

Internet. Hacking

Przejdź do produktu na ksiegarnia.beck.pl

Spis treści

Autorzy	XIII
Wstęp	XVII
Introduction	XXI
Wykaz skrótów	XXV
Wykaz literatury i innych źródeł	XXIX

Część I

Cyberbezpieczeństwo, ataki i przeciwdziałanie cyberprzestępczości

Rozdział 1. Contemporary Damocles sword: Cryptographic tools facing anamorphic schemes (<i>Mirostaw Kutylowski</i>)	3
Rozdział 2. Metadane – otwartość danych i świadomość zagrożeń (<i>Bogdan Fischer</i>)	13
Rozdział 3. Krajowy system certyfikacji cyberbezpieczeństwa (<i>Agnieszka Besiekierska</i>)	28
Rozdział 4. Metody zabezpieczeń urządzeń mobilnych (<i>Tomasz Chomicki, Kamil Grondys, Mariusz Rawski</i>)	40
Rozdział 5. Ochrona przed hackingiem w usługach medycznych (<i>Krzysztof Świtala</i>)	49
Rozdział 6. Toolbox 5G: Ocena profilu ryzyka dostawców i ograniczenia dla dostawców uznawanych za dostawców wysokiego ryzyka (<i>Marcin Wysocki</i>)	59

Rozdział 7. Program e-rezydencji a bezpieczeństwo funkcjonowania administracji publicznej w Estonii (<i>Patryk Kuzior</i>)	79
--	----

Część II

Dane osobowe i ich ochrona przed naruszeniami

Rozdział 8. Konstytucyjna wolność i tajemnica komunikowania się oraz prawo do ochrony danych osobowych – wspólny obszar ochrony przed hackingiem (<i>Marlena Sakowska-Baryła</i>)	99
Rozdział 9. Uprawnienia osób fizycznych przysługujące w związku z przetwarzaniem ich danych osobowych w monitoringu wizyjnym (<i>Anna Zubrycka</i>)	111
Rozdział 10. Standards for using biometric data based on facial recognition, following the case-law of the European Court of Human Rights (<i>Marek Świerczyński</i>)	122
Rozdział 11. Problematyka ochrony danych osobowych w sektorze energetyki (liczniki zdalnego odczytu). Aspekty prawne (<i>Mariusz Szyrski</i>)	128
Rozdział 12. Certyfikacja w zakresie ochrony danych osobowych (<i>Piotr Drobek</i>)	137
Rozdział 13. Systemy DLP a ochrona danych osobowych – zasada (<i>Mateusz Jakubik, Karol Witas</i>)	161
Rozdział 14. Inspirations from EU financial law for privacy protection by information obligations in Active and Assisted Living technologies (<i>Maksymilian Kuźmicz</i>)	172

Część III

Sztuczna inteligencja i tożsamość cyfrowa

Rozdział 15. Przepięczone i złośliwe wykorzystywanie sztucznej inteligencji (<i>Jerzy Cytoński</i>)	197
---	-----

Rozdział 16. Wykorzystanie sztucznej inteligencji w cyberatakach (<i>Agnieszka Gryszczyńska</i>)	211
Rozdział 17. Zapobieganie atakom adwersarskim na medyczną AI z perspektywy prawnej (<i>Jarosław Greser</i>)	221
Rozdział 18. Digital content manipulation techniques using artificial intelligence algorithms (<i>Rafał Kasprzyk</i>)	234
Rozdział 19. Elektroniczna tożsamość cyfrowa – ochrona czy zagrożenie dla tożsamości? (<i>Kamil Czaplicki</i>)	249
Rozdział 20. Tożsamość cyfrowa w Niemczech (<i>Mateusz Badoński</i>)	260
Rozdział 21. Hackowanie ludzi (<i>Gabriela Tokarska</i>)	268

Część IV

Wzmacnianie kompetencji cyfrowych i cyberhigieny

Rozdział 22. Zagrożenia związane z przetwarzaniem danych osobowych w szkole wyższej (<i>Beata Zbarachewicz</i>)	283
Rozdział 23. Edukacyjne gry wideo w kształtowaniu cyberhigieny dzieci (<i>Konrad Stefan Radomiński</i>)	296
Rozdział 24. Wykorzystanie infografiki w kształtowaniu cyberhigieny wśród użytkowników przestrzeni cyfrowej (<i>Wawrzyniec Święcicki</i>)	317
Rozdział 25. Model podnoszenia kompetencji cyfrowych (<i>Grażyna Szpor</i>)	325
Indeks rzeczowy	337

[Przejdź do księgarni →](#)



ksiegarnia.beck.pl