При истощении ключевого набора Памяти раньше, чем выполнится очередная синхронизация модулей, используется преобразование F_3, которое позволяет существенно расширить набор сеансовых ключей с небольшим понижением их криптографических характеристик и обеспечить непрерывность работы.

Цикл формирования сеансовых ключей повторяется необходимое количество раз. Обновление набора сеансовых ключей происходит аналогичным образом.

В некоторых случаях качестве преобразований F_1 и F_2 (в зависимости от требуемых свойств информации) может выступать одно из простейших преобразований: побитовое сложение, арифметическое сложение (по mod 2^n), операция циклического сдвига, – или их комбинации, что позволяет существенно повысить производительность алгоритма по сравнению с известными алгоритмами шифрования и обеспечить при этом достаточную стойкость. При использовании более сложного набора преобразований стоит учитывать, что необходимый объем вычислений приводит к потере производительности всей системы в целом.

Несмотря на отсутствие у представленного алгоритма аналога S-блокам, требуется значительный объем дополнительной памяти для хранения сеансовых ключей шифрования. Однако при использовании функции расширения это можно расценивать и как преимущество, т.к. большой объем исходной ключевой последовательности позволяет значительно увеличить количество сеансовых ключей, хранящихся в Памяти.

Необходимость процедуры синхронизации возникает только в том случае, если произошел сбой в канале связи, нарушен протокол обмена, обнаружены атаки на подсистему. Благодаря сопутствующей функции взаимной аутентификации легко обнаруживаются нарушения нормального функционирования информационного обмена.

Заключение. Представленный алгоритм имеет малое количество операций, что повышает общее быстродействие устройства, снижает энергопотребление; позволяет синхронизировать сеансовые ключи.

Применение методов расширения ключевой последовательности в большинстве случаев позволит избежать преждевременной процедуры обновления набора ключей.

Предлагаемый алгоритм может служить концептуальной и логической основой для построения эффективной подсистемы защиты информации в каналах передачи и позволит эффективно распознавать и предотвращать различные кибератаки, включая jackpotting-атаки.

1. Шеннон К. Работы по теории информации и кибернетике. Теория связи в секретных системах. – М.: ИЛ, 1963. – С. 333-369.
2. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. – 2015. – № 1 (9). – С. 26–43.
3. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. – 2015. – № 2 (10). – С. 2–10.
4. Островский Д.Е., Рафиков А.Г. Криптозащищенный микроконтроллер // 3-я Международная научно-техническая конференция. – М., 2012.
5. Островский Д.Е., Рафиков А.Г. Генератор истинно случайных чисел // 3-я Международная научно-техническая конференция. – М., 2012.
6. Rukhin A, Soto J, Nechvatal J. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST special publication 800-22, 2010.
7. Сабанов А.Г. Обзор технологий идентификации и аутентификации // Документальная электросвязь. – 2006. – № 17. – С. 23–27.
8. Сабанов А.Г. Аутентификация как часть единого пространства доверия // Электросвязь. – 2012. – С. 40–44.
9. Деднев М.А., Дыльнов Д.В. и др. Защита информации в банковском деле и электронном бизнесе. – М.: КУДИЦ-ОБРАЗ, 2012. – 512 с.
10. Кривченко И. Аппаратно-защищенные микросхемы семейства Crypto Authentication: потенциальные применения ATSHA204A // Компоненты и технологии. –2015. – № 10. – С. 87–93.
11. Jan Axelson. USB Complete: The Developer's Guide (Complete Guides series). Lakeview Research, English, 2015. ISBN/ASIN: 1931448280, ISBN13: 9781931448284.
12. NIST S. Guide to Integrating Forensic Techniques into Incident Response. 2006. – P. 80-86.

УДК620.130

ГИСТЕРЕЗИСНЫЕ МЕТОДЫ КОНТРОЛЯ ОБЪЕКТОВ В ИМПУЛЬСНЫХ МАГНИТНЫХ ПОЛЯХ

Павлюченко В.В., Дорошевич Е.С.
Белорусский Национальный Технический Университет
Минск, Республика Беларусь

Контроль свойств объектов с помощью пленочных преобразователей магнитного поля и расчеты магнитных полей описаны в [1–4]. Определение удельной электропроводности и магнитной проницаемости объектов, а также их толщины и параметров дефектов в них осуществлено в работах авторов в импульсных магнитных полях с применением разработанных гистерезисных методов контроля [5–8]. Целью работы является повышение точности измерения магнитных полей и контроля свойств объектов путем использования численных расчетов,

проводимых предварительно, в данном случае с помощью программного языка Delphi [9].

На электропроводящий объект с приложенным к его поверхности преобразователем магнитного поля воздействовали одиночными импульсами магнитного поля различной амплитуды H_{0m} и конфигурации и определяли величину максимальной напряженности магнитного поля H_m вблизи поверхности исследуемого объекта. Импульсное магнитное поле создавали линейными, плоскими и объемными источниками.

Датчики магнитного поля изготавливали из магнитного носителя (МН). При этом использовали как сплошные, так и дискретные датчики магнитного поля (ДДМП), представляющие собой набор магнитных полос из МН, жестко укрепленных на немагнитной основе.

Воздействие на ДДМП осуществляли серией одиночных импульсов магнитного поля с чередующейся полярностью и получали на датчике распределения остаточных магнитных полей, по которым определяли свойства объектов. Информацию с ДДМП считывали индукционной магнитной головкой (МГ), на выходе которой получали зависимость $U=U(t)$ величины электрического U напряжения от времени t.

Контролировали объекты из алюминия, меди, свинца и других металлов. В качестве МН использовали магнитные ленты разного типа, магнитооптическую пленку, магнитные флюкс детекторы и другие преобразователи магнитного поля. На ДДМП производили запись суммарной напряженности магнитного поля $H_{\Sigma m}$. Путем сканирования ДДМП магнитной головкой, подключенной к входу цифрового осциллографа, находили величину индуцированного МГ напряжения, по которой в соответствии с градуировочными характеристиками МН определяли величину $H_{\Sigma m}$.

Точность определения свойств объекта значительно повышали за счет применения разработанных гистерезисных методов контроля в импульсных магнитных полях. Рассчитаем величину тангенциальной составляющей напряженности магнитного поля по линии замера, перпендикулярной оси линейного индуктора, в направлении x от проекции его оси по формуле:

$$H_1=100(x^2+1). \qquad (1)$$

Здесь x измеряется в cm, а H_1 – в А/cm. Расстояние от оси излучателя до МН равно 1 cm. Зависимость (1) показана на рис.1 (кривая 1).

На рис.1 показано также распределение импульсного магнитного поля, вызванного локальной неоднородностью в объекте (зависимость 2).

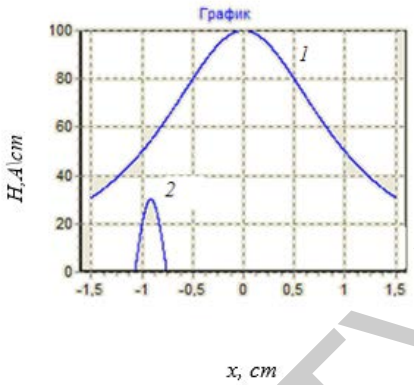

Рисунок 1 – Зависимость величины напряженности магнитного поля H от расстояния x до проекции оси излучателя

Осуществим записи поля на магнитный носитель с использованием его гистерезисной ветви. Пусть величина электрического напряжения $U_m = U_m(x)$, снимаемого с преобразователя магнитного поля, принимает попеременно значения $U_m = 25$ mv и $U_m = -25$ mv.

Зададим интервал следования разнополярных импульсов относительно напряженности магнитного поля равный $H_1 = 5$ А/cm.

Тогда функции (1) на рис. 1 будет соответствовать штрихкодовое распределение электрического напряжения в виде прямоугольных полос, показанное на рис. 2.

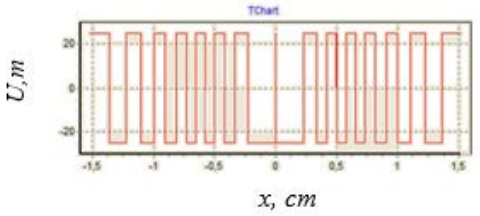

Рисунок 2 – Штрихкодовое распределение электрического напряжения

Если на каком-то участке зависимости, содержащей информацию о свойствах объекта, величина напряженности магнитного поля отличается от параметров зависимости 1, то прямоугольные участки будут сдвинуты относительно начальной зависимости. Разность штрих-кодовых линий на этих участках будет характеризовать изменение величины напряженности магнитного поля и, следовательно, параметры неоднородности объекта.

Так, штрихкодовое распределение прямоугольных полос, изображенное на рисунке 3, соответствует суммарному полю зависимостей 1 и 2 на рис. 1.

По ширине указанных штрихов и их местоположению определяют параметры неоднородных магнитных полей и параметры неоднородностей структуры в объекте. Метод

применим для магнитных, электрических и любых других полей.

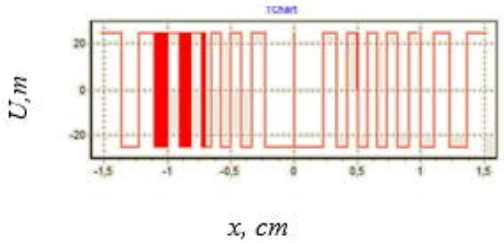

Рисунок 3 – Штрихкодовое распределение электрического напряжения

1. Новиков, В.А., Кушнер, А.В., Шилов, А.В Магнитографический контроль объектов при их намагничивании перемещаемым постоянным магнитом через магнитоноситель. Схемы намагничивания / В.А. Новиков, А.В. Кушнер, А.В. Шилов // Дефектоскопия. – 2010. – № 6. – С.30–35
2. Грузинцев, А.А., Михайлов, С.П. Самосогласованный расчет магнитного поля для задач магнитной дефектоскопии. I. Исходная модель для расчета поля магнитной ленты, намагниченной от проводника с током. / А.А. Грузинцев, С.П. Михайлов // Дефектоскопия. – 2011. – № 2. – С.22–30.
3. Суханов, Д.Я., Совпель, Е.С. Магнитоиндукционный интроскоп для дефектоскопии металлических объектов / Д.Я. Суханов, Е.С. Совпель // Дефектоскопия. – 2015. – № 5. – С.56-62.
4. Новиков, В.А. , Шилов, А.В., Кушнер, А.В. Визуализация полей дефектов ферромагнитных объектов с помощью пленки “Flux-detector” / В.А. Новиков, А.В. Шилов, А.В. Кушнер // Контроль. Диагностика. – 2010. – № 5. – С. 18-22.
5. Павлюченко, В.В., Дорошевич, Е.С. Одним импульсом / В.В. Павлюченко, Е.С. Дорошевич – LAP LAMBERT Academic Publishing, 2013. – 174с.
6. Павлюченко, В.В. Неразрушающий контроль объектов из электропроводящих материалов в импульсных магнитных полях / В.В. Павлюченко, Е.С.Дорошевич // Дефектоскопия. – 2010. – № 11. – С. 29-40.
7. Павлюченко, В.В. Использование магнитного гистерезиса при контроле объектов из электропроводящих материалов в импульсных магнитных полях / В.В. Павлюченко, Е.С.Дорошевич // Дефектоскопия. – 2013. – № 6. – С. 53-68.
8. Павлюченко, В.В. Расчет распределений остаточных магнитных полей при гистерезисной интерференции импульсного магнитного поля / В.В. Павлюченко, Е.С.Дорошевич, В.Л. Пивоваров // Дефектоскопия. – 2015. – №1. – С. 11-20.
9. Фленов, М. Библия Delphi / М. Фленов ,СПб: БХВ-Петербург, 2011, – 688с.

E-mail: es_doroshevich@mail.ru

УДК 681.7.069.3

ДАТЧИКИ КОНТРОЛЯ СВОЙСТВ СМАЗОЧНЫХ МАСЕЛ

Баранов В.В., Батурля И.В., Кузьмич А.И., Петрович В.А., Серенков В.Ю., Шахлевич Г.М.
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Методы диагностирования состояния силовых агрегатов по параметрам используемых масел базируется на том, что масла являются неотъемлемым компонентом узлов трения. Это обусловливает актуальность задачи разработки конструкции датчиков, способных контролировать эксплуатационные параметры жидких сред (масел) по зависящим от них электрофизическим характеристикам.

В настоящее время базовым подходом к созданию датчиков контроля характеристик жидких диэлектриков, в том числе масел, является использование емкостных ячеек, которые позволяют на различных частотах зондирующего сигнала получать отклик, содержащий конкретную информацию о диэлектрических потерях.

В качестве контролируемого параметра масел в настоящее время используется измерение тангенса угла потерь (tgδ).

Ранее нами исследованы зависимости tgδ масла марки М14В2 с использованием конструкции конденсатора с плоскопараллельными никелевыми пластинами [1, 2].

В настоящей работе использованы дополнительно иные разновидности емкостных датчиков (на рисунке 1 показаны в центре и справа):

– плоскопараллельный конденсатор, в качестве обкладок которого использовалась сетка с ячейкой 1 × 1 мм. Сетка представляет собой стальной каркас, гальванически покрытый цинком;

– конденсатор с коаксиальными спиралевидными медными обкладками.

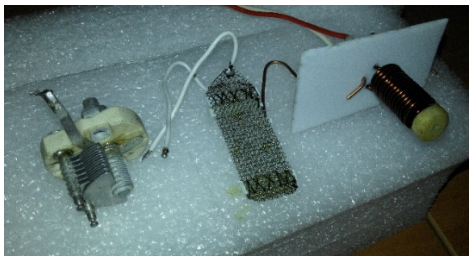

Рисунок 1 – Общий вид датчиков

Недостаток ранее использованного датчика – анизотропия скорости смены диэлектрической среды (масла) между сплошными обкладками в процессе измерения относительно осей координат обкладок. По осям *X, Y* смена масла проблем не вызывает, а по оси *Z*, перпендикулярной