

OBSAH

Souhrn.....	5
Summary.....	6
1. Definování užitých pojmů.....	7
2. Kybernetická versus informační bezpečnost.....	11
2.1. Formulace problému	11
2.2. Bezpečnost	11
2.3. Informační bezpečnost	16
2.4. Bezpečnost informačních a komunikačních technologií	18
2.5. Kybernetická bezpečnost	19
2.6. Širší souvislosti kybernetické bezpečnosti.....	21
2.1. Bezpečnost v ČR.....	23
2.2. Kybernetická bezpečnost v ČR	25
3. Bezpečností hrozby ČR.....	27
3.1. Stávající stav	27
3.2. Terorismus a extremismus jako bezpečnostní hrozba ČR	28
3.2.1. Terorismus.....	28
3.2.2. Extremismus.....	29
3.2.3. Vztah mezi terorismem a extremismem.....	30
3.2.4. Vybrané současné metody výzkumu v oblasti terorismu.....	30
3.2.5. Terorismus a extremismus v ČR	31
3.3. Kybernetický prostor jako možné místo útoku	32
4. Kritická infrastruktura.....	36
4.1. Formulace problému	36
4.2. Petri sítě.....	36
4.2.1. Popis Petriho sítě.....	36
4.2.2. Place/Transition Petri sítě.....	37
4.2.3. Stochastické Petri sítě.....	39
4.3. Neurčitost.....	40
4.4. Informační entropie.....	40
4.5. Spravedlivost.....	41
4.6. Model elektrárenské sítě ČR	42
4.7. Výsledky simulace	44
5. Modelové chování útočníka	49
5.1. Systémové myšlení a systémová dynamika	49
5.1.1. Předpoklady sestavení dynamického modelu	50
5.1.2. Příčinné smyčkové diagramy	51
5.1.3. Diagram hladin a toků	54

5.2.	Dynamický model chování útočníka na kritickou infrastrukturu	55
5.2.1.	Model 1 – Změna hodnoty KI v závislosti na změně míry zranitelnosti	56
5.2.2.	Model 2 – Změna hodnoty KI v závislosti na změně množství útoků	59
5.2.3.	Model 3 – Míra zranitelnosti, jako endogenní veličina.....	62
5.3.	Hodnocení simulací.....	66
6.	Závěr.....	67
	Použitá literatura	68
	Seznam tabulek.....	75
	Seznam obrázků.....	76
	Rejstřík.....	78
	Přílohy.....	80