

концентрация наночастиц 10%, частота ФМР — 42 ГГц, удельная проводимость массива 100–120 (Ом м)<sup>-1</sup>.

Показано, что магнитная проницаемость массива УНГ в X области нелинейно зависит от частоты, причем ее реальная и мнимая части растут с увеличением частоты. В K<sub>d</sub> диапазоне эти зависимости переходят в немонотонные. Полученные результаты говорят о наличии магнетизма углеродной подсистемы, который вероятно носит индуцированный характер.

## **ВОДОСОДЕРЖАЩИЕ ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ ДЛЯ ЗАЩИТЫ РАДИОЭЛЕКТРОННОЙ АППАРАТУРЫ**

С.Э. САВАНОВИЧ, В.Б. СОКОЛОВ

При обработке, передаче и хранении конфиденциальной информации с помощью технических средств наиболее актуальными являются вопросы, связанные с уменьшением уровней излучений применяемых устройств по информационным каналам.

Одним из методов защиты утечки информации по электромагнитным каналам является экранирование, как отдельных блоков аппаратуры, так и помещения в целом, которое осуществляется с помощью различных металлических экранов и сеток, специальных тонкопленочных покрытий, ферритовых и полупроводниковых материалов, материалов с различными диэлектрическими и магнитными потерями, а также влагосодержащих материалов.

Наиболее перспективными поглощающими материалами являются конструкции экранов на основе водных растворов и их включений.

В качестве экранирования излучающих блоков технических средств и помещений применялся экран, в виде стеклопакета, заполненного жидким раствором наполнителем на основе воды.

Основным недостатком поглотителей на основе водосодержащих материалов является большой вес конструкции при увеличении её размера и необходимость герметизации. Уменьшения массы конструкции можно достичь применением материалов с меньшей удельной плотностью, содержащих газовую (воздушную), жидкую или твердую фазы.

Для минимизации массы и сохранения поглощающих свойств исследуемого экрана, были проведены исследования аналогичной конструкции, объем которой заполнялся строительным материалом с размером фракций от 0,01–0,02 м.

В результате исследований поглощающих свойств предлагаемой конструкции можно сделать следующие выводы:

– массогабаритные размеры предлагаемой конструкции уменьшились в два раза по сравнению с конструкцией, заполненной жидким раствором наполнителем на основе воды;

– значения коэффициентов отражения и прохождения практически не изменяются во всем диапазоне измеряемых частот.

## **ВЛИЯНИЕ УСЛОВИЙ ФОРМИРОВАНИЯ ДИЭЛЕКТРИЧЕСКИХ ПЛЕНОК НА ИХ ОДНОРОДНОСТЬ**

С.М. САЦУК, М.М. ПИНАЕВА

Электрическая прочность диэлектрика связана с однородностью анодных оксидных пленок (АОП) по толщине. Для исследования влияния природы редкоземельных металлов (РЗМ), рН и концентрации пирофосфорной кислоты на однородность АОП по толщине исследовали зависимость электродного потенциала (ЭП) от толщины АОП.

Исследовали зависимости ЭП от толщины АОП, сформированных при напряжении 10 В и содержащих иттербий, европий и гадолиний. Полученные кривые свидетельствуют о неоднородности по толщине всех рассматриваемых АОП. Условно кривые можно

разделить на несколько характерных участков, характеризующих определенную область в АОП, каждая из которых имеет свою среднюю скорость травления. Можно выделить три характерных участка на кривых. Первый участок — вблизи границы раздела «оксид-электролит», второй участок, где ЭП постоянен и диэлектрическая пленка однородна по толщине и третий участок — вблизи границы раздела «оксид-металл».

Анализ полученных результатов позволяет говорить о том, что первый участок представляет собой область с максимальным количеством внедренных анионов. Причем в этой области наблюдается резкое уменьшение ЭП при приближении к границе раздела «оксид-электролит». Такой вид кривой характерен и для профиля распределения РЗМ в АОП. Скорость травления области АОП (Eu) в семь раз ниже, чем у АОП (Yb) и АОП (Gd). По мере травления первого участка АОП ЭП уменьшается и принимает значение  $-1,2$  В, что соответствует потенциалу «чистого» оксида.

Исследования также показывают, что толщина однородного или «чистого» оксида зависит от состава электролита и его рН. Наибольшей толщине «чистого» оксида соответствует рН формовочного электролита 4,0 независимо от природы РЗМ, а наилучшим элементом с этой точки зрения является европий, у которого толщина однородной области составляет 74% при концентрации кислоты 1 масс. %.

## **ЛАВИННЫЙ ЭФФЕКТ В АЛГОРИТМАХ ШИФРОВАНИЯ НА ОСНОВЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ**

К.С. МУЛЯРЧИК

Одним из условий обеспечения стойкости алгоритма шифрования к дифференциальному криптоанализу, является наличие в преобразованиях лавинного эффекта. Суть эффекта заключается в значительном — «лавинном» — изменении бит в выходной последовательности преобразования при малом изменении («возмущении») бит во входной последовательности преобразования по сравнению с исходными («невозмущенными») значениями.

Выделяют несколько критериев стойкости алгоритма шифрования, основанные на лавинном эффекте: лавинный критерий (AVAL) — требует изменения в среднем половины бит в зашифрованном значении при изменении каждого отдельно взятого бита в исходном значении; строгий лавинный критерий (SAC) — требует изменения с вероятностью  $\frac{1}{2}$  каждого отдельно взятого бита в выходном значении при изменении каждого отдельно взятого бита во входном значении. При анализе алгоритма шифрования указанные критерии могут быть применены, в общем случае, как к S-блоку (таблице подстановки, дискретному отображению), так и к базовому преобразованию.

В данной работе представлены результаты исследования значений «лавинных параметров» — численные значения отклонения вероятностей изменения бит в выходной последовательности от требуемого значения, равного  $\frac{1}{2}$ . Данные параметры являются более наглядной характеристикой степени лавинного эффекта в преобразовании.

В результате проведенных исследований — при анализе характера лавинного эффекта в паре «входное значение — выходное значение» обусловлен выбор базового преобразования в виде дискретного тент-отображения. Этот же вид хаотического отображения выбирается при анализе характера лавинного эффекта в паре «управляющий параметр — выходное значение» в процессе генерации раундовых ключей.