

# Internet. Cyberodporność

Przejdź do produktu na [ksiegarnia.beck.pl](https://ksiegarnia.beck.pl)

## Spis treści

Autorzy .....	V
Wykaz skrótów .....	XVII
Literatura .....	XXVII
Wstęp .....	LIII
Introduction .....	LXI

### Część I. Aktualne zagrożenia i ich przewyżczenie

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

**Część II. Ramy regulacyjne cyberodporności**

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

**Część III. Cyberodporność systemów ochrony zdrowia**

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

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

## Część V. Cyberodporność danych

<b>Rozdział 24. Współpraca i relacje między organami nadzoru rynku wyznaczanymi mocą aktu o cyberodporności a organami właściwymi ds. ochrony danych osobowych</b>	
<i>Miroslaw Wróblewski</i> .....	321

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

[Przejdź do księgarńi →](#)

[ksiegarnia.beck.pl](https://ksiegarnia.beck.pl)