УДК: 681.3

О.А. Щелконогов, старший преподаватель,
(Институт Автоматики и Электротехники НУК, Украина)

СИСТЕМА КОНТРОЛЯ ВСКРЫТИЯ АППАРАТУРЫ НА ОСНОВЕ ТЕХНОЛОГИИ СЕНСОРНЫХ СЕТЕЙ

В статье рассматривается использование технологии сенсорных сетей при разработке системы контроля вскрытия аппаратуры (СКВА). Проанализированы существующие системы, указаны их недостатки. Предложена СКВА на основе технологии ZigBee , описаны ее структура и алгоритм работы.

Система контроля вскрытия аппаратуры (СКВА) предназначена для перекрытия доступа к внутреннему монтажу с целью осуществления несанкционированных действий. Такими действиями могут быть:

- нарушение целостности аппаратуры, например, вывод ее из строя;
- изменение режима работы аппаратуры, в т.ч. приводящее к возможности изменения программного обеспечения;
- загрузка постороннего программного обеспечения;
- встраивание дополнительных несанкционированных технических средств.

Кроме того, использование СКВА позволяет контролировать соблюдение технологической дисциплины, когда при техническом обслуживании, профилактике или ремонте может быть оставлен незакрытым какой-нибудь корпус, кожух или не вставлен разъем.

СКВА, построенные по традиционному принципу, описаны в [1-3]. В них можно выделить 3 основные составляющие:

- датчики вскрытия аппаратуры;
- цепь сбора сигналов;
- специальное рабочее места или устройство централизованного контроля.

В [1] рассмотрены требования к датчикам, различные схемы построения цепей сбора сигналов, а также приведены примеры вариантов функциональных схем СКВА на дискретных элементах. В качестве датчиков используются обычные микропереключатели или герконы. Ресурс на количество срабатываний особой роли не играет, т.к. корпуса открываются нечасто. Герконы могут иметь преимущество, т.к. их не надо настраивать с такой точностью, как микропереключатели.

В [3] рассмотрена реализация СКВА с использованием микроконтроллеров, обладающая хорошей масштабируемостью, гибкостью и удобством эксплуатации. Основными недостатком предложенных систем является:

1. К каждому контролируемому объекту должны быть подведены линии связи, которые, с одной стороны, увеличивает стоимость системы на величину стоимости линий связи и работ по их прокладке и обслуживанию, а с другой стороны, демаскирует систему защиты.
2. При перемещении контролируемого объекта необходимо или заранее обеспечивать чрезмерность по длине линий связи, или прокладывать новые.
3. Прохождение линий связи по неконтролируемой территории облегчает злоумышленнику задачу несанкционированных действий.

В [2] предлагается использовать уже имеющиеся сетевые кабели (2 неиспользуемые витые пары в них). Такой подход снимает часть проблем. Однако это требует использования устройств сбора сигналов с датчиков, составляющих пару каждому хабу, вмешательство или в аппаратную часть сетевых адаптеров или использование специальных переходников для разделения сигналов сети и сигналов СКВА. Кроме того, при защите устройств, не имеющих подключения к компьютерной сети или имеющих беспроводное подключение, все равно потребуются свои кабельные линии связи.

Одним из основных элементом СКВА, определяющих стоимость, масштабируемость, область охвата, надежность и безопасность являются цепи сбора сигналов. Поэтому представляется целесообразным в принципе изменить подход к этому элементу СКВА: использовать не проводную, а беспроводную среду передачи данных. Это позволяет:

- снизить стоимость системы за счет отсутствия проводов и кабелей;
- обеспечить быстрое развертывание СКВА;
- не ограничивать месторасположение объектов контроля кабельными линиями;
- повысить уровень маскировки СКВА.

Для этих целей хорошо подходит технология беспроводных сенсорных сетей ZigBee (на основе стандарта IEEE 802.15.4 – Low-Rate Wireless Personal Area Networks (LR-WPAN)). Существуют и другие беспроводные технологии, однако, их сравнительный анализ на предмет использования для СКВА вне данной статьи.

Технология ZigBee имеет следующие, полезные для рассматриваемой области применения, свойства:

1. Возможность реализации практически любой топологии, включая сотовую.
2. Низкая стоимость (заявленная).
3. Низкое энергопотребление.
4. Хорошая масштабируемость.
5. Устойчивость к отказам и свойство самоорганизации.
6. Рабочая частота в разрешенном нелицензируемом диапазоне.
7. Маленькие физические размеры устройств.

Кроме того, ее использование позволяет достичь следующих целей:

8. Стандартная технология позволяет обеспечить совместимость с другими подсистемами защиты информации на основе компьютерных технологий.
9. Встроенные средства защиты на уровне технологии снижают усилия по защите самой СКВА от несанкционированного доступа.

Имеется и ряд недостатков. Кроме тех, которые присущи беспроводной среде как таковой, стоит отметить следующие:

1. Отсутствие единого поставщика стека протоколов ZigBee, т.е. могут быть проблемы при взаимодействии устройств разных производителей.
2. Потенциальные уязвимости в механизмах самовосстановления.
3. Отсутствие контроля за маршрутизацией на уровне приложений.

Структура сети сбора сигналов строится по стандартной схеме для сенсорных сетей (рис. 1).

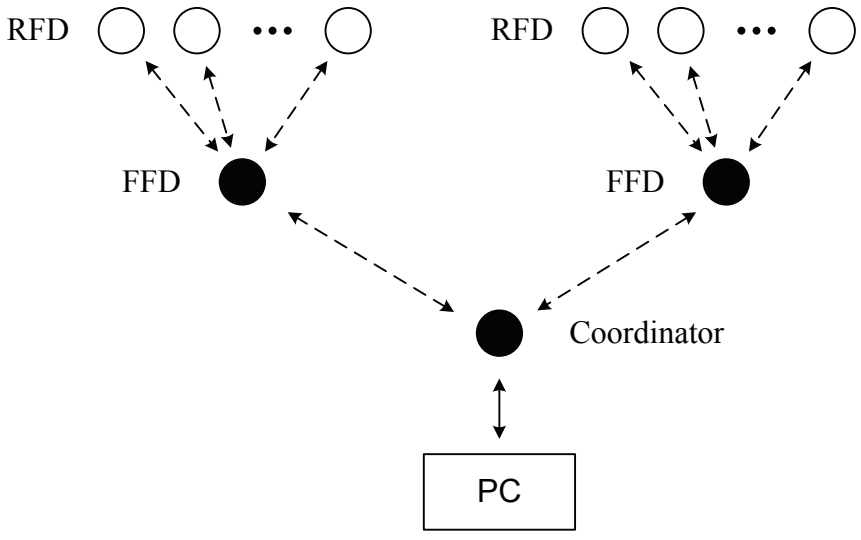

Рис. 1. Структура сети сбора сигналов СКВА

В качестве оконечных устройств, установленных внутрь корпусов, используются устройства с ограниченным набором функций (Reduced Function Device, RFD). Полнофункциональное устройство (Full Function Device, FFD) устанавливается одно на помещение. Координатор сети (Coordinator) инициирует процесс самоорганизации сети. Терминальная станция (PC), предназначена для получения, хранения и обработки данных о состоянии сети сбора сигналов (беспроводной сети).

Упрощенный алгоритм функционирования сети сбора сигналов можно представить рис.2.

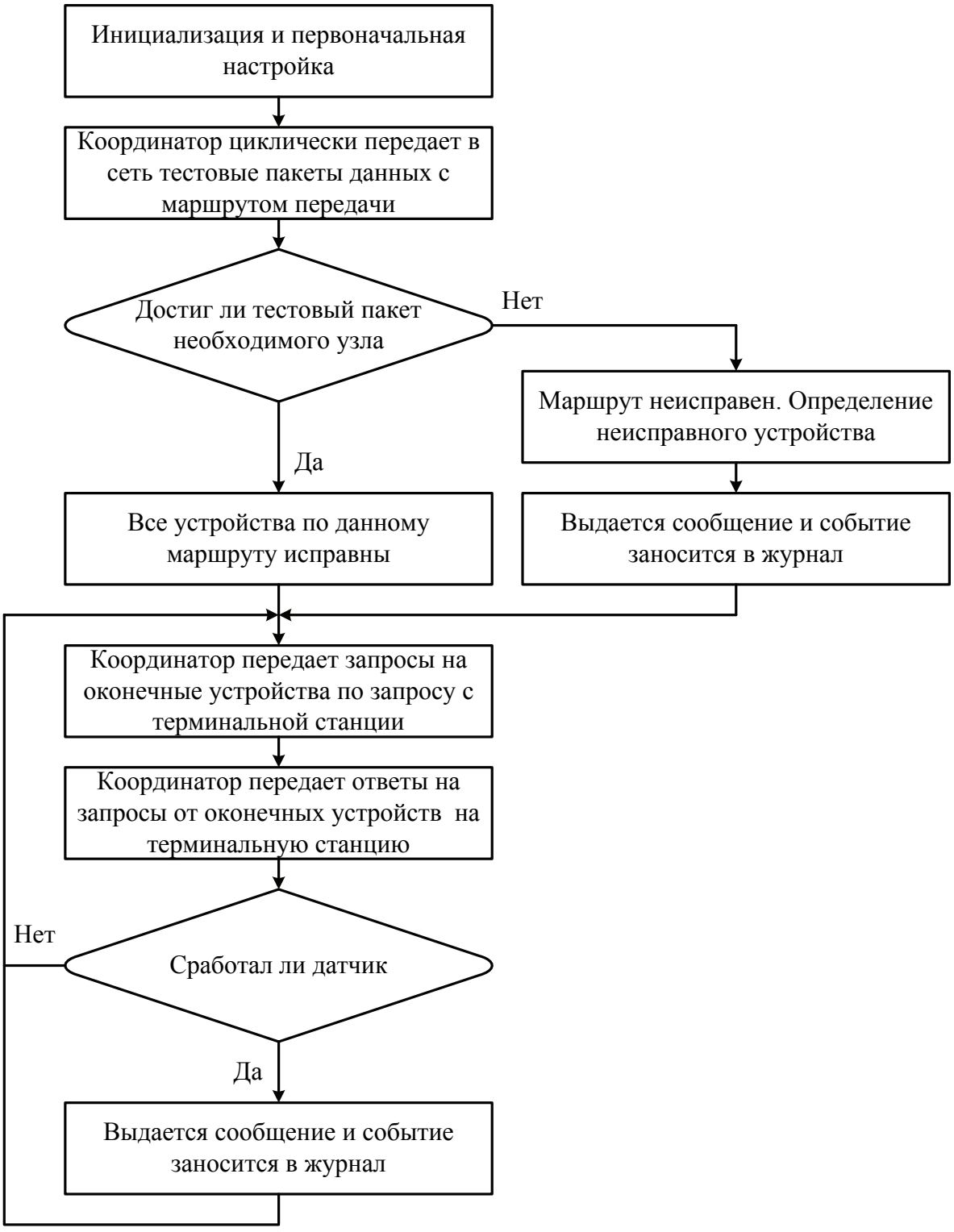

Рис. 2. Алгоритм функционирования сети сбора сигналов СКВА

Оператор может вручную создать запрос на получение информации от определенного датчика, подключенного к беспроводной сети. В этом случае координатор посылает соответствующий запрос на конечное устройство беспроводной сети, которое, в виде ответа на запрос от координатора, посылает в сеть необходимые данные.

Оконечные устройства имеют автономное питание, а кроме того, имеют возможность подключаться к 12В блоков питания компьютеров (или к свободным разъемам вентиляторов материнской платы).

На сегодняшний день наибольшим недостатком СКВА, выполненной на основе сенсорной сети, является сравнительно высокая стоимость RFD и FFD устройств: заявленное разработчиками технологии однокристальное решение оконечного устройства стоимостью 1$ пока не выполняется. Средняя цена RFD колеблется в районе 5$, а стоимость FFD устройств в несколько раз выше, что повышает общую стоимость системы. Некоторого снижения можно добиться, если в оконечных устройствах использовать только передатчик без образования двусторонней связи. Это приведет к некоторому снижению функциональности СКВА, однако позволит обеспечить большую энергоэффективность.

Несмотря на имеющиеся недостатки, СКВА на основе сенсорной сети не имеет конкуренции, если компьютерная сеть разворачивается в зданиях, где прокладка кабеля недопустима (например, в зданиях исторической важности), в беспроводных сетях (иначе теряется сам смысл беспроводной сети, если все элементы сети будут связаны кабелями СКВА), при быстром разворачивании системы защиты информации или организации временной защиты.

Выводы

Использование технологии сенсорных сетей позволяет построить систему контроля вскрытия аппаратуры, имеющую определенные преимущества по сравнению с традиционными системами с проводными цепями сбора сигналов. Удешевление элементов сенсорных сетей, увеличение их вычислительной мощности создаст еще большие преимущества.

Список литературы

1. *Мельников В.В.* Защита информации в компьютерных системах. – Москва: Финансы и статистика, Электронинформ, 1997. – 364 с.

2. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. – Санкт-Петербург: Наука и Техника, 2004. – 384 с.

3. *Щелконогов О.О.* Розробка системи контролю розкриття апаратури. VI Міжнародної науково-практичної конференції “Інформаційні технології та безпека в управлінні ” 14 вересня – 18 вересня 2009 р.