

## **ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМЕ УДАЛЕННОГО МОНИТОРИНГА С ПЕРЕДАЧЕЙ ИНФОРМАЦИИ ПО ПРОВОДАМ ЭЛЕКТРОСЕТИ**

**В.П. ЛУГОВСКИЙ**

Система удаленного мониторинга осуществляет контроль работоспособности различного оборудования посредством сбора и передачи данных. Использование в качестве среды передачи данных проводов электросети позволяет упростить и снизить стоимость соединений, поскольку оборудование всегда имеет электрическую подводку. При передаче информации в системе удаленного мониторинга весьма актуальной является проблема ее защиты. Для исключения несанкционированного доступа к информации системы удаленного мониторинга в процессе ее передачи можно воспользоваться средствами шифрования сигнала в виде 56-битовой технологией DES. Однако этот известный алгоритм шифрования имеет неудовлетворительную на сегодняшний день длину ключа шифрования — 56 бит; кроме этого он крайне медленный. По современным оценкам считается, что при длине ключа шифрования не менее 128 бит и нормальных размерах

сообщения расшифровка статистическими методами на современной технике за разумное время практически невозможна. В силу этого следует отдать предпочтение 128-битным ключам AES. Кроме того, доступ к устройствам системы удаленного мониторинга может быть разрешен только тем пользователям, чьи серийные номера, номера карт доступа или другие уникальные идентификаторы известны диспетчерам. Перечисленные возможности следует реализовать как дополнение к различным внутренним механизмам безопасности — паролированию, программным правам доступа к ресурсу и т.п. В конечном результате может быть достигнут уровень безопасности системы удаленного мониторинга такой, как и в беспроводных сетях стандартов семейства IEEE 802.X.