Для реализации метода необходимо разработать программы мониторинга и управления. Программа управления должна иметь функцию задания маски имен отслеживаемых файлов, а также функцию графического отображения маршрута перемещений. Модуль мониторинга должен устанавливаться на конечных ПК локальной сети и следить за изменениями целевых файлов по предложенной выше схеме.

Литература

1. *Алиев А.Т.* Разработка моделей, методов и алгоритмов перспективных средств защиты информации в системах электронного документооборота на базе современных технологий скрытой связи: дис. …канд. техн. наук: 05.13.13/А. Т. Алиев; Ростов-на-Дону, 2008 – 216 с

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

А.П. Жук, А.А. Гавришев, В.А. Бурмистров

Сегодня в мире основными технологиями беспроводной передачи информации являются GSM, 3G, HSPA+/HSPA+ Advanced (4G), WiMAX, LTE (4G). В последнее время данные технологии активно внедряются во многие системы передачи информации, например в охранно-пожарные системы безопасности. Однако, в силу уязвимости беспроводного канала связи для несанкционированного доступа актуальным является вопрос обеспечения его защищенности. В настоящее время защищенность радиоканала, в основном, обеспечивается средствами криптографической защиты информации (СКЗИ). СКЗИ имеют следующие минусы: дороговизна, значительное время выполнения команд шифрования-расшифрования, изученность основных алгоритмов. Альтернативным методом защиты радиоканала является применение генераторов стохастических ортогональных сигналов [1], заключающимся в том, что для передачи сообщений, сменяемых от одного информационного символа к другому, предлагается использовать сформированные стохастическим образом ортогональные системы сигналов, описываемые собственными векторами диагональной симметрической матрицей А размерностью N. При этом используется свойство ортогональности собственных векторов, заключающееся в том, что собственные векторы, соответствующие различным собственным значениям нормального оператора, попарно ортогональны. Данный метод отличается увеличенным числом структур сигналов и уменьшенной вероятностью их раскрытия за счет расширения диапазона n возможных значений диагональных коэффициентов матрицы А.

Литература

1. *Жук А.П. и др.* Способ передачи информации на основе хаотически формируемых ансамблей дискретных многоуровневых сигналов / Патент РФ № 2428795, 10.09.2011.

ПРОТОКОЛОВ ЗАЩИТЫ ИНФОРМАЦИИ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ ПРЯМЫХ

А.М. Захаревич

В последнее время все больше и больше внедряются в нашу повседневную жизнь информационные технологии, пытаясь захватить в ней все: от важнейших государственных проектов до решения обычных бытовых проблем. Вместе с огромной пользой и, казалось бы, неограниченными возможностями новые технологии приносят и новые проблемы. Одной из них является проблема защиты информации от несанкционированного посягательства теми, кто доступа к этой информации иметь не должен. В связи с этим почти одновременно с развитием информационных и компьютерных технологий начали развиваться и технологии защиты информации, развитие которых с некоторой точки зрения гораздо более критично, чем развитие непосредственно информационных технологий. Ведь с совершенствованием систем защиты, совершенствуются и методы взлома, обхода этих защит, что требует постоянного пересмотра и увеличения надежности защиты информации.

Практически любая "современная" криптосистема может быть "переложена" на эллиптические кривые, но не для всех схем это дает выигрыш в стойкости. Например, для

Библиотека БГУИР