

Пособие предназначено для руководителей органов власти и предприятий, а также специалистов ИТ-подразделений и подразделений по технической защите информации, отвечающих за выполнение требований и рекомендаций «Основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», которые были разработаны в целях реализации положений Стратегии национальной безопасности РФ до 2020 года и утверждены в середине 2012 года Советом безопасности Российской Федерации.

В пособии рассмотрены требования к обеспечению безопасности АСУ ТП критически важных объектов инфраструктуры Российской Федерации. Проведен критический анализ известных и новых методов анализа и синтеза названных систем в защищенном исполнении. Даны методические рекомендации для надлежащей технической защиты критически важной инфраструктуры.

Введение

Глава 1. Актуальность проблемы

1.1. Концепция доминирования НАТО в киберпространстве

- Роль НАТО
- Превосходство в киберпространстве
- Эволюция наступательных киберопераций
- Создание адаптивных и самоорганизующихся безопасных информационных сетей
- Обнаружение и поражение малозаметных целей
- Операции в городской местности
- Разработка пилотируемых и беспилотных систем нового поколения
- Обнаружение и локализация подземных целей
- Поддержка космической инфраструктуры

1.2. Вычисления с памятью критически важных информационных систем в условиях кибератак

- Состояние вопроса
- Математическая постановка проблемы организации устойчивых вычислений
- Технология выявления подобия между деструктивными воздействиями на ИС и природными моделями теории катастроф

Глава 2. Методы анализа

2.1. Выявление аппаратных угроз кибер безопасности

- Инвазивные и полуинвазивные методы исследования
- Приоритетные направления
- Постановка задачи исследования
- Построение эталонной модели и выявление срабатывания А-трояна на основе скрытых марковских моделей (СММ)
- Вариант методики выявления А-трояна на основе косвенных признаков

2.2. Исследование недеklarированных возможностей сверхбольших интегральных схем с процессорными ядрами

- Методы выявления аппаратных закладок
- Обоснование выбора подхода для выявления НДВ СБИС ПЯ
- Демаскирующие признаки НДВ СБИС ПЯ
- Тестирование СБИС ПЯ на наличие НДВ. НДВ СБИС ПЯ как технологический дефект
- Особенности тестирования СБИС ПЯ с учетом методологии использования СФ-блоков
- Применение эмуляции для экспресс-анализа СБИС ПЯ на наличие НДВ
- Подтверждение достоверности испытаний

2.3. Обнаружение несанкционированных модификаций программирующих последовательностей микросхем

- Реализованная методика анализа САПР
- Дизассемблирование (IDA Pro)
- Отладка, отслеживание (Stalker, FileMonitor)
- Разработка модулей автоматизации обработки массивов данных



2.4. Модель угроз информационной безопасности телефонных сетей общего пользования

- Модель нарушителя
- Виды активов, свойства безопасности активов
- Модель уязвимостей
- Способы реализации угроз, оценивание последствий реализации описанных угроз, определение уровня риска

2.5. Анализ средств исследования нанотехнологического оборудования для восстановления его функционально-логической структуры

- Принцип действия и устройство атомно-силового микроскопа
- Сканирующий ближнепольный оптический и туннельный микроскоп
- Магнитно-силовой микроскоп

2.6. Модель угроз целостности вычислений в автоматизированных системах

- Обеспечение целостности данных, программ и вычислений
- Элементы описания угроз, средства сертификации программ

Глава 3. Методы синтеза

3.1. Ситуационное моделирование процессов функционирования компьютерных сетей и сетевого оборудования

- Элементы компьютерной сети и маршрутизатора
- Определение понятия «Продукция»
- Определение понятия «Ситуационная модель на продукциях с многосортной логикой представления знаний о ситуациях»

3.2. Продукционное представление знаний для моделирования источников атак в сети

- Процесс активизации продукций в зависимости от истинности и ложности
- Система управления продукциями SPR
- Некоторые типы продукций источников атак

3.3. Выявление и нейтрализация недеklarированных возможностей программ

- Дизассемблирование и восстановление программы
- Формирование управляющего графа программы
- Преобразование управляющего графа в схему Янова
- Установление подозрения на НДВ программ

3.4. Контроль нарушения целостности вычислений на основе метрических эталонов

- Метрическая модель программы
- Алгоритм создания процесса вычислений
- Основные этапы метода распознавания вредоносных воздействий

3.5. Метод восстановления неизвестных протоколов передачи данных на основе теории взаимодружающих последовательных процессов Ч. Хоара

- Общая схема композиционного метода проектирования
- Программа обработки потоков данных протокола
- Окружение неизвестного протокола

3.6. Модель функционирования приложения IP-телефонии

- Взаимодействие различных типов приложений IP-телефонии
- Элементы поведенческой модели

Глава 4. Инновационные подходы

4.1. Биоинспирированный подход при построении систем кибербезопасности

4.2. Антиципация: от живых организмов к киберсистемам

4.3. Анализ способностей живых организмов при проектировании систем кибербезопасности

4.4. Формализация семантики для моделирования киберсистем

4.5. Аппликативный подход к представлению знаний систем кибербезопасности

Заключение