

OBSAH

1 ÚVOD	5
1.1 Automatizační systém	6
1.2 Bezpečnost	7
1.2.1 Komunikační bezpečnost	8
2 ŘEŠENÍ ZABEZPEČENÍ AUTOMATIZAČNÍCH SÍTÍ	9
2.1 Analýza bezpečnostních hrozeb	9
2.1.1 Zaměření bezpečnostních hrozeb	9
2.1.2 Hodnocení bezpečnostních hrozeb	10
2.2 Bezpečnostní zařízení pro automatizační sítě	11
2.2.1 Filtr datových zpráv	11
2.2.2 Systém detekce a prevence neoprávněného vniknutí	12
2.2.3 Způsoby detekce útoků	12
2.2.4 Architektura systému detekce a prevence neoprávněného vniknutí	13
2.2.5 Definice IDMEF zpráv použitých pro IDS	14
3 REALIZACE	15
3.1 Systém detekce neoprávněného vniknutí	15
3.1.1 Implementace správce bezpečnostních událostí	17
3.2 Filtr datových zpráv	20
3.2.1 Architektura programového vybavení filtru	21
3.2.2 Řídící program filtru datových zpráv	22
3.3 Konfigurační seznamy příkazů filtru datových zpráv	23
3.3.1 Komunikační modul filtru datových zpráv	23
3.4 Ověření funkčnosti filtru datových zpráv	24
4 ZÁVĚR	26
5 REFERENCE	27
6 PŘÍLOHY	30