Warszawa, dnia 15 listopada 2018 r.

Poz. 109

DECYZJA NR 322
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 24 października 2018 r.

w sprawie programu nauczania na kursie specjalistycznym w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową

Na podstawie § 54 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 19 czerwca 2007 r. w sprawie szczegółowych warunków odbywania szkoleń zawodowych oraz doskonalenia zawodowego w Policji (Dz. U. poz. 877, z późn. zm.[1)]) postanawia się, co następuje:

§ 1. Określa się program nauczania na kursie specjalistycznym w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową, stanowiący załącznik do decyzji.

§ 2. Realizację kursu, o którym mowa w § 1, powierza się Wyższej Szkole Policji w Szczytnie, Centrum Szkolenia Policji w Legionowie oraz Szkole Policji w Pile.

§ 3. Kurs specjalistyczny w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową, rozpoczęty i niezakończony przed dniem wejścia w życie niniejszej decyzji, prowadzi się na podstawie programu nauczania obowiązującego w dniu rozpoczęcia kursu.

§ 4. Traci moc decyzja nr 872 Komendanta Głównego Policji z dnia 5 grudnia 2007 r. w sprawie programu kursu specjalistycznego w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową (Dz. Urz. KGP poz. 185 oraz z 2008 r. poz. 117).

§ 5. Decyzja wchodzi w życie z dniem podpisania.

Komendant Główny Policji
z upoważnienia
Pierwszy Zastępca Komendanta Głównego Policji
nadinsp. dr Andrzej SZYMCZYK

[1)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. U. z 2007 r. poz. 1644, z 2008 r. poz. 1116, z 2010 r. poz. 1381, z 2012 r. poz. 899, z 2014 r. poz. 1312, z 2015 r. poz. 593, z 2016 r. poz. 1526 oraz z 2018 r. poz. 208.

Załącznik do decyzji nr 322
Komendanta Głównego Policji
z dnia 24 października 2018 r.

PROGRAM NAUCZANIA NA KURSIE SPECJALISTYCZNYM W ZAKRESIE UZYSKIWANIA INFORMACJI Z INTERNETU DLA POLICJANTÓW ZWALCZAJĄCYCH PRZESTĘPCZOŚĆ KOMPUTEROWĄ

SPIS TREŚCI

I. ZAŁOŻENIA ORGANIZACYJNO - PROGRAMOWE

1. Nazwa kursu

Kurs specjalistyczny w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową, zwany dalej „kursem”.

2. Cel kursu

Celem kursu jest pogłębienie wiedzy policjantów z zakresu zwalczania przestępczości komputerowej i uzyskiwania informacji z Internetu, służące usprawnieniu prowadzenia postępowań przygotowawczych w sprawach o przestępstwa komputerowe.

3. Kryteria formalne, jakim muszą odpowiadać kandydaci kierowani na kurs

Na kurs kierowani są policjanci, którzy spełniają łącznie następujące kryteria:
- zajmują się bezpośrednio zwalczaniem przestępczości komputerowej – uzyskiwaniem informacji z Internetu,
- zajmują stanowiska wykonawcze w komórkach zajmujących się zwalczaniem przestępczości gospodarczej, kryminalnej lub cyberprzestępczości,
- posiadają podstawową wiedzę informatyczną rozumianą, jako znajomość obsługi komputera klasy PC z zainstalowanym systemem MS Windows,
- znają polskie prawo karne w zakresie przestępczości komputerowej.

Kierowanie na kurs powinno odbywać się w porozumieniu z kierownikami komórek organizacyjnych właściwych do walki z przestępczością gospodarczą, kryminalną lub cyberprzestępczością.

4. System prowadzenia kursu

Kurs prowadzony jest w systemie stacjonarnym.

5. Czas trwania kursu

Kurs trwa 5 dni szkoleniowych. Na całkowity wymiar czasu trwania kursu składają się:

Przedsięwzięcia	**Czas realizacji (w godzinach lekcyjnych)**
Rozpoczęcie, zapoznanie z regulaminami i organizacją kursu	1
Zajęcia programowe	38
Zakończenie kursu	1
Ogółem	**40 (5 dni szkoleniowych)**

Program kursu przewiduje realizację 40 godzin lekcyjnych. Jako podstawę dziennego wymiaru czasu pracy uczestników kursu przyjęto 8 jednostek lekcyjnych dziennie.

Podczas prowadzenia zajęć, można regulować ich czas w sposób zapewniający optymalne osiągnięcie zakładanych celów, z zastrzeżeniem rozpoczęcia kolejnej jednostki metodycznej w czasie przyjętym w rozkładzie zajęć dydaktycznych.

6. Liczebność grupy szkoleniowej

Treści kształcenia należy realizować w grupie szkoleniowej, której liczebność, z uwagi na efektywność stosowanych metod (technik) dydaktycznych oraz cele dydaktyczne zajęć, nie powinna przekraczać **12 osób**.

7. Warunki niezbędne do realizacji i osiągnięcia celów kształcenia

Zasadniczą formą realizacji kursu są zajęcia dydaktyczne prowadzone metodą wykładu, ćwiczeń, pokazu i zajęć praktycznych w jednostce szkoleniowej.

Zajęcia prowadzi kadra dydaktyczna jednostki szkoleniowej oraz zaproszone osoby posiadające odpowiednie doświadczenie zawodowe oraz wiedzę i umiejętności z zakresu realizowanego kursu. W celu uzyskania lepszej efektywności kształcenia zaleca się realizowanie zajęć praktycznych przez dwóch prowadzących.

Każdy z uczestników kursu musi posiadać osobiste stanowisko pracy, na które składa się zestaw komputerowy z dostępem do Internetu on-line, zapewniający stabilne warunki pracy – minimalna prędkość łącza dla grupy to 10 Mb/s.

8. Zakres tematyczny oraz system oceniania

<table>
<tr><th>Temat</th><th>Czas realizacji (w godzinach lekcyjnych)</th><th>System oceniania</th></tr>
<tr><td>I. Charakterystyka przestępczości komputerowej</td><td>4</td><td rowspan="6">Nabywane przez słuchaczy umiejętności podlegają bieżącemu ocenianiu według obowiązującej skali ocen: 6 – 1 (słuchacz powinien uzyskać co najmniej dwie oceny bieżące).

Końcowe zadanie praktyczne realizowane jest w ramach Tematu V: Procedury postępowania w sprawach o przestępstwa komputerowe i polega na samodzielnym wykonaniu, określonego przez prowadzącego zajęcia dydaktyczne, zadania dotyczącego postępowania Policji w przypadku uzyskania informacji o popełnionym przestępstwie komputerowym. Końcowe zadanie praktyczne podlega bieżącemu ocenianiu według obowiązującej skali ocen: 6 – 1.

Każda ocena negatywna, uzyskana w trakcie trwania kursu, musi być poprawiona na ocenę pozytywną.</td></tr>
<tr><td>II. Środowisko komputerowe</td><td>4</td></tr>
<tr><td>III. Usługi w sieciach komputerowych</td><td>13</td></tr>
<tr><td>IV. Uzyskiwanie informacji ze źródeł ogólnodostępnych</td><td>4</td></tr>
<tr><td>V. Procedury postępowania w sprawach o przestępstwa komputerowe</td><td>13</td></tr>
</table>

9. Forma zakończenia kursu

Absolwent otrzymuje świadectwo ukończenia kursu specjalistycznego z wpisanym ogólnym wynikiem nauki, który jest średnią arytmetyczną ocen bieżących.

II. TREŚCI KSZTAŁCENIA

TEMAT NR I. CHARAKTERYSTYKA PRZESTĘPCZOŚCI KOMPUTEROWEJ

CELE: Słuchacz po zakończeniu tematu będzie potrafił:

- wskazać trudności w szczegółowej klasyfikacji przestępczości komputerowej,
- wskazać zakres międzynarodowych regulacji prawnych dotyczących przestępczości komputerowej,
- wskazać zakres regulacji prawnych dotyczących przestępczości komputerowej w krajowym systemie prawa,
- identyfikować zachowania stanowiące naruszenia prawa polskiego oraz możliwości ścigania przestępstw popełnianych poza granicami Polski.

Nr	Zagadnienia	Czas realizacji w godz. lekcyjnych	Metoda	Wskazówki do realizacji
1.	Cechy przestępczości komputerowej	1	wykład	Omów cechy charakterystyczne przestępczości komputerowej: – sposoby popełniania przestępstw, – specyfikę śladów i dowodów przestępczości komputerowej, – ograniczenia w zakresie przeszukania, – zabezpieczenia techniczne. Przedstaw charakterystykę sprawców, szczególnie w aspekcie transgraniczności: – rodzaje sprawców, – motywy działania, – dostęp do narzędzi, – trudności w ustaleniu miejsca popełnienia przestępstwa, – różnice w regulacjach prawnych dotyczących tego samego zachowania w prawie krajowym.
2.	Regulacje międzynarodowe	1	wykład	Omów Konwencję o cyberprzestępczości. Zwróć uwagę na znaczenie tego aktu prawnego w aspekcie współpracy międzynarodowej. Przedstaw historię i klasyfikację cyberprzestępczości. Odnieś przepisy Konwencji do prawa krajowego. Przedstaw organizacje i porozumienia międzynarodowe (CERT). Omów Protokół Dodatkowy do Konwencji o cyberprzestępczości, dotyczący kryminalizacji aktów natury rasistowskiej i ksenofobicznej popełnianych przy pomocy systemów komputerowych. Omów Dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne.
3.	Prawo krajowe	2	wykład	Przedstaw i omów przepisy kodeksu karnego dotyczące przestępstw przeciwko ochronie informacji (Rozdział XXXIII). Przedstaw i omów pozostałe przepisy kodeksu karnego mające związek z cyberprzestępczością: 115 § 14, 130 § 3, 165 § 1, 167 § 2, 190a § 1 i 2, 196, 200, 200a, 200b, 202, 254a, 256, 257, 270, 278 § 2, 285, 287, 293, 299.

				Przedstaw i omów przepisy kodeksu postępowania karnego (143 § 1, 217 § 1, 218 § 1, 218a, 218b, 236a). Przedstaw i omów przepisy ustawy o prawie autorskim i prawach pokrewnych (23, 115, 116, 117, 118, 119). Omów przepisy w pozostałych aktach prawnych związanych z cyberprzestępczością (prawo telekomunikacyjne, ustawa o świadczeniu usług drogą elektroniczną, ustawa o usługach płatniczych, ustawa o ochronie danych osobowych, ustawa o ochronie informacji niejawnych).

TEMAT NR II. ŚRODOWISKO KOMPUTEROWE

CELE: Po zrealizowaniu tematu słuchacz będzie potrafił:

- wskazać różnice w sposobie i zakresie zbierania, dokumentowania i taktyki prowadzenia postępowania w zależności od środowiska komputerowego, obejmującego pojedyncze stanowisko komputerowe, sieć wewnętrzną firmy i sieć Internet,
- określić działania policjantów wskazane przy planowaniu i prowadzeniu postępowań w sprawach o przestępstwa komputerowe.

Nr	Zagadnienia	Czas realizacji w godz. lekcyjnych	Metoda	Wskazówki do realizacji
1.	Stanowisko komputerowe	2	wykład, dyskusja	Omów typy i budowę najczęściej spotykanych rodzajów komputerów. Wskaż najważniejsze elementy i urządzenia peryferyjne. Omów inne urządzenia przetwarzające dane: palmtop, IoT, smartfon, tablet. Omów rodzaje nośników danych, wskaż różnice pomiędzy nośnikami stałymi i wymiennymi. Omów sposoby zabezpieczania poszczególnych rodzajów nośników i opisz sposoby dokumentowania czynności. Omów strukturę danych, organizację kont użytkowników najpopularniejszych systemów operacyjnych: MS Windows, MAC OS, Linuks, Android, iOS. Poproś słuchaczy o wskazanie najważniejszych elementów stanowiska komputerowego i poproś o opis zabezpieczania poszczególnych elementów.
2.	Sieci komputerowe	2	wykład	Podczas omawiania rodzajów sieci komputerowych opisz typy sieci wymiany danych, najpopularniejsze topologie sieci oraz normy i standardy stosowane w sieciach komputerowych. Omów podstawy protokołu TCP/IP uwzględniając szczególnie model OSI, budowę pakietów (nagłówek IP, TCP, UDP), używanie snifferów i tworzenie pułapek. Omów polityki w zakresie przyznawania i zarządzania adresami internetowymi. Przedstaw adresację IP i domenową. Wskaż organizacje odpowiadające za przydział domen i bazy danych whois.

TEMAT NR III. USŁUGI W SIECIACH KOMPUTEROWYCH

CELE: Po zrealizowaniu tematu słuchacz będzie potrafił:

- określić sposoby pozyskiwania informacji na temat użytkowników sieci komputerowych,
- zidentyfikować poszczególne rodzaje usług sieciowych,
- zidentyfikować różnice w sposobach zbierania i zabezpieczania informacji w zależności od rodzaju usługi sieciowej,
- sprawnie posługiwać się pocztą elektroniczną, zabezpieczać kopie do celów dowodowych oraz ustalać tożsamość źródeł danych.

Nr	Zagadnienia	Czas realizacji w godz. lekcyjnych	Metoda	Wskazówki do realizacji
1.	Strony WWW	2	wykład, ćwiczenia	Wspólnie ze słuchaczami sprawdź kilka stron WWW (statyczne, dynamiczne, zabezpieczone, ukryte), poproś słuchaczy o scharakteryzowanie poszczególnych rodzajów i ich znaczenia dla toczącego się postępowania. Omów rodzaje i lokalizacje serwerów stron WWW. Przedstaw metody zbierania danych o autorach, właścicielach, lokalizacjach: – sposoby uzyskiwania informacji o domenach, serwerach, adresach, – kontakt z administratorem, – możliwości przeglądania kodu źródłowego, – systemy wymiany banerów, – księgi gości, liczniki odwiedzin.
2.	Poczta elektroniczna	4	wykład, ćwiczenia	Przedstaw podstawy działania poczty elektronicznej omawiając jej standardy, protokoły, bezpieczeństwo i programy do jej obsługi. Przedstaw możliwości ustalania trasy i autora listu poprzez przeglądanie nagłówka wiadomości pocztowej i korzystania z różnego oprogramowania (zarówno klienta e-mail jak i programów do dekodowania poczty). Poproś słuchaczy o ustalenie trasy i autora kilku wybranych wiadomości e-mail zarówno poprzez przeglądanie nagłówka wiadomości, jak i wykorzystanie oprogramowania. Przedstaw sposoby anonimizacji wiadomości elektronicznej i związane z tym możliwości wykrywcze (anonimowa poczta (SMTP), anonimizery, przechwytywanie poczty elektronicznej na serwerze, podsłuch i kontrola korespondencji internetowej, przeglądanie poczty przechowywanej w programach pocztowych). Przedstaw formalno-prawne ograniczenia w zbieraniu dowodów. Poproś słuchaczy o wysłanie anonimowej wiadomości e-mail oraz wskazanie kierunków wykrywczych. Dokonaj przeglądu usług e-mail dostępnych za pośrednictwem sieci TOR i przedstaw możliwości wykrywcze.

3.	Pozostałe sposoby wymiany danych i informacji	4	wykład, ćwiczenia	Przedstaw wybrane sposoby na wymianę danych w sieciach komputerowych i omów ich możliwości wykrywcze: systemy typu klient serwer (np. FTP, serwery newsowe – grupy binarne, przechowywanie plików w chmurze), systemy typu P2P (np. BitTorrent, .eDonkey, P2Mail), udostępnianie zasobów lokalnych (np. dyski sieciowe, udziały lokalne, lokalne serwery plików). Omów wybrane sposoby wymiany informacji np.: grupy dyskusyjne, fora dyskusyjne, systemy randkowe, portale ogłoszeniowe, systemy komentarzy, portale społecznościowe. Wskaż możliwości wykrywcze. Omów ideę działania komunikatorów i chatów, wskaż najpopularniejsze. Wskaż możliwości wykrywcze. Omów bramki SMS, serwisy z dostępem warunkowym – SMS i systemy VoIP. Omów handel elektroniczny w Internecie, także w DarkWeb. Wskaż różnice pomiędzy serwisami ogłoszeniowymi, systemami aukcyjnymi i sklepami. Wskaż możliwości wykrywcze. Omów system bankowości elektronicznej, wskaż jego podatności na nadużycia i sposoby zabezpieczania. Omów pojęcie płatności elektronicznej, pojęcie kryptowaluty i pojęcie blockchain. W ramach ćwiczeń słuchacze powinni skonfigurować software'owy portfel bitcoinowy (poprawnie zainstalować i skonfigurować program komputerowy, który jest odpowiedzialny za przechowywanie i przesyłanie kryptopwalut) i opisać sposób dokonywania transakcji oraz wskazać sposoby na monitorowanie wybranych płatności. Omów operacje na kryptowalutach wykonywane na PC i smartfonie.
4.	Sposoby identyfikacji i zabezpieczania informacji	3	wykład, ćwiczenia	Wskaż sposoby ustalania tożsamości źródeł danych (serwery whois, współpraca z administratorem sieci/systemu, skanowanie sieci). Wskaż sposoby zabezpieczania danych (sposoby zabezpieczania transmisji sieciowej, uwierzytelnianie użytkowników, urządzenia do administrowania siecią, sposoby zabezpieczania a możliwość utraty danych, informacje możliwe do uzyskania w czasie badań laboratoryjnych, zabezpieczenia techniczne). Wskaż sposoby zabezpieczania kopii do celów dowodowych (możliwości współpracy z administratorem systemu/sieci, uzyskiwanie kopii z serwera macierzystego, uzyskiwanie kopii z serwerów cechujących, uzyskiwanie kopii z innych źródeł). Poproś słuchaczy o wskazanie źródeł informacji dla kilku podanych przykładów. Omów formalno-prawne ograniczenia w zbieraniu dowodów.

TEMAT NR IV. Uzyskiwanie informacji ze źródeł ogólnodostępnych

CELE: Po zrealizowaniu tematu słuchacz będzie potrafił:

- opisać pojęcie białego wywiadu,
- identyfikować poszczególne źródła informacji,
- wskazać podstawowe metody, techniki, narzędzia stosowane przy pozyskiwaniu informacji,
- prawidłowo analizować dane i interpretować otrzymane wyniki,
- ocenić przydatność danych do realizacji wybranego zagadnienia.

Nr	Zagadnienia	Czas realizacji w godz. lekcyjnych	Metoda	Wskazówki do realizacji
1.	Uzyskiwanie informacji ze źródeł ogólnodostępnych.	4	wykład, ćwiczenia	Omów podstawowe pojęcia związane z białym wywiadem: Open Source Data (OSD), Open Source Information (OSIF), Open Source Intelligence (OSINT), walidacja OSINT (OSINT-V). Omów sposoby zbierania i łączenia danych w oparciu o strony WWW (metody, źródła, mechanizmy weryfikacji danych). Przeprowadź pokaz i poproś słuchaczy o wykonanie ćwiczeń z wykorzystaniem oprogramowania MALTEGO i FOCA według zadanych parametrów zadania.

TEMAT NR V. PROCEDURY POSTĘPOWANIA W SPRAWACH O PRZESTĘPSTWA KOMPUTEROWE

CELE: Po zrealizowaniu tematu słuchacz będzie potrafił:

- opisać sposoby pozyskiwania informacji na temat użytkowników sieci komputerowych,
- identyfikować poszczególne rodzaje usług sieciowych,
- określić różnice w sposobach zbierania i zabezpieczania informacji w zależności od rodzaju usługi sieciowej,
- określić działania policjantów wskazane przy planowaniu i prowadzeniu działań procesowych i operacyjno-rozpoznawczych w sprawach o przestępstwa komputerowe.

Nr	Zagadnienia	Czas realizacji w godz. lekcyjnych	Metoda	Wskazówki do realizacji
1.	Zabezpieczanie dowodów uzyskanych w związku z przestępstwem popełnionym przy użyciu sprzętu komputerowego	2	wykład	Opisz procedurę postępowania podczas zabezpieczania dowodów ujmując najważniejsze elementy: – rozpoznanie, planowanie, przygotowanie operacji, – dbanie o bezpieczeństwo danych, – odpowiednie dokumentowanie, – możliwości współpracy z ekspertem. Omów ograniczenia formalno-prawne, wynikające z prawa procesowego i innych przesłanek. Omów ograniczenia techniczne. Omów taktykę działań: – rodzaj przestępstwa a siły i środki użyte do działań Policji, – zakres rozpoznania, – rodzaje planów (czas, miejsce działań), – skład grupy.
2.	Wyszukiwanie i zabezpieczanie śladów w sieciach komputerowych	9	wykład, ćwiczenia	Omów ograniczenia formalno-prawne wynikające z: – prawa krajowego (adekwatność użytych środków – osoba trzecia, zwróć uwagę na zabezpieczenie dowodów zawierających tajemnice), – umów międzynarodowych. Omów ograniczenia techniczne. Omów możliwości współpracy z: – ekspertem, – administratorem (administratorami) sieci, – pionem odpowiedzialnym za bezpieczeństwo sieci, – międzynarodowymi organizacjami wymiaru sprawiedliwości,

				– z organizacjami pozapolicyjnymi, – konsultantami krajowymi i zagranicznymi. Omów taktykę działań: – rodzaj przestępstwa a siły i środki użyte do działań Policji, – zakres rozpoznania, – rodzaje planów (czas, miejsce działań), – skład grupy. Wskaż na różnice w procedurach postępowania w przypadkach małych sieci lokalnych a dużych sieci firmowych. Na podstawie wydanych założeń dotyczących hipotetycznego przestępstwa komputerowego słuchacze powinni wykonać plan działań oraz wyszukać żądane rodzaje informacji i podać odpowiednie procedury postępowania.
3.	Przyjęcie zawiadomienia o przestępstwie	2	wykład, ćwiczenia	Omów ograniczenia formalno-prawne wynikające z prawa krajowego, umów międzynarodowych. Omów ograniczenia techniczne. Wskaż na problemy dotyczące ustalenia jednostki organizacyjnej Policji właściwej do prowadzenia sprawy. Słuchacze na podstawie podanych założeń powinni zaplanować działania Policji (uwzględniając odpowiednie i adekwatne środki, skład grupy, możliwości współpracy, koordynację działań). Dokonaj oceny końcowego zadania praktycznego.