



20069 Организация безопасного обмена данными центрального офиса компании-поставщика ИТ-решений с филиалами

Введение 5

1 Аналитическая часть 7

1.1 Технико-экономическая характеристика предметной области и предприятия (Установление границ рассмотрения) 7

1.1.1 Общая характеристика предметной области 7

1.1.2 Организационно-функциональная структура предприятия 9

1.2 Анализ рисков информационной безопасности 14

1.2.1 Идентификация и оценка информационных активов 14

1.2.2 Оценка уязвимостей активов 22

1.2.3 Оценка угроз активам 28

1.2.4 Оценка существующих и планируемых средств защиты 34

1.2.5 Оценка рисков 43

1.3 Характеристика комплекса задач, задачи и обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации на предприятии 49

1.3.1 Выбор комплекса задач обеспечения информационной безопасности 49

1.3.2 Определение места проектируемого комплекса задач в комплексе задач предприятия, детализация задач информационной безопасности и защиты информации 51

1.4 Выбор защитных мер 54

1.4.1 Выбор организационных мер 54

1.4.2 Выбор инженерно-технических мер 62

2 Проектная часть 72





2.1	Комплекс организационных мер обеспечения информационной безопасности и защиты информации предприятия	72
2.1.1	Отечественная и международная нормативно-правовая основа создания системы обеспечения информационной безопасности и защиты информации предприятия	72
2.1.2	Организационно-административная основа создания системы обеспечения информационной безопасности и защиты информации предприятия	75
2.2	Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности и защиты информации предприятия	83
2.2.1	Структура программно-аппаратного комплекса информационной безопасности и защиты информации предприятия	83
2.2.2	Контрольный пример реализации проекта и его описание	92
3	Обоснование экономической эффективности проекта	102
3.1	Выбор и обоснование методики расчёта экономической эффективности	102
3.2	Расчёт показателей экономической эффективности проекта	103
	Заключение	109
	Список использованной литературы	112
	Приложение 1. Политика использования VPN	115

