

## Spis treści

Autorzy .....	IX
Wykaz skrótów .....	XIII
Wykaz literatury .....	XIX
Wstęp .....	XXXI

### Część I

#### Prawne aspekty ochrony sieci i informacji

Europejska regulacja bezpieczeństwa sieci i systemów informacyjnych a suwerenność państwa ( <i>Grażyna Szpor</i> ) .....	3
Europejskie standardy prawnokarnej ochrony sieci i informacji oraz ich implementacja do ustawodawstwa polskiego ( <i>Andrzej Adamski</i> ) .....	23
Organizacyjno-prawne aspekty implementacji dyrektywy Parlamentu Europejskiego i Rady z 6.7.2016 r. ( <i>Marek Balcerzak, Piotr Durbajło</i> ) .....	47
Podział kompetencji w zapewnianiu cyberbezpieczeństwa ( <i>Piotr Trąbiński</i> ) .....	69
Umowne partnerstwo publiczno-prywatne w kontekście bezpieczeństwa sieci i informacji administracji publicznej ( <i>Małgorzata Ganczar</i> ) .....	83

## Część II

### Cyberataki i cyberterroryzm

Ryzyko – wybrane aspekty w kontekście współczesnych zagrożeń ( <i>Piotr Kolmann</i> ) .....	97
Polityka cyberbezpieczeństwa w świetle zagrożenia cyberterroryzmem ( <i>Marcin Skolimowski</i> ) .....	105
Walka z terroryzmem i cyberterroryzmem a ochrona konstytucyjnych praw i wolności jednostki ( <i>Kamil Stępnia</i> k) .....	119
Co zmieni ustawa antyterrorystyczna? ( <i>Katarzyna Beška</i> ) .....	129
Czy cyberterroryzm jest realnym zagrożeniem? ( <i>Dawid Dulak</i> ) .....	137
Udział instytucji państwowych w cyberatakach na infrastrukturę teleinformatyczną państw Europy Zachodniej i USA ( <i>Piotr Niemczyk</i> ) .....	147
Zagrożenia związane z wojną hybrydową ( <i>Maciej Białek</i> ) .....	157
Post-prawda jako zagrożenie dla podstaw etycznych społeczeństwa informatycznego ( <i>Karol Dobrzaniecki</i> ) .....	175

## Część III

### Metody i techniki zwalczania cyberprzestępczości

Regulacje polityki zwalczania cyberprzestępczości w Polsce i w Unii Europejskiej ( <i>Izabela Wilk</i> ) .....	187
Tworzenie specyfikacji wymagań w postępowaniach publicznych dotyczących bezpieczeństwa informatycznego – wybrane aspekty ( <i>Bolesław Szafranski</i> ) .....	195
Wykorzystanie technologii RFID i GPS do lokalizowania zasobów i osób ( <i>Maciej Kiedrowicz</i> ) .....	205

<b>Przestępstwo phishingu i metody przeciwdziałania</b> ( <i>Kamil Czapllicki</i> ) .....	215
<b>Profilowanie a cyberbezpieczeństwo</b> ( <i>Elżbieta Niezgódka</i> ) .....	229
<b>Kradzież tożsamości w czasach społeczeństwa informacyjnego</b> ( <i>Klara Dygaszewicz</i> ) .....	251
<b>Przeciwdziałanie cyberatakom przez przedsiębiorstwa</b> ( <i>Jowita Sobczak</i> ) .....	259
<b>Dostęp do danych telekomunikacyjnych i internetowych w kontroli operacyjnej</b> ( <i>Małgorzata Olszewska</i> ) .....	269
<b>Część IV</b>	
<b>Stan i perspektywy ochrony infrastruktury informacyjnej</b>	
<b>Nowe zagrożenia bezpieczeństwa rejestrów publicznych</b> ( <i>Agnieszka Gryszczyńska</i> ) .....	293
<b>Dostęp do informacji publicznej a cyberbezpieczeństwo</b> ( <i>Piotr Sitniewski</i> ) .....	311
<b>Pomiędzy wolnym a ograniczonym dostępem do kultury – perspektywa dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego</b> ( <i>Kamil Zeidler</i> ) .....	321
<b>Bitcoin a piramidy finansowe</b> ( <i>Maria Ocalewicz</i> ) .....	339
<b>Wpływ rozporządzenia eIDAS na podniesienie poziomu bezpieczeństwa e-usług</b> ( <i>Piotr Pieńkosz</i> ) .....	351
<b>Indeks rzeczowy .....</b>	363