А.А. ВОРОНИН, доцент каф. ИЗИ;
И.Н. ГОРОШКО, студентка гр. КЗИ-108.

БЕСПРОВОДНЫЕ СЕТИ В ВОПРОСАХ ЗАЩИТЫ ИНФОРМАЦИИ

В ходе данной работы был произведен анализ рынка производителей оборудования и программного обеспечения для беспроводных сенсорных сетей. Целью данного анализа является подбор необходимого оборудования для повышения инженерно-технической защищенности, а именно для организации системы контроля за перемещением людей и техники.

Также были рассмотрены вопросы безопасности сенсорных сетей, а именно шифрование данных, защита от погодных условий и вандализма.

Ключевые слова: СЕНСОРНЫЕ СЕТИ, ПРОИЗВОДИТЕЛИ, ОБОРУДОВАНИЕ, БЕЗОПАСНОСТЬ.
12 источников.

In the course of this research an analysis of market of equipment and software for wireless sensor networks was done. The purpose of this analysis is the selection of the necessary equipment to improve engineering and technical security, namely, for organization of control a flow of people and machinery.

Also security of sensor networks, namely, data encryption, protection from the weather and vandalism, was considered.

Keywords: SENSOR NETWORKS, MANUFACTURERS, STANDARTS, EQUIPMENT, SECURITY.
12 sources.

Цель исследования: разработать варианты применений технологий беспроводных сенсорных сетей в области инженерно-технической защиты объекта.

Задачи исследования:

- Анализ рынка беспроводных сенсорных сетей
- Исследование вопросов безопасности беспроводных сенсорных

Инженерно-техническая защита — это совокупность специальных органов, технических средств и мероприятий по их использованию в целях защиты конфиденциальной информации.

Наиболее интересные области применения сенсорных сетей:

- контроль за перемещением людей и техники;
- контроль периметра и удаленное наблюдение;
- мониторинг имущества и ценностей;
- охранно-пожарная сигнализация;

Элементами беспроводной сенсорной сети являются:

Сенсоры – устройства, которые осуществляют непосредственный сбор информации от датчиков и передают эти данные либо другим сенсорам, либо на контроллер.

Контроллеры – Устройства, которые собирают информацию с сенсоров и передает их на центральный диспетчерский пункт

ПО - обеспечивает возможность обработки информации от сенсоров и управление ими.

Разработка электроники для сенсоров – задача весьма сложная, так как необходимо совместить функциональность устройства, необходимую мощность с малыми габаритами и низким энергопотреблением.

В области сенсорных сетей есть несколько типов компаний. Во-первых, это производители приемопередатчиков и микроконтроллеров для таких сетей. В дополнение к основной продукции они бесплатно предоставляют программные сетевые стеки, например, стандарта ZigBee. К этой группе относятся известные производители полупроводниковой элементной базы: Texas Instruments, Freescale, Atmel, NXP, Ember и т.д. Их продукция в полной мере доступна и активно применяется российскими разработчиками.

На западном рынке также существует несколько компаний, которые разработали проприетарные стеки сетевых протоколов и предлагают OEM-модули для интеграции в изделия пользователей в виде готовых блоков. Как правило, это небольшие и узкоспециализированные компании. Из них стоит упомянуть Dust Networks, Millennial Net и Digi International.

К третьему типу относятся поставщики готовых решений: беспроводных датчиков, шлюзов и сервисного программного обеспечения. Например, компании Wireless Sensors, MicroStrain и Emerson.

С целью выбора оптимального поставщика оборудования было проведено сравнение, результаты которого представлены в таблице 1.

Таблица 1 – Сравнение поставщиков оборудования

Наименование производителя	***Сенсоры***	***Контроллеры***	***ПО***	***Отеч. производитель***	***Протокол***	***Диапазон частот***	***Лицензирование***
Crossbow Technologies	+ IRIS, MICAz, IRISOEM (от $30)	-	+ MoteWorks 2.0 (free)	-	ZigBee	2405 - 2475 МГц	Не требуется
RFM	+ XDM2510H (от $109)	+ XG2510HE (от $1094,50)	+ (free)	-	TSMP + WirelessHART	2405 - 2480 МГц	Не требуется

Millenial Net	+ MeshScape GO OEM End Node Module	+ MeshScape Go wireless gateway (от $1495)	+ MeshScape GO Software (free)	-	IEEE 802.15.4	2405 - 2475 МГц	Не требуется
MicroStrain	+ HS-Link-S (от $545)	+ WSDA -Base-104	+ Node Commander (free)	-	IEEE 802.15.4	2405 - 2480 МГц	Не требуется
Libelium	+ Wapsmote ($330)	+ Meshlium ($1547)	+ Meshlium Manager System (open source)	-	ZigBee	2.4ГГц - 868МГц - 900МГц	Не требуется
National Instruments	+ NI WSN-3202 ($690)	+ NI 9792 ($ 1,895)	+ LabVIEW WSN Pioneer (free)	-	ZigBee	2400 - 2483.5 МГц	Не требуется
Dust Networks	+ LTP5902-IPM	+ LTP5902-IPR	+ LTspice IV (free)	-	IEEE 802.15.4	2400 - 2483.5 МГц	Не требуется
РТЛС	+ RTLS Анкер	+ RTLS Шлюз	+ RTLS Серверное ПО	+	ZigBee	2405 – 2485 МГц	Не требуется

В результате сравнения можно сделать следующие выводы:

- Рынок оборудования для сенсорных сетей в основном представлен зарубежными производителями.
- Не все компании предоставляют комплексные решения для организации сенсорных сетей. Многие из них специализируются на производстве микроконтроллеров для сенсоров и шлюзов, не производя при этом готовые устройства.
- Практически все устройства имеют один и тот же диапазон рабочих частот (2405 - 2480 МГц) и протокол передачи данных (IEEE 802.15.4/ ZigBee).
- При выборе оборудования для организации сенсорной сети необходимо учитывать конкретную задачу. Проблема состоит в том, что конкретный сенсор может поддерживать не все виды датчиков.

Защита от атак по радиоканалу.

Отличительной чертой сетей ZigBee является гарантированная, устойчивая к помехам, многолучевому затуханию, различным сбоям и отказам передача данных.

Система безопасности в соответствии со спецификацией ZigBee основана на 128-битном AES алгоритме. Предусмотренные спецификацией ZigBee службы безопасности определяют создание ключей, управление устройствами и защиту данных.

ZigBee использует 128-битные ключи для реализации механизмов безопасности. Ключ может быть ассоциирован либо с сетью (и использоваться уровнями ZigBee и MAC подуровнем) либо с каналом связи.

В защищенной сети назначается одно специальное устройство, которому другие устройства доверяют распределение ключей безопасности – центр управления безопасностью. В идеале каждое устройство в сети должно иметь предварительно загруженные адрес центра управления безопасностью и первоначальный главный ключ. Приложения без особых требований к безопасности могут использовать сетевой ключ, передаваемый центром управления безопасностью через не защищенный на момент передачи канал. Таким образом, центр управления безопасностью поддерживает ключ сети и обеспечивает безопасность точка-точка. Устройства будут принимать только сообщения, зашифрованные с использованием ключа, предоставленного центром управления безопасностью, за исключением первоначального главного ключа.

Защита от подлога.

Защищенность от подлога в сенсорных система и сетях обеспечивается средствами стека протоколов обмена данными. В сенсорных сетях, так же как и при использовании обычного Wi-Fi, используется шифрование. Без ключа невозможно вообще подключиться к сенсорной сети, ключ хранится в сенсоре в зашифрованном виде. В Zig-Bee за безопасность соединения и передачи данных отвечает отдельный центр безопасности, выполняющий функции контроля за сенсорами и разрешения доступа. Таким образом, не получится просто подменить адрес устройства, чтобы стать часть сенсорной сети.

Защита от помех.

Одна из первых помех – это наводки по питанию, она возникает из-за того, что несколько устройств подключены к одной системе питания. Сенсоры слабо уязвимы в этом плане, так как большинство решений имеет автономное питание, однако встречаются варианты с комбинированным питанием, или питанием от сети. В данном случае проблема решается установкой фильтров по цепи питания.

Для передачи данных сенсоры используют радиоканал. В радиочастотном диапазоне работают еще множество других устройств, которые также могут создавать помехи при работе сенсора. Во избежание данной проблемы практически все сенсоры работают в диапазоне 2,4 ГГц. Такой диапазон наименее чувствителен к внешним источникам помех, что не маловажно, так как мощность передатчика сенсоров, как правило, не превышает 10 мВт.

Ультракороткий диапазон также обеспечивает отличное прохождение волн в городской или производственной среде. Такие волны хорошо проходят через элементы строительных конструкций, однако дальность при этом страдает, средняя дальность действия сенсора, как правило, не превышает 300 метров.

Защита от метеоусловий.

В жарком климате необходимы защитные оболочки либо козырьки, предотвращающие избыточный нагрев конструкции, а в качестве отделки кожуха рекомендуются отражающие либо белые покрытия.

При отрицательных температурах целесообразно обеспечить подогрев, специальное покрытие электроники, приспособление для «холодного» пуска.

Помимо температурных условий большую роль играет влажность среды использования, корпус должен быть герметичен, стыки прорезинены, если имеются элементы управления, то они должны быть выполнены во влагозащищенном или водонепроницаемом варианте исполнения.

Следует учитывать и пылезащищенность, при использовании сенсоров на открытом пространстве и в производственных помещениях. Помимо вышеперечисленных природных факторов, могут быть и техногенные, так например анодированный алюминий с полиуретановым эмалевым покрытием используется для обеспечения высокого уровня защиты от метеоусловий, однако для коррозионно опасных сред он не годится. Или, например, на заводах при наличии в воздухе аэрозолей солевых растворов следует использовать для корпуса нержавеющую сталь либо специальные пластмассы.

Литература

1. Проектирование беспроводных сенсорных сетей, 2012 [Электронный ресурс] – Режим доступа: http://isca.su/index.php?option=com_content&task= view&id=42&Itemid=61.

2. *Недев М.Д., Шевчук Ю.В.* - Сенсорная сеть с организацией извне, 2012 [Электронный ресурс] – Режим доступа: http://cmm.ipu.ru/sites/default/cmm12cd/CD/Papers/paper_pdfed_.pdf.

3. Сайт исследовательской группы, занимающейся изучением беспроводных сенсорных сетей, 2012 [Электронный ресурс] – Режим доступа: http://www.sensor-networks.org.

4. *Яманов А.Д., Алевский Д.А., Плеханов А.Е*. - Технология развертывания локальных беспроводных радиосетей ZigBee в системах промышленной автоматизации и диспетчеризации. Журнал «ИСУП», № 6(36), 2011 [Электронный ресурс] – Режим доступа: http://www.isup.ru/articles/3/1212/.

5. Официальный сайт компании Libelium, 2012 [Электронный ресурс] – Режим доступа: http://www.libelium.com.

6. *Семенов Ю.А.* - Беспроводные сети ZigBee и IEEE 802.15.4, 2012 [Электронный ресурс] – Режим доступа: http://book.itep.ru/4/41/zigbee.htm#6/

7. Спецификация ZigBee.Безопасность. 2012 [Электронный ресурс] – Режим доступа: http://habrahabr.ru/post/158355/.

8. Официальный сайт компании LabView, 2012 [Электронный ресурс] – Режим доступа: http://www.labview.ru/products/304/item1682/.

9. Официальный сайт компании National Instruments, 2012 [Электронный ресурс] – Режим доступа: http://sine.ni.com/nips/cds/view/p/lang/ru/nid/206916.

10. Официальный сайт компании RTLS, 2012 [Электронный ресурс] – Режим доступа: http://www.rtlsnet.ru/technology/view/4.

11. Официальный сайт компании Linear Technologies, 2012 [Электронный ресурс] – Режим доступа: http://www.linear.com/product/LTP5902-IPM#simulate.

12. Официальный сайт компании Microstrain, 2012 [Электронный ресурс] – Режим доступа: http://www.microstrain.com/wireless/wsda-base-analog.