



PROGRAM KURSU „ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI”

Obszar kursu	Zagadnienia	Liczba godz.
Podstawy dotyczące Bezpieczeństwa Informacji w Organizacjach	Prawne aspekty związane z bezpieczeństwem informacji; Ochrona informacji w ujęciu kognitywnym; Przykłady kradzieży i wycieku danych z przedsiębiorstw; Świat nie kończy się na „RODO” czyli chrońmy dane osobowe, ale bez uszczerbku dla innych ważnych informacji; Klasyfikacja i podział dokumentów z punktu widzenia stopnia ochrony.	5
Zagrożenia występujące w Bezpieczeństwie Informacji	Zagrożenia przy korzystaniu z Internetu: poczta e-mail, strony www, serwisy społecznościowe; Czy pendrive od znajomego może być niebezpieczny; Etyczny hacking, czyli jak ustrzec naszą organizację przed prawdziwym atakiem; Bezpieczeństwo i zasady stosowania haseł; „Najsłabsze ogniwo” i „podejrzane e-maile” – przykłady ataków socjotechnicznych; Zagrożenia w przypadku niestosowania się do zasad bezpieczeństwa informacji.	5
Bezpieczeństwo Informacji na spotkaniach i przy pracy poza organizacją	Organizacja spotkań biznesowych – zgodnie z zasadami bezpieczeństwa informacji; Podstawy negocjacji - negocjacje biznesowe jako skuteczne narzędzie zdobywania przewagi informacyjnej; Jak pracować poza organizacją – praca zdalna, praca w terenie, aby stosować zasady bezpieczeństwa informacji; Profilowanie kluczowych osób w organizacji celem pozyskania dostępu do informacji.	4
Skuteczność wdrożenia Systemu Bezpieczeństwa Informacji	Polityka i zasady bezpieczeństwa informacji firmy jako skuteczne narzędzie ochrony informacji.	2