**Лаврова Дарья Сергеевна Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

доктор наук Лаврова Дарья Сергеевна

ВВЕДЕНИЕ

1 Специфика обеспечения информационной безопасности современных промышленных систем

1.1 Специфика современных промышленных систем с точки зрения информационной безопасности

1.2 Исследования, посвященные проблеме обнаружения компьютерных атак на промышленные системы

1.3 Исследования, посвященные проблеме прогнозирования компьютерных атак на промышленные системы

1.4 Исследования, посвященные проблеме противодействия компьютерным атакам на промышленные системы

1.5 Выводы

2 Методология предотвращения компьютерных атак на современные промышленные системы

2.1 Постановка задачи предотвращения компьютерных атак на промышленные системы

2.2 Графовая модель функционирования промышленных систем

2.3 Типы целевой функции промышленных систем

2.4 Представление компьютерных атак в терминах универсальной графовой модели

2.5 Теорема о полноте графовой модели

2.6 Выводы

3 Обнаружение и адаптивное прогнозирование компьютерных атак на

промышленные системы

3.1 Предварительная обработка данных от промышленных систем для задачи предотвращения компьютерных атак

3.1.1 Обработка данных от конечных устройств промышленных систем

3.1.2 Обработка сетевого трафика от промышленных систем

3.2 Метод обнаружения компьютерных атак на основе мультифрактального анализа

3.3 Метод обнаружения компьютерных атак на основе дискретного вейвлет-преобразования и выявления разладки

3.4 Метод обнаружения компьютерных атак на основе адаптивного прогнозирования

3.4.1 Общий алгоритм работы фильтра Калмана

3.4.2 Определение матриц фильтра Калмана для компонентов промышленных систем

3.4.3 Определение матриц для оценки положения тела

3.4.4 Фильтр Калмана и машинное обучение

3.4.5 Экспериментальные исследования для оценки эффективности разработанного метода

3.5 Выводы

4 Саморегуляция промышленных систем на основе автоматической реконфигурации структуры системы

4.1 Аналогия между задачей саморегуляции промышленных систем и задачей сборки генома

4.2 Метод саморегуляции промышленных систем на основе реконфигурации структуры системы

4.3 Саморегуляция на основе заранее подготовленных сценариев

4.4 Саморегуляция на основе графов де Брёйна или графов перекрытий

4.5 Пример саморегуляции с использованием графов де Брёйна

4.6 Выводы

5 Подход к оценке и обеспечению киберустойчивости промышленных систем

5.1 Применение эволюционного подхода к промышленным системам

5.2 Подход к оценке киберустойчивости промышленных систем

5.3 Анализ динамики эволюционного процесса в промышленных системах

5.4 Пример оценки киберустойчивости

5.5 Выводы

6 Архитектура системы предотвращения компьютерных атак на промышленные системы и экспериментальные исследования

6.1 Архитектура системы предотвращения компьютерных атак на ПС

6.1.1 Исследование интеллектуальных подходов к управлению сложными системами

6.1.2 Теория функциональных систем П.К. Анохина

6.1.3 Архитектура системы предотвращения компьютерных атак на промышленные системы

6.2 Интеллектуальные сети энергоснабжения Smart Grid как пример развивающихся ПС нового типа

6.2.1 Концепция и принципы функционирования Smart Grid

6.2.2 Сетевая инфраструктура Smart Grid

6.3 Экспериментальные исследования метода обнаружения компьютерных атак на основе адаптивного прогнозирования

6.4 Экспериментальные исследования метода саморегуляции промышленных систем на основе реконфигурации структуры системы

6.5 Экспериментальные исследования подхода к оценке киберустойчивости

6.6 Выводы

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Приложение А

Приложение Б

Приложение В

Приложение Г

Приложение Д

Приложение Е

Приложение Ж

Приложение И

Приложение К

Приложение Л

Приложение М

Приложение Н

Приложение П

Приложение Р