



Пособие предназначено для руководителей органов власти и предприятий, а также специалистов ИТ-подразделений и подразделений по технической защите информации, отвечающих за надлежащую организацию безопасных Cloud Computing (облачных вычислений) в рамках реализации отечественной государственной программы «Информационное общество (2011–2020)».

В пособии рассмотрены требования к организации доверенной среды облачных вычислений федеральных государственных и коммерческих центров обработки данных. Проведен критический анализ известных и новых методов анализа и синтеза требуемой безопасной среды облачных вычислений. Даны необходимые методические рекомендации по организации доверенной среды облачных вычислений критически важных объектов Российской Федерации.

Введение

Глава 1. Актуальность проблемы

1.1. Инфраструктурные модели операторов персональных данных

- Направления развития операторов связи и контент-провайдеров
- Динамика и инфраструктура проекта «Электронное правительство»

1.2. Доверенная среда облачных вычислений

- Цикл развития облачных технологий, три основные модели облачных служб
- Классификация типовых атак на облачные вычислители
- Модель организации доверенной облачной среды
- Схема организации совместного функционирования доверенных и недоверенных компонентов в составе АПП
- Каноническая схема организации защищенной обработки данных

1.3. Модели перспективных облачных CERT/CSIRT

- Состояние вопроса, карта CERT/CIRT Европы, «облачные» перспективы CERT/CSIRT
- Эскизный проект центра CSIRT АПСИБ и основные шаги его построения
- Исследовательская группа 17 и ее основные направления деятельности
- Рекомендации ITU-T серии X.800-X.849

1.4. Безопасные сетевые технологии нового поколения

- Технология программно-конфигурируемых или определяемых сетей
- Особенности реализации SDN
- Характеристика проекта «Центр прикладных исследований компьютерных сетей»

Глава 2. Методы анализа

2.1. Оценивание требований к защищенности информации от несанкционированного доступа в автоматизированных системах

- Требования по технической защите информации и физической защите технических средств сети, оценка достаточности требований
- Пример шкал качественных и количественных оценок
- Примерный перечень показателей защищенности сетевого трафика

2.2. Модель угроз удаленной идентификации программного обеспечения при сканировании компьютерных сетей

- Пассивные и активные методы сбора информации о сети
- Пример использования NMap для решения задач определения версии удаленной ОС
- Клиент-серверный прокол SMB, его формат и схема работы

2.3. Модель угроз информационной безопасности мобильных персональных устройств

- Анализ защищенности операционных систем мобильных персональных устройств
- Типы атак на МПУ
- Схема реализации уязвимостей на объекте, модель воздействия на объект
- Схема взаимодействия клиент-серверной модели безопасности мобильного устройства

2.4. Механизмы реализации типовых атак на компоненты беспроводных сетей передачи данных

- Вероятные сценарии атак на БСПД
- Уязвимые стадии информационного обмена в БСПД с использованием протокола SRP

2.5. Модель угроз безопасности беспроводных сетей передачи данных IEEE 802.11, 802.16

- Типы и условия реализации угроз в БСПД на сигнальном уровне, при пассивном и активном мониторинге трафика, при реализации НСД и др.

Глава 3. Методы синтеза

3.1. Организация защиты информации в гетерогенных вычислительных сетях

- Уровни работы распределенной неоднородной вычислительной сети
- Особенности построения защиты. Межсетевые экраны – требования и схемы применения

3.2. Нейтрализация скрытых угроз и атак в АС электронного документооборота

- Анализ скрытых угроз и атак
- Технологический процесс разработки и архитектурные особенности специального программно-аппаратного комплекса защиты информации
- Защита электронного документооборота (схемы использования и формирования ключей)

3.3. Метод организации защищенного электронного документооборота с использованием коллективной подписи

- Сравнительный анализ систем защищенного электронного документооборота
- Применение эллиптических кривых в системах электронной цифровой подписи

3.4. Подход к защите информации в мобильных персональных устройствах на основе клеточных автоматов

- Криптосистемы на клеточных автоматах.
- Алгебра клеточных автоматов

3.5. Метод контролируемого многомодельного доступа к среде передачи беспроводных сетей

- Основные методы (группы методов) доступа к среде передачи в БСПД IEEE 802.11, 802.16

Глава 4. Специальные методы

4.1. Выявление уязвимостей RSA-подобных криптосистем

- Закон распределения делителей натурального нечетного числа. Модель числа
- Закон распределения делителей (ЗРД) составных нечетных натуральных чисел
- Каноническая форма закона распределения делителей составных чисел

4.2. Атака на модуль RSA-шифра

4.3. Альтернативные режимы шифрования данных в системах электронного документооборота

- Базовые режимы блочного шифрования
- Альтернативные режимы шифрования

4.4. Угрозы информационно-психофизиологической безопасности пользователей АС

- Возможные каналы доставки скрытых вредоносных информационных вложений
- Основные типы информационно-психофизиологических воздействий
- Взаимосвязь реализации и проявлений вредоносных информационных воздействий в мультимедийных файлах

4.5. Построение модели коммуникации для решения задач защиты от негативного информационного воздействия

- Модель Шэннона – Уивера
- Модель де Флера
- Циркулярная модель Осгуда – Шрамма
- Модель коммуникационного процесса Дж. Гербнера
- Модель Уэстли – Маклейна
- Модель Г. Малецке

4.6. Многоуровневая система защиты пользователей от негативного интернет-контента

- Обеспечение защиты психики пользователей от потенциально опасных материалов (меры законодательного характера, а также программно-технические методы)
- Обобщенная схема системы защиты пользователей от скрытого вредоносного воздействия мультимедийного контента сети Интернет
- Структурная схема многомерного размытого классификатора

Заключение