199 стр. PDF 2019 г.

В настоящем методическом пособии рассмотрена лучшая практика управления *киберустойчивостью* (*Cyber Resilience*) современных цифровых предприятий *Индустрии 4.0*. Предложены возможные методические рекомендации и решения для обеспечения требуемой киберустойчивости государственных организаций и коммерческих структур в условиях как известных, так и ранее неизвестных деструктивных программных воздействий.

Пособие содержит две основные части, которые посвящены:

- разработке Концепции управления киберустойчивостью цифровых предприятий Индустрии 4.0 в условиях разнородно-массовых кибератак (и особенно, ранее неизвестных кибератак) злоумышленников;
- технической реализации корпоративных программ управления устойчивостью (*Resilience*) на основе лучшей практики (стандартов) серии *ISO 22301 «Business continuity management systems»* (2018), *MITRE «Cyber Resiliency Engineering Framework»* (2015), *NIST SP 800-160* (2014-2018), а также оригинальных авторских моделей, методов и методик управления киберустойчивостью.

По мнению автора, пособие может быть полезно следующим основным группам читателей:

- руководителям крупных государственных и коммерческих организаций, ответственным за выполнение национальных программ *«Цифровая экономика»* по направлению «Информационная безопасность»;
- директорам служб ИТ (CIO) и ИБ (CISO), ответственным за реализацию корпоративных программ устойчивости бизнеса (*Enterprise Resilience Program*) и построение обеспечивающей информационной инфраструктуры;
- конструкторам и инженерам-исследователям, которые отвечают за техническое проектирование, разработку и внедрение *киберустойчивой информационной инфраструктуры*.

1.2. Проблема обнаружения «цифровых бомб»

1.2.1. Задача обнаружения программных закладок

- Критический анализ известных способов
- Основные процессы реинжиниринга
- Способы выявления дефектов программ
- Формальная постановка задачи

1.2.2. Методы выявления дефектов программ

- Этап 1. Подготовка исходных данных
- Этап 2. Выявление подозрительных участков кода программы
- Этап 3. Принятие решения по установлению типа дефекта
- Этап 4. Рекомендации по определению важности дефекта
- Пример обнаружения дефектов программы
- Развитие метода выявления дефектов программ
- Постановки задачи исследования

1.2.3. «Паспортизация» программ инвариантами подобия

- Математическая постановка задачи
- Управляющий граф программы
- Построение системы уравнений подобия
- Пример уравнения подобия
- Контроль возможных деструктивных воздействий
  - *Этап 1. Формирование паспорта программы в инвариантах подобия*
  - *Этап 2. Формирование инвариантов подобия в условиях воздействий*
  - *Этап 3. Формирование базы данных инвариантов подобия в контрольных точках УГП*
  - *Этап 4. Проверка критерия семантической корректности вычислительных процессов*
  - *Этап 5. Формирование сигнала о нарушении семантики вычислений и частичное восстановление вычислений по паспорту программы*

1.2.4. Метод нейтрализации программных закладок

- Модели статического анализа кода
- Основная процедура динамического контроля
- Пример

1.3. Проблема управления киберустойчивостью

1.3.1. Основные понятия и определения

- Сопроблемы обеспечения киберустойчивости
- Замысел разрешения проблемы
- Методика контроля киберустойчивости

1.3.2. Учет трендов цифровой трансформации

- Социальный компьютинг
- Большие данные (Big Data)
- Мобильные технологии (Mobility)
- Искусственный интеллект
- Технология блокчейн
- Технологии робототехники

1.3.3. Постановка задачи

- Первичные понятия
- Возмущенные машинные вычисления
- Характерные особенности возмущений
- Модель гипервизора киберустойчивости
- Управление киберустойчивостью
- Моделирование поведения в условиях возмущений
- Облик системы управления киберустойчивостью
- Промежуточные итоги исследований

Глава 2. Корпоративная программа киберустойчивости

2.1. Управление непрерывностью бизнеса, BCM

2.1.1. Практика управления непрерывностью бизнеса

2.1.2. Основные этапы жизненного цикла BCM

- BIA (Business Impact Analysis)
  - *Роль оценки рисков (RA)*
  - *Выбор оптимальных решений BC*
- Планы BCP/DRP

2.1.3. Рекомендации по разработке планов BCP/DRP

- Подход SANS Institute
  - Инициация проекта
  - Анализ рисков – Risk Analysis (RA)
  - Анализ воздействия на бизнес – Business Impact Analysis (BIA)
  - Разработка планов BCP/DRP
- Подход DRI
  - Этап 1. Инициация проекта – Project Initiation Phase
  - Этап 2. Анализ требований – Functional Requirements Phase
  - Этап 3. Разработка плана – Design and Development Phase
  - Этап 4. Внедрение плана – Implementation Phase
- Способы тестирования BCP/DRP
- Задачи тестирования
- Виды тестов плана BCP
  - Тест проверки списков вызова и инвентаризации
  - Настольный тест
  - Частичный тест
  - Полный тест
- План тестирования BCP/DRP
- Методика процесса тестирования
  - Планирование теста
  - Подготовка теста
  - Тестирование
  - Документирование результатов
  - Отчет и предложения
  - Рекомендации по выбору тестовых сценариев
- Пример. Настольный тест Плана BCP

2.2. Управление проектами устойчивости бизнеса

2.2.1. Подготовка Плана проекта устойчивости бизнеса

- Этап обследования инфраструктуры
- Выявление зависимостей между компонентами инфраструктуры
- Оценка возможного ущерба
- Интеграция процесса BCM в бизнес-культуру компании

2.2.2. Разработка прогнозных моделей

- Модель А
- Модель Б
- Модель В

2.2.3. Формирование динамических профилей

- Математическая постановка задачи
- Селекция параметров наблюдения
- Эталонное профилирование поведения
- Процедура итерационного диагностирования
- Динамические профили