

Spis treści

Autorzy	V
Wykaz skrótów	XVII
Literatura	XXVII
Wstęp	LIII
Introduction	LXI

Część I. Aktualne zagrożenia i ich przewyżczanie

Rozdział 1. Strategiczne działania Ministra Cyfryzacji w przewyżczaniu cyberzagrożeń	
<i>Krzysztof Gawkowski</i>	3
Rozdział 2. Zagrożenia dla cyberodporności w czasie wojny kognitywnej	
<i>Dominika Kasprowicz</i>	15
Rozdział 3. Formy prawne przeciwdziałania nowym zagrożeniom w samorządzie terytorialnym	
<i>Irena Lipowicz</i>	25
Rozdział 4. Determinanty skutecznej karnoprawnej reakcji na cyberzagrożenia	
<i>Agnieszka Gryszczyńska</i>	39
Rozdział 5. Budowanie organizacji odpornej na cyberzagrożenia	
<i>Jakub Syta</i>	57
Rozdział 6. Cyberodporność łańcucha dostaw	
<i>Krzysztof Zieliński</i>	79

Część II. Ramy regulacyjne cyberodporności

Rozdział 7. Europejskie rozumienie cyberodporności	
<i>Wojciech Rafał Wiewiórowski</i>	95
Rozdział 8. Cyberodporność wspierana przepisami prawa UE: akt o cyberodporności (CRA) i dyrektywa NIS 2	
<i>Krzysztof Silicki</i>	105
Rozdział 9. Cyberodporność podmiotów krytycznych	
<i>Marcin Wysocki</i>	119
Rozdział 10. Zadania CERT Polska związane z identyfikacją i katalogowaniem publicznie ujawnionych podatności	
<i>Michał Dondajewski</i>	137
Rozdział 11. Cyberodporność jako kluczowy filar bezpieczeństwa SOC	
<i>Sebastian Szczerba</i>	147
Rozdział 12. Ramy regulacyjne cyberodporności. Obowiązki podmiotów gospodarczych. Obowiązki producentów w ramach rozporządzenia CRA (Cyber Resilience Act)	
<i>Tomasz Chomicki, Joanna Grubicka</i>	163
Rozdział 13. Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej	
<i>Katarzyna Kupka</i>	183

Część III. Cyberodporność systemów ochrony zdrowia

Rozdział 14. Sektorowy zespół reagowania na incydenty bezpieczeństwa komputerowego w sektorze ochrony zdrowia	
<i>Małgorzata Olszewska</i>	203
Rozdział 15. Interoperacyjność dokumentacji medycznej	
<i>Sebastian Sikorski, Michał Dziobkowski</i>	211
Rozdział 16. Normatywny kontekst cyberodporności w rozwiązaniach e-zdrowia	
<i>Bartłomiej Michalak, Krzysztof Świtata</i>	225

Rozdział 17. Wpływ dyrektywy NIS 2 na technologiczne bezpieczeństwo w placówkach ochrony zdrowia	
<i>Marzenna Miłek</i>	237
Rozdział 18. Świadoma zgoda pacjenta w kontekście wymogów dotyczących systemów AI w środowisku usług i świadczeń medycznych (początek)	
<i>Kamil Strzypek</i>	247
Część IV. Cyberodporność systemów sztucznej inteligencji	
Rozdział 19. Cyberbezpieczeństwo generatywnej sztucznej inteligencji w perspektywie zarządzania ryzykiem	
<i>Jerzy Surma</i>	263
Rozdział 20. Epistemologiczne i operacyjne implikacje podatności modeli językowych na mechanizmy jailbreak: perspektywa bezpieczeństwa adaptacyjnego	
<i>Agata Ślusarek</i>	273
Rozdział 21. Deepfake a odporność systemów wideoweryfikacji tożsamości. Aspekty prawne	
<i>Agnieszka Besiekierska</i>	285
Rozdział 22. Wykorzystanie sztucznej inteligencji do zapewnienia cyberbezpieczeństwa obrotu i zarządzania nieruchomościami	
<i>Mateusz Badowski</i>	293
Rozdział 23. Problemy instytucjonalne polskiego projektu ustawy o systemach sztucznej inteligencji na tle prawnooporównawczym	
<i>Paweł Hajduk</i>	301
Część V. Cyberodporność danych	
Rozdział 24. Współpraca i relacje między organami nadzoru rynku wyznaczanymi mocą aktu o cyberodporności a organami właściwymi ds. ochrony danych osobowych	
<i>Mirostław Wróblewski</i>	321

Rozdział 25. Znaczenie analizy ryzyka i planu reagowania na incydenty w utrzymaniu cyberodporności	
<i>Małgorzata Ganczar</i>	327
Rozdział 26. Proceduralne instrumenty cyberodporności ochrony danych osobowych	
<i>Marlena Sakowska-Baryła</i>	341
Rozdział 27. Cyberodporność aplikacji mObywatel. Czy dane osobowe zawarte w aplikacji mObywatel są bezpieczne?	
<i>Kamil Czapllicki</i>	353
Rozdział 28. Ochrona dzieci i młodzieży w mediach cyfrowych przez edukację – warunek konieczny budowania odporności społecznej	
<i>Konrad Ciesiołkiewicz</i>	361
Rozdział 29. Wybrane aspekty prawnokarne i procesowe postępowań przygotowawczych w sprawach o oszustwo metodą „na wnuczka”	
<i>Adam Białas</i>	373
Rozdział 30. Gra wideo zwiększająca cyberodporność społeczną w zakresie ochrony danych osobowych	
<i>Konrad Radomiński</i>	389
Indeks rzeczowy	403