22220 Выявление инцидентов ИБ при помощи СОВ

Введение 2

1 Анализ систем обнаружения и предотвращения вторжений 4

1.1 Анализ систем обнаружения вторжений (IDS) 4

1.2 Анализ систем предотвращения вторжений 5

1.3 Анализ существующей классификации СОВ 9

1.4 Анализ методов обнаружения вторжений 14

1.5 Анализ системы сетевого обнаружения вторжений 17

1.6 Сравнение систем обнаружения вторжений 18

2 Методика настройки snort 20

2.1 Общие требования к функционированию системы обнаружения вторжений 20

2.2 Руководство по настройке СОВ snort 26

2.2.1 Предварительная настройка виртуальных машин 26

2.2.2 Установка и настройка СОВ Snort 30

2.2.3 Установка Barnyard2 37

2.2.4 Установка PulledPork 42

2.2.5 Установка web-интерфейса 44

3 Разработка правил snort для мониторинга и выявления инцидентов ИБ 48

3.1 Создание правил для СОВ snort 49

3.2 Правила выявления инцидентов 56

Заключение 66

ПРИЛОЖЕНИЕ А 67