## АНАЛИЗ ЭФФЕКТИВНОСТИ И ПОМЕХОЗАЩИЩЕННОСТИ МНОГОКАНАЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДОВЫМ УПЛОТНЕНИЕМ

В.О. Сидорович, А.Е. Варюшина

Практика построения современных СПИ показывает, что наиболее дорогостоящими звеньями трактов передачи являются линии связи (кабельные, волоконно-оптические, сотовой мобильной радиосвязи, радиорелейной и спутниковой связи и т. д.). Поскольку экономически нецелесообразно использовать дорогостоящую линию связи для передачи информации единственной паре абонентов, то возникает необходимость построения многоканальных СПИ, обеспечивающих передачу большого числа сообщений различных источников информации по общей линии связи [1].

В многоканальной СПИ по общему высоко-частотному тракту передаются сообщения от нескольких источников информации. На передающей стороне многоканальной системы сообщения от каждого из источников информации модулируют по какому-либо параметру выделенные данному источнику канальные сигналы. Затем промодулированные канальные сигналы объединяются по тому или иному правилу, в результате чего формируется суммарный (групповой) сигнал. Данная операция называется уплотнением каналов. Полученный групповой сигнал затем модулирует несущее колебание, которое поступает на передачу. При использовании общей несущей канальные сигналы иногда называют поднесущими колебаниями. В ряде случаев, когда источники информации территориально сосредоточены, общая несущая не используется и канальные сигналы формируются непосредственно на несущих частотах. На приемной стороне многоканальной радиолинии после демодуляции несущей осуществляется операция, обратная операции уплотнения – из группового сигнала выделяются сигналы отдельных каналов. Данная операция называется разделением (селекцией) каналов [2].

**Литература**

1. Принципы многоканальной передачи информации. Элементы теории разделения сигналов [Электронный ресурс]. – 2011. – Режим доступа : http://studopedia.org/8-106652.html – Дата доступа: 26.01.2017.

2. Уплотнение информации в аналоговых системах связи [Электронный ресурс]. – 2017. – Режим доступа: http://studopedia.org/2-74270.html – Дата доступа: 11.03.2017.

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ АВТОМАТИЗАЦИИ ЗДАНИЙ

Д.С. Смоляк, Т.А. Пулко

Одним из частных случаев интернет вещей (физических предметов) (IoT) являются системы автоматизации зданий, такие как системы домашней автоматизации «умный дом», позволяющие автоматизировать ряд рутинных задач и обеспечить контроль и мониторинг использования ресурсов, а также обеспечить владельцу возможность удаленного управления. При построении систем типа «умный дом», рассчитанных на широкого потребителя используются решения, использующие беспроводные протоколы передачи данных. Большое распространение на текущий момент времени получают системы, использующие беспроводные протоколы передачи данных на не лицензируемых радиочастотах, позволяющие использовать оборудование для реализации решения без дополнительных согласований, такие как ZigBee и Z-Wave. В Республике Беларусь телекоммуникационная компания Белтелеком в своей услуге «Умный дом» предлагает решения, рассчитанные на массового потребителя и основанные на беспроводном протоколе ZigBee [1]. Однако, использование беспроводных решений влечет за собой ряд угроз для потенциального потребителя. Например, исследователи из компании Qihoo360 обнаружили возможность перехвата ключей шифрования сетевых сообщений для ряда устройств [2]. Исследователями Eyal Ronen, Colin O'Flynn были обнаружены уязвимости в продукте Philips Hue, позволяющие загрузить вредоносное программное обеспечение в «умную лампочку» [3]. Таким образом, в связи с ростом применения продуктов IoT, следует подвергнуть критической оценке, представленные на рынке решения, оценить уровень их защищенности к различным атакам, а также повысить осведомленность потребителей о возможных последствиях использования небезопасных решений.