

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Пярин В.А., Кузьмин А.С., Смирнов С.М.* Безопасность электронного бизнеса. – М.: Гелиос АРВ, 2009. – 432 с.
2. *Девятков А.С.* Электронные деньги и платежные системы. Краткий справочник. – М.: АСТ-Пресс, 2008. – 319 с.
3. *Захарченко В.С.* Деньги виртуального мира // Банковский форум Банкир.Ру – 14.03.2005 - <http://bankir.ru/analytics/it/3/27881>.
4. *Лейман Р.Д.* Электронные деньги. – М.: Дрофа, 2006. – 284 с.
5. *Калмыков И.А., Дагаева О.И.* Разработка псевдослучайной функции повышенной эффективности // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 160-169.
6. *Панасенко С.В.* Алгоритмы шифрования. – М.: БХВ-Петербург, 2009. – 576 с.
7. *Бабаи А.В., Шанкин Г.П.* Криптография / Под ред. В.П. Шерстюка. – М.: СОЛОН-ПРЕСС, 2007. – 512 с.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Калмыков Игорь Анатольевич – Институт информационных технологий и телекоммуникаций Северо-Кавказского федерального университета, г. Ставрополь; e-mail: kia762@yandex.ru; 355040, г. Ставрополь, ул. Шпаковская, 92, кор. 1, кв. 28; тел.: 88652731380, 89034163533; кафедра информационной безопасности автоматизированных систем; д.т.н., профессор.

Дагаева Ольга Игоревна – e-mail: scorpio@bk.ru; 355040 г. Ставрополь, пр. Кулакова, 33 кв. 56; тел.: 88652956546; кафедра информационной безопасности автоматизированных систем; аспирант.

Kalmykov Igor Anatol'evich – Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol; e-mail: kia762@yandex.ru; 92, k. 1, fl. 28, Shpakovskaya street, Stavropol, 355000, Russia; phone: +78652731380, +79034163533; the department for information security of automated systems; dr. of eng. sc.; professor.

Dagaeva Olga Igorevna – e-mail: scorpio@bk.ru; 33, Chehova street, fl. 66, Stavropol, 355013, Russia; phone: +79197389273; the department for information security of automated systems; postgraduate student.

УДК 681.587.5

А.А. Бошляков, В.В. Ковалев, В.И. Рубцов

ДИАГНОСТИКА ВЫСОКОТОЧНЫХ СКАНИРУЮЩИХ МЕХАТРОННЫХ МОДУЛЕЙ

Качество работы высокоточных сканирующих модулей зависит от большого числа параметров, поэтому их диагностика представляет собой сложную техническую задачу и требует высококвалифицированного персонала. В статье предлагается методика, которая позволяет упростить как контроль мехатронного модуля, так и принятие соответствующего решения о неисправности.

Методика предполагает автоматизированную диагностику изделий на основе анализа сигналов, передаваемых штатным контроллером системы управления мехатронного модуля, и предоставление персоналу рекомендаций по выявлению и устранению имеющихся дефектов.

Мехатронный модуль; диагностика; математическое моделирование; сканирующая система.

A.A. Boshlyakov, V.V. Kovalev, V.I. Rubtsov

DIAGNOSTICS OF HIGH-PRECISION SCANNING MECHATRONIC MODULES

The quality of the work of high-precision scanning modules depends on a large number of parameters, and so the diagnosis is a complex technical task and requires highly qualified staff. In this article we propose a methodology, which allows to simplify the control of the mechatronic module and the adoption of the corresponding decision of the fault.

The method requires an automated diagnosis of products on the basis of the analysis of signals transmitted controller of mechatronics module, and the provision of staff of the recommendations on the identification and elimination of existing defects.

Mechatronics module; diagnosis; mathematic simulation; scanning system.

Введение. Современные высокоточные системы сканирования предъявляют жесткие требования к качеству работы своих мехатронных модулей. Необходим тщательный контроль параметров мехатронных модулей, как на этапе изготовления, так и этапе работы в составе системы.

При серийном или удаленном производстве сложных мехатронных изделий, при их эксплуатации на объекте также остро встает вопрос об их диагностике. В идеальном случае процесс диагностики и дальнейшее принятие решения о пригодности изделия к эксплуатации должны осуществляться в автоматизированном режиме и без участия высококвалифицированных специалистов.

Предлагаемая методика диагностики позволяет упростить как контроль мехатронного модуля, так и принятие соответствующего решения о неисправности даже неквалифицированным персоналом.

Суть предлагаемой методики.

1. Строится математическая модель исследуемой системы. Полученная модель должна учитывать физические параметры объекта, характер внешних воздействий и внутренних дефектов изделия и влияние этих дефектов на работу системы в целом. Адекватность полученной модели должна быть подтверждена сравнением выходных сигналов модели с выходными сигналами, полученными экспериментальным путем при одних и тех же тестовых воздействиях [1].
2. Каждое из выпускаемых изделий исследуется в соответствии с предлагаемой методикой. Исследование отдельных экземпляров изделий может проводиться неоднократно, например, для изделий уже прошедших эксплуатацию или различные формы испытаний. Систему испытаний следует планировать таким образом, чтобы по измерению минимального числа величин можно было сделать вывод о соответствии объекта предъявляемым требованиям.
3. Все результаты проведенных испытаний заносятся в базу для дальнейшего анализа, сравнения и обработки. Список максимально информативных параметров объекта заносится в паспорт изделия, вводятся допуски на величину изменения этих параметров и при дальнейшей диагностике измеряемые параметры сравниваются с эталонными, указанными в паспорте.

Предлагаемая методика отличается от уже существующих [1, 2, 3] тем, что качество работы мехатронного модуля оценивается по данным, полученным из системы управления самого модуля. Предполагается, что модуль работает под управлением штатного контроллера, который позволяет при этом получать данные, являющиеся выходными либо промежуточными сигналами системы управления. Например, такими данными могут быть выходы отдельных звеньев корректирующего фильтра (КФ), сигналы рассогласования по координате, скорости и

пройденному пути, а также выходы различных нелинейных звеньев, в случае их присутствия в системе. Данный подход может быть использован для диагностики широкого спектра мехатронных устройств.

Средством диагностики в предлагаемой методике выступает контроллер системы управления. На вход системы подается набор тестовых воздействий, выходные характеристики записываются для дальнейшего анализа, либо контроллер управляет модулем в штатном режиме, при этом предоставляя пользователю возможность записывать внутренние сигналы и параметры системы управления. Такими данными могут являться показания датчиков обратной связи, сигнал управления, который представляет собой выходной сигнал КФ, заданная и вычисленная скорости объекта и т.п. Из полученных характеристик формируется экспериментальная база данных, которая позволяет сравнивать полученные характеристики, и делать выводы о влиянии различных модификаций и дефектов на работу отдельных изделий.

Данная методика успешно используется для диагностики прецизионных сканирующих модулей в составе комплекса авиационной оптико-локационной станции (ОЛС). Сканер ОЛС представляет собой высокоточный мехатронный модуль, осуществляющий позиционирование объекта регулирования по двум координатам (азимуту и углу места).

Построение модели мехатронного модуля. На первом этапе, была построена математическая модель сканера ОЛС. В математической модели были учтены следующие реальные физические параметры двигателей [4, 5], механической части изделия и датчиков.

- ◆ момент инерции приводов;
- ◆ максимальный момент двигателя при максимальном подаваемом напряжении;
- ◆ электро-магнитная постоянная обмоток двигателя;
- ◆ момент сухого трения;
- ◆ момент вязкого трения;
- ◆ величина трения покоя (момент трения, при превышении которого моментом двигателя начинается движение);
- ◆ угол магнитного гистерезиса двигателя.

Помимо модели сканера была введена математическая модель контроллера, в которой учитываются:

- ◆ квантование показаний датчиков по уровню/времени;
- ◆ чувствительность датчика в радианах;
- ◆ квантование выходных напряжений по уровню/времени;
- ◆ коэффициенты КФ.

На основании этих двух моделей была построена математическая модель модуля в целом, характеристики которой (полученные после подачи в систему набора входных воздействий) максимально совпадают с наблюдаемыми характеристиками реальных объектов, полученными во время проведения экспериментов. Данная модель была принята за эталонную. В ней не учитываются следующие факторы:

- ◆ механические дефекты изделия;
- ◆ возмущения, вызванные внешними факторами;
- ◆ разброс параметров отдельных серийных изделий;
- ◆ параметры и характеристики узлов и деталей, влияние которых на работу системы несущественно (сопротивление кабелей, потери в выходных каскадах, влияние механических передач).

Таким образом, за эталонную модель системы взята модель, максимально приближенно отражающую поведение идеального объекта. Идеальными, в этом случае, принимаются и выходные характеристики системы. Характеристики, полученные в результате экспериментов с реальным мехатронным модулем, должны сравниваться с эталонными, и по полученным различиям должен быть локализован набор дефектов модуля, подлежащих устранению.

Диагностика параметров мехатронного модуля. Методика предполагает автоматизированную диагностику изделий и предоставление персоналу рекомендаций по выявлению и устранению имеющихся дефектов.

Для этого с помощью полученных экспериментально данных строятся модели реальных изделий с учетом наличия различных дефектов [6, 7], а затем данные, полученные при работе реального изделия в составе системы, сравниваются с результатами моделирования этого изделия с учетом дефектов. С помощью математических методов возможен поиск в полученных данных составляющих, характерных для тех или иных дефектов и принятие решения о наличии этих дефектов в изделии.

На основании анализа работы для сканера ОЛС, был выделен набор параметров, по отклонениям которых от нормы осуществляется входной контроль изделий.

При входных воздействиях, задающих движение с постоянной скоростью, по выходной координате предлагается следующий набор параметров:

1. Средний уровень сигнала управления. Отклонение средней величины сигнала управления без учета участков вблизи реверса может свидетельствовать об избыточном или недостаточном моменте, затрачиваемом на поворот узла. Это может быть вызвано следующими факторами: избыточным трением в подшипнике, механическим дефектом, затрудняющим движение, недостаточной затяжкой подшипника;
2. Различие по модулю среднего уровня сигнала управления при движении узла в противоположные стороны может свидетельствовать о дисбалансе по массе в механической части узла.
3. Разброс уровня сигнала управления сигнализирует о наличии механических дефектов в определенных местах передачи, причем, соотнеся графики показаний датчиков и сигнала управления, мы можем судить о координатах дефектной области.
4. Время реверса при вращении. Позволяет оценить способность объекта управления реагировать на резкие изменения задания за необходимое время (способность двигателя перемещать объект с необходимым ускорением).
5. Форма кривой изменения координат при реверсе (ее симметричность относительно экстремума, наличие только одного экстремума в области реверса). Несимметричность формы кривой может говорить о дисбалансе и неравномерности движения узла, а наличие дополнительных экстремумов может свидетельствовать о механическом ударе в моменте реверса, вызванном, например, люфтом между осью и ротором, статором и неподвижной частью изделия и т.д.

При ступенчатом воздействии использовался следующий набор параметров:

1. **Время переходного процесса.** Время, прошедшее с момента задания системой управления координаты до выхода объекта на эту координату без дальнейших возмущений. Слишком затянутый переходной процесс сви-

детельствует о недостаточной мощности двигателя, повышенном трении, чрезмерно большой массе объекта, неправильной настройке системы управления.

2. **Величина перерегулирования при переходном процессе.** Слишком большой выброс означает завышенную мощность двигателя, низкое трение, меньшую, чем обычно массу подвижного узла, неправильную настройку системы управления.

При испытаниях с наличием внешних воздействующих факторов (климатических или виброакустических) появляется новый набор параметров, подлежащих контролю.

При климатических испытаниях мы можем судить о влиянии температуры на механические процессы по процентному отклонению среднего уровня сигнала управления от нормы или по форме функции сигнала управления. При слишком большом отклонении следует подобрать материалы и детали, рассчитанные на больший диапазон рабочих температур.

При виброакустических испытаниях следует обратить внимание на размах колебаний координат датчика при стабильном входном воздействии. Слишком большой разброс свидетельствует о недостаточной жесткости конструкции или разболтанности отдельных узлов.

Анализ полученных экспериментальных данных позволяет выявить недостатки реализации электромеханической части мехатронного модуля, дефекты объекта управления, отследить неправильную настройку системы управления (например, неправильной настройкой коэффициентов или неправильным выбором алгоритма управления), недостатки реализации алгоритма управления на используемом контроллере (например, слишком большой шаг квантования по уровню или по времени).

Выводы. Использование предложенной методики позволяет с высокой точностью осуществлять диагностику реального мехатронного модуля.

Конечным развитием данной методики может стать ее полная автоматизация, т.е. проведение диагностики и принятие решений без вмешательства оператора. Система может провести весь комплекс тестовых испытаний, проанализировать полученные данные, аналитическими или численными методами выявить требуемые параметры и их отклонения от эталонных и предоставить оператору список возможных недоработок, дефектов и рекомендаций по их устранению. Такие рекомендации могут быть представлены в текстовом формате, либо визуально. Конечной целью может являться упрощенное графическое представление изделия с указанием неисправных узлов и деталей, подлежащих замене. Таким образом, процесс диагностики ускоряется, что особенно важно в условиях мелкосерийного и серийного производства, и может быть выполнен оператором без специальной подготовки,

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Edwards S., Lees A.W. and Friswell M.I.* Fault Diagnosis of Rotating Machinery // Shock and Vibration Digest. – 1998.
2. *Басинюк В.Л., Ишин Н.Н. и др.* Устройство для диагностики динамически нагруженных приводов. Патент №20964 от 10.12.2001.
3. *Кузеев И.Р., Баширов М. Г. и др.* Способ диагностики механизмов и систем с электрическим приводом. Патент №2431152 от 23.11.2009.
4. *Pragasan Pillay, Krishnan R., Pragasan Pillay.* Modelling of Permanent Magnet Motor Drives // IEEE Transactions on Industrial Electronics. – 1988. – Vol. 35, № 4.

5. *Лысов М.С., Стариков А.В., Стариков В.А.* Линеаризованная математическая модель синхронного электродвигателя при различных способах управления его скоростью // Вестн. сам. гос. техн. ун-та. Сер.: физ.-мат. науки. – 2008. – №1 (16). – С. 102-107.
6. *Florent Morel.* Permanent Magnet Synchronous Machine Hybrid Torque Control, Jean-Marie Retid, Xuefang Lin-Shi, and Clarie Valentin // IEEE Transactions on Industrial Electronics. – 2008. – Vol. 55, № 2.
7. *Estima J.O., Marques Cardoso A.J.* The Occurrence of Faults in Permanent Magnet Synchronous Motor Drives and its Effects on the Power Supply Quality // University of Coimbra, FCTUC/IT.

Статью рекомендовал к опубликованию д.т.н., профессор В.Х. Пшихопов.

Большаков Андрей Анатольевич – МГТУ им. Н.Э. Баумана; e-mail: boshlyakov@mail.ru; 105005, г. Москва ул. 2-я Бауманская, 5; тел.: 84992636778; кафедра специальной робототехники и мехатроники; доцент.

Ковалев Владимир Вячеславович – кафедра специальной робототехники и мехатроники; аспирант.

Рубцов Василий Иванович – кафедра специальной робототехники и мехатроники; доцент.

Boshlyakov Andrey Anatolevich – BMSTU; e-mail: boshlyakov@mail.ru; 5, 2-ya Baumanskaya street, Moscow, 105005, Russia; phone: +74992636778; the department of robotics and mechatronics; associate professor.

Kovalev Vladimir Vyacheslavovich – the department of robotics and mechatronics; postgraduate student.

Rubtsov Vasily Ivanovich – the department of robotics and mechatronics; associate professor.

УДК 51-77

К.Д. Майзаков, Д.А. Эдель, В.А. Новосядлый

АЛГОРИТМИЧЕСКАЯ ОПТИМИЗАЦИЯ ВЫЧИСЛЕНИЯ ПРООБРАЗОВ НЕОБРАТИМЫХ ХЭШ-ФУНКЦИЙ MD5 И MD4

Рассматривается способ эффективного вычисления прообразов хэш-функции MD5 [1] и MD4 [2]. Обзор существующих способов атак – поиск коллизий, полный перебор – приведен в [3]. Рассмотрены существующие программные реализации [4, 5]. Показано, что данные реализации имеют возможность вычислять прообразы длиной до 16 байт и являются частным случаем предлагаемого. Приведены результаты численных экспериментов, показывающие, что предлагаемый способ в случае хэш-функции MD5 имеет возможность вычислять прообразы длиной до 55 байт и имеет скорость вычислений в среднем на 15 % выше существующих.

Хэш-функции; MD5; MD4; вычисление прообразов.

K.D. Mayzakov, D.A. Edel, V.A. Novosiadliy

ALGORITHMIC OPTIMIZATION OF INVERSE IMAGE COMPUTATION FOR MD5 AND MD4 DIGEST ALGORITHMS

Current paper reports on the method of efficient inverse image computation for MD5 [1] and MD4 [2] digest algorithm. A review of existing attack methods is given in [3]. Existing software implementations [4, 5] are discussed. They are shown to be able to compute inverse image of up to 16 bytes length and implement a special case of proposed method. The results of computational experiments are given, which show the possibility of inverse image calculation of up to 55 bytes length, with computational speed better than existing implementations up to 15 % in average.

Digest algorithm; MD5; MD4; inverse image computation.