OBSAH

1 POJEM KYBERNETICKÉ BEZPEČNOSTI V ČESKÉM PRÁVU 9
1.1 Metodologie práva kybernetické bezpečnosti 9
1.2 Základy legislativního řešení kybernetické bezpečnosti 12
1.3 Principy české a evropské právní úpravy kybernetické bezpečnosti 17

2 INSTITUTY ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI 27
2.1 Bezpečnostní opatření 28
2.2 Protiopatření 30
2.3 Odpovědnost za nedbalost a prevenční povinnosti 33
2.4 Disciplinární odpovědnost a disciplinární povinnosti 36

3 INDIVIDUÁLNÍ ODPOVĚDNOST ZA KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT 41
3.1 Kybernetická bezpečnost jako agenda výkonné moci 41
3.2 Individuální odpovědnost a ochrana prostředí 42
3.3 Postih nezodpovědného uživatele 45
3.4 Postih příliš aktivního operátora 48
3.5 Interní instrukce jako bezpečnostní opatření 51
3.6 Nevhodný obsah interních bezpečnostních instrukcí 52
3.7 Zákonná konformita interní instrukce 56
3.8 Srozumitelnost interní instrukce a bezpečnost z podstaty 58
3.9 Interní instrukce a problém soukromí na pracovišti 60

4 PERSPEKTIVY DALŠÍHO VÝVOJE ČESKÉHO PRÁVA KYBERNETICKÉ BEZPEČNOSTI 65
4.1 Zákonná typologie uživatelů vybraných systémů a sítí 66
4.2 Omezená odpovědnost běžných uživatelů 68
4.3 Specifická úprava outsourcingu 70
4.4 Další vývojové perspektivy práva kybernetické bezpečnosti 72

5 PERSPEKTIVY DALŠÍHO POLITICKÉHO A ORGANIZAČNÍHO VÝVOJE AGENDY KYBERNETICKÉ BEZPEČNOSTI V ČR 75
5.1 Certifikace a compliance check 75
5.2 Aktivní obrana – best practices 82
5.3 Kybernetická bezpečnost jako agenda podpory investic 84
5.4 Kybernetická bezpečnost jako agenda rozvojové pomoci 86

6 MECHANISMY ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI 89
6.1 Spolupráce na národní úrovni 90
6.2 Spolupráce na mezinárodní úrovni 93

7 POVINNOSTI SPRÁVCŮ INFRASTRUKTUR 95
7.1 Skupiny povinných osob dle ZoKB 95
7.2 Povinnosti povinných osob dle ZoKB 99
7.3 Nové povinné osoby a jejich povinnosti v ZoKB podle směrnice NIS 102
7.4 Povinnosti vyplývající s ostatních právních předpisů 106

8 SDÍLENÍ INFORMACÍ V KYBERNETICKÉ BEZPEČNOSTI 109
8.1 Sběr informací pomocí analýzy datového provozu 109
8.2 Dobrovolné sdílení informací v kybernetické bezpečnosti 117
8.3 Exkurs – srovnání přístupu v ZoKB s úpravou sdílení informaci v USA 120

9 SPOLUPRÁCE BEZPEČNOSTNÍCH SLOŽEK 125
9.1 Orgány činné v trestním řízení 125
9.2 Zpravodajské služby 136
9.3 Kybernetická obrana 138

10 VYMEZENÍ ZÁJMU STÁTU V KYBERPROSTORU 141
10.1 Kybernetická a informační suverenita 141
10.2 Česká republika: hodnotové zakotvení 151

11 KYBERNETICKÁ VÁLKA A POUŽITÍ SÍLY 161
11.1 Clausewitz a „kybernetická válka“ 161
11.2 Kybernetická operace jako použití síly 168

12 TECHNOLOGICKÁ VÝZVA HUMANITÁRNÍMU PRÁVU .. 179
12.1 Martensova klauzule 179
12.2 Rozlišování při použití kybernetických prostředků 187

Summary 201
Literatura a další použité zdroje 203