ется ухудшение эксплуатационных показателей смазочного масла, засорение масляных фильтров и отсутствие теоретически обоснованной системы контроля технического состояния ДЭС с элементами прогнозирования.

В третьей главе рассмотрены принципы построения самоочищающихся систем смазки, разработаны и предложены их математические модели, а также приведены результаты математического моделирования.

Четвертая глава посвящена синтезу самоочищающихся систем смазки, изменения её параметров при различных значениях и характерах нагрузки в процессе эксплуатации. Приведены результаты исследования изменения гидравлических сопротивлений масляных фильтров в процессе их загрязнения и регенерации.

В пятой главе рассмотрены вопросы диагностирования технического состояния ДЭС по параметрам элементов системы смазки. Приведены исследования частотных характеристик очистителей на испытательном стенде и при натурных испытаниях на экспериментальной установке. Предложена методика оценки технического состояния ДЭС по параметрам элементов системы смазки.

Шестая глава посвящена информационной системе мониторинга и прогнозирования технического состояния ДЭС. Предложены методические основы прогнозирования информационных параметров ДЭС и разработаны алгоритмы сбора данных системы мониторинга и прогнозирования параметров ДЭС. Предложены модели данных информационных систем и алгоритмы прогноза. Приведена оценка экономической эффективности применения информационных систем мониторинга и прогнозирования параметров ДЭС.

Настоящее издание предназначено для инженеров и предпринимателей, работающих на российском рынке средств автономной и резервной энергетики, а также может быть использовано как учебное пособие для технических вузов, занимающихся вопросами электроснабжения или его управлением.

СИЛОВЫЕ ПОЛУПРОВОДНИКОВЫЕ ВЫПРЯМИТЕЛИ НА ОСНОВЕ МНОГОФАЗНЫХ ТРАНСФОРМАТОРОВ С ВРАЩАЮЩИМСЯ МАГНИТНЫМ ПОЛЕМ (монография)

Атрощенко В.А., Сингаевский Н.А.

Кубанский государственный технологический университет, Краснодар, e-mail: isemenuta@rambler.ru

В монографии изложены схемотехнические основы построения многофазных трансформаторов и силовых полупроводниковых выпрямителей (СППВ) на их основе.

Рассмотрены перспективные конструкции многофазных трансформаторов с вращающимся магнитным полем (ТВП), особенности технологии их изготовления и расчета.

Дано описание математической модели СППВ на основе ТВП, базирующейся на классических методах расчета электромагнитных преобразователей электрической энергии.

В настоящее время СППВ мощностью от единиц до нескольких сотен киловатт относятся к наиболее востребованным типам преобразователей электрической энергии.

Источники бесперебойного питания компьютерных систем, систем автоматики и телемеханики, радиотехнических комплексов, источники питания оперативных цепей подстанционного оборудования, электропривода постоянного тока, сварочного оборудования, систем электрохимической защиты металлических подземных сооружений от коррозии – вот не полный перечень оборудования и систем, в составе которых используются эти преобразователи. При этом область их применения постоянно расширяется.

Большинство современных СППВ выполняются по трехфазным мостовым схемам, которые, с одной стороны, представляют собой симметричную нагрузку по отношению к трехфазной сети, а с другой – в меньшей степени подвержены влиянию ассиметрии питающих напряжений.

Вместе с тем известно, что выпрямители с трехфазными мостовыми схемами имеют низкий коэффициент мощности (не более 0,7) и являются мощными источниками кондуктивных помех. Поэтому применение СППВ, особенно в системах электроснабжения с источниками соизмеримой мощности, создают серьезные проблемы в части их электромагнитной совместимости с электроустановками этих систем.

Одним из перспективных способов повышения уровня электромагнитной совместимости силовых полупроводниковых выпрямителей и улучшения качества преобразования трехфазного переменного тока в постоянный, является увеличение фазности выпрямления за счет использования в составе СППВ, так называемых, преобразователей числа фаз – многофазных трансформаторов.

В настоящей монографии рассмотрены принципы построения многофазных трансформаторов на примерах известных технических решений. На основе анализа этих решений в качестве перспективного многофазного трансформатора для СППВ предложен трансформатор с вращающимся магнитным полем.

Дано описание ряда конструкций ТВП и особенностей технологии их изготовления.

Изложены основы расчета силовой части СППВ на основе ТВП, в которых учтен многолетний практический опыт авторов монографии в разработке, изготовлении и экспериментальных исследований различных конструкций ТВП.

Издание состоит из пяти глав. В первой главе рассмотрены вопросы качества электроэнергии и электромагнитной совместимости в системах электроснабжения с СППВ. В качестве выводов отмечено, что причиной снижения качества электроэнергии является нелинейные искажения потребляемых токов и пульсации выпрямленного напряжения. Одним из направлений повышения качества электроэнергии является повышение фазности выпрямления.

Вторая глава посвящена принципам формирования многофазного напряжения. Охарактеризованы пять принципов формирования многофазного напряжения, одним из которых является применение трансформаторов с вращающимся магнитным полем.

В третьей главе рассмотрены конструктивные схемы и технология изготовления ТВП. Рассмотрены различные варианты схем построения магнитопроводов и обмоток ТВП, приведены результаты математического моделирования и экспериментальных исследований.

Четвертая глава посвящена особенностям работы ТВП в составе СППВ, методике расчета параметров магнитопроводов и выбору обмоток ТВП.

В пятой главе рассмотрены вопросы математического моделирования ТВП и СППВ на его основе, базирующиеся на классических методах расчетов электромагнитных преобразователей электрической энергии.

Настоящее издание предназначено для специалистов в области силовой преобразовательной техники, аспирантов и студентов электротехнических специальностей высших учебных заведений.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (учебное пособие)

Бабенко Л.К., Ищуковой Е.А.

Южный федеральный университет, Ростов-на-Дону, e-mail: jekky82@mail.ru

Учебное пособие по курсу «Криптографические методы и средства обеспечения информационной безопасности» опубликовано в 2011 году в издательстве ТТИ ЮФУ, Таганрог. Текст пособия изложен на 148 страницах, имеет 53 рисунка, 33 таблицы и 9 библиографических ссылок. Рецензентами пособия являются д.т.н., профессор, профессор ТГПИ им. Чехова Ромм Я.Е. и д.т.н., профессор, профессор ТГПИ им. Чехова Витиска Н.И. Пособие посвящено изучению алгоритмов блочного шифрования: принципов их построения и анализа. Рассматриваются способы проведения атак на блочные симметричные алгоритмы шифрования с помощью таких методов криптоанализа, как линейный и дифференциальный криптоанализ.

Современная криптография основана на понятии односторонней функции $f(x)$. Не вдаваясь в формальные математические определения, отметим одно ее свойство: инвертировать функцию, т. е. вычислить x, зная только $f(x)$, крайне сложно. Стойкость шифров, помимо собственно алгоритма шифрования, во многом определяется и длиной ключа. Современная криптография исходит из того, что сам алгоритм рано или поздно все равно станет известен противнику. Все сообщения, передаваемые по открытым каналам связи, могут быть перехвачены, так что ключ шифра остается его единственным секретом.

Современные алгоритмы блочного шифрования разрабатываются таким образом, чтобы аналитик имел как можно меньше шансов отыскать секретный ключ, с помощью которого были зашифрованы данные, даже если ему известен сам алгоритм шифрования и есть в наличии несколько текстов и соответствующих им шифртекстов. Приступая к задаче анализа, первым делом аналитик определяет тот набор данных, который ему изначально известен.

Так, если известен алгоритм шифрования и есть хотя бы одна пара открытый – шифрованный текст, то самым естественным способом анализа, который сразу приходит в голову, является последовательное опробование всех возможных вариантов ключа, которые могли быть использованы. Опробование производят до тех пор, пока зашифрование открытого текста на очередном ключе не приведет к получению имеющегося шифрованного сообщения. Такой способ анализа в разных источниках литературы имеет разные названия, например «Метод полного перебора или «Метод грубой силы» или «Метод атаки в лоб» или «Brut-force атака». У этого метода анализа есть одно неоспоримое преимущество: рано или поздно искомый ключ будет найден и для этого будет необходим минимальный набор данных. Быстрота нахождения секретного ключа будет зависеть от его длины и от вычислительной мощности, которая есть в наличии у аналитика. А также от доли везения. Ведь может случиться так, что искомый ключ встретится одним из первых. В работе достаточно подробно описано как оценивать сложность подобного рода анализа.

В криптографии принято время анализа с помощью метода полного перебора считать эталонным. Это значит, что если аналитику удастся провести анализ алгоритма шифрования быстрее, чем это можно сделать с помощью полного перебора, то данный алгоритм шифрования будет считаться уязвимым, в связи с чем его использовать для шифрования данных будет нецелесообразно.

Вначале 90-х годов прошлого века были предложены два способа анализа алгоритма шифрования DES, которые позволяли осуществлять атаку быстрее, чем это можно было