

242467 Интеграция SIEM-решения в комплексную систему управления информационной безопасности предприятия

ВВЕДЕНИЕ	3
1 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ	5
1.1 Характеристика объекта исследования	5
1.2 Обоснование необходимости внедрения SIEM	11
1.3 SIEM-системы	15
1.3.1 Решаемые задачи и принципы работы	15
1.3.2 Модели SIEM-систем	26
1.4 Сравнение SIEM систем	30
2 ВНЕДРЕНИЕ SIEM СИСТЕМЫ	40
2.1 Установка программного обеспечения MaxPatrol	40
2.2 Настройка правил SIEM-системы	47
ЗАКЛЮЧЕНИЕ	50
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ	51
ПРИЛОЖЕНИЯ	55