



Krajowa Szkoła Administracji Publicznej
im. Prezydenta Rzeczypospolitej Polskiej
Lecha Kaczyńskiego

PROGRAM STUDIUM W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA

Edycja 2020

Moduł:	Blok i temat szkolenia	Wykładowca	Część	Liczba godzin szkoleniowych	Termin
Dzień – 1 (online)					
1	Inauguracja studium, cele i rezultaty Studium	Marcin Dobruk	Organizacyjna	0,5	13.11
2	Jaki jest stan obecny i perspektywy cyfryzacji i cyberbezpieczeństwa Rzeczypospolitej Polskiej?	Jakub Dysarz	Teoretyczna	2	13.11
3	Jak żyć w gąszczu przepisów prawa i standardów związanych z bezpieczeństwem IT?	Jakub Dysarz	Teoretyczna	2	13.11
4	Jak zbudować kulturę bezpieczeństwa i świadomość użytkowników w mojej organizacji?	Jakub Syta	Teoretyczna	1,5	13.11
5	Co to w ogóle jest ryzyko i jak zarządzać ryzykiem bezpieczeństwa IT?	Jakub Syta	Praktyczna	3	13.11

Dzień – 2 (online)					
6	Czy można wskazać najlepsze modele i strategie bezpieczeństwa w zarządzaniu organizacjami?	Sebastian Burgemejster	Teoretyczna	2	17.11
7	Jak wyglądają podstawy budowy skutecznych systemów bezpieczeństwa i tzw. odporności?	Sebastian Burgemejster	Teoretyczna	2	17.11
8	W jaki sposób stworzyć procesy bezpieczeństwa informacji w organizacji?	Radek Kaczorek	Teoretyczna	1,5	17.11
9	Procesy bezpieczeństwa informacji – zapewne nie można wykluczyć, że już są w organizacji, tylko użytkownicy o nich nie wiedzą?	Radek Kaczorek	Praktyczna	3	17.11
Dzień – 3 (online)					
10	W jaki sposób ustanowić system zarządzania incydentami bezpieczeństwa w organizacji?	Tomasz Wodziński	Teoretyczna	2	23.11
11	A jeśli incydent w organizacji się pojawi, to co?	Tomasz Wodziński	Praktyczna	2	23.11
Dzień – 4 (online)					
12	Jakie są najczęściej występujące błędy popełniane przez jednostki administracji publicznej w obszarze bezpieczeństwa IT? Podsumowanie wyników kontroli realizowanych przez Kancelarię Prezesa Rady Ministrów	Małgorzata Sokołowska – zastępca dyrektora Centrum Oceny Administracji KPRM	Teoretyczna	1,5	27.11.
13	Jak wygląda Ramowy program kontroli działania systemów teleinformatycznych?	Michał Golec (KPRM)	Praktyczna	1,5	27.11
14	Dlaczego nie należy się bać kontroli i audytu. Jak współpracować z tymi, którzy nas oceniają?	Marcin Dobruk	Praktyczna	1,5	27.11

Dzień – 5 (online)					
15	W jaki sposób ustanowić procesy odporności i ciągłości działania w jednostce?	Piotr Welenc	Praktyczna	2	2.12
16	Ile może kosztować poczucie bezpieczeństwa, że organizacja jest bezpieczna i zadziała w sytuacjach kryzysowych?	Piotr Welenc	Praktyczna	2	2.12
Dzień – 6 (online)					
17	Jak stworzyć dokumentację procesów i działań w zakresie bezpieczeństwa IT i.... się nie napracować?	Eryk Trybulski	Praktyczna	2	11.12
18	Kiedy można powiedzieć, że dokumentacja procesów i działań bezpieczeństwa jest wystarczająca?	Eryk Trybulski	Praktyczna	2	11.12
Dzień – 7 (online)					
19	Skąd czerpać dobre praktyki w zakresie architektury bezpieczeństwa informacji i bezpieczeństwa technicznego?	Sebastian Burgemejster	Teoretyczna	2	18.12
20	Kompleksowa architektura bezpieczeństwa IT w organizacji, czyli co?	Tomasz Wodziński	Praktyczna	2	18.12
21	Co z tym RODO w IT? Integracja prywatności i RODO w bezpieczeństwie	Piotr Kawczyński	Teoretyczna	2	18.12
22	Co z tym RODO w IT? Integracja prywatności i RODO w bezpieczeństwie	Piotr Kawczyński	Praktyczna	2	18.12
23	Podsumowanie i zakończenie szkolenia	Marcin Dobruk	Organizacyjna	0,5	18.12