Н. А. Бажаев, *аспирант, Университет ИТМО, г. Санкт-Петербург, nurzhan_nfs@hotmail.com*
А. Е. Давыдов, *докт. техн. наук, Университет ИТМО, г. Санкт-Петербург, alex.davydov@mail.ru*
И. Е. Кривцова*, старший преподаватель, Университет ИТМО, г. Санкт-Петербург, ikr@cit.ifmo.ru*
И. С. Лебедев*, докт. техн. наук, доцент, Университет ИТМО, г. Санкт-Петербург, lebedev@cit.ifmo.ru*
К. И. Салахутдинова*, магистрант, Университет ИТМО, г. Санкт-Петербург, kainagr@mail.ru*

Подход к анализу состояния информационной безопасности беспроводной сети

В статье рассмотрены вопросы информационной безопасности специфической архитектуры беспроводной сети. Произведена оценка состояния информационной безопасности системы на основе показателей интенсивности событий, возникающих в процессе злонамеренного воздействия согласно теории массового обслуживания. Проведен анализ возможностей потенциального нарушителя для проведения «мягких» атак на беспроводную сеть. Выведены аналитические зависимости, позволяющие оценивать состояния информационной безопасности элементов архитектуры беспроводной сети. Осуществлено моделирование деструктивного информационного воздействия нарушителя информационной безопасности. Представлены результаты, показывающие достоверность выдвинутых предположений об экспоненциальном законе распределения длительности обслуживания заявок узлами сети.

Ключевые слова: информационная безопасность, беспроводные сети, мультиагентные системы, уязвимость, доступность устройств, модель информационной безопасности.

Введение

Внедрение беспроводных технологий требует решения дополнительных задач, связанных с обеспечением информационной безопасности в различных специфических архитектурах взаимодействия устройств. Реализация технологий беспроводных сетей, их применение в системах обработки, приема и передачи данных определяют необходимость анализа состояния информационной безопасности для обеспечения требуемого уровня защиты.

Большое количество устройств, обеспечивающих интеллектуальную передачу, сбор, обработку информационных пакетов, их относительная удаленность, автономность функционирования, динамически изменяющаяся топология, слабая проработка моделей, методов и алгоритмов оперативного обнаружения некорректной информации от скомпрометированных узлов определяют сложность создания классических систем защиты [3–5].

Особенности функционирования отдельных узлов могут создавать предпосылки к появлению потенциально возможных уязвимостей. Одна из них, показанная в работе [6], связана с необходимостью обмена служебной информацией, что обеспечивает увеличение «мусорного» трафика в сети за счет рассылки служебных сообщений между узлами.

Постановка задачи исследования

Типовой узел сети включает в себя приемо-передающее устройство, элемент питания, процессорный модуль, к которому могут быть подключены различные датчики.