Społeczna Akademia Nauk
Warszawa

Instytut Bezpieczeństwa
Wydział Nauk o Zarządzaniu i Bezpieczeństwie
2017/2018

Pytania specjalistyczne

/bezpieczeństwo informacji i ochrona danych osobowych/

na kierunku studiów bezpieczeństwo narodowe II ST / egzamin magisterski/

1. Typologia współczesnych zagrożeń bezpieczeństwa narodowego i globalnego.
2. Właściwości służb specjalnych RP w kształtowaniu bezpieczeństwa demokratycznego państwa prawnego.
3. Prawne aspekty ochrony prywatności oraz danych osobowych w świetle unormowań międzynarodowych oraz narodowych.
4. Wskazać organy administracji publicznej właściwe w zakresie bezpieczeństwa i porządku publicznego.
5. Omówić strukturę systemu ochrony informacji niejawnej w świetle narodowych i międzynarodowych unormowań prawnych.
6. Omówić konstytucyjne kompetencje organów władzy wykonawczej w zakresie kształtowania bezpieczeństwa narodowego.
7. Wyjaśnić istotę kluczowych zasad bezpieczeństwa informacji niejawnych, w świetle aktualnych unormowań prawnych RP oraz dokumentów międzynarodowych.
8. Omówić procedurę związaną z uzyskaniem świadectwa bezpieczeństwa przemysłowego.
9. Zaprezentować kompetencje Inspektora Ochrony Danych według nowych unormowań prawnych UE – RODO.
10. Scharakteryzować podstawowe źródła informacji wykorzystywane w pracy operacyjnej służb specjalnych.

11. Omówić podmiotowy i przedmiotowy zakres stosowania ustawy o ochronie danych osobowych.

12. Scharakteryzować zasadnicze kierunki nowelizacji ochrony danych wynikające z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 /ogólnego rozporządzenia o ochronie danych, - „RODO".

13. Wskazać okoliczności, w których należy powołać Administratora Bezpieczeństwa Informacji – ABI, według procedur wynikających z RODO.

14. Scharakteryzować strukturę systemu ochrony informacji niejawnych w jednostce organizacyjnej administracji publicznej.

15. Wskazać i omówić różnice występujące w poszczególnych stopniach bezpieczeństwa przemysłowego.

16. Dokonać klasyfikacji zagrożeń informacji niejawnej przetwarzanej w procedurze bezpieczeństwa przemysłowego.

17. Omówić istotę bezpieczeństwa zasobów informacyjnych w jednostkach organizacyjnych administracji publicznej.

18. Omówić zasady klasyfikacji danych osobowych w myśl aktualnych unormowań prawnych.

19. Wskazać zasadnicze różnice wynikające ze stopni bezpieczeństwa przemysłowego, a także procedur uzyskania określonego świadectwa.

20. Określić rolę Krajowej Władzy Bezpieczeństwa w ochronie informacji niejawnej międzynarodowej.

21. Wskazać i określić kompetencje instytucji odpowiedzialnych za przygotowanie i ochronę obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa.

22. Omówić procedury związane z osiąganiem oraz utrzymaniem wymaganego poziomu bezpieczeństwa osobowego związanego z dostępem do informacji niejawnej.

23. Zaprezentować ścieżki obiegu informacji niejawnej wchodzącej oraz wychodzącej z jednostki organizacyjnej administracji publicznej /system tradycyjny i elektroniczny/.

24. Wskazać organy administracji rządowej odpowiedzialne za kształtowanie bezpieczeństwa w cyberprzestrzeni RP.

25. Omówić podstawy prawne funkcjonowania służb specjalnych, a także kompetencje organów władzy (administracji rządowej) nadzorujących ich działalność.

26. Scharakteryzować podstawowe zasady dotyczące gromadzenie i przetwarzanie danych osobowych w świetle aktualnych unormowań prawnych RP.

27. Jaki rodzaj zagrożeń w cyberprzestrzeni ma istotny wpływ na bezpieczeństwo i porządek publiczny w państwie?

28. Scharakteryzować wymagania dla strefy ochrony informacji niejawnej w jednostce organizacyjnej administracji publicznej przetwarzającej informacje o klauzuli: ŚCIŚLE TAJNE oraz TOP SECRET.

29. Omówić istotę bezpieczeństwa informacyjnego w administracji publicznej.

30. Scharakteryzować procedury ochrony informacji niejawnych w sytuacji nadzwyczajnych zagrożeń w jednostce organizacyjnej lub jej otoczeniu.