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

бы сделать с помощью метода полного перебора. Метод линейного криптоанализа (linear cryptanalysis) был предложен японским ученым М. Матсуи и позволял проводить анализ путем опробования 2^{47} пар текстов, зашифрованных на одном секретном ключе. Следует отметить, что хоть степенной показатель в количестве опробований сократился со значения 56 до значения 47, возникло условие практически невыполнимое – наличие огромного объема информации, зашифрованной на одном и том же ключе! Метод дифференциального криптоанализа (differential cryptanalysis) был предложен Э. Бихамом и А. Шамиром. С помощью этого метода сложность анализа сократилась до 2^{37}. Однако опять же, для проведения анализа необходимо было иметь 2^{37} особым образом подобранных текстов, зашифрованных на одном и том же секретном ключе. Не смотря на накладываемые ограничения в использовании новых предложенных методов анализа – это был прорыв. Дальнейшее развитие этих методов показало возможность их применения к целому классу блочных шифров, позволило выявить слабые места других используемых алгоритмов шифрования. Сегодня оба эти метода, а также некоторые их усовершенствования, например, линейно-дифференциальный метод, метод невозможных дифференциалов, широко используются для оценки стойкости вновь создаваемых шифров. Именно поэтому специалисту по защите информации необходимо иметь представление о механизмах анализа блочных шифров с использованием современных методов криптоанализа.

Для того, чтобы научиться применять методы анализа на практике, необходимо что называется «в живую потрогать» их, то есть иметь возможность применить эти методы к блочному шифру от начала и до конца, начиная с анализа самого алгоритма шифрования и заканчивая получением секретного ключа. Встает вопрос: а как это лучше всего сделать? Если использовать какой-либо известный алгоритм шифрования, то это будет трудоемкая, практически невыполнимая задача. В 2003 году авторами был разработан целый комплекс лабораторных работ по изучению современных методов криптоанализа блочных шифров. В основу его было положено использование простых учебных алгоритмов шифрования. В состав комплекса вошли работы по изучению методов линейного и дифференциального криптоанализа блочных шифров, имеющих различные схемы построения (схему Фейстеля, и сеть SPN), а также работа по изучению метода слайдовой атаки (slide attack). В течение пяти лет данные лабораторные работы были опробованы на кафедре Безопасности Информационных Технологий тогда еще Таганрогского радиотехнического университета (ТРТУ), а ныне Таганрогского технологического института Южного федерального университета (ТТИ ЮФУ). Сами лабораторные работы были довольно подробно представлены в учебном пособии «Современные алгоритмы шифрования и методы их анализа», вышедшем в 2006 году в издательстве Гелиос АРВ. За время использования данных лабораторных работ были выявлены существенные недостатки, как в самом используемом Учебном алгоритме шифрования, так и в изложении материала, что побудило нас коренным образом переработать и усовершенствовать материал для лучшего понимания механизмов работы методов анализа криптосистем. В настоящем учебном пособии представлено подробное описание механизмов работы методов линейного и дифференциального анализа блочных алгоритмов шифрования. Для закрепления навыков используются две работы по поиску секретного ключа шифрования на основе изученных методов анализа с применением специально разработанного учебного алгоритма шифрования.

Пособие рассчитано на студентов специальностей 090103, 090104. Изучив данное пособие, студенты смогут самостоятельно применять полученные знания на практике, разрабатывая новые стойкие алгоритмы шифрования.

НАНОТЕХНОЛОГИИ В ЭНЕРГЕТИКЕ (учебное пособие)

Беззубцева М.М., Волков В.С.

Санкт-Петербургский государственный аграрный университет, Санкт-Петербург, e-mail: mysnegana@mail.ru

Рецензенты: Ракутько С.А., д-р техн. наук, профессор СПбГАУ; Орлов В.В., д-р техн. наук, профессор СПбГУНТиПТ.

Переход на стандарты третьего поколения предусматривает внедрение в учебный процесс инновационных дисциплин, отвечающих запросам отрасли и реализующих выполнение законов РФ и международных стандартов ИСО: ФЗ РФ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации»; стандарты серии управления энергоэффективностью BS EN 16001:2009 и ISO 50001, Федеральный закон от 29 декабря 2006 года № 264-ФЗ «О развитии сельского хозяйства», постановления Правительства Российской Федерации от 14 июля 2007 года № 446 «О Государственной программе развития сельского хозяйства и регулирования рынков сельскохозяйственной продукции, сырья и продовольствия на 2008–2012 годы», постановления от 2011 г., «Стратегия инновационного развития агропромышленного комплекса российской Федерации на период до 2020 года».

Подготовка кадрового обеспечения решения отраслевой проблемы повышения энергоэф-