Warszawa, dnia 17 stycznia 2019 r.

Poz. 15

# DECYZJA NR 7
# KOMENDANTA GŁÓWNEGO POLICJI

z dnia 15 stycznia 2019 r.

**w sprawie programu nauczania na kursie specjalistycznym dla policjantów realizujących zadania w zakresie zwalczania cyberprzestępczości**

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 dla policjantów realizujących zadania w zakresie zwalczania cyberprzestępczości, stanowiący załącznik do decyzji.

**§ 2.** Realizację kursu, o którym mowa w § 1, powierza się Wyższej Szkole Policji w Szczytnie.

**§ 3.** Kurs specjalistyczny dla policjantów w zakresie zwalczania cyberprzestępczości, 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 331 Komendanta Głównego Policji z dnia 22 października 2015 r. w sprawie programu nauczania na kursie specjalistycznym dla policjantów w zakresie zwalczania cyberprzestępczości (Dz. Urz. KGP poz. 84).

**§ 5.** Decyzja wchodzi w życie z dniem podpisania.

Komendant Główny Policji

**gen. insp. Jarosław 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 7
Komendanta Głównego Policji
z dnia 15 stycznia 2019 r.

**PROGRAM NAUCZANIA**
**NA KURSIE SPECJALISTYCZNYM DLA POLICJANTÓW REALIZUJĄCYCH ZADANIA W ZAKRESIE ZWALCZANIA CYBERPRZESTĘPCZOŚCI**

**SPIS TREŚCI**

## I. ZAŁOŻENIA ORGANIZACYJNO-PROGRAMOWE

### 1. Nazwa kursu

Kurs specjalistyczny dla policjantów realizujących zadania w zakresie zwalczania cyberprzestępczości, zwany dalej „kursem”.

### 2. Cel kursu

Celem kursu jest uzyskanie wiedzy i umiejętności przygotowujących policjanta do realizacji zadań dotyczących zwalczania cyberprzestępczości w zakresie:

1) analizy sprawy/stanu faktycznego;
2) oceny zachowania sprawcy i możliwości jego identyfikacji;
3) ujawnienia i zabezpieczenia śladów i dowodów działalności cyberprzestępczej wraz z ich wstępną weryfikacją;
4) ukierunkowanego prowadzenia rozpoznania internetowego oraz dokumentowania ww. czynności.

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

Na kurs kierowani są policjanci służby kryminalnej i śledczej, którzy realizują zadania związane z prowadzeniem spraw w zakresie cyberprzestępczości.

### 4. System prowadzenia kursu

Kurs jest prowadzony w systemie stacjonarnym.

### 5. Czas trwania kursu

Kurs trwa 10 dni szkoleniowych. Na całkowity wymiar czasu trwania kursu składają się:

| **Przedsięwzięcia** | **Czas realizacji (w godzinach lekcyjnych)** |
|---|---|
| Zapoznanie z regulaminami i organizacją kursu | 1 |
| Zajęcia programowe | 78 |
| Zakończenie kursu | 1 |
| **Ogółem** | **80** |

Liczba godzin lekcyjnych, liczonych w 45-minutowych jednostkach nie powinna przekraczać 8 godzin lekcyjnych dziennie.

### 6. Liczebność grupy szkoleniowej

Poszczególne treści kształcenia należy realizować w grupie szkoleniowej, której liczebność, z uwagi na cele dydaktyczne zajęć oraz efektywność stosowanych metod dydaktycznych, nie powinna przekraczać 15 osób.

## 7. Warunki niezbędne do realizacji i osiągnięcia celów kształcenia

Zajęcia realizuje nauczyciel policyjny, który w ramach pełnionej służby specjalizuje się w tematyce objętej programem kursu. Zajęcia praktyczne prowadzi dwóch nauczycieli policyjnych. Zajęcia mogą być realizowane przy współudziale przedstawicieli innych jednostek organizacyjnych Policji oraz instytucji pozapolicyjnych. Zajęcia prowadzone są w sali dydaktycznej wyposażonej w stanowiska komputerowe z pełnym dostępem do Internetu, bez blokad stron. Wskazane w programie metody realizacji zajęć są wg autorów najbardziej optymalne do osiągnięcia zakładanych celów kształcenia. Prowadzący zajęcia może wybrać inną metodę gwarantującą osiągnięcie celów. Zajęcia dydaktyczne powinny być realizowane z wykorzystaniem materiałów opracowanych we współpracy z komórkami organizacyjnymi właściwymi w sprawach cyberprzestępczości. Nauczyciel policyjny podczas prowadzenia zajęć może regulować czas ich trwania, dostosowując go do osiągnięcia zakładanych celów kształcenia.

## 8. Zakres tematyczny oraz system oceniania

| Temat | Czas realizacji w godz. lekcyjnych | System oceniania |
|---|---|---|
| **Nr 1. Wstęp do informatyki** | **8** | Słuchacz podlega bieżącemu ocenianiu. Warunkiem ukończenia kursu jest zaliczenie wszystkich ćwiczeń przewidzianych w programie. Do oceny stopnia przyswojenia wiedzy i opanowania umiejętności tematów stosuje się wyłącznie dwustopniową skalę ocen z wpisem uogólnionym zaliczono (zal.) albo nie zaliczono (nzal.). Każda ocena negatywna musi być poprawiona na ocenę pozytywną. |
| **Nr 2. Uregulowania prawne i taktyka prowadzenia wybranych czynności dowodowych** | **16** | |
| **Nr 3. Wstęp do działań operacyjnych w Internecie** | **12** | |
| **Nr 4. Podstawy informatyki śledczej** | **20** | |
| **Nr 5. Analiza śledcza w sprawach związanych z cyberprzestępczością** | **12** | |
| **Nr 6. Live Forensics, metody TRIAGE** | **10** | |
| Razem: | **78** | |

## 9. Forma zakończenia kursu

Absolwent kursu otrzymuje świadectwo ukończenia kursu specjalistycznego, na którym w miejsce wyniku stosuje się wpis "pozytywnym".

## II. TREŚCI KSZTAŁCENIA

### TEMAT NR 1: Wstęp do informatyki

**CELE:** Po zrealizowaniu tematu, słuchacz będzie potrafił:

- wskazać cechy charakterystyczne systemów operacyjnych Windows, Linux, macOs, oraz wykonać podstawowe polecenia systemowe,
- wykonać operacje związane z uzyskaniem informacji nt. sprzętowej konfiguracji komputera, interfejsów sieciowych, artefaktów systemu,
- interpretować zapisy logów systemowych, plików konfiguracyjnych, zapisów rejestrów.

| Zagadnienia | Czas realizacji w godz. lekcyjnych | Metoda | Wskazówki do realizacji |
|---|---|---|---|
| 1. Wstęp do systemów operacyjnych z rodziny Windows.<br>2. Wstęp do systemów operacyjnych z rodziny Linux.<br>3. Wstęp do systemów operacyjnych z rodziny macOs.<br>4. Wstęp do sieci komputerowych (adresacja IP, DNS, TOR). | 8 | wykład, ćwiczenia | Skorzystaj z systemów operacyjnych pracujących na maszynach wirtualnych.<br><br>Przeprowadź ćwiczenia i następnie dokonaj oceny pracy słuchaczy. |

**TEMAT NR 2: Uregulowania prawne i taktyka prowadzenia wybranych czynności dowodowych**

**CELE:** Po zrealizowaniu tematu, słuchacz będzie potrafił:

- określić ustawowe znamiona przestępstw popełnianych w cyberprzestrzeni,
- zinterpretować podstawowe pojęcia, w tym dowodu elektronicznego i cyfrowego, oględzin, przeszukania,
- przeprowadzić oględziny sprzętu komputerowego i elektronicznych nośników danych oraz sporządzić dokumentację,
- przeprowadzić przeszukanie (pomieszczenia, systemu komputerowego),
- zabezpieczyć fizycznie sprzęt elektroniczny i nośniki danych.

| Zagadnienia | Czas realizacji w godz. lekcyjnych | Metoda | Wskazówki do realizacji |
|---|---|---|---|
| 1. Znamiona i specyfika wybranych przestępstw popełnianych w cyberprzestrzeni wraz z kwalifikacją prawną.<br><br>2. Pojęcie dowodu elektronicznego w aspekcie art. 115 §14 kk oraz przepisów KPK - definicje.<br><br>Oględziny:<br>- pojęcie oględzin,<br>- przedmiot oględzin.<br><br>Przeszukanie:<br>- pojęcie przeszukania,<br>- sposób prowadzenia przeszukania.<br><br>3. Krajowe i międzynarodowe uregulowania prawne (Konwencja Rady Europy, Europejski Nakaz Dochodzeniowy, współpraca międzynarodowa).<br><br>4. Zabezpieczenie fizyczne sprzętu. | 16 | wykład, burza mózgów, ćwiczenia | Do wykładu i burzy mózgów wykorzystaj wiedzę uczestników kursu i zaproszonych prelegentów (w szczególności funkcjonariuszy wydziałów dw. z cyberprzestępczością).<br><br>Podczas wykładu przedstaw obowiązujące przepisy prawa, według których należy kwalifikować przestępstwa popełniane w cyberprzestrzeni.<br><br>Podziel grupę na trzy zespoły.<br>Przygotuj pomieszczenia, elektroniczne urządzenia, oraz nośniki danych, które będą podlegały oględzinom, przeszukaniu oraz zabezpieczeniu, w tym zabezpieczeniu fizycznemu.<br>Wykorzystaj maszyny wirtualne z zainstalowanymi, systemami operacyjnymi.<br><br>Przeprowadź ćwiczenia i następnie dokonaj oceny pracy słuchaczy. |

**TEMAT NR 3: Wstęp do działań operacyjnych w Internecie**

**CELE:** Po zrealizowaniu tematu, słuchacz będzie potrafił:

- omówić możliwości pracy operacyjnej w Internecie oraz jej ograniczenia,
- samodzielnie uzyskiwać, interpretować i analizować dane z otwartych źródeł informacji,
- samodzielnie wykorzystywać narzędzia do zaawansowanego wyszukiwania informacji,
- stworzyć, wykorzystywać, weryfikować i interpretować tożsamość internetową.

| Zagadnienia | Czas realizacji w godz. lekcyjnych | Metoda | Wskazówki do realizacji |
|---|---|---|---|
| 1. Możliwości prowadzenia pracy operacyjnej w Internecie.<br>2. Metody pozyskiwania danych z Internetu przy użyciu ogólnodostępnych baz danych, ustalenia teleinformatyczne i internetowe.<br>3. Zaawansowane metody pozyskiwania informacji z Internetu przy użyciu wyszukiwarek Internetowych.<br>4. Tożsamość internetowa.<br>5. Weryfikacja autentyczności uzyskanych informacji.<br>6. Ustalenia w trybie art.20 i art.20c Ustawy o Policji, oraz procedura przekazywania uzyskanych danych do postępowania karnego. | 12 | wykład, burza mózgów, ćwiczenia | Do wykładu i burzy mózgów wykorzystaj wiedzę uczestników kursu i zaproszonych prelegentów (w szczególności funkcjonariuszy wydziałów dw. z cyberprzestępczością).<br><br>Podczas wykładu przedstaw obowiązujące zasady składania wniosków do operatorów i podmiotów zagranicznych (Facebook, Twitter, Instagram, etc.).<br><br>Do ćwiczeń wykorzystaj dostępne wyszukiwarki Internetowe, strony agregujące informacje o użytkownikach Internetu z otwartych źródeł oraz jak zweryfikować autentyczność uzyskanych danych.<br><br>Przeprowadź ćwiczenia i następnie dokonaj oceny pracy słuchaczy. |

**TEMAT NR 4: Podstawy informatyki śledczej**

**CELE:** Po zrealizowaniu tematu, słuchacz będzie potrafił:

- omówić zasady, charakterystykę, stosowane narzędzia i oprogramowanie,
- ujawnić i zabezpieczyć materiał dowodowy z Internetu,
- ujawnić i zabezpieczyć materiał dowodowy z komputerów,
- ujawnić i zabezpieczyć materiał dowodowy z urządzeń mobilnych oraz wyszukać w materiale dowodowym wskazane zagadnienia.

| Zagadnienia | Czas realizacji w godz. lekcyjnych | Metoda | Wskazówki do realizacji |
|---|---|---|---|
| 1. Wstęp do informatyki śledczej – zasady, charakterystyka, stosowane narzędzia i oprogramowanie.<br><br>2. Ujawnianie i zabezpieczanie materiału dowodowego z Internetu.<br><br>3. Ujawnianie i zabezpieczanie materiału dowodowego pozyskiwanego z komputerów.<br><br>4. Ujawnianie i zabezpieczanie materiału dowodowego z urządzeń mobilnych (tablety, telefony).<br><br>5. Wstępna weryfikacja zawartości materiału dowodowego. | 20 | wykład, ćwiczenia | Przygotuj sprzęt, oprogramowanie i nośniki wykorzystywane do ćwiczeń.<br><br>Wykorzystaj maszyny wirtualne z zainstalowanymi systemami operacyjnymi.<br><br>Przedstaw i zapoznaj słuchaczy z narzędziami i oprogramowaniem, które będą wykorzystane do ćwiczeń.<br><br>Przeprowadź ćwiczenia i następnie dokonaj oceny pracy słuchaczy. |

**TEMAT NR 5: Analiza śledcza w sprawach związanych z cyberprzestępczością**

**CELE:** Po zrealizowaniu tematu, słuchacz będzie potrafił:

- przeprowadzić podstawową ocenę zabezpieczonego materiału dowodowego,
- ujawnić i zabezpieczyć ślady korzystania z kryptowalut,
- ujawnić i zabezpieczyć ślady korzystania z sieci anonimizujących.

| Zagadnienia | Czas realizacji w godz. lekcyjnych | Metoda | Wskazówki do realizacji |
|---|---|---|---|
| 1. Wstępna ocena cyfrowego materiału dowodowego.<br><br>2. Kryptowaluty.<br><br>3. Sieci anonimizujące. | 12 | wykład, ćwiczenia | Przygotuj darmowe oprogramowanie forensics.<br><br>Wykorzystaj portfele do zobrazowania przepływów kryptowalut.<br><br>Wykorzystaj opracowaną metodykę zabezpieczania kryptowalut.<br><br>Skorzystaj z sieci VPN, Tor i Darknetu, ujawnij ślady pozostałe po korzystaniu z ww. rozwiązań.<br><br>Przeprowadź ćwiczenia i następnie dokonaj oceny pracy słuchaczy. |

**TEMAT NR 6: Live Forensics, metody Triage**

**CELE:** Po zrealizowaniu tematu, słuchacz będzie potrafił:

- przeprowadzić sprawdzenie uruchomionego systemu- Live Forensics,
- korzystać z oprogramowania Triage,
- ujawnić oprogramowanie antiforensics.

| Zagadnienia | Czas realizacji w godz. lekcyjnych | Metoda | Wskazówki do realizacji |
|---|---|---|---|
| 1. Zasady, charakterystyka, stosowane narzędzia i oprogramowanie.<br><br>2. Wstępna weryfikacja danych pozyskiwanych w ramach Live Forensics, metod Triage'owych.<br><br>3. Rozpoznawanie oprogramowania antiforensics. | 10 | wykład, ćwiczenia | Przygotuj sprzęt, oprogramowanie i nośniki wykorzystywane do ćwiczeń.<br><br>Wykorzystaj maszyny wirtualne z zainstalowanymi, systemami operacyjnymi.<br><br>Przeprowadź ćwiczenia i następnie dokonaj oceny pracy słuchaczy. |