

---

# Spis treści

---

Wstęp .....	9
-------------	---

## Rozdział 1

### Bezpieczeństwo funkcjonowania jednostki w sieci

– Sylwia Wojciechowska-Filipek .....	13
1.1. Społeczeństwo funkcjonujące w sieci .....	13
1.1.1. Cechy społeczeństwa informacyjnego .....	14
1.1.2. Wskaźniki rozwoju społeczeństwa informacyjnego .....	19
1.1.3. Media społecznościowe jako nowoczesna platforma komunikacji .....	28
1.1.4. Wykluczenie cyfrowe ( <i>digital divide</i> ) jako wykluczenie ze społeczeństwa ....	31
1.2. Zagrożenia związane z funkcjonowaniem w sieci .....	35
1.2.1. Zagrożenia psychospołeczne .....	36
1.2.1.1. Przeciążenie technologią i siecią .....	36
1.2.1.2. Uzależnienie od Internetu .....	40
1.2.2. Ryzyko prywatności .....	44
1.2.2.1. Nadużycia w celach komercyjnych .....	46
1.2.2.2. Naruszenie prywatności wynikające z działań niekomercyjnych ....	49
1.2.3. Ryzyko związane z przeprowadzaniem transakcji w sieci .....	52
1.2.4. Zagrożenia wynikające z działań przestępczych .....	56
1.3. Sposoby zapewnienia bezpieczeństwa w sieci .....	61
1.3.1. Ochrona przed zagrożeniami psychospołecznymi .....	61
1.3.1.1. Profilaktyka .....	61
1.3.1.2. Ochrona prawna .....	66
1.3.2. Ochrona prywatności w cyberprzestrzeni .....	69
1.3.2.1. Zapewnienie prywatności przez usługodawcę .....	69
1.3.2.2. Prawne sposoby ochrony prywatności .....	72
1.3.2.3. Informatyczne sposoby ochrony prywatności .....	75
1.3.3. Zapewnienie bezpieczeństwa transakcjom w sieci .....	77
1.3.3.1. Ochrona logistycznej obsługi sprzedaży .....	78
1.3.3.2. Zabezpieczenia rozliczeń transakcji .....	82

## Rozdział 2

### Bezpieczeństwo funkcjonowania organizacji w sieci

– Sylwia Wojciechowska-Filipek .....	91
2.1. Wirtualizacja działalności organizacji .....	92
2.1.1. Definicja i cechy organizacji wirtualnej .....	95
2.1.2. Korzyści z wirtualizacji działalności .....	98
2.1.3. Typologia e-organizacji .....	102
2.1.3.1. E-administracja .....	102
2.1.3.2. E-biznes .....	107
2.1.3.3. E-handel .....	111
2.1.3.4. E-bankowość .....	118
2.1.3.5. E-zdrowie .....	129
2.1.3.6. E-edukacja .....	133
2.2. Ryzyko funkcjonowania organizacji w sieci .....	137
2.2.1. Zagrożenia informacji i systemów informacyjnych .....	138
2.2.2. Ryzyko wirtualnej współpracy .....	144
2.2.3. Ryzyko prawne .....	149
2.3. Zabezpieczenia działania organizacji w cyberprzestrzeni .....	155
2.3.1. Nietechniczne środki ochrony .....	156
2.3.1.1. Polityka bezpieczeństwa i zarządzanie ryzykiem .....	156
2.3.1.2. Podnoszenie jakości usług jako ochrona przed ryzykiem funkcjonowania w sieci .....	162
2.3.1.3. Prawne środki ochrony .....	167
2.3.2. Techniczne środki ochrony .....	172
2.3.2.1. Urządzenia techniczne .....	173
2.3.2.2. Środki programowe .....	176
2.3.2.3. Środki kontroli dostępu .....	178
2.3.2.4. Środki kryptograficzne .....	181
2.3.2.5. Protokoły .....	184

## Rozdział 3

### Bezpieczeństwo państwa w cyberprzestrzeni – Zbigniew Ciekanski .....

3.1. Państwo a współczesne technologie informatyczne .....	187
3.1.1. E-społeczeństwo .....	189
3.1.2. Wymagania sieci teleinformatycznych .....	191
3.1.3. Ochrona danych osobowych i informacji niejawnych .....	194
3.1.4. Podział informacji .....	197
3.1.5. Dostęp do informacji .....	200
3.2. Zagrożenia w cyberprzestrzeni .....	203

3.2.1. Cyberprzestępczość .....	203
3.2.2. Cyberterroryzm.....	205
3.2.3. Zagrożenia związane z Internetem .....	207
3.2.4. Zagrożenia bezprzewodowe .....	209
3.2.5. Szpiegostwo komputerowe.....	210
3.2.6. Cyberwojny jako nowoczesny sposób walki.....	211
3.2.7. Zagrożenia dla instytucji państwowych .....	216
3.3. Zapewnienie bezpieczeństwa w cyberprzestrzeni .....	218
3.3.1. Ocena bezpieczeństwa systemów teleinformatycznych.....	218
3.3.2. Cyberterroryzm w prawodawstwie międzynarodowym .....	222
3.3.3. Cyberprzestępczość – uwarunkowania prawne.....	223
3.3.4. Strategia Bezpieczeństwa Polski .....	225
3.3.5. Międzynarodowa współpraca przy zwalczaniu cyberterroryzmu.....	228
3.3.6. Uwarunkowania budowania bezpieczeństwa w cyberprzestrzeni .....	232
3.3.7. Europejskie organizacje w walce z cyberprzestępczością.....	236
3.3.8. Ochrona cyberprzestrzeni w Polsce .....	237
3.3.9. Wyspecjalizowane instytucje zajmujące się ochroną cyberprzestrzeni.....	239
3.3.10. Zadania policji w walce z cyberprzestępczością.....	241
3.3.11. Systemy osobowego i kryptograficznego zabezpieczenia infrastruktury teleinformatycznej.....	244
<b>Podsumowanie.....</b>	<b>257</b>
<b>Bibliografia .....</b>	<b>261</b>
Pozycje zwarte .....	261
Artykuły.....	266
Źródła prawa .....	272
Netografia .....	273