

242447 Повышение уровня информационной безопасности в банке за счет внедрения SIEM системы

Введение	23
1 Аналитическая часть	25
1.1 Анализ рисков информационной безопасности и обоснование необходимости совершенствования системы защиты информации	25
1.2 Инциденты информационной безопасности и SIEM системы	34
1.2.1 Инциденты информационной безопасности	34
1.2.2 SIEM-системы	39
2 Обзор и выбор SIEM системы	54
2.1 Техничко-экономическая характеристика предметной области и предприятия	54
2.2 Критерии сравнительного анализа SIEM на российском рынке	59
2.2.1 Программный комплекс HPE ArcSight	61
2.2.2 Программный комплекс Ankey SIEM	63
2.2.3 Программный комплекс NeuroDAT SIEM	65
2.2.4 Программный комплекс RuSIEM	66
2.2.5 Программный комплекс КОМПАД	67
2.2.6 Программный комплекс SearchInform SIEM	70
2.2.7 Программный комплекс MaxPatrol SIEM	76
2.2.8 Программный комплекс WAZUH	79
2.2.9 Kaspersky Unified Monitoring and Analysis Platform	82
2.3 Сравнение SIEM систем	83

3	Внедрение выбранной SIEM системы в компании и оценка экономической эффективности	94
3.1	Техническое задание на внедрение выбранной SIEM-системы	94
3.2	Порядок внедрения выбранной системы в информационную систему компании	100
3.3	Оценка экономической эффективности выбранных средств защиты информации	107
3.4	Выбор методики расчёта экономической эффективности и расчет показателей	117
	Заключение	125
	Список использованных источников	128