МОНИТОРИНГ ХАРАКТЕРА АТАКУЮЩИХ ВОЗДЕЙСТВИЙ

Мали В.А., Морозов А.А.

Пензенский государственный университет
440026, г. Пенза, ул. Красная, 40,кафедра ИБСТ, т. (841-2) 36-82-23, e-mail: maly@beda.stup.ac.ru

Аннотация. Рассмотрен способ повышения эффективности мониторинга состояния занятых каналов связи.

Для повышения информационной безопасности систем связи необходимо проводить мониторинг состояния занятых каналов связи на приемной стороне с целью определения основных характеристик преднамеренных или непреднамеренных атакующих аддитивных сигналов. Одной из задач мониторинга состояния занятых каналов связи на приемной стороне является определение спектрально-временных и статистических характеристик кратковременных атакующих сигналов. Мониторинг осуществляет система информационной безопасности автоматизированной системы. Средства мониторинга подключаются параллельно приемному тракту.

В общем случае в тракте мониторинга анализу подвергается атакованный сигнал (смесь информационного сигнала с атакующим сигналом). Для повышения эффективности мониторинга предлагается выделять кратковременные атакующие сигналы из атакованного сигнала и накапливать их для дальнейшего анализа. Выделение фрагментов может производится для тех посылок, для которых текущее соотношение сигнал/шум будет определено как "угрожающее" или "опасное" с позиции правильного приема переданного бита |1|. Выделение атакующего сигнала может производиться в соответствии с методом |2|.

Так как команда на выделение требуемого фрагмента формируется в конце текущей посылки, то атакованный информационный сигнал необходимо предварительно записывать в ОЗУ. Минимальный объем ОЗУ должен соответствовать количеству отсчетов частоты дискретизации на одной посылке.

При цифровой обработке информационного сигнала в устройстве преобразования сигналов на приемной стороне частота дискретизации (Fд) выбирается по теореме Котельникова, исходя из верхней частоты среза входного фильтра. Однако в тракте мониторинга при детальном анализе положения в пределах одной посылки импульсных или кратковременных шумоподобных атакующих сигналов такой частоты дискретизации недостаточно. Для целей мониторинга частота дискретизации должна быть выше в 2-3 раза, чем Fд в тракте приемника.

Предлагается вместо двух АЦП с разными частотами дискретизации в трактах приема и мониторинга использовать один АЦП с частотой, кратной частоте дискретизации Fд. При этом в тракт мониторинга будут поступать все отсчеты сигнала, а в приемный тракт – только кратные отсчеты входного сигнала.

Повышение частоты дискретизации приведет к увеличению вычислительной сложности алгоритмов ЦОС в тракте мониторинга, но это те ресурсы, которые необходимо использовать для повышения информационной безопасности системы связи.

Литература

1. Экспресс-анализ помеховой обстановки в канале связи./Гридасов В.Г., Кашаев Е.Д., Пензенский государственный университет, Пенза, 2000.-Деп. 31.03.00, №869-В00.
2. Обнаружение атак на информационные ресурсы физического уровня автоматизированных систем (Тезисы доклада)/ Мали В.А. НТК, Санкт-Петербург, 2000 г.

MONITORING of ATTACKING INFLUENCES CHARACTER

Mali W., Morozov A.

The Penza state university
440026, Penza, Krasnaja street, 40, faculty ISST, ph. (841-2) 36-82-23, e-mail: maly@beda.stup.ac.ru

For increase of information security of communication systems it is necessary to carry out monitoring of a condition of the engaged communication channels. One of the monitoring tasks is to define the spectrum-time and statistical characteristics of short attacking signals. The system of information security of the automated system carry out the monitoring. Monitoring tools are connected by parallel way to receiver.

For effective monitoring we offer to allocate short attacking signals from the attacked signal and to accumulate them for the further analysis. The allocation of an attacking signal can be made according to a method |1,2|.

In a path of monitoring the sampling rate should be above in 2-3 times, than in a path of the receiver, during the detailed analysis of a position pulse or short noise attacking signals in the one packet.

We offer to use one ADC with the sampling rate, which is multiple the sampling rate in receiver path, instead two ADC with different sampling rates.

The increase of the sampling rate will result to increase of computing complexity of algorithms DSP in a path of monitoring, but it is those resources, which are necessary for using for increase of information security of communication system.

Bibliography

1. Express-analysis of noise conditions in the communication channel. /Gridasov V.G., Kashaev E.D., Penza state university, Penza, 2000.-Dep. 31.03.00, № 869-B00.

2. Detection of attacks on information resources of a physical level of the automated systems/ Mali W.A. STC, St.-Petersburg, 2000.