

Оглавление

Введение	9
1. Анализ автоматизированных банковских систем как объекта реализации угроз с использованием скрытых каналов	13
1.1. Описательная модель автоматизированной банковской системы	13
1.2. Понятие и классификация атак с использованием скрытых каналов, реализуемых в автоматизированных банковских системах	16
1.3. Анализ и классификация моделей скрытых каналов	20
1.4. Модель злоумышленника, реализующего атаки с использованием скрытых каналов	40
1.5. Постановка задач исследования	42
2. Разработка моделей реализации атак с использованием скрытых каналов в автоматизированной банковской системе	44
2.1. Обобщенная модель реализации атак с использованием скрытых каналов в автоматизированной банковской системе	44
2.2. Разработка модели организации скрытых каналов с использованием заголовка протокола TCP/IP	51
2.3. Разработка модели организации скрытых каналов с использованием протокола DNS	54
2.4. Разработка модели организации скрытых каналов поверх ICMP	55
2.5. Разработка модели организации скрытых каналов в протоколе HTTP	57
2.6. Разработка модели организации скрытых каналов по времени	59
2.7. Разработка модели возможности существования скрытого канала в автоматизированной банковской системе	61
2.8. Основные выводы по главе	70
3. Анализ политик информационной безопасности коммерческих банков	73
3.1. Сравнительный анализ политик информационной безопасности коммерческих банков	73
3.2. Рекомендации по совершенствованию политики безопасности	73
Заключение	74