Нынешняя стратегия развития Приморского края направлена на реализацию новых, в ряде случаев уникальных проектов, основанных на инновационных технологиях. В Приморье есть потенциал для создания новых производств, в т.ч. и в области информационных технологий.

1. Государственная программа Приморского края «Информационное общество» на 2013-2017 годы».

2. Журнал «Дальневосточный капитал». - 2014. - № 2(162) февраль. - 64 с.

3. Инвестиционный портал Приморского края [Электронный ресурс]. - Режи доступа: http://invest.primorsky.ru План создания инвестиционных объектов и объектов инфраструктуры в Приморском крае на период 2013-2017 гг.

4. Сайт администрации Приморского края [Электронный ресурс]. - Режи доступа: http://primorsky.ru

5. Сайт Дальневосточного управления Росграницы [Электронный ресурс]. - Режи доступа: http://www.rosgranitsa.ru/ agency/to/dvcu.

УДК 004.056.53

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ЗАЩИТЫ КАНАЛА СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

А.А. Мамаков, научный сотрудник НМЦ

Владивостокский государственный университет экономики и сервиса, г. Владивосток

Защита каналов связи охранных радиосистем от несанкционированного проникновения в них, как правило, основана на шифровании сигнала тревоги (предполагающего значительные вычислительные затраты на его криптоанализ), или на синтезе динамично изменяющихся сигнально-кодовых конструкций (СКК) с избыточностью, исключающей их имитацию в реальном режиме времени. Оба принципа приводят к усложнению технических средств связи и повышают стоимость охранных систем в целом. Однако средства, затраченные на высокую сложность технических устройств, оказываются бесполезными в условиях противодействия со стороны организованных преступных групп (ОПТ), которые в своей противоправной деятельности применяют высокие технологии из области радиоэлектронного подавления (используя преднамеренные радиопомехи, например).

Для повышения устойчивой работы средств связи охранных систем предлагается программно-аппаратный комплекс, выполняющий интеллектуальные функции:

1. Синтез СКК создающей перед сторонним наблюдателем дополнительный барьер неопределенности. В основе этого барьера динамичное изменение псевдослучайного телеграфного сигнала (ДИПТС), устойчивого к случайным и имитационным помехам [1].

2. Синхронизацию канала связи для скрытной передачи тревоги в случае возникновения опасной ситуации.

3. Аппаратно-программную реализацию алгоритма анализа синтезированной СКК.

Материальной основой для реализации интеллектуальных функций, заложенных в аппаратно-программный комплекс, служит электронный блок принятия решений, обладающий следующими характеристиками:

1. Способность принимать решение в многоальтернативной ситуации, при наличии замкнутое группы гипотез о значении искомого параметра синхропоследовательности.

2. Обеспечить заданную достоверность принятого решения о фазе синхропоследовательности при существенном сокращении объема выборки элементов СКК ДИПТС (в сравнении с существующими аналогами на базе ЦРСТС - цифровых разомкнутых систем тактовой синхронизации).

3. Возможность согласования создаваемого блока с приемопередающими модулями действующих свстем охранной сигнализации: Alligator, Mongoose, Jaguar, Scher-khan, Sheriff, Black bug, Pantera, Pondora [2].

Как известно, цикловой синхронизации, обеспечивающей разделение потока данных на блоки и кодовые комбинации, предшествует тактовая, определяющая временные границы элементов сигнала. Для тактовой синхронизации в узкополосных каналах связи используется синхропоследовательность в виде меандра. Спектр меандра имеет характерную линейчатую структуру (рисунок 1а). Дискретное распределение энергии меандра по спектру упрощает систему связи, но одновременно облегчает поиск и перехват сигналов тактовой, а за ней и цикловой синхронизации правонарушителями. Идентификация последней упрощает навязывание ложного режима работы охранным устройствам с их стороны.