



## 72021 Обеспечение защиты информации компании при попытке её захвата рейдерами

ВВЕДЕНИЕ	2
1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	4
1.1 Инциденты информационной безопасности	4
1.2 Методики выявления инцидентов ИБ	7
1.2.1 Модели качественного и количественного анализа угроз и рисков информационной безопасности по методике Домарева	7
1.2.2 Модели качественного и количественного анализа угроз и рисков информационной безопасности по методике OCTAVE	8
1.2.3 Риск-модель CRAMM	9
1.3 Основные особенности рейдерского захвата как угрозы информационной безопасности компании	10
2 ИССЛЕДОВАНИЕ СОСТОЯНИЯ СИСТЕМЫ ЗАЩИТЫ КОМПАНИИ	17
2.1 Характеристика компании	17
2.2 Обоснование необходимости применения средств защиты информации	22
3 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ОЦЕНКА ЕЕ ЭФФЕКТИВНОСТИ	41
3.1 Выделение информационных потоков компании и существующих рисков	41
3.2 Основные положения политики безопасности	49





3.3 Модернизация информационной системы компании с помощью  
выбранных средств защиты информации 57

3.4 Оценка эффективности проведенной модернизации по защите  
корпоративной информации в сети предприятия 65

ЗАКЛЮЧЕНИЕ 72

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 74

