



72024 Сравнительный анализ современных подходов к выявлению инцидентов ИБ в организации

ВВЕДЕНИЕ	2
1 ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ	5
1.1 Основные угрозы информационной безопасности некредитных финансовых организаций	5
1.2 Требования законодательства по обеспечению информационной безопасности некредитных финансовых организаций	13
2 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МЕНЕДЖМЕНТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	20
2.1 Инциденты информационной безопасности	20
2.2 Методики выявления инцидентов ИБ	25
2.2.1 Модели качественного и количественного анализа угроз и рисков информационной безопасности финансово-кредитных учреждений по методике Домарева	25
2.2.2 Модели качественного и количественного анализа угроз и рисков информационной безопасности систем ДБО по методике OSTATE	26
2.2.3 Риск-модель SRAMM	27
3 СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К ВЫЯВЛЕНИЮ ИНЦИДЕНТОВ ИБ	28
3.1.1 Метод анализа иерархий	28
3.1.2 Метод предельного ущерба	32





3.1.3	Метод CAESAR	35
3.2	Обоснование полученных результатов исследования	40
4	ЗАКЛЮЧИТЕЛЬНАЯ РЕКОМЕНДАТЕЛЬНАЯ ГЛАВА	49
4.1	Выбор методики качественного и количественного выявления инцидентов ИБ	49
4.2	Структура SIEM-системы	59
4.3	Анализ рынка SIEM-систем	61
4.4	Выбор siem-системы для применения в организации	64
	ЗАКЛЮЧЕНИЕ	70
	Список использованной литературы	72

