



## **10884 Автоматизация процесса выявления инцидентов информационной безопасности в коммерческом банке на основе SIEM-системы**

Оглавление	
Список сокращений	2
Введение	3
1 Теоретическая часть	5
1.1 Инциденты информационной безопасности	5
1.2 Описание системы информационной безопасности банка	12
1.3 Анализ информационных угроз и обоснование необходимости применения SIEM-систем	18
2 Аналитическая часть	23
2.1 SIEM-системы	23
2.1.1 Решаемые задачи и принципы работы	23
2.1.2 Модели SIEM-систем	33
2.2 Выбор средств обеспечения информационной безопасности банка	37
2.2.1 Анализ рынка SIEM-систем	37
2.2.2 Выбор siem-системы для применения в банке	40
2.2.3 Структура выбранной siem-системы	47
3 Практическая часть	53
3.1 Техническое задание на внедрение выбранной SIEM-системы	53
3.2 Порядок внедрения выбранной системы в информационную систему банка	58
3.3 Оценка экономической эффективности применения выбранных средств защиты информации	66



**План дипломной работы**  
Полная версия работы доступна на сайте <http://diplom-it.ru/>  
ICQ 644867081 Skype diplom-it.ru E-mail admin@diplom-it.ru

Заключение 70

Список использованных источников 72