1. Kuntze, T. Plastic Optics Enable LED Lighting Revolution. When Highest Precision Meets Low Prices / T. Kuntze // Optik & Photonik. - 2007. - №4. -P.42-45.
2. Ding, Y., Liu, X., Zheng, Z., Gu, P. Freeform LED lens for uniform illumination / Y. Ding, X. Liu, Z. Zheng, P. Gu // Optics Express. - 2008. - Vol. 16, № 17. - P.12958-12966.
3. Журавок, А.А. Определение устойчивости элементов неизображающей вторичной оптики к изменению показателя преломления материала / А.А. Журавок, Д.В, Балохонов, Т.В. Колонтаева, С.П. Сернов // Приборостроение – 2012: материалы 5-й Междунар. науч.-техн. конф., Минск, 21-23 ноября 2012 г. / БНТУ ; редкол.: О.К. Гусев [и др.]. - Минск, 2012.- С. 279-281.
4. Сернов, С.П. Эффективность применения вторичной оптики в автомобильной светодиодной светотехнике / С.П. Сернов, Д.В. Балохонов // Наука – образованию, производству, экономике: материалы девятой Международной науч.-техн. конф., Минск, 2011г. : в 4 т./ Белорус. нац. техн. университет ; редкол.: Б. М. Хрусталев, Ф. А. Романюк, А. С. Калиниченко.- Минск, 2011. – Т.4. - С. 402.

УДК 681.2

СЕНСОРНЫЕ СЕТИ НА ОСНОВЕ СВЕРХШИРОКОПОЛОСНЫХ СИГНАЛОВ ДЛЯ ПЕРЕДАЧИ ЗАЩИЩЕННОЙ ИНФОРМАЦИИ

Сидоренко А. В., Мулярчик К.С., Ходасевич А.И., Солодухо Н.А.
Белорусский государственный университет
Минск, Республика Беларусь

I. Введение. В последние годы возрастает роль инновационных технологий для решения задач мониторинга и контроля объектов управления. Одним из достижений в этой области является использование беспроводных сенсорных сетей. Среди беспроводных сетей выделяются сети с использованием сверхширокополосных приемопередатчиков [1], в основу функционирования которых положены принципы нелинейной динамики. При передаче данных в беспроводных сенсорных сетях существенным является обеспечение их защиты для исключения несанкционированного доступа.

В предлагаемой работе задача обеспечения защиты передаваемых данных решается внедрением функций шифрования непосредственно в приемопередатчики, что позволяет установить безопасное соединение между отдельными приемопередатчиками.

II. Структурная схема защищенной передачи информации. Структурная схема защищенной передачи информации приведена на рисунке 1.

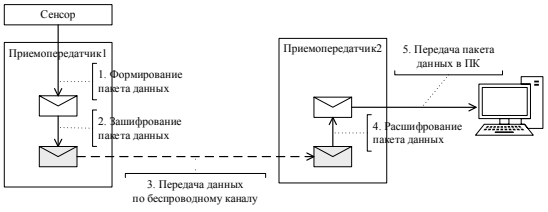


Рисунок 1 – Схема зашифрованной передачи информации в сенсорной сети

Приемопередатчик 1 производит регистрацию текущих показателей с сенсора и формирует информационный пакет, зашифровывает его, используя текущие в узле настройки шифрования, и отправляет в эфир. предложенного алгоритма шифрования выполнена на базе сверхширокополосных прямохаотических приемопередатчиков серии ППС-40А, используемых в качестве узлов при построении беспроводных сенсорных сетей.

Внешний вид и структурная схема приемопередатчика серии ППС-40А представлены на рисунке 2, а технические характеристики приведены в таблице 1.

Приемопередатчик 2 принимает пакет из эфира, расшифровывает его, используя текущие в узле настройки шифрования, и осуществляет его дальнейшую обработку путем передачи в компьютер или ретрансляцию в эфир.

Следует отметить, что функция шифрования данных в приемопередатчике осуществляет шифрование всего тела пакета данных целиком, не затрагивая при этом заголовок пакета и байты контрольной суммы. Выбор такой схемы преобразования продиктован необходимостью защиты информации о маршрутизации, поскольку одной из целей пассивного прослушивания является извлечение идентификаторов узлов, что позволит построить схему маршрутизации и выявить расположение узлов в сети.

III. Алгоритм шифрования и его аппаратно-программная реализация. Обеспечение функции шифрования данных в приемопередатчиках осуществляется с использованием разработанного нами алгоритма шифрования [2], в основу которого положены принципы нелинейной динамики.

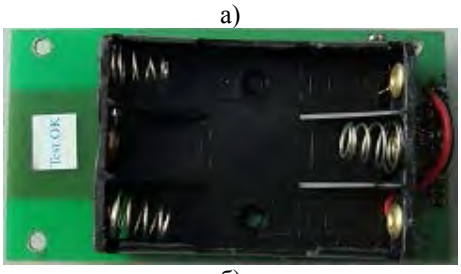
Итеративная схема Шеннона используется в блочном симметричном алгоритме шифрования, где в качестве базового преобразования применена сеть Фейстеля, а нелинейного блока – дискретное хаотическое отображение.

Совместное использование в разработанном

алгоритме шифрования таких структурных элементов, как итеративной схемы Шеннона, сети Фейстеля и дискретного хаотического отображения, делает возможным выбор и установление требуемой длины ключа шифрования и длины блока обрабатываемого текста, при этом длина блока текста должна быть кратна двум. Это является существенным преимуществом разработанного алгоритма при его использовании в узлах беспроводной сенсорной сети, поскольку в зависимости от характера передаваемой информации (размера пакета), а также условий передачи (например, зашумленность, вероятность возникновения ошибки при передаче) может выбираться та или иная длина блока текста.

Аппаратно-программная реализация.

а)



б)

Рисунок 2 – Приемопередатчик для беспроводных сенсорных сетей

Таблица 1 – Технические характеристики приемопередатчика

Наименование характеристики	Значение
Полоса выходного сигнала	3,1–5,1 ГГц
Средняя мощность излучаемого сигнала (скорость 2,5 Мбит/с)	–10 дБм
Средняя мощность излучаемого сигнала (скорость 0,1 Мбит/с)	–21 дБм
Дальность приема	до 20 м
Физическая скорость передачи/приема данных	2,5/2,5 Мбит/с
Интерфейс сопряжения с ПК и датчиками	UART
Напряжение питания	4,5 В

Центральным узлом цифрового блока является микроконтроллер Atmel ATmega 168, обладающий следующими характеристиками: 8–разрядная архитектура; тактовая частота – до 20 МГц; объем памяти для хранения данных (RAM) – 1 Кбайт; объем памяти для хранения программного кода (ROM) – 16 Кбайт; объем энергонезависимой памяти EEPROM – 512 байт.

IV. Экспериментальные исследования опытной сенсорной сети. Для экспериментального исследования реализуемых средств защиты построена опытная беспроводная сенсорная сеть, в которой в качестве узлов использованы сверхширокополосные приемопередатчики серии ППС-40А. Сеть организована таким образом, что в ней осуществляется однонаправленная передача данных от сенсорных узлов к координатору сети напрямую либо через узлы ретранслятора. В процессе экспериментальной проверки разработанной аппаратно-программной реализации алгоритма шифрования выполнена инсталляция (прошивка) разработанного программного обеспечения в микроконтроллеры приемопередатчика. Проанализировано изменение характеристик программного кода микроконтроллера приемопередатчика до и после реализации функции шифрования. Результаты представлены в таблице 2.

Таблица 2 – Характеристики реализации функции шифрования в микроконтроллере приемопередатчика

Размер блока текста, байт	Объем памяти для хранения данных, байт		Количество тактов микроконтроллера для зашифрования блока текста	
	суммарный	на один байт блока текста	суммарное	на один байт блока текста
4	223	56	12911	3228
8	241	30	14167	1771
12	259	22	15423	1285
16	277	17	16679	1042
20	295	15	17935	897
24	313	13	19191	800
28	331	12	20447	730
32	349	11	21703	678

V. Выводы. В работе рассмотрены особенности реализации беспроводных сенсорных сетей на основе сверхширокополосных приемопередатчиков для передачи защищенной информации. Проведены экспериментальные исследования опытной беспроводной сети.

1. Дмитриев, А.С. Сверхширокополосные прямохаотические приемопередатчики серии ППС для сетей передачи информации / А.С. Дмитриев, А.В. Сидоренко, Ю.В. Андреев, К.С. Мулярчик // Электроника инфо. –2013. – № 6. – С.36-37.
2. Сидоренко А.В.. Шифрование данных на основе дискретных хаотических систем и отображений / А.В. Сидоренко, К.С. Мулярчик //Доклады БГУИР. – 2013. – № 1. – С. 62-67.