

СРЕДСТВО АДАПТИВНОГО МАСКИРОВАНИЯ ВИДЕОКАДРОВ В КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

В.К. Железняк, А.В. Барков

Развитие методов и средств обнаружения и восстановления видеосигналов из шумов высокого уровня в каналах утечки информации определило обоснование разработки новых методов и средств обеспечения защищённости видеосигналов. Анализ средств маскирования выявил, что известные генераторы шума не формируют синхронных с маскируемым сигналом статических маскирующих помех для достижения положительного технического эффекта. Реализация современных методов и средств защиты видеосигналов возможна разработкой адаптивных методов их маскирования для улучшения защищённости синхронным накоплением.

Предложено средство формирования видеосуммовых кадров из хаотических импульсных последовательностей для обеспечения защищённости видеосигнала от утечки по электромагнитным каналам, которое реализует метод адаптивного маскирования статических видеок кадров систем передачи и средств вычислительной техники формированием статического (неподвижного) видеосуммового кадра.

Исследовано количественное изменение защищённости видеок кадра предложенным методом адаптивного маскирования статическим видеосуммовым кадром. Эффективность метода маскирования синхронными и адаптивными видеосуммовыми кадрами подтверждена исследованием количественного изменения защищённости видеок кадра, обосновано обеспечение лучшего качества маскирования и исключение ухудшения отношения сигнал/шум при маскировании статическими видеосуммовыми кадрами по отношению к динамическому шуму пропорционально корню квадратному отношения числа видеок кадров к количеству смен видеосуммового кадра.

Исследования подтвердили преимущества маскирования статического видеок кадра синхронными видеосуммовыми кадрами, которое по сравнению с динамическим шумом не позволяет выделить видеок кадр, уменьшает его разборчивость и повышает защищённость видеосигнала.

ИНЖЕНЕРНАЯ МЕТОДИКА ВЫЯВЛЕНИЯ ИСТОЧНИКОВ СЪЁМА ИНФОРМАЦИИ

А.Л. Матюшков, К.С. Миденко, Е.В. Свиридов

В настоящее время, в связи с участвовавшими случаями промышленного шпионажа, остро становится вопрос защиты информации на крупных предприятиях, заводах и в банках. Одним из самых распространённых способов несанкционированного съёма информации (НСИ) является использование различных радиопередающих устройств. Для выявления источников НСИ необходимы эффективные методики и мероприятия по их обнаружению. В данной работе была разработана методика, позволяющая доступными средствами осуществить поиск источников радиоизлучений в контролируемом помещении.

Исследования проводились в лаборатории БГУИР в сложной электромагнитной обстановке (ЭМО). Для измерения использовался анализатор спектра АКС-1301 фирмы АКТАКОМ, селективный вольтметр SMV 8.5 фирмы RFT, ненаправленная антенна и узконаправленная антенна УКВ диапазона, тестовые радиопередатчики на несущих частотах 65 и 434 МГц.

На начальном этапе с помощью ненаправленной антенны, составляется база всех источников излучений (ИИ) в различных частотных диапазонах, характерных для подконтрольного объекта, в разное время суток. Путём анализа данных о распределении частотного ресурса, аудио мониторинга полученной базы с помощью селективного вольтметра SMV 8.5 и отключения электроэнергии в контролируемом помещении проводится выборка потенциально «опасных» ИИ.

Далее, с помощью узконаправленной антенны и радиотриангуляционного метода, определяется их местоположение.

Методика также позволяет обнаружить и выявить местоположение передающих устройств, находящихся в смежных помещениях.

Экспериментальные исследования показали, что при использовании УКВ антенны с диаграммой направленности 30 градусов возможно определение местоположения НСИ с ошибкой не более 10%. Предложенная методика отличается простой и доступностью используемого оборудования. Студенты кафедры РТС БГУИР по указанной методике успешно осуществили поиск тестовых радиопередатчиков с неизвестными им параметрами.