i zakres czynności do wykonania przez biegłego. |
| 6. Oszustwo komputerowe. | * Opis i definicja przestępstwa/ataku. * Typy i rodzaje przestępstw/ataków wraz z przykładami. * Analiza zawiadomienia lub materiału inicjującego postępowanie. * Rozpoznanie typu ataku, potencjalnego zasięgu i dokonanie ustalenie ustaleń co do celowości ataku * Analiza wykorzystania elementów socjotechnicznych przy popełnieniu przestępstwa. * Wyznaczenie kierunku postępowania i wstępnej kwalifikacji prawnej. * Zakres działań zleconych w ramach czynności sprawdzających lub wstępnych czynności śledztwa. * Praktyczne aspekty gromadzenie kompletnego materiału dowodowego i jego ocena w tym: wykorzystanie dowodów elektronicznych i ich zabezpieczanie, ustalanie użytkowników adresów IP, analiza komputerów, analiza informatycznych nośników danych, wykorzystanie techniki triage i live forensic, powołanie i zakres czynności do wykonania przez biegłego. |
| 7. Oszustwo popełniane za pomocą sieci Internet. | * Opis i definicja przestępstwa/ataku. * Typy i rodzaje przestępstw/ataków wraz z przykładami. * Analiza zawiadomienia lub materiału inicjującego postępowanie. * Rozpoznanie typu ataku, potencjalnego zasięgu i dokonanie ustalenie ustaleń co do celowości ataku * Analiza wykorzystania elementów socjotechnicznych przy popełnieniu przestępstwa. * Wyznaczenie kierunku postępowania i wstępnej kwalifikacji prawnej. * Zakres działań zleconych w ramach czynności sprawdzających lub wstępnych czynności śledztwa. * Praktyczne aspekty gromadzenie kompletnego materiału dowodowego i jego ocena w tym: wykorzystanie dowodów elektronicznych i ich zabezpieczanie, ustalanie użytkowników adresów IP, analiza komputerów, analiza informatycznych nośników danych, wykorzystanie techniki triage i live forensic, powołanie i zakres czynności do wykonania przez biegłego. |
| 8. Przestępstwa przeciwko wolności  seksualnej i obyczajności. | * Opis i definicja przestępstw/ataków. * Typy i rodzaje przestępstw/ataków wraz z przykładami. * Analiza zawiadomienia lub materiału inicjującego postępowanie. * Rozpoznanie typu ataku, potencjalnego zasięgu i dokonanie ustalenie ustaleń co do celowości ataku * Analiza wykorzystania elementów socjotechnicznych przy popełnieniu przestępstwa. * Wyznaczenie kierunku postępowania i wstępnej kwalifikacji prawnej. * Zakres działań zleconych w ramach czynności sprawdzających lub wstępnych czynności śledztwa. * Praktyczne aspekty gromadzenie kompletnego materiału dowodowego i jego ocena w tym: wykorzystanie dowodów elektronicznych i ich zabezpieczanie, ustalanie użytkowników adresów IP, analiza komputerów, analiza informatycznych nośników danych, wykorzystanie techniki triage i live forensic, powołanie i zakres czynności do wykonania przez biegłego. |
| 9. Kryptowaluty. | * Opis i definicja kryptowalut. * Przykłady wykorzystania kryptowalut cyberprzestępczości. * Zabezpieczenie kryptowalut. |