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-

фективности (приоритетный в АПК) будет результативной только после целенаправленного функционирования набора изучаемых дисциплин и их содержания.

Дисциплина «Нанотехнологии в энергетике» органично сочетается и образует логичную взаимосвязанную целостность с дисциплинами по выбору студента профессионального цикла ООП бакалавриата «Агроинженерия» (профиль «Электрооборудование и электротехнологии в сельском хозяйстве»).

Целью учебного пособия «Нанотехнологии в энергетике» является формирование у студентов системы компетентных знаний в области понятий, методов и приемов, применяемых при изучении, проектировании и производстве наноструктур, устройств и систем, включающих целенаправленный контроль и модификацию формы, размера, взаимодействия и интеграции составляющих их наномасштабных элементов, способствующих улучшению (либо появлению) дополнительных эксплуатационных и/или потребительских характеристик и свойств получаемых продуктов для энергетики АПК, ознакомление студентов с современными достижениями в области наноиндустрии и перспективами их использования.

Особое внимание в учебном пособии уделено формированию мировоззрения интеграции фундаментальных исследований и современных достижений науки и техники в области нанотехнологий в профессиональную деятельность будущих специалистов; формированию мировоззрения принятия нестандартных научно-обоснованных решений при внедрении в практику производства инновационных разработок по нанотехнологиям, обеспечивающих реализацию Государственных программ и международных стандартов ИСО.

Учебное пособие состоит из предисловия, 4 глав и библиографического списка.

Главы учебного пособия:

– общие определения и межотраслевая классификация нанотехнологий,

– физические основы нанотехнологий,

– принципы моделирования и методы измерений наносистем,

– применение, стадии развития и внедрения нанотехнологий в сфере энергетики.

В первой главе на основе анализа международного опыта и практики в организации научных исследований, стандартизации и статистического учета приведены базовые определения нанотехнологий и проект классификации их направлений. Во второй главе достаточно компактно, доступно и на высоком научном уровне представлена обзорно-аналитическая информация о физических основах нанотехнологий, обоснованы приоритетные направления научных исследований. Третья глава является логическим продолжением и посвящена вопросам моделирования и измерений наносистем. Приведены и проанализированы методы и приемы, применяемые при изучении, проектировании и производстве наноструктур для нужд энергетики. В четвертой главе представлены тенденции и перспективы развития нанотехнологий в теплоэнергетике, в электроэнергетике, в альтернативной и солнечной энергетике. Проанализированы коммерческие перспективы от внедрения нанотехнологий по секторам отрасли.

Актуальность и степень освещения практических вопросов достаточна для их применения в энергетической сфере производств АПК. С методической точки зрения учебное пособие отличается взаимосвязанностью глав, доступностью изложения, наличием примеров и визуального материала. В учебном пособии даны точные определения и формулировки с использованием общепринятой терминологии. Уровень изложенного материала соответствует современным достижениям в области нанотехнологий для энергетики. Список литературы достаточно полно освещает вопросы рассматриваемых разделов.

Учебное пособие предназначено для бакалавров по направлению «Агроинженерия», профиль «Электрооборудование и электротехнологии». Представляет интерес для инженеров и специалистов теплоэнергетиков и электроэнергетиков агропромышленного комплекса. Вне сомнения учебное пособие «Нанотехнологии в энергетике» также может быть рекомендовано для заочного и дистанционного обучения.

ИССЛЕДОВАНИЕ ВИБРОУСТОЙЧИВОСТИ ПРОДОЛЬНОГО ТОЧЕНИЯ НЕЖЕСТКИХ ВАЛОВ (монография)

[1]Васильевых С.Л., [2]Саитов В.Е.

[1]ФГБОУ ВПО «Вятский государственный университет», Киров;
[2]ФГБОУ ВПО «Вятская государственная сельскохозяйственная академия», Киров,
e-mail: vicsait-valita@e-kirov.ru

Среди большого многообразия деталей машин свыше 30% занимают детали по форме тел вращения. Такие детали условно делят на три типа в зависимости от соотношения длины L к наибольшему наружному диаметру D. При $L/D > 1$ это валы, оси, шпиндели, штоки, гильзы, стержни, стволы и т. п.; при $2 > L/D > 0{,}5$ включительно – втулки, стаканы, пальцы, барабаны и др., при $L/D < 0{,}5$ включительно – диски, кольца, фланцы, шкивы и т.п.

Наиболее трудоемкими из них при изготовлении являются детали, обладающие малой жесткостью, особенно нежесткие валы.

К нежесткими относятся валы, собственная податливость которых значительно превышает податливость технологической системы. Отношение длины L к диаметру D таких валов