232500 Повышение уровня информационной безопасности компании с помощью внедрения SIEM системы MaxPatrol

Введение 3

1 Аналитическая часть 5

1.1 Технико-экономическая характеристика предметной области и предприятия (Установление границ рассмотрения) 5

1.1.1 Общая характеристика предметной области 5

1.1.2 Организационно-функциональная структура предприятия 6

1.2 Анализ рисков информационной безопасности 10

1.2.1 Идентификация и оценка информационных активов 10

1.2.2 Оценка уязвимостей активов 16

1.2.3 Оценка угроз активам 22

1.2.4 Оценка существующих и планируемых средств защиты 28

1.2.5 Оценка рисков 36

1.3 Характеристика комплекса задач, задачи и обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации на предприятии 45

1.3.1 Выбор комплекса задач обеспечения информационной безопасности 45

1.3.2 Определение места проектируемого комплекса задач в комплексе задач предприятия, детализация задач информационной безопасности и защиты информации 49

1.4 Инциденты информационной безопасности 53

1.5 SIEM-системы 58
1.5.1 Решаемые задачи и принципы работы 58
1.5.2 Модели SIEM-систем 69
2 Обзор и выбор SIEM системы 74
2.1 Критерии сравнительного анализа SIEM на российском рынке 74
2.2 Программный комплекс HPE ArcSight 75
2.3 Программный комплекс Ankey SIEM 77
2.4 Программный комплекс NeuroDAT SIEM 79
2.5 Программный комплекс RuSIEM 80
2.6 Программный комплекс КОМРАД 81
2.7 Программный комплекс SearchInform SIEM 84
2.8 Программный комплекс MaxPatrol SIEM 90
2.9 Программный комплекс WAZUH 93
2.10 Kaspersky Unified Monitoring and Analysis Platform 96
2.11 Сравнение SIEM систем 97
3 Внедрение выбранной SIEM системы в компании и оценка экономической эффективности 103
3.1 Техническое задание на внедрение выбранной SIEM-системы 103
3.2 Порядок внедрения выбранной системы в информационную систему компании 109
3.3 Выбор и обоснование методики расчёта экономической эффективности 116
3.4 Расчёт показателей экономической эффективности проекта 118

Заключение 124

Список использованных источников 126