

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ШИФРОВАНИЯ MPEG ВИДЕОДАНЫХ

А.А. БОРИСКЕВИЧ, И Ю. Г. КОЧУБЕЕВ

Сетевые приложения мультимедиа, такие, как Видео-По-Требованию, широкоэвещательная передача видео и видеоконференции требуют проведения исследований в области безопасности мультимедиа. Из-за особенностей мультимедийных данных возникает необходимость в разработке специальных алгоритмов шифрования MPEG видеоданных, которые должны быть одновременно высокозащищенными, высокоскоростными и не ухудшать уровень сжатия.

Стандарт MPEG является одним из наиболее универсальных принятых международных стандартов для кодирования и передачи динамических видеоизображений. Предлагается следующая классификация современных методов шифрования MPEG данных:

- 1) методы, использующие особенности формата MPEG;
- 2) методы, основанные на статистических особенностях потока MPEG;
- 3) методы, использующие возможности кодирования при шифровании MPEG видеоданных.

Рассмотрен селективный алгоритм шифрования наиболее важных частей потока MPEG (I-кадров), относящийся к первой группе. Он обеспечивает четыре уровня защиты с разным объемом шифруемой информации. Представителем второй группы является алгоритм видео шифрования (VEA), использующий шифры с разной вычислительной сложностью и обеспечивающий высокое быстродействие (на 48 % быстрее прямого шифрования), высокую защищенность. К третьей группе относится алгоритм с изменяемой моделью адаптивного кодека (ИМАК), обеспечивающий высокую скорость, защищенность и не увеличивающий исходный поток данных. Он основан на применении для каждого байта не сжатой информации своей таблицы Хаффмана.

Из сравнительного анализа следует, что более предпочтительными по всем критериям являются алгоритмы VEA и ИМАК. Они обеспечивают высокую защищенность наряду с высоким быстродействием и малым размером зашифрованного потока MPEG.

## МАГНИТНАЯ ЗАЩИТА НОСИТЕЛЯ ИНФОРМАЦИИ НА ОСНОВЕ ИМПУЛЬСНОГО МАГНИТНОГО МАРКЕРА

А.А. БОРИСКЕВИЧ, В.Я. КУЛИК

Метод защиты основан на имплантировании в материальный носитель информации маркера со специфической магнитной структурой, обеспечивающей эффект быстропротекающего перемагничивания вещества маркера. Данный эффект наблюдается в виде скачкообразного изменения намагниченности при помещении маркера в переменное магнитное поле. Магнитная структура маркера, представляющая собой два или больше доменов, намагниченных встречно, идентифицирует носитель. Под воздействием внешнего возбуждающего магнитного поля в направлении намагниченности одного из доменов при пороговом значении поля происходит спонтанное перемагничивание домена с противоположным полю исходным направлением намагниченности. Такой процесс повторяется при циклическом перемагничивании маркера.

При помещении считывающей обмотки вблизи маркера в момент его скачкообразного перемагничивания поместить в ней возбуждается импульс напряжения. Форма и другие характеристики импульса существенно зависят от материала маркера, его геометрии, способа и режимов его получения, обработки сигнала с выхода приемной катушки.

К достоинствам магнитной защитной маркировки на основе импульсного магнитного маркера следует отнести стабильность параметров регистрируемого импульса напряжения, технологичность получения и встраивания маркера в корпус носителя, высокую надежность, объективность и бесконтактность контроля подлинности.

## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА АТС

Д.В. ШИПОВАЛОВ

В докладе рассматриваются некоторые аспекты обеспечения информационной безопасности АТС, которая должна достигаться с помощью системы комплексной защиты информации (КЗИ) от перехвата информации в каналах связи, несанкционированного доступа к информации, утечки информации по побочным каналам, внедрения специальных технических устройств перехвата информации, программно-технических воздействий и программ-вирусов. Исследуются вопросы защиты от наличия в составе программного обеспечения (ПО) возможных программных закладок (ПЗ), активация которых может дезорганизовать работу как отдельной станции, так и всей сети.

Рассматривается необходимость реализации на АТС ряда эксплуатационных правил, регламентирующих периодическое выполнение копирования на специально выделенный внешний носитель (ВНН) рабочих областей оперативного запоминающего устройства (ОЗУ), станционных управляющих устройств, а также областей ОЗУ, хранящих программы, текущие переменные и постоянные данные о ресурсах станции и системы.