МОНИТОРИНГ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ С ИСПОЛЬЗОВАНИЕМ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ

***Шевцов О.И., Тищенко Д.В., Кривуля Г.Ф.**, Харьковский национальный университет радиоэлектроники*

Эффективное функционирование современных промышленных предприятий в значительной степени зависит от уровня и средств их автоматизации, которые используют компьютерные системы контроля и управления различного уровня. При этом от информационной защищенности компьютерных систем управления промышленными объектами зависит не только их бесперебойное функционирование, но и национальная безопасность государства, имеющего развитую промышленную структуру в виде большого количества сложных технических объектов. Актуальность проблемы защищенности данных систем значительно возросла после серии инцидентов с применением специально созданных вредоносных компьютерных вирусов. В этих случаях конкурирующие корпорации и кибертеррористы используют недостаточную защищенность промышленных систем и их компонентов для нарушения нормального функционирования таких систем.

К основным тенденциям развития современных методов обнаружения вторжений и аномалий для киберсистем относятся повышение достоверности и точности обнаружения вторжений и аномалий, которые могут быть решены на основе непрерывного мониторинга и решения задачи диагностирования состояния технического объекта как некоторой части промышленной системы.

Недостатком современных систем мониторинга при диагностировании сложных технических объектов является невозможность определить начальную стадию возникновения неисправности (вторжения или аномалии) объекта. Решение задач диагностирования позволяет не только сравнивать контролируемые параметры с их эталонными значениями, но и прогнозировать возможность наступления аномалий и сбоев как отдельных элементов, так и объекта в целом. При этом перспективным направлением в процессе создания таких систем функционального диагностирования является использование беспроводных сенсорных сетей, которые сочетают преимущества традиционных систем централизованного контроля и современных интеллектуальных средств.

В настоящее время технология беспроводных сенсорных сетей на основе стандартов 802.15.4/ZigBee является единственной смарт технологией, с помощью которой можно эффективно решить задачи мониторинга и контроля производственных параметров и окружающей среды. Объединенные в беспроводную сенсорную сеть датчики образуют распределенную, самоорганизующуюся систему сбора, обработки и передачи информации. Основной областью применения такой сети является контроль и мониторинг измеряемых параметров различной физической природы.

Преимущества применения сенсорных сетей – возможность расположения в труднодоступных местах, куда сложно и дорого проложить обыкновен-

ные проводные решения; – оперативность и удобство развертывания и обслуживания системы; – надежность сети в целом (в случае выхода из строя одного из них, информация передается через соседние элементы); – возможность добавления или исключения любого количества устройств из сети; – высокий уровень проникновения сквозь препятствия (стены, потолки) и стойкость к электромагнитным помехам (благодаря высокой частоте работы системы 2.4ГГц); – длительное время работы без замены элементов питания.

Сенсорная сеть обладает способностью к ретрансляции сообщений по цепочке от одного к другому, что позволяет в случае выхода из строя одного из узлов организовать передачу информации через соседние узлы без потери качества. При этом сама сеть определяет оптимальный маршрут. Использование беспроводных устройств позволяет создать диспетчерскую систему, обеспечивающую оператору непрерывный доступ к информации о состоянии обслуживаемых объектов.

На рисунке 1 представлена структура диспетчерского центра на основе беспроводных технологий.

Рис. 1 – Диспетчерский центр на основе беспроводных технологий

При диагностировании беспроводных сенсорных сетей рассматриваются следующие виды основных отказов:

Нарушение процесса передачи информации в беспроводной среде (замирания сигнала, помехи, интерференция в канале);

– отказ аппаратного обеспечения компьютерной системы;

– отказ программного обеспечения (сбои и «зависание») системы;

– отказ вследствие целенаправленной кибератаки на систему.