В. В. Семенов, *аспирант, Университет ИТМО, младший науч. сотрудник, СПИИРАН, г. Санкт-Петербург, semenov@corp.ifmo.ru*

И. С. Лебедев, *докт. техн. наук, профессор, СПИИРАН, г. Санкт-Петербург, lebedev@cit.ifmo.ru*

М. Е. Сухопаров, *канд. техн. наук, СПИИРАН, г. Санкт-Петербург, sukhoparovm@gmail.com*

Идентификация состояния отдельных элементов киберфизических систем на основе внешних поведенческих характеристик

Авторами исследована задача определения состояния информационной безопасности объектов с использованием информации сигналов наводок электромагнитных излучений отдельных элементов устройств киберфизических систем. Рассмотрены основные побочные каналы, с помощью которых представляется возможным произвести мониторинг состояния системы и анализ программно-аппаратной среды. Подобные «независимые» способы мониторинга позволяют проанализировать состояние системы на основе внешних поведенческих характеристик в рамках концептуальных моделей автономных агентов. В статье рассмотрены статистические характеристики сигналов, позволяющих идентифицировать изменения состояния локальных устройств систем. Проведен эксперимент, направленный на получение статистической информации о работе отдельных элементов киберфизических систем. Исследована эффективность подхода на основе нейронных сетей для решения описанной задачи классификации, в частности, двухслойных нейронных сетей прямого распространения с сигмоидальной передаточной функцией в скрытых слоях. Результаты экспериментов показали, что предложенный подход превосходит по качеству детектирования аномальных состояний классификацию на основе внутренних показателей функционирования системы. При минимальном времени накопления статистической информации с использованием предложенного подхода на основе нейронных сетей становится возможным выявить требуемое состояние системы с вероятностью близкой к 0,85. Предложенный подход к анализу статистических данных на основе нейронных сетей может быть использован в качестве дополнительного независимого элемента для определения состояний информационной безопасности автономных устройств киберфизических систем.

Ключевые слова: информационная безопасность, нейронные сети, анализ сигналов, системы мониторинга информационной безопасности, киберфизические системы.

Введение

Современные технологии разработки программных и аппаратных средств направлены на получение готового продукта заданного качества с минимальными затратами по времени и стоимости. Данные подходы к проектированию и созданию информационных систем и устройств приводят к необходимости использования различных отлаженных компонент, библиотек сторонних разработчиков, обеспечивающих независимые поведенческие модели и онтологии. Элементы программной инженерии и аппа-