

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пермский национальный исследовательский
политехнический университет»

**ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ:
ТЕОРИЯ, ИНСТРУМЕНТЫ, ПРАКТИКА**

Материалы IX Международной
интернет-конференции молодых ученых,
аспирантов, студентов
(20 ноября – 31 декабря 2017 г.)

Издательство
Пермского национального исследовательского
политехнического университета
2018

УДК 685.325.05

Представлены работы молодых ученых, аспирантов, а также лучшие работы студентов.

Конференция посвящена вопросам системных исследований и моделирования, информационно-измерительных и управляющих систем, систем телекоммуникации и связи, энергетики и энергоресурсосбережения, информационных технологий и средств автоматизации, аппаратно-программного обеспечения информационно-управляющих систем.

Публикуемые результаты исследований могут быть интересны молодым исследователям, преподавателям и специалистам, интересующимся теоретическими и прикладными разработками в данной предметной области.

Редакционная коллегия:

А.М. Костыгов, доцент, канд. техн. наук;

Б.В. Кавалеров, доцент, д-р техн. наук;

А.В. Кычкин, доцент, канд. техн. наук (отв. редактор);

А.Б. Петроченков, доцент, канд. техн. наук;

Н.М. Труфанова, профессор, д-р техн. наук;

Р.А. Файзрахманов, профессор, д-р экон. наук;

А.Г. Щербинин, профессор, д-р техн. наук;

А.А. Южаков, профессор, д-р техн. наук

Рецензент

Заслуженный деятель науки РФ, заслуженный машиностроитель Республики Башкортостан, доктор техн. наук, профессор кафедры автоматизированных систем управления Уфимского государственного авиационного технического университета *Г.Г. Куликов*

Секция 1

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ЗАПИСИ, ДОКАЗАТЕЛЬСТВА И ПОощРЕНИЯ РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОГО ТРУДА

Р.А. Андреев, П.А. Андреева, Л.Н. Кротов
Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассматривается возможность применения технологии блокчейн как доказательства интеллектуального труда. Предлагается использовать постоянные распределенные записи об интеллектуальных достижениях и соответствующих поощрениях, основанные на технологии блокчейн, которая реализует и демократизирует образовательную репутацию вне академических кругов.

Ключевые слова: блокчейн, интеллектуальный труд, смарт-контракт, консенсусный метод.

BLOCKCHAIN TECHNOLOGY FOR RECORD, PROOF AND REWARD OF INTELLECTUAL WORK

R.A. Andreev, P.A. Andreeva, L.N. Krotov
Perm national research polytechnic university, Perm

This paper reviews the possibility of applying blockchain technology as evidence of intellectual work. The use of permanent distributed records of intellectual achievements and related rewards based on blockchain technology, which implements and democratizes the educational reputation outside the academic community is proposed.

Keywords: blockchain, intellectual work, smart contract, the consensus method.

Для того чтобы понять значение технологии блокчейн для образования, важно понимать ее компоненты, поскольку любой из них может быть адаптирован для использования в образовательных целях.

Во-первых, есть сам блокчейн – распределенная запись цифровых событий. Блокчейн представляет собой длинную цепочку связанных элементов данных, хранящихся на каждом участвующем компьютере, где следующий элемент может быть добавлен только консенсусом большинства участников. Есть публичный блокчейн – любой человек может получить доступ к нему и потенциально добавить в него блок, а в организации или консорциуме используются частные блокчейны. Наиболее известный, но не единственный блокчейн – основа системы цифровых денег биткоин [1].

Во-вторых, существует метод «распределенного консенсуса» для согласования, является ли новый блок законным и что он должен быть добавлен к цепочке. Это делается путем требования от компьютера участника выполнения значительного объема вычислительной работы («доказательство работы» или «майнинг»), прежде чем можно будет пытаться добавить новый элемент в общую цепочку. Создание ложного блокчейна и получение согласия на основе консенсуса будут непомерно трудными. Неудачным следствием требования «доказательства работы» является то, что компьютер, выполняющий операцию майнинга для создания нового блока, должен расходовать значительную вычислительную мощность и электричество только для того, чтобы представить доказательства работы. Альтернативные варианты разрабатываются для распределенной проверки новых блоков, в том числе по методу «подтверждение доли», где для добавления нового блока участник должен продемонстрировать определенный объем валюты или репутации, которая будет потеряна, если этот блок не будет принят консенсусом [2].

В-третьих, каждый блок в цепи может содержать небольшой объем данных (обычно до 1 МБ), который может представлять собой любую информацию, которая должна быть защищена. Это может быть учет валютных операций (как и в биткоин) или для образования учетных данных или записей об обучении. Эти сведения хранятся на всех компьютерах-участниках и могут быть просмотрены любыми лицами, обладающими криптографическим «открытым ключом», но не могут быть изменены даже автором. К записям данных добавлены метки времени, обеспечивая надежную и своевременную запись добавленных данных.

Наконец, существуют смарт-контракты – сегменты компьютерных кодов, которые принимают блокчейн-транзакции при соблюдении определенных условий. Это позволяет хранить и выполнять коммерческие и юридические соглашения в Интернете, например для автоматизации выставления счетов.

Очевидное использование в образовании заключается в хранении записей о достижениях и удостоверениях, таких как документы об образовании. Данные о сертификатах будут добавлены высшим учебным заведением в блокчейн, к которому студент может получить доступ, которым он может поделиться с работодателями или на который может получить ссылку из онлайн-резюме. Он обеспечивает постоянную

публичную запись, которая защищается от изменений в учреждении или утраты его личных записей. Это открывает возможности для прямой выдачи сертификатов и пропусков доверенными экспертами и преподавателями. Блокчейн предоставляет публичные доказательства того, что студент получил диплом (документ об образовании) от учреждения, но сам по себе не проверяет достоверность каждой из сторон. Университет по-прежнему может выдать фиктивный сертификат или студент все еще может сжульничать на экзамене. Блокчейн решает проблему быстрой и надежной проверки появления события, такого как выдача диплома, но не его действительность.

Рассмотрим систему, в которой любое лицо может разместить открытую запись «большой идеи», например изобретения или творческой работы. Эта запись связывается с выражением работы (например, текстом или иллюстрацией). Каждая идея идентифицируется с ее автором и имеет метку времени, чтобы указать, когда она была впервые записана. После того как она была подана, она не может быть изменена, но она может быть заменена более поздней версией. Это может служить постоянным электронным портфолио интеллектуальных достижений для личного использования в качестве регистрационного журнала или для представления работодателю. Она также служит в качестве метода коллективного подряда для патентования. Нет необходимости в том, чтобы какое-либо лицо создавало и доказывало свои претензии в отношении изобретения – запись должна быть видима. Стартап-компания Blockai уже внедрила блокчейн-систему, чтобы помочь творческим работникам зарегистрировать свою работу для ее защиты от нарушения авторских прав [3].

Проблема с блокчейном как записью знаний или интеллектуального труда аналогична той, которая возникает при использовании блокчейна в качестве цифрового хранилища для сертификатов: это доказывает существование данных, но не гарантирует, что данные, хранящиеся в записи, являются действительными, аутентичными или полезными.

В настоящее время основное использование блокчейна является механизмом для регистрации операций цифровой валюты биткоин. Это общедоступная книга, которая регистрирует транзакции биткоин (хотя она может хранить и другие типы записей). Биткоин, как и традиционные валюты, можно использовать для оплаты товаров и услуг продавцов, которые их принимают. Таким образом, микроплатежи

биткоин могут использоваться в качестве вознаграждения за небольшие образовательные услуги, например, студент, выполняющий задачу коллегиальной оценки, которая будет автоматически вознаграждена.

Представьте, что торговля научной репутацией может быть расширена за пределы академического мира и заложить основу для экономики образования. Рассмотрим следующее предложение. Новый публичный блокчейн, созданный для управления образовательными записями и наградами, предложен консорциумом образовательных учреждений и компаний. Каждому признанному образовательному учреждению, новаторской организации и интеллектуальному работнику предоставляется первоначальная награда «валюта для получения образования». Учреждение может выделить часть своего первоначального фонда данной валюты сотрудникам, чьей репутации он хочет содействовать. Каждый человек и учреждение хранят свой фонд в виртуальном «бумажнике» на универсальном образовательном блокчейне. После этого любое учреждение или физическое лицо может создать сделку с репутацией. Учебно-воспитательному учреждению, такому как университет, может быть присужден диплом или сертификат, что предполагает размещение сертификата на блокчейне, а также перевод некоторых почетных премий из выдающего учреждения в принимающее. Для отдельных лиц он может поддерживать экономику интерактивного репетиторства, при этом студенты платят наставнику за интерактивное обучение в финансовой (например, биткоин) валюте, который затем заплатит студенту валюту-репутацию за прохождение теста или завершение курса. Механизм смарт-контрактов позволяет осуществлять такие одноранговые микроплатежи в различных валютах [4].

Любой человек (не обязательно тот, кто уже имеет кредитную репутацию) может также разнести заметку в учебном блокчейне. Это может быть творческое или научное производство, искусство или «великая идея», которая имеет метку времени и заархивирована. Таким образом, простая разноска является постоянной записью авторства, а также номенклатурой в личном, но распределенном электронном портфеле.

Кроме того, лицо, имеющее репутацию, может принять решение о том, чтобы присоединить репутацию к одному или нескольким постам в блокчейн, вплоть до суммы, которую он удерживает в своем бумажнике. Эта сумма не будет израсходована, но будет являться

свидетельством стоимости работы или идеи. Затем другие люди могут передать часть своего кредита на репутацию автору, чтобы повысить репутацию артефакта или идеи этого лица. Они могут сделать это, чтобы поощрить эту идею или ассоциироваться с ней.

Следствием этого является то, что образовательный блокчейн будет представлять собой единый универсальный отчет о поданных творческих идеях или произведениях, каждое из которых связано с кредитом репутации. Сумма «репутации», связанная с каждым товаром, указывает на его ценность для автора и таким образом в случае необходимости его реальную валютную стоимость (например, для приобретения копии творческой работы).

И наконец, репутация может быть «добываемой» учреждениями, которые зависят от их репутации в том, что касается добавления в цепочку допустимых блоков (с помощью алгоритма доказывания), за которые они вознаграждены за счет дополнительной репутации. В теории нет ограничений на предметы, которые можно было бы добавить в учебные блокчейн-присваивания, записи блога, комментарии, но при хранении и обслуживании распределенной образовательной записи существует вычислительная стоимость. Эта запись является публичной, поэтому каждый может определить, каким образом человек получил репутацию, а правила связывания ценности согласованы на основе консенсуса добровольцев, которые завоевали эти блоки.

Каковы могут быть последствия для образования от доверенных распределенных образовательных записей в сочетании с системой торговой репутации? Первое преимущество заключается в обеспечении единого гарантированного уровня образования, доступного и распространяемого во многих учреждениях. После того как образовательный блокчейн будет общепризнанным, студенты так же, как и учреждения, смогут хранить надежные публичные записи о личных достижениях. Во-вторых, общая система управления репутацией, связанная с блокчейн-технологией, могла бы способствовать открытию системы научной репутации, которая в настоящее время связана с научными кругами. Для этого потребуется разработать приемлемую и надежную практику приобретения общественной репутации, однако уже имеются примеры управления репутацией на работе в таких компаниях, как AirBnB, а также в системах образования, включая iSpot. В-третьих, и в более спорном отношении репутация может продаваться, будучи связанной с академическими наградами, а также

выноситься в качестве залога для важных идей или для проверки добавления нового блока в цепочку.

Существуют глубокие практические и идеологические вопросы, возникающие в связи с торговой репутацией в качестве валюты. Одна из практических проблем заключается в том, как создать коэффициент пересчета между репутацией и деньгами. Какова финансовая стоимость новой идеи или диссертации? Одна из основных идеологических проблем заключается в том, что система торговой репутации еще больше укрепила бы товарную систему образования, в которой учащиеся просматривают, покупают и потребляют учебные продукты, что не имеет отношения к стипендии или интеллектуальной ценности. Вместе с тем можно утверждать, что репутация как товар уже давно является составной частью академических кругов, несмотря на цитирование, факторы воздействия и национальные исследования в области оценки. Блокчейн и репутация могут привести к снижению уровня образования на рынке знаний или же они могут расширить сообщество исследователей и изобретателей для тех, кто готов поделиться хорошими идеями.

Библиографический список

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, October 2008 [Электронный ресурс]. – URL: <http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf> (дата обращения: 18.09.2017).
2. Buterin V. Understanding Serenity, Part 2: Casper, 28 December 2015 [Электронный ресурс]. – URL: <https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/> (дата обращения: 20.09.2017).
3. На А. Blockai uses the blockchain to help artists protect their intellectual property [Электронный ресурс]. TechCrunch, 15 March 2016. – URL: <http://techcrunch.com/2016/03/14/blockai-launch/> (дата обращения: 20.09.2017).
4. Devine P. Blockchain learning: can crypto-currency methods be appropriated to enhance online learning? [Электронный ресурс] // ALT Online Winter Conference, 7th–10th December 2015. Schlegel, H.: Reputation Currencies. Institute of Customer Experience. – URL: <http://ice.humanfactors.com/money.html> (дата обращения: 21.09.2017).

Сведения об авторах

Андреев Роман Александрович – аспирант Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: abusedroman@gmail.com

Андреева Полина Андреевна – аспирантка Пермского национального исследовательского политехнического университета, Пермь, e-mail: feofilovap@gmail.com

Кротов Лев Николаевич – доктор физико-математических наук, профессор кафедры «Прикладная физика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: levkrotov@yandex.ru

About the authors

Andreev Roman Alexandrovich – Graduate Student Perm National Research Polytechnic University, Perm, e-mail: abusedroman@gmail.com

Andreeva Polina Andreeva – Graduate Student Perm National Research Polytechnic University, Perm, e-mail: feofilovap@gmail.com

Krotov Lev Nikolaevitch – Doctor of Physics and Mathematics, Professor Department of Applied Physics Perm National Research Polytechnic University, Perm, e-mail: levkrotov@yandex.ru

РАЗРАБОТКА ФУНКЦИОНАЛЬНЫХ МОДЕЛЕЙ ПРОЦЕССОВ ТЕСТИРОВАНИЯ ЗНАНИЙ

Е.В. Бабенко, П.К. Понаморов

Московский государственный технологический
университет «СТАНКИН», Москва

Тестирование и оценивание знаний в информационной среде являются важным элементом образовательной деятельности и основой не только определения степени освоения обучаемым содержания учебного материала, но и для последующей оценки компетенции и квалификации.

Ключевые слова: электронное обучение, электронное тестирование, проектирование.

DEVELOPMENT OF FUNCTIONAL MODELS OF PROCESSES OF KNOWLEDGE TESTING

E.V. Babenko, P.K. Ponomarev

Moscow State Technological University "STANKIN", Moscow

Testing and evaluation of knowledge in the information environment is an important element of educational activities and is the basis not only determine the degree of development of the trainees content of the training material, but also for subsequent assessment of competence and qualifications.

Keywords: e-learning, electronic testing, design.

IDEFO – метод функционального моделирования, был разработан для описания функций различных систем путем создания наглядной графической модели. Функциональные модели строятся методом декомпозиции от главной (контекстной) функции к более мелким простым с учетом их взаимной связи. Цель моделирования и степень детализации модели определяются разработчиком. Элементы модели каждого уровня представляют собой действия по переработке информационных или материальных ресурсов при определенных условиях (ограничениях, управляющих воздействиях) с использованием определенных механизмов. Как правило, моделирование средствами IDEFO является начальным этапом изучения любой системы. Модели используются для детального функционального анализа с целью улучшения структуры функций объекта (реинжиниринга). Для

построения функциональной модели необходимо определить входные и выходные данные, а также способы или нормативные документы управления моделью и механизмы этого управления. Для подсистемы тестирования (рис.1), которая входит в систему электронного обучения, механизмами управления будут являться электронно-информационная образовательная среда (ЭИОС), программный продукт «1С:Электронное обучение. Конструктор курсов», разработчик тестов или преподаватель и компьютерный класс, где будет происходить процесс электронного контроля знаний. Управление данной подсистемой будет производиться с учетом образовательной программы дисциплины (ОП), ФГОСа, рабочей программы дисциплины (РПД), учебно-методического материала (УММ).



Рис. 1. Контекстная диаграмма подсистемы тестирования

На входе подсистемы тестирования должны быть требования к результатам обучения по дисциплине, типы тестовых вопросов и обучаемые. На выходе – результат обучения по дисциплине, результаты апробации, анализ тестовых вопросов и уровень знаний обучаемых (рис. 2). Также должно осуществляться проведение комплекса мер по обеспечению корректности ввода данных и безопасному хранению накопленной информации в программном продукте, который используется для проведения электронного тестирования и обработки результатов. Система должна проверять достоверность вводимых данных и обеспечивать качество выходных данных на этапе завершения тестирования.

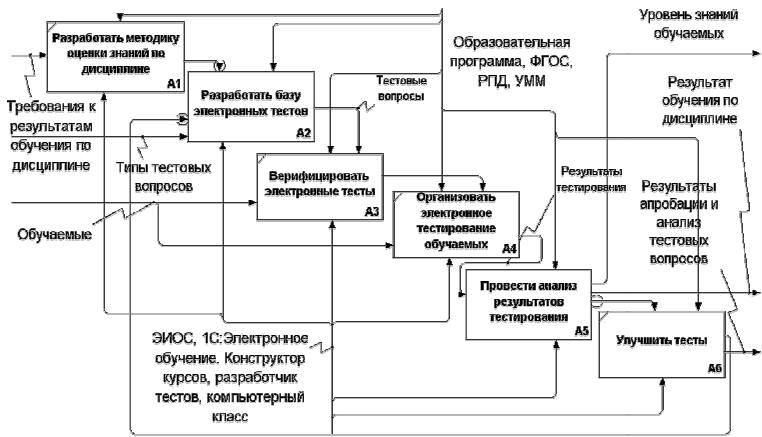


Рис. 2. Функциональная модель процессов тестирования

Контекстная диаграмма декомпозирована на 6 блоков (см. рис. 2): разработать методику оценки знаний по дисциплине, разработать базу электронных тестов, верифицировать электронные тесты, организовать электронное тестирование обучаемых, провести анализ результатов тестирования и улучшить тесты.

На рис. 3 представлена декомпозиция второго уровня диаграммы процессов тестирования.



Рис. 3. Функциональная модель процессов разработки базы электронных тестов

Механизмы и потоки управления для процессов тестирования, процессов разработки базы электронных тестов (см. рис. 3) и процессов проведения результатов тестирования остаются такими же, как и в контекстной диаграмме подсистемы тестирования.

Библиографический список

1. Свиридов А.П. Стандартизированные методы на примере контроля и диагностирования знаний: монография. – М.: Изд-во РГСУ, 2011. – 294 с.

2. Соловов А.В. Электронное обучение: проблематика, дидактика, технология. – Самара: Новая техника, 2006. – 464 с.

3. ГОСТ Р 55751-2013. Информационно-коммуникационные технологии в образовании. Электронные учебно-методические комплексы. Требования и характеристики // Доступ из справочно-правовой системы КонсультантПлюс.

4. ГОСТ Р 53625-2009. Информационная технология. Обучение, образование и подготовка. Менеджмент качества, обеспечение качества и метрики. Ч. 1: Общий подход // Доступ из справочно-правовой системы КонсультантПлюс.

Сведения об авторах

Бабенко Евгения Васильевна – магистрант Московского государственного технологического университета «СТАНКИН», Москва, e-mail: vasiljevna.ev@yandex.ru

Понаморов Петр Константинович – магистрант Московского государственного технологического университета «СТАНКИН», Москва, e-mail: fere12015@yandex.ru

About the authors

Babenko Evgeniya Vasilievna – Master Student Moscow State Technological University "STANKIN", Moscow, e-mail: vasiljevna.ev@yandex.ru

Ponamoren Petr Konstantinovich – Master Student Moscow State Technological University "STANKIN", Moscow, e-mail: Fere12015@yandex.ru

АВТОМАТИЗИРОВАННАЯ СИСТЕМА СБОРА И ОБРАБОТКИ ИНФОРМАЦИИ ОБ УСПЕВАЕМОСТИ СТУДЕНТОВ

И.А. Боброва, И.С. Полевщиков

Пермский национальный исследовательский
политехнический университет, Пермь

В статье приведено описание функциональных требований и преимуществ разрабатываемой автоматизированной системы сбора и обработки информации об успеваемости студентов.

Ключевые слова: автоматизированные системы обработки информации, учет успеваемости, язык UML.

AUTOMATED SYSTEM FOR COLLECTING AND PROCESSING INFORMATION ABOUT STUDENTS' PROGRESS

I.A. Bobrova, I.S. Polevshchikov

Perm National Research Polytechnic University, Perm

The article describes the functional requirements and advantages of the developed automated system for collecting and processing information on student performance.

Keywords: automated information processing systems, learning achievement, language UML.

Важнейшей составляющей учебной работы преподавателя вуза является учет успеваемости студентов, в рамках которого осуществляются сбор и обработка информации о контроле знаний, умений и навыков (ЗУН) и посещаемости занятий студентами [1–2].

Без использования соответствующих средств автоматизации процесс учета успеваемости (в частности, в ПНИПУ) обладает недостатками, связанными с трудоемкостью выполнения преподавателем таких задач, как:

- определение промежуточных результатов работы студента на протяжении семестра и подведение итогов в завершении семестра;
- проверка отдельных видов работ в дистанционном формате с возможностью хранения и просмотра в удобном виде истории проверки;
- анализ данных о результатах изучения дисциплины за некоторый интервал времени (например, семестр или учебный год).

Проблеме автоматизации учета информации об успеваемости посвящен ряд научных работ, например [3–5]. Проведен анализ нескольких разработанных и используемых информационных систем учета успеваемости [6–8].

Анализ показал, что проблема создания автоматизированной системы учета успеваемости решена в неполной мере. Фактически отсутствуют системы, позволяющие ликвидировать все перечисленные выше недостатки, эффективно обрабатывать большой объем данных об успеваемости, сделать процесс учета успеваемости «прозрачным» для студента и преподавателя.

Принято решение о создании новой автоматизированной системы учета успеваемости студентов вуза. Функциональные требования к системе разработаны с применением диаграмм вариантов использования языка UML [9]. В частности, требования к функциям личного кабинета преподавателя в системе показаны на рис. 1.

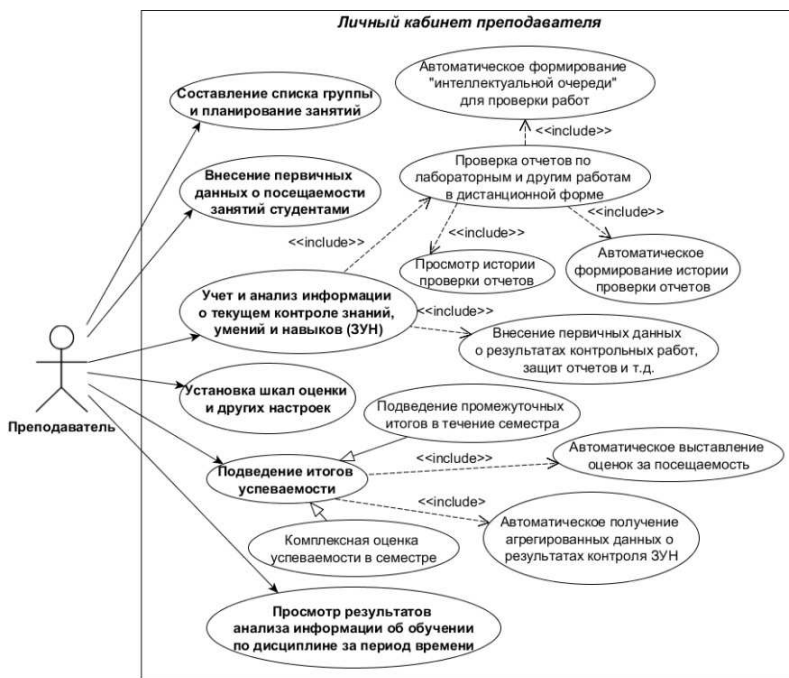


Рис. 1. Функциональные требования к личному кабинету преподавателя

Важным преимуществом разрабатываемой системы является хранение всей информации в структурированном виде в базе данных и предоставление ее в удобной форме для просмотра и редактирования.

Использование системы позволит избавить преподавателя от таких рутинных операций, как получение различных агрегированных и итоговых оценок об успеваемости студентов. Все эти действия будут выполняться автоматически.

Предусмотрена проверка работ студентов (лабораторных, практических и т.д.) в дистанционной форме с возможностью просмотра автоматически формируемой истории проверок.

Отличительной особенностью является организация «интеллектуальной очереди» при проверке преподавателем работ в дистанционной форме. Такая очередь должна быть удобна для студента и преподавателя. В частности, студент должен как можно меньше ждать результатов проверки работы, особенно в случаях, когда работа уже проверялась минимум один раз и осталось небольшое число замечаний от преподавателя.

Очередь динамически обновляется при поступлении на проверку новой работы. Место каждой работы в очереди зависит от ряда параметров: даты и времени поступления на проверку; степени выполнения (и, как следствие, проверки преподавателем) данной работы; среднего числа проверок работ данного студента; среднего времени проверки данной работы и т.д.

Степень выполнения работы зависит от количества правильно выполненных заданий и общего числа заданий, предусмотренных в работе, уровня сложности этих заданий.

Система будет включать удобные пользовательские интерфейсы (экранные формы). Например, при выставлении отметок о посещаемости занятий, помимо выставления отметок для каждого студента, будут предусмотрены опции «отметить, что все присутствуют», «отметить, что все отсутствуют», «отметить, что все присутствуют, кроме уже отмеченных» и подобные им.

Функциональные требования к личному кабинету студента в форме диаграммы вариантов использования UML приведены на рис. 2.

Существенным преимуществом разрабатываемой системы для студента является возможность в детальном виде и в удобное время просмотреть информацию о своей текущей успеваемости в семестре с целью повышения качества процесса обучения.



Рис. 2. Функциональные требования к личному кабинету студента

Продолжением настоящего исследования будут являться детальное проектирование и реализация системы в соответствии с указанными функциональными требованиями, с применением современных технологий программирования и методов интеллектуального анализа данных.

Библиографический список

1. Боброва И.А., Полевщиков И.С. Автоматизация учета успеваемости студентов вуза с применением информационной системы // Решение: материалы VI Всерос. науч.-практ. конф.; г. Березники, 20 октября 2017. – Пермь, 2017. – С. 78–80.
2. Боброва И.А., Полевщиков И.С. Автоматизированная система учета успеваемости студентов вуза // Автоматизированные системы управления и информационные технологии: материалы всеросс. науч.-техн. конф.; г. Пермь, 23 мая 2017 г. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2017. – Т. 1. – С. 176–180.

3. Романов Е.Л. Автоматизация учета рейтинга успеваемости студентов // Открытое и дистанционное образование. – 2014. – № 2(54). – С. 55–62.

4. Кравченко К.В. Ведение учета успеваемости студентов в комплексной информационной системе вуза // Символ науки. – 2015. – № 5. – С. 211–212.

5. Камальдинова З.Ф. Информационно-коммуникационная технология комплексного управления учебной и внеучебной деятельностью студента в вузе: автореф. дис. ... канд. техн. наук: 05.13.10. – М., 2011.

6. Шмакова Е.Е. Электронная система бального контроля успеваемости студентов по дисциплине «Инженерная графика». – URL: ds02.infourok.ru/uploads/doc/0d51/0001a778-c11d635e.docx (дата обращения: 25.01.2017).

7. Чуйко О.И., Белозерова С.И. Разработка информационной системы учета успеваемости студентов на основе облачных технологий // Наукovedenie: интернет-журнал. – 2015. – Т. 7. – № 5. – URL: naukovedenie.ru/PDF/97PVN515.pdf (дата обращения: 25.01.2017).

8. Братищенко В.В. Автоматизированная система управления Байкальского государственного университета экономики и права // Вестник Моск. город. пед. ун-та. Сер. Информатика и информатизация образования. – 2007. – № 9. – С. 156–158.

9. Леоненков А.В. Самоучитель UML. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2006. – 432 с.

Сведения об авторах

Боброва Ирина Александровна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: bobrovairina1812@gmail.com

Полевщиков Иван Сергеевич – старший преподаватель кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: i.s.polevshchikov@mail.ru

About the authors

Bobrova Irina Aleksandrovna – Student Perm National Research Polytechnic University, Perm, e-mail: bobrovairina1812@gmail.com

Polevshchikov Ivan Sergeevich – Senior Lecturer of the department for information technologies and computer-based systems Perm National Research Polytechnic University, Perm, e-mail: i.s.polevshchikov@mail.ru

АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ И СРЕДСТВ ТЕСТИРОВАНИЯ ANDROID-ПРИЛОЖЕНИЙ

С.А. Гонин, И.С. Полевщиков

Пермский национальный исследовательский
политехнический университет, Пермь

В статье приведен аналитический обзор методов и средств тестирования мобильных приложений на базе ОС Android. Проанализированы пять популярных библиотек для тестирования Android-приложений, выявлены их достоинства и недостатки, выбрана наиболее подходящая библиотека и рассмотрены демонстрационные примеры тестирования на основе этой библиотеки.

Ключевые слова: тестирование программного обеспечения, мобильные приложения, Android.

ANALYTICAL REVIEW OF METHODS AND FACILITIES OF TESTING ANDROID-APPLICATIONS

S.A. Gonin, I.S. Polevshchikov

Perm National Research Polytechnic University, Perm

The article provides an analytical overview of methods and tools for testing mobile applications based on the Android OS. Five popular libraries for testing Android-applications are analyzed, their advantages and disadvantages are revealed, the most suitable library is selected and test demonstration examples based on this library are considered.

Keywords: software testing, mobile applications, Android.

Android – это не просто операционная система (ОС) для смартфона, а целая инфраструктура. Android является первой бесплатной операционной системой с открытым исходным кодом. На нем работают телефоны, планшеты, телевизоры, умные часы и другие гаджеты. На сегодняшний день число активных устройств на базе этой ОС превышает 2 миллиарда [1].

К разработке программного обеспечения для такой широкой аудитории следует подходить с внимательностью и осторожностью, поскольку даже небольшое изменение в программе может повести к серьезным проблемам [2]. Для предотвращения подобных проблем разработчики покрывают программный код различными тестами, чтобы можно было отследить дефекты в программе еще на этапе разработки.

Основными типами тестов для Android являются локальный, инструментальный и UI-тесты. Рассмотрим особенности каждого типа.

Локальный тест предназначен для проверки кода, который не зависит от компонентов Android API, т.е. тестируемый код – это «чистый» Java-код, не связанный с Activity, Fragment, Context и т.д., поэтому для запуска не нужен Android-эмулятор или реальное устройство. Локальные тесты запускаются прямо на вашем компьютере, используя Java-машину. Однако при разработке Android-приложений «чистой» Java никак не обойтись. Обязательно будут классы, которые взаимодействуют с классами из Android API.

В этом случае уже не получится запустить тест локально на Java-машине компьютера, т.е. локальные тесты тут не подходят. Нужен Android-эмулятор или реальное устройство. Именно на них будут выполняться **инструментальные тесты**. В этих тестах можно использовать различные Android-классы.

Следует отметить, что в качестве исключения присутствует возможность писать некоторые локальные тесты, которые смогут проверить объекты, связанные с Android. Тем не менее иногда есть необходимость запустить тест именно на Android, чтобы результат проверки был точнее [3].

Третий тип теста – **UI-тест** – воспроизводит работу тестирующего (QA-инженера). UI-тест может запускать приложение, вводить в поля значения, нажимать кнопки и т.п. После этого он может проверить, в каком состоянии находятся View на экране, что они отображают и т.п. [4].

Для аналитического обзора выбраны 5 популярных библиотек: Appium, Selendroid, Robotium, UI Automator и Espresso. Рассмотрим каждую из них и выявим достоинства и недостатки [5] (таблица).

Результаты сравнения библиотек

Библиотека	Достоинства	Недостатки
Appium	<ul style="list-style-type: none"> 1) Бесплатная, свободно распространяемая платформа с открытым кодом. 2) Поддерживает автоматизированное тестирование нативных, мобильных и гибридных приложений как на реальных устройствах, так и на эмуляторах или симуляторах 	<ul style="list-style-type: none"> 1) Appium прямо поддерживает версии Android, начиная с 17-й и выше. Более ранние версии не поддерживаются. 2) Отсутствует прямая поддержка обработки предупреждений Android. 3) Более 50 открытых ошибок, связанных с iOS

Библиотека	Достоинства	Недостатки
Selendroid	<ol style="list-style-type: none"> 1) Работает как на реальных устройствах, так и на эмуляторах. 2) Специальный инструмент разработки тестов Inspector для проверки пользовательского интерфейса (UI) приложения. 3) Поддержка Android API, начиная с 10-й версии. 4) Возможность изменять аппаратные устройства (plug and unplug) во время тестирования без перезапуска или остановки теста. 5) Запись кликов 	<ol style="list-style-type: none"> 1) У пользователя нет возможности автоматизировать действия вне приложения – камера, карты и т.п. 2) Selendroid достаточно медленный. Его сложно использовать на устройствах с оперативной памятью меньше 4GB
Robotium	<ol style="list-style-type: none"> 1) Может использоваться как для тестирования приложений с доступным исходным кодом, так и для приложений, в которых доступны только файл APK и детали исполнения. 2) Robotium поддерживает следующие функции Android: действия, всплывающие сообщения, меню и контекстные меню. 3) Несложный для написания тест кейсов. 4) Быстрое исполнение тест-кейсов. 5) Интеграция с Maven или Ant. 6) Автоматическая синхронизация и задержки 	<ol style="list-style-type: none"> 1) Возможность проведения только одного тестирования одновременно. 2) Robotium не работает с Flash- или веб-компонентами
UI Automator	<ol style="list-style-type: none"> 1) Доступ к состоянию устройства. 2) Пользователи могут создавать тесты с использованием API, предоставляемого платформой, и запускать на нем тесты. 3) Библиотека UI Automator поставляется с Android SDK и предоставляет доступ к сотням материалов 	<ol style="list-style-type: none"> 1) Необходима версия Android 4,3 (API 18) или выше. 2) Java – единственный напрямую поддерживаемый язык программирования. 3) Недостаточная поддержка тестирования гибридных приложений
Espresso	<ol style="list-style-type: none"> 1) Является частью Android Support Library. 2) Android API 8 и выше. 3) Open source. 4) Синхронизация с UI потоком. 5) Более простой и легко расширяемый API. 6) Информативные сообщения о причинах невыполнения теста. Espresso покажет view hierarchy и сообщит, почему не выполнен какой-либо view-action или check. 7) Быстро запускается. 8) Поддержка Gradle и Android Studio 	<p>Относительно небольшой стандартный API, который можно расширить своими силами [6]</p>

По результатам аналитического обзора выбрана библиотека Espresso [7] благодаря таким преимуществам, как:

- самый низкий min API (level 8), это почти 100 % устройств;
- расширяемость функционала;
- поддержка «из коробки»;
- простота в использовании;
- встроенная аналитика;
- синхронизация с UI;
- быстроедействие.

Рассмотрим на примерах особенности тестирования с помощью Espresso.

Предположим, что в некотором приложении пользователь должен ввести свое имя. После того как введено имя, он нажимает на кнопку «Далее» и перенаправляется на другую Activity, на которой отображается приветственное сообщение [8].

Соответствующий сценарий теста будет выглядеть так:

```
onView(withId(R.id.user_name)).perform(typeText
("John"));
onView(withId(R.id.next)).perform(click());
onView(withId(R.id.greeting_message)).check
(matches(withText("Hello John!")));
```

Мы не указываем явно, с какими View взаимодействуем (EditText или Button), а просто отмечаем, что ищем View с конкретным идентификатором. При нажатии кнопки «Далее», а также при проверке текста не требуется писать специальный код, чтобы указать Espresso о перемещении на другую Activity.

Предположим, что есть приложение, в котором мы должны выбрать страну из Spinner: название выбранного пункта отображается рядом со Spinner. Соответствующий сценарий теста будет выглядеть так:

```
onView(withId(R.id.country_spinner)).perform
(click());
onData(allOf(is(InstanceOf(String.class)),
is(COUNTRY))).perform(click());
onView(withId(R.id.selected_country)).check
(matches(withText("selected: " + COUNTRY)));
```

Spinner основан на массиве строк. Если вместо строк используется собственный класс, то необходимо указать на это [9].

Таким образом, проведенный анализ показал, что существует достаточно большое число эффективных средств автоматизации тестирования мобильных приложений.

Дальнейшим развитием подобных средств могла бы стать автоматизация тех трудоемких фаз жизненного цикла процесса тестирования, которые обычно возложены на человека (планирование, разработка тест-кейсов и т.д.).

Библиографический список

1. Цифра дня: Сколько активных устройств работает на Android? – URL: macrumors.com/2017/05/17/2-billion-active-android-devices/ (дата обращения: 25.12.2017).

2. Martin Robert C. Clean Code: A Handbook of Agile Software Craftsmanship. – 2008. – 464 p.

3. Зачем нужны тесты и как они работают. – URL: startandroid.ru/ru/courses/testing/26-course/testing/480-urok-1-zachem-nuzhny-testy-i-kak-oni-rabotajut.html (дата обращения: 25.12.2017).

4. Android. Программирование для профессионалов / Б. Харди, Б. Филлипс, К. Стюарт, К. Марсикано. – СПб.: Питер. 2016. – 640 с.

5. Тестирование мобильных приложений – лучшие инструменты. – URL: geteasyqa.com/ru/blog/лучшие-инструменты-тестирования (дата обращения: 25.12.2017).

6. Автоматическое тестирование в Android. – URL: bravedevelopers.com/android-test-with-espresso/ (дата обращения: 25.12.2017).

7. Приятное тестирование с Espresso. – URL: habrahabr.ru/post/212425 (дата обращения: 25.12.2017).

8. Espresso Android Developers. – URL: developer.android.com/training/testing/espresso/index.html (дата обращения: 25.12.2017).

9. Введение в Android Espresso. – URL: java-help.ru/introduction-to-android-espresso (дата обращения: 25.12.2017).

Сведения об авторах

Гонин Сергей Александрович – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: sergon146@gmail.com

Полевщиков Иван Сергеевич – старший преподаватель кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: i.s.polevshchikov@mail.ru

About the authors

Gonin Sergey Aleksandrovich – Student Perm National Research Polytechnic University, Perm, e-mail: sergon146@gmail.com

Polevshchikov Ivan Sergeevich – Senior Lecturer of the department for information technologies and computer-based systems Perm National Research Polytechnic University, Perm, e-mail: i.s.polevshchikov@mail.ru

АНАЛИЗ ВОЗМОЖНОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ИЗУЧЕНИЯ АНАТОМИИ ЧЕЛОВЕКА

А.В. Горелова, А.В. Кузьмин

Пензенский государственный университет, Пенза

Данная статья посвящена проблеме применения информационных технологий в медицине и при изучении анатомии человека в частности. Рассмотрены примеры обучающих информационных систем анатомии человека, проанализированы их возможности. Выявлена и обоснована необходимость разработки развитой информационной инфраструктуры для систем изучения анатомии человека.

Ключевые слова: информационные технологии; медицина; образование; обучающая информационная система; анатомия человека.

TRAINING INFORMATION SYSTEM OF ANATOMY OF MAN

A.V. Gorelova, A.V. Kuzmin

Penza State University, Penza

This article is devoted to the problem of application of information technologies in medicine, and in the study of human anatomy in particular. The examples of educational information systems of human anatomy are considered, their possibilities are analyzed. Revealed and substantiated the necessity of developing an advanced information infrastructure for system study of human anatomy.

Keywords: information technologies; medicine; education; educational information system; human anatomy.

Удовлетворение потребности граждан Российской Федерации в квалифицированной медицинской помощи является одной из приоритетных целей государственной политики, важнейшей задачей развития здравоохранения. А для качественного обслуживания необходимо уделять особое внимание обучению новых специалистов при помощи новых информационных технологий.

Анатомия нуждается в этом, возможно, больше других дисциплин. Изучение анатомии в настоящий момент требует от студента, изучающего столь непростой предмет, больших усилий, чтобы «уложить» в голове трехмерное понимание анатомии из текстовой информации в учебниках и двухмерных изображений различных атласов, ведь каждый из них отличается своим стилем составления и масштабом изображений, не дающих полного представления об изучаемом органе. Виртуальная анатомия человека решает эти проблемы.

Рост потребительского спроса на технологии цифровой медицины, подкрепленный целенаправленной политикой многих государств на повышение здоровья нации и пропагандой здорового образа жизни, породил достаточное активное развитие данной области.

К главным двигателям роста рынка информационных технологий в медицине можно отнести и обучающие приложения. В 2014 г. объём рынка приложений в области здравоохранения составил \$10,5 млрд, а в ближайшие пять лет, по данным компании Allied Market Research, он будет расти в среднем на 33,5 % в год [1].

Обучающие информационные системы для изучения анатомии человека реализованы как для использования на персональных компьютерах, так и на мобильных устройствах. Примерами данных программ являются: Виртуальная анатомия 3.0 (АРТЕКСА) [2], Нормальная анатомия человека (Фармакоша) [3], Атлас анатомии человека (eDeux) [4], Человеческое тело (TrySportsNow) [5], InBody Anatomy (inbody.pro) [6].

Для их анализа использовались 7 основных критериев:

– 3D-модели органов. Это является важной характеристикой программы в процессе обучения, так как для точного изучения необходимо рассмотреть объект со всех возможных ракурсов и масштабах. Такой возможностью обладают лишь «Виртуальная анатомия 3.0», «Человеческое тело» и «InBody Anatomy»;

– тестирование пользователей. Для лучшего усвоения предоставленного материала необходимо проводить тестирование. Однако только «InBody Anatomy» имеет такую возможность;

– удобство поиска объектов. Возможность поиска значительно экономит время обучающегося, что играет большую роль в изучении («Виртуальная анатомия 3.0», «Нормальная анатомия человека», «Человеческое тело», «InBody Anatomy»);

– наличие справочной информации. Помимо визуального обучения большую роль играет информационное содержание обучающей информационной системы. Справочная информация по анатомии человека дает более подробное изучение предмета. Данной возможностью обладают «Нормальная анатомия человека», «Атлас анатомии человека» и «Человеческое тело»;

– дружественный интерфейс. Анатомия человека требует долгого и подробного изучения, поэтому интерфейс должен быть легко восприимчивым, приятным глазу и эргономичным. Данными критериями обладают «Нормальная анатомия человека», «Человеческое тело» и «InBody Anatomy»;

– возможность использования в режиме офлайн. Возможность использовать программу всегда и везде является большим преимуществом («Виртуальная анатомия 3.0», «Нормальная анатомия человека», «Человеческое тело», «InBody Anatomy»);

– распространение в Интернете. Большую роль играет легкость приобретения программы для пользователей. Программы «Виртуальная анатомия 3.0», «Нормальная анатомия человека», «Человеческое тело», «Атлас анатомии человека» являются свободно распространяемыми. Для их приобретения достаточно зайти на официальный сайт или Play Маркет и оплатить покупку онлайн, если это требуется.

Основные недостатки данных программных продуктов заключаются в отсутствии развитой сетевой информационной инфраструктуры для систем изучения анатомии человека. Каждая система по большей части функционирует автономно и оставляет пользователя «один на один» с задачей изучения предмета. Невозможность обмена знаниями, создания своих учебных программ, относительно небольшие возможности для тестирования, а также для взаимодействия пользователя и разработчика сокращают функциональные возможности и диапазон возможных применений данных приложений.

Процесс обучения необходимо реализовать таким образом, чтобы заинтересовать пользователя обучающей информационной системы в подробном изучении предоставленной информации и успешном прохождении тестирования.

Вопросы тестирования должны быть созданы не только на основе лекционной информации, но и визуальной. Таким образом, любой вопрос может быть связан с определенной 3D-моделью, пройденной в данном курсе, и ответом будет определенный объект анатомии человека, выбранный из 3D-сцены.

Успехи пользователя должны регистрироваться и вознаграждаться присваиванием особого уровня пользователя, что позволит открывать новые темы для обучения и даст возможность улучшения своего интерфейса с помощью цветовых и графических изменений. Из результатов тестирования пользователей системы необходимо составлять рейтинговые таблицы по определенным курсам, а также в целом, что будет стимулировать пользователей поднимать свой уровень относительно других.

Также пользователю необходимо предоставить возможность делиться своими знаниями, успехами и впечатлениями на сетевом форуме пользователей системы. В случае обнаружения ошибок программы или возникновения предложений для улучшения пользователь должен

иметь возможность взаимодействия с разработчиком, что можно реализовать на базе официального сайта программы или разработчика.

Для пользователей, осуществляющих преподавательскую деятельность и обладающих необходимыми компетенциями, требуется дать возможность вносить в систему свои методические разработки, к которым другие пользователи смогут получать доступ.

Выделенные преимущества обеспечат более широкие возможности применения и более высокую конкурентоспособность обучающей информационной системы анатомии человека в соответствующем секторе рынка программных продуктов, предназначенных для реализации соответствующих образовательных программ. Таким образом, разработка сетевой информационной инфраструктуры для систем изучения анатомии человека является актуальной задачей.

Библиографический список

1. URL: <https://cyberleninka.ru/article/v/rossiyskiy-gynok-meditinskih-izdeliy-itogi-2014-goda> (дата обращения: 15.09.2017).
2. URL: <http://arteksa.ru/index.php/ru/> (дата обращения: 15.09.2017).
3. URL: <http://medical-club.net/normalnaya-anatomiya-cheloveka-farmakosha/> (дата обращения: 15.09.2017).
4. URL: <http://medical-club.net/atlas-anatomii-cheloveka-edex/> (дата обращения: 15.09.2017).
5. URL: <http://ru.formidapps.com/mac/app.human-anatomy-3d-xiEpAqzD.aspx> (дата обращения: 15.09.2017).
6. URL: <https://inbody.pro/> (дата обращения: 15.09.2017).

Сведения об авторах

Горелова Алена Вячеславовна – магистрант Пензенского государственного университета, Пенза, e-mail: Leka20008@gmail.com

Кузьмин Андрей Викторович – кандидат технических наук, доцент Пензенского государственного университета, Пенза, e-mail: flickerlight@inbox.ru

About the authors

Gorelova Alena Vyacheslavovna – Master Student Penza State University, Penza, e-mail: Leka20008@gmail.com

Kuzmin Andrey Viktorovich – Ph.D. in Technical Sciences, Associate Professor Penza State University, Penza, e-mail: flickerlight@inbox.ru

ПРОВЕРКА МОДЕЛИ ПРЕДМЕТНОЙ ОБЛАСТИ, ОСНОВАННАЯ НА ТЕСТЕ С ЗАКРЫТЫМИ ВОПРОСАМИ

Е.В. Ерискина, Д.С. Курушин

Пермский национальный исследовательский
политехнический университет, Пермь

Рассматривается модель предметной области как основной элемент создания прикладных программ. Описан способ построения такой модели на основе денотатного графа. Рассмотрены проблемы адекватности построения модели предметной области на основе денотатного графа и способы их решений. Описан эксперимент по верификации предметной области с привлечением рабочей группы. Составлен алгоритм программы, способной автоматически решать тесты, основанные на закрытых вопросах. На основе результатов тестирования алгоритма и экспериментов с рабочей группой сделаны выводы о достоинствах и недостатках построенной модели предметной области.

Ключевые слова: модель предметной области, денотатный граф, осмысление, основное содержание, верификация, n -граммы, Python, Pymystem, Tokenize, Rutmextract, библиотека Python.

VERIFICATION OF A DOMAIN MODEL BASED ON THE TEST WITH CLOSED QUESTIONS

E.V. Eriskina, D.S. Kurushin

State National Research Politechnical University, Perm

This article describes the domain model used as a core element of creating application. The described method of constructing a model based on denotative graph. Paper describes experimental verification of the domain model based on automatic test solving and human testing. The algorithm for automatically test solving is described. Based on the results of testing the algorithm and experiments with the working group made conclusions about the advantages and disadvantages of the constructed domain model.

Keywords: domain model, denotatum graph, understanding, the main content, verification, n -grams, Python, Pymystem, Tokenize, Rutmextract, the Python library.

Модель предметной области – основной элемент создания любой прикладной программы. С её помощью разработчик определяет программный код, способы хранения сущностей и в некоторых случаях структуру и поведение пользовательского интерфейса [1]. В качестве такой модели может быть использован денотатный граф, отражаю-

ший иерархическую модель денотатов и их отношений, что соответствует модели фрагмента реальной ситуации. Методика построения такого графа была разработана А.И. Новиковым [2]. Модель предметной области, основанная на денотатном графе, представлена «денотатными цепочками» – парами «денотат–отношение–денотат». Для такой модели существует атрибут «направление связи», который характеризует «важность» связи относительно конкретного обрабатываемого текста [3].

Для того чтобы убедиться в существовании возможности построения модели предметной области на основе денотатного графа, провели следующий эксперимент: построили пробный граф предметной области «Искусственный интеллект» с опорой на тезаурус предметной области и литературу по выбранной теме, фрагмент которого представлен на рис. 1.

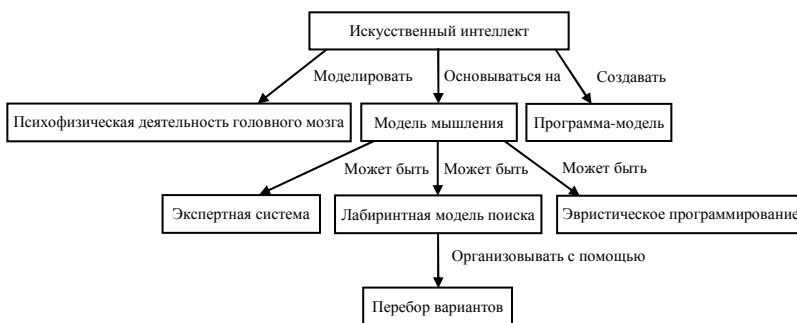


Рис. 1. Фрагмент денотатного графа предметной области «Искусственный интеллект»

Построенная модель включает в себя 40 денотатных пар, что достаточно для тестирования алгоритма. Понимание предметной области включает в себя не только её разбор на основные термины и поиск их эквивалентов в тезаурусе, но и процесс осмысления и построения связей между этими понятиями, а также и применение этих связей для построения цепочек «денотат–отношение–денотат» [4].

Проблема адекватности представления модели предметной области в виде денотатного графа заключается в том, что основным процессом формирования графа является понимание или корректное выделение основного содержания. Процесс понимания по своей

природе очень субъективен и напрямую зависит от того, кто занимается перекодированием предметной области из линейной структуры в графовую. Именно поэтому сам процесс перекодировки необходимо представить как «задачу на осмысление», в которой будет «данная величина» осмысляемой предметной областью и «искомая величина» – её денотатной структурой [5].

Проблема адекватности может быть решена в том случае, если удастся доказать однозначность и связность предметной области, представленной в виде денотатного графа. Для того чтобы проверить модель на соответствие этим критериям, на основе денотатного графа был составлен тест, состоящий из десяти вопросов. Ответить на тест, было предложено выбранной рабочей группе, причем ответы на вопросы текста нужно было дать, основываясь только на данных, представленных в графе, не опираясь на собственный опыт и знания. По результатам опроса составлена таблица, с помощью которой определили, какие из вопросов или сегментов графа имеют неточности или совсем не соответствуют понятиям предметной области. Если вопрос однозначен и понятен и ему соответствует конкретная денотатная пара в графе, имеющая правильную связь, значит, сегмент предметной области составлен верно. Если вопросу подходит не один, а несколько вариантов ответа, значит, можно говорить о том, что некорректно составлено задание. И, наконец, если на вопрос дано 50 % и менее правильных ответов, значит, ошибку следует искать в модели предметной области. По результатам тестирования мы получили следующие результаты: из 10 вопросов 100 % правильных ответов было дано на 3 из них, 80 % правильных ответов на 5 вопросов и на 2 вопроса 50 % и менее. Для наглядности представим полученные результаты в виде функции распределения случайной величины, которая отражает вероятность возникновения того или иного события и ограничивается конечным числом вхождений. В нашем случае случайной величиной является распределение вариантов ответов, событием – вариант ответа, а конечным числом вхождений – количество опрошенных людей [6]. Диаграмма разброса результатов тестирования представлена на рис. 2.

Такие результаты могут означать, что качество построенной модели данных хотя и приемлемо для понимания предметной области, но нуж-

дается в более детальной проработке в виде добавления новых имен денотатов и связей между уже существующими денотатами. Для проверки этой гипотезы необходимо «прогнать» составленный тест через программу, которая с помощью поиска в предметной области сможет решить его в соответствии с теми данными, которые представлены в графе. Работа такой программы основана на наборе некоторых функций.

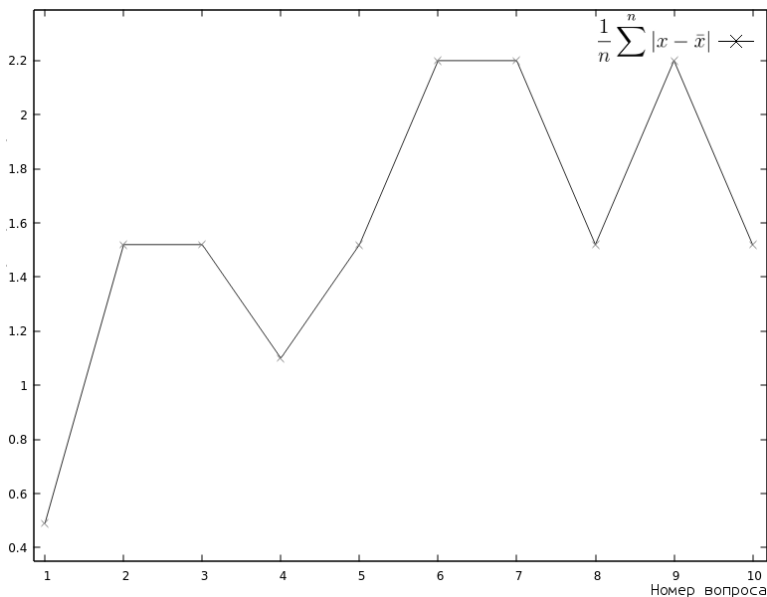


Рис. 2. Результаты тестирования рабочей группы

В первую очередь используем библиотеку PyMystem3 [7] для определения начальной формы слов в вопросе и ответах теста, Rutmextract [8] для определения и разбиения на ключевые слова и Tokenize [9] для разбиения каждого вопроса на отдельные элементы. Алгоритм программы построен следующим образом: сначала вопрос разбивается на токены, на основе которых формируются ключи. Затем полученные токены разбиваем на n -граммы – блоки, состоящие из трех букв. Затем начинаем по очереди сравнивать n -граммы вопроса с n -граммами каждого ответа. В ходе сравнения выделяются все, повторяющиеся из найденных. Каждая n -грамма имеет свою вероятность, которая никогда не превосходит единицу. Если вероятность найденной части более 0,55, то найденную

цепочку «денотат–отношение–денотат» выводим к соответствующему ответу, тем самым увеличивается вес этого ответа. После того как перебор всех n -грамм завершится, выставляем единицы к тем ответам, которые программа посчитала верными, остальным ответам (неправильным) соответствует «0» [10]. Псевдокод алгоритма ответа на закрытый вопрос представлен на рис. 3.

```

def answer(knowledge, questions):
    ans = {}
    for q in questions:
        ans.add_question(q)
        for variant in questions[q].keys():
            text =
get_variant_text(q, questions[q][a])
            terms =
get_terms_from_text(text)
            neg =
is_negative(text)
            significat_keys =
get_significat_keys(terms)
            real_keys =
get_real_keys(significat_keys, knowledge)
            found_keys =
find_kb_keys(real_keys, knowledge)
            ans[q].add_answer(
                {
                    variant:{
                        weight = neg *
len(found_keys),
                        vartext =
questions[q][a]
                        explanation =
found_keys
                    }
                }
            )
    return threshold(sigma(ans))

```

Рис. 3. Псевдокод алгоритма ответа на вопрос

Особенностью реализации на языке Python является тот факт, что объекты `ans` и `knowledge` являются словарями и, следовательно, не имеют жестко заданного порядка элементов. В результате функция `threshhold` может выбирать разные варианты ответов при одинаковом весе. Этот факт моделирует ситуацию, в которой тестируемый человек выбирает ответ «наугад», когда не знает правильного варианта. Для того чтобы проанализировать полученные результаты, запустим программу несколько раз, выведем все найденные для каждого ответа денотатные пары и обработаем результаты вручную. С помощью повторяющихся запусков выяснилось, что программа дает либо 3 либо 4 правильных ответа из 10, из чего можно сделать следующие выводы:

- не менее двух вопросов теста нуждаются в переформулировке, потому что и программа, и рабочая группа не смогли определить нужную связь между двумя именами денотатов;
- необходимо дополнить и расширить граф для более детального охвата предметной области;
- в алгоритм программы необходимо добавить подключение к тезаурусу «Искусственный интеллект»;
- нуждается в доработке и сам алгоритм.

Основных проблем в работе программы две: повторяющиеся денотатные пары выводятся и учитываются столько раз, сколько раз они найдены программой. Это искажает работу алгоритма. Граф просматривается не полностью. Из распечатки результатов видно, что программа не просматривает полностью всю модель и каждую связь в отдельности. Это может быть как ошибкой алгоритма, так и ошибкой в построенной предметной области.

Следовательно, создание модели предметной области является фундаментальной задачей для создания приложения. Мы находимся в самом начале пути исследования денотативного анализа как метода построения программной модели предметной области. Удалось выяснить, что с помощью правильной постановки задачи и верно описанной предметной области представляется возможным «заставить» интеллектуальную систему строить цепочки, которые вполне похожи на логические умозаключения человека. Дальнейшие исследования в этой области способны привести к возникновению нового способа построения моделей предметных областей, базирующихся на денотатном анализе предметной области.

Библиографический список

1. Андреев Н.Д., Новиков Ф.А. Фабрики прикладного программирования, управляемые моделями предметных областей // Информационно-управляющие системы. – 2013. – № 3.
2. Новиков А.И., Нестерова Н.М. Реферативный перевод научно-технических текстов / Академия наук СССР; Институт языкознания. – М., 1991.
3. Экспериментальные исследования денотативной модели понимания в приложениях автоматического реферирования текста / Н.А. Герте., Д.С. Курушин, Н.М. Нестерова, О.В. Соболева // Инженерный вестник Дона. – 2015. – № 4.
4. Люгер Джордж Ф. Проблемы семантических сетей // Понимание естественных языков и семантическое моделирование. – М.: Вильямс, 2003.
5. Нестерова Н.М. Реферативный перевод: проблема смыслового свертывания и семантической адекватности // Вестник Челяб. гос. ун-та. – 2011. – № 25.
6. Статистика // Российское хемометрическое общество. – URL: <http://rcs.chemometrics.ru/Tutorials/statistics.htm> (дата обращения: 28.11.2017).
7. Обработка и разметка полученной коллекции текстов. Грамматический парсер MYSTEM (библиотека «pymystem3» для языка программирования Python) // Vuzlit.ru. – URL: https://vuzlit.ru/399009/obrabotka_razmetka_poluchennoy_kollektsii_tekstov_grammaticheskij_parser_mystem_biblioteka_pymystem3_yazyka (дата обращения: 23.11.2017).
8. Rutmextract 0.3 // python. – URL: <https://pypi.python.org/pypi/rutmextract> (дата обращения: 23.11.2017).
9. Tokenize – Токенизатор для исходного кода Python // python-lab. – URL: <http://python-lab.ru/documentation/27/stdlib/tokenize.html#module-tokenize> (дата обращения: 23.11.2017).
10. Test_solver // github. – URL: https://github.com/daniel-kurushin/test_solver (дата обращения: 28.11.2017).

Сведения об авторах

Ерискина Екатерина Викторовна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: eriskina.katena@mail.ru

Курушин Даниил Сергеевич – кандидат технических наук, доцент кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: dan973@yandex.ru

About the authors

Eriskina Ekaterina Viktorovna – Student State National Research Politechnical University, Perm, e-mail: eriskina.katena@mail.ru

Kurushin Daniil Sergeevich – Ph.D. in Technical Sciences, Associate Professor State National Research Politechnical University, Perm, e-mail: dan973@yandex.ru

РАЗРАБОТКА СИСТЕМЫ СУДЕЙСТВА СПОРТИВНОГО СОРЕВНОВАНИЯ

А.А. Журавлёв

Пермский национальный исследовательский
политехнический университет, Пермь

Описаны проектирование и разработка новой системы для выставления и сохранения оценки по результатам выступления спортсмена на соревнованиях (система судейства спортивного соревнования). В статье представлено исследование предметной области, смоделированы разрабатываемая система и процесс взаимодействия, составлена схема взаимодействия объектов, описана работа с модулями устройства на операционной системе Android.

Ключевые слова: система, платформа, приложение, клиент, сервер.

DEVELOPMENT OF A SPORTS JUDGING SYSTEM

A.A. Zhuravlev

Perm National Research Polytechnic University, Perm

This article describes the design and development of a new system for exhibiting and retaining an evaluation based on the results of an athlete's performance at competitions (judging system of a sports competition). The article presents the research of the domain, modeled the system and the interaction process, a scheme of interaction of objects is designed, work with the device modules on the Android operating system is described.

Keywords: system, platform, application, client, server.

На сегодняшний день сфера информационных технологий развивается стремительными темпами. Если ещё несколько лет назад были популярны десктопные приложения, то сейчас наиболее распространены приложения на мобильных устройствах. Смартфоны и планшеты позволяют максимально быстро получить нужную информацию или связаться с любым человеком, что намного удобнее и проще, чем выполнять те же действия на настольном компьютере или ноутбуке.

Использование мобильных устройств может упростить не только повседневные задачи. Возможности таких устройств могут пригодиться для обработки большого числа данных на массовых мероприятиях, например, на спортивных соревнованиях, когда большое количество участников выступают сразу друг за другом, и каждый должен получить оценку за выступление как можно быстрее.

Использование каждым членом жюри смартфона или планшета для выставления оценки имеет ряд преимуществ:

- скорость обработки данных. Выставление оценки занимает минимум времени, итоговая оценка считается и сохраняется автоматически на сервере;

- простота использования и обслуживания системы. Оценка выставляется буквально в несколько касаний, а настройка и обслуживание системы максимально упрощены;

- доступность. Стоимость мобильных устройств в разы меньше, чем стоимость ноутбуков или персональных компьютеров;

- минимальная вероятность ошибки. Весь процесс автоматизирован, факт наличия ошибок минимален.

Система состоит из нескольких клиентов и одного сервера.

Каждый судья имеет собственное мобильное устройство. Клиентом является предустановленное мобильное приложение на операционной системе Android, которое передаёт серверу данные с помощью технологии Bluetooth. После запуска и получения оценки от судьи приложение соединяется с сервером (выполняет синхронизацию) и затем выполняет передачу данных (оценки) на сервер.

Судья-регистратор высылает разрешение на принятие оценки серверу. Сервер, получив разрешение, выполняет настройку соединения, а затем принимает соединение от каждого из клиентов. В случае успешного соединения с клиентом сервер начинает приём данных от клиента. Следующим этапом являются обработка данных (подсчёт итоговой оценки) и вывод данных. Диаграмма активности представлена на рис. 1.

Последовательность выставления оценки через данную систему можно разделить на следующие этапы:

- 1) спортсмен выступает перед судьями;
- 2) судья-регистратор направляет разрешение серверу на получение оценок;
- 3) судья выставляет оценку в клиентское приложение;
- 4) клиент передаёт оценку на сервер;
- 5) сервер выводит итоговую оценку.

Диаграмма последовательности действий, отображающая на временной шкале выполнение каждого этапа, представлена на рис. 2.



Рис. 1. Диаграмма активности

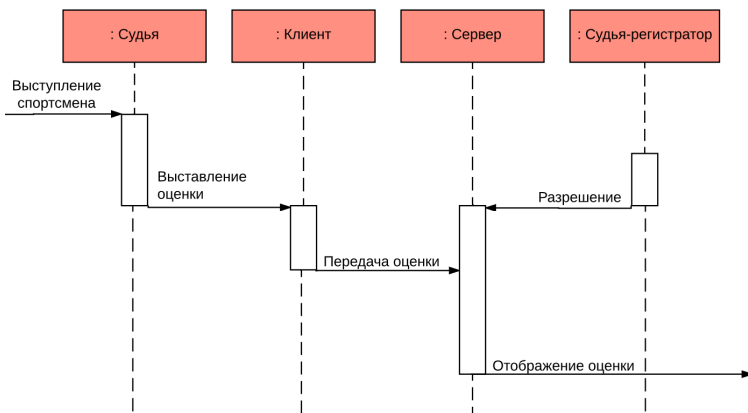


Рис. 2. Диаграмма последовательности

Для описания функциональности и поведения системы судейства была построена диаграмма use-case (диаграмма вариантов использования). На диаграмме, представленной на рис. 3, отображены взаимоотношения актёров (actor) и прецедентов (Use Case).

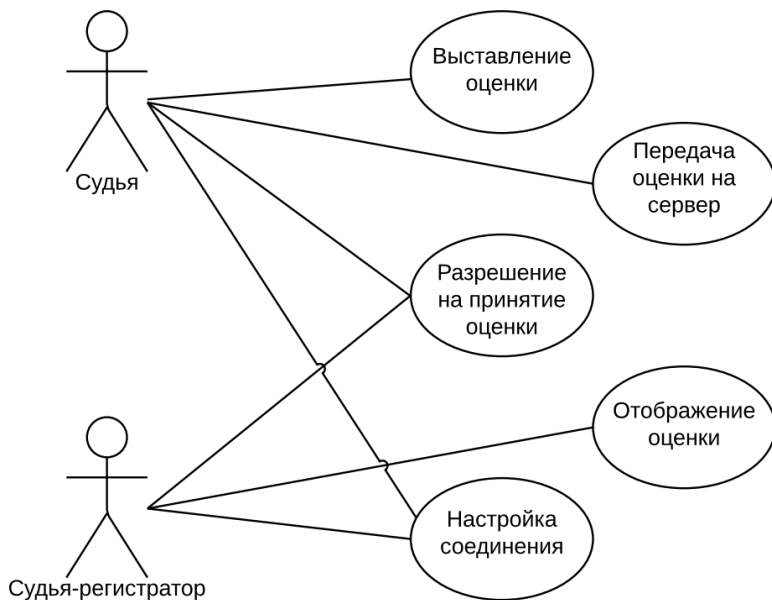


Рис. 3. Диаграмма прецедентов (диаграмма вариантов использования)

Данная система может быть адаптирована под соревнования по большинству видов спорта, что делает её универсальной.

Разработка приложения для операционной системы Android была выполнена в Android Studio на языке программирования Java [1]. В качестве примера для приложения был выбран вид спорта «тхэквандо». Клиентское приложение состоит из двух элементов:

- кнопка (Button),
- текстовое поле (TextView).

Изменение оценки производится во время выступления с помощью кнопок (Button), расположенных на экране. Текущая актуальная оценка отображается в текстовом поле (TextView) в нижней части экрана. Каждое нажатие кнопки обрабатывается методом `setOnClickListener`. Пример представлен на рис. 4.

```

rightButton.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View v) {
        if (result0 >= 0.1) {
            result0 -= 0.1;
            result0 = rounding(result0);
            String finalResult0 = Double.toString(result0);
            textView5.setText (finalResult0);
            updateResult ();
        }
    }
});

```

Рис. 4. Исходный код кнопки «-0.1»

При нажатии кнопки «Сохранить» результат из текстового поля отправляется на сервер и сохраняется. Главный экран приложения представлен на рис. 5.



Рис. 5. Главный экран мобильного приложения (клиент)

Для взаимодействия клиента и сервера используется Bluetooth-модуль. С помощью класса `BluetoothAdapter` производится поиск удаленного bluetooth устройства (сервера) и установка соединения с ним [2]. В случае удачного соединения полученная информация (имя, класс и MAC-адрес) сохраняется на устройстве.

Чтобы соединить два устройства, одно из устройств должно открыть серверный сокет, а второе – инициализировать соединение, используя MAC-адрес сервера. Сервер и клиент считаются соединенными, когда они оба имеют активный `BluetoothSocket` на одном и том же RFCOMM-канале. После этого они могут получать и отправлять потоки данных.

При соединении устройств одно из них должно вести себя как сервер, т.е. удерживать открытый `BluetoothServerSocket`. Цель сервера – ждать запроса на входящее соединение, и когда оно подтверждено, создать `BluetoothSocket`. После этого `BluetoothServerSocket` закрывается.

Для инициализации соединения с удаленным устройством (устройством, которое держит открытым серверный сокет) необходимо получить объект `BluetoothDevice`, содержащий информацию о нем. Этот объект используется для получения `BluetoothSocket` и инициализации соединения [3].

После успешного соединения каждое из соединенных устройств имеет объект `BluetoothSocket`, с помощью которого реализуется передача/приём данных:

1) с помощью методов `getInputStream()` и `getOutputStream()` получение объектов `InputStream` и `OutputStream`, управляющих передачей через сокет;

2) читать и писать данные в поток с помощью методов `read(byte[])` и `write(byte[])`.

Приложение использует отдельный поток для чтения и записи данных. Это важно, поскольку методы `read(byte[])` и `write(byte[])` являются блокирующими, и их вызов в основном потоке может парализовать программу.

Главный цикл в этом отдельном потоке считывает данные из `InputStream`.

Библиографический список

1. Oracle. Официальный сайт компании Oracle. США [Электронный ресурс]. – URL: <http://www.oracle.com/technetwork/java/javase/downloads/index.html> (дата обращения: 15.09.2017).
2. Голощапов А. Google Android. Создание приложений для смартфонов и планшетных ПК. – СПб., 2014.
3. Mark L. Murphy. The Busy Coder's Guide to Advanced Android Development. – Чикаго, США, 2016.

Сведения об авторе

Журавлёв Анатолий Андреевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: a.and.zhur@gmail.com

About the author

Zhuravlev Anatoly Andreevich – Student Perm National Research Polytechnic University, Perm, e-mail: a.and.zhur@gmail.com

АВТОМАТИЗАЦИЯ ПРОЦЕССА ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ ПОСТРОЕНИЯ ДИАГРАММ ПРИЧИН-СЛЕДСТВИЙ

М.В. Калинин, И.С. Полевщиков

Пермский национальный исследовательский
политехнический университет, Пермь

В статье рассмотрены особенности прототипа системы для тестирования программного обеспечения на основе построения диаграмм причин-следствий. Приведен пример тестирования программы с помощью данного прототипа.

Ключевые слова: тестирование программного обеспечения, автоматизированная система, диаграмма причин-следствий.

AUTOMATION OF THE SOFTWARE TESTING PROCESS BASED ON THE CONSTRUCTION OF CAUSE-EFFECT DIAGRAMS

M.V. Kalin, I.S. Polevshchikov

Perm National Research Polytechnic University, Perm

In the article features of the prototype of the system for software testing based on the construction of cause-effect diagrams are considered. An example of testing a program using this prototype is given.

Keywords: software testing, automated system, cause-effect diagram.

Известно, что для создания хорошего программного обеспечения (ПО) требуется правильная организация всех этапов процесса разработки, основанная на применении технологических принципов, и, в частности, грамотная организация этапа тестирования как неотъемлемого, наиболее устоявшегося средства современной системы обеспечения качества программного продукта [1].

С целью уменьшения трудоемкости процесса тестирования разрабатываются и применяются различные средства автоматизации [2], обладающие как большим количеством преимуществ, так и рядом недостатков.

Далее представлены результаты исследования проблем автоматизации тестирования ПО на примере разработки прототипа системы для автоматизации тестирования методом, основанным на построении диаграмм причин-следствий.

Диаграммы причинно-следственных связей используются для проектирования тестовых вариантов и обеспечивают формальную запись логических условий и соответствующих действий [1, 3]. При этом тестируемая программа рассматривается как «черный ящик», поведение которой можно определить только исследованием его входов и выходов.

Метод тестирования ПО, основанный на построении диаграмм причин-следствий, включает следующие шаги [3, 4]:

- 1) для тестируемой программы (или отдельного тестируемого модуля) выявляются причины (условия ввода или классы эквивалентности условий ввода) и следствия (действия или условия вывода); каждой причине и следствию присваивается свой идентификатор;

- 2) разрабатывается граф причинно-следственных связей;

- 3) граф преобразуется в таблицу решений;

- 4) столбцы таблицы решений преобразуются в тестовые варианты;

- 5) осуществляется сравнение реальных и ожидаемых результатов работы программы.

Существует множество средств автоматизации тестирования ПО – от небольших программ, решающих частные задачи, до мощных инструментальных средств. Примеры наиболее известных продуктов [3, 5]:

- 1) JUnit – библиотека для модульного тестирования программного обеспечения на языке Java;

- 2) Selenium – фреймворк для автоматизации процесса тестирования веб-приложений;

- 3) Katalon Studio – инструмент для автоматизации процесса тестирования веб-приложений, мобильных приложений и веб-сервисов;

- 4) Watir – инструмент с открытым исходным кодом для автоматизации тестирования веб-приложений, использующий библиотеки Ruby.

Важным недостатком существующих программных продуктов для автоматизации тестирования является то, что многие сложные интеллектуальные задачи (например, разработка тест-кейсов) остаются фактически возложенными на человека – специалиста по тестированию.

В частности, при тестировании ПО-методом, основанным на построении диаграмм причин-следствий, с помощью перечисленных выше средств шаги №1-4 будут выполняться вручную человеком. Требуется автоматизация этих действий для повышения производительности работы специалиста по тестированию.

С целью устранения указанных недостатков разработан прототип системы для автоматизации тестирования ПО на основе построения диаграмм причин-следствий. Сформулированы функциональные требования к системе:

- 1) пользователь задает количество причин и следствий;
- 2) система создает текстовые поля для заполнения причин и следствий;
- 3) пользователь создает граф причин-следствий (в прототипе граф строится на основе заполнения экранных форм);
- 4) система должна отобразить таблицу решений;
- 5) система показывает пользователю тестовые варианты, по которым будет осуществляться поверка ПО, и на основе этих тестовых вариантов сравнивает реальные и ожидаемые результаты выполнения программы.

Прототип системы является веб-приложением, построенным на основе технологий HTML, CSS, JavaScript в среде разработки NetBeans IDE [6].

Рассмотрим пример автоматизации тестирования ПО с помощью созданного прототипа. Требуется протестировать программу расчета числа аккумуляторных батарей для обеспечения бесперебойного электроснабжения в зависимости от времени и частоты отключения электричества. Для случая, когда частота отключения электричества не более 1 раза в месяц:

- 1) если среднее время отключения электричества меньше или равно 1 часу, то достаточно K батарей;
- 2) если среднее время отключения электричества больше 1 часа и меньше 12 часов, то достаточно $1,5K$ батарей;
- 3) если среднее время отключения электричества больше или равно 12 часам, то достаточно $2K$ батарей.

Для случая, когда частота отключения электричества больше 1 раза в месяц, полученное значение увеличивается на 50 %.

Изначально пользователь вводит количество причин и следствий (рис. 1). После чего нажимает кнопку «Подтвердить количество причин и следствий».

Далее пользователь заполняет в созданных текстовых полях названия причин (рис. 2) и следствий (рис. 3).

Шаг 1. Определение причин и следствий:

Примечание:

Буквой "С" с номером будут обозначаться причины.

Буквой "Е" с номером будут обозначаться следствия.

Введите кол-во причин (С):

Введите кол-во следствий (Е):

Подтвердить кол-во причин и следствий

Рис. 1. Пользователь вводит количество причин и следствий

Причины:

№	Условное обозначение причины	Название причины
1	C1	Частота отключения электричества НЕ более 1 раза в месяц
2	C2	Частота отключения электричества больше 1 раза в месяц
3	C3	Среднее время отключения электричества меньше или равно часу
4	C4	Среднее время отключения электричества больше 1 часа и меньше 12 часов
5	C5	Среднее время отключения электричества больше или равно 12 часов

Рис. 2. Заполнение информации о причинах

Следствия:

№	Условное обозначение следствия	Название следствия
1	E1	Достаточно К батарей
2	E2	Достаточно 1.5 * К батарей (Пояснение: это E1 увеличенное на 50 %)
3	E3	Достаточно 2 * К батарей
4	E4	Достаточно (1.5 * К) + (1.5 * К)/2 батарей (Пояснение: это E2 увеличенное на 50 %)
5	E5	Достаточно (2 * К) + (2 * К)/2 батарей (Пояснение: это E3 увеличенное на 50 %)

Рис. 3. Заполнение информации о следствиях

После чего пользователь устанавливает количество связей (рис. 4) и нажимает на кнопку «Подтвердить количество связей».

Шаг 2. Установка причинно-следственных связей:

Введите кол-во связей:

Подтвердить кол-во связей

Рис. 4. Установка количества связей

Далее пользователь описывает граф причин-следствий с помощью раскрывающихся списков (рис. 5). После установки связей нажимает кнопку «Подтвердить связи».

№	1-я причина		2-я причина		Следствие
1	C1	▼	C3	▼	E1 ▼
2	C1	▼	C5	▼	E3 ▼
3	C1	▼	C4	▼	E2 ▼
4	C2	▼	C3	▼	E2 ▼
5	C2	▼	C4	▼	E4 ▼
6	C2	▼	C5	▼	E5 ▼

Подтвердить связи

Рис. 5. Создание графа причин-следствий

Система на основе вышеописанных входных данных генерирует и отображает на экране таблицу решений (рис. 6) и тестовые варианты (рис. 7).

Шаг 3. Создание таблицы решений:

		ТВ1	ТВ2	ТВ3	ТВ4	ТВ5	ТВ6
Причины	C1	1	1	1	0	0	0
	C2	0	0	0	1	1	1
	C3	1	0	0	1	0	0
	C4	0	0	1	0	1	0
	C5	0	1	0	0	0	1
Следствия	E1	1	0	0	0	0	0
	E2	0	0	1	1	0	0
	E3	0	1	0	0	0	0
	E4	0	0	0	0	1	0
	E5	0	0	0	0	0	1

Рис. 6. Таблица решений

Шаг 4. Тестовые варианты:

№ ТВ	Исходные данные	Ожидаемые результаты
ТВ1	Частота отключения электричества НЕ более 1 раза в месяц Среднее время отключения электричества меньше или равно часу	Достаточно К батарей
ТВ2	Частота отключения электричества НЕ более 1 раза в месяц Среднее время отключения электричества больше или равно 12 часов	Достаточно 2 * К батарей
ТВ3	Частота отключения электричества НЕ более 1 раза в месяц Среднее время отключения электричества больше 1 часа и меньше 12 часов	Достаточно 1.5 * К батарей (Пояснение: это E1 увеличенное на 50 %)
ТВ4	Частота отключения электричества больше 1 раза в месяц Среднее время отключения электричества меньше или равно часу	Достаточно 1.5 * К батарей (Пояснение: это E1 увеличенное на 50 %)
ТВ5	Частота отключения электричества больше 1 раза в месяц Среднее время отключения электричества больше 1 часа и меньше 12 часов	Достаточно (1.5 * К) + (1.5 * К)/2 батарей. (Пояснение: это E2 увеличенное на 50 %)
ТВ6	Частота отключения электричества больше 1 раза в месяц Среднее время отключения электричества больше или равно 12 часов	Достаточно (2 * К) + (2 * К)/2 батарей. (Пояснение: это E3 увеличенное на 50 %)

Рис. 7. Тестовые варианты

Дальнейшее развитие созданного прототипа:

- добавление возможности визуального построения графа причин-следствий (визуальное представление графа для рассмотренной выше задачи показано на рис. 8.);
- применение математических функций для описания следствий;
- автоматизация сравнения реальных и ожидаемых результатов работы программы на основе полученных тестовых вариантов.

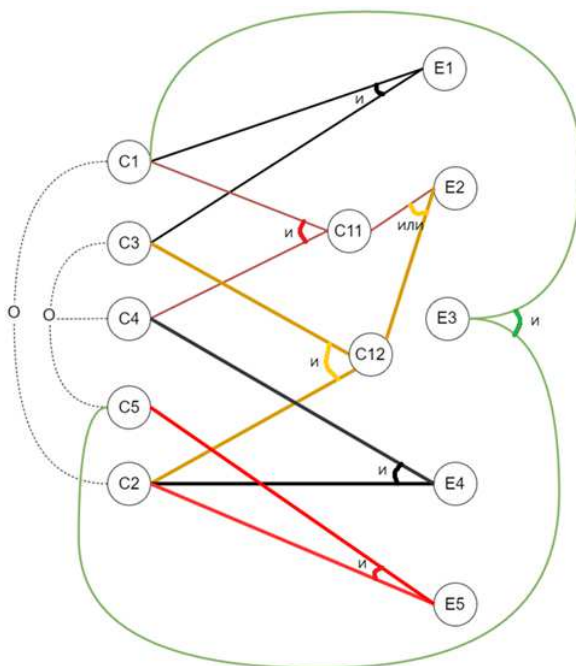


Рис. 8. Граф причин-следствий

Таким образом, разрабатываемый программный продукт позволит уменьшить временные затраты в ходе тестирования на основе построения диаграмм причин-следствий.

Библиографический список

1. Орлов С.А., Цилькер Б.Я. Технологии разработки программного обеспечения: учебник для вузов. – 4-е изд. – СПб.: Питер, 2012. – 608 с.

2. Куликов С.С. Тестирование программного обеспечения. Базовый курс. – Минск: Четыре четверти, 2017. – 312 с.

3. Тестирование программного обеспечения: метод. указания / сост. И.С. Полевщиков. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2017. – 98 с.

4. Полевщиков И.С., Кондратович М.А., Селиванова О.И. Разработка методического пособия на тему «Способ диаграмм причин-следствий» (для студентов и магистрантов направления «Информатика и вычислительная техника») // Педагогика и современность. – 2012. – № 2. – С. 79–84.

5. Топ 10 инструментов автоматизации тестирования 2018. – URL: habrahabr.ru/post/342234 (дата обращения: 19.12.2017).

6. Web-технологии. – URL: intuit.ru/studies/courses/485/341/info (дата обращения: 20.12.2017).

Сведения об авторах

Калин Матвей Викторович – студент Пермского национально-исследовательского политехнического университета, Пермь, e-mail: matthewk@mail.ru

Полевщиков Иван Сергеевич – старший преподаватель кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: i.s.polevshchikov@gmail.com

About the authors

Kalin Matthew Viktorovich – Student Perm National Research Polytechnic University, Perm, e-mail: matthewk@mail.ru

Polevshchikov Ivan Sergeevich – Senior Lecturer of the department for information technologies and computer-based systems Perm National Research Polytechnic University, Perm, e-mail: i.s.polevshchikov@mail.ru

РАЗРАБОТКА МЕТОДИКИ ОБРАБОТКИ 3D-МОДЕЛЕЙ ДЛЯ СОЗДАНИЯ 3D-ПЕРСОНАЖЕЙ НА ОСНОВЕ КОНЦЕПТА

Е.И. Никитиных

Российский государственный университет
им. А.Н. Косыгина, Москва

В данной статье представлена разработанная методика, которая включает в себя определение оптимальных параметров сканирования; анализ концепта персонажа; работу над геометрией скана и определение инструментария и шагов обработки с использованием программы ZBrush; создание одежды с помощью Marvelous Designer и последующей её детализации; оптимизацию модели с учетом требований заказчика модели; текстурирование модели в Substance Painter 2 и создание карт.

Ключевые слова: методика, 3D-модели.

DEVELOPMENT OF THE METHODS OF PROCESSING 3D-MODELS FOR CREATING 3D-CHARACTERS BASED ON THE CONCEPT

Elena Igorevna Nikitinyh

Russian State University named after A.N. Kosygina, Moscow

This article presents the developed methodology, which includes the definition of optimal scanning parameters; analysis of the concept of the character; work on the geometry of the scan and determine the tools and processing steps using the ZBrush program; creation of clothes with the help of Marvelous Designer and its further detailing; Optimization of the model taking into account the requirements of the customer model; texturing the model in Substance Painter 2 and creating maps.

Keywords: method, 3D model.

В настоящее время область 3D-графики стремительно развивается, услуги сканирования становятся всё более доступными большому количеству людей, и появляется спрос на персонафикацию в различных областях: люди заинтересованы в персональных фигурках, портретных куклах, в своих трехмерных аватарах и т.д. С развитием технологий сканирования обычным людям стали доступны многие сферы применения собственных сканов.

Моделирование по фотографиям является очень трудоемким способом создания модели, к тому же результат может быть недостаточно схож с вариантом заказа клиента. Поэтому все больше компаний прибегают к 3D-сканированию людей. Основными игроками на

российском рынке персональных фигурок являются MiniMe3d и VeIn3d, компании, которые имеют собственное оборудование и полный цикл производства. Последние производят сканирование на 3D-сканере Portal компании Texel.

Большие надежды возлагают на дальнейшую работу с 3D-контентом, полученным в результате сканирования. Для того чтобы проект был конкурентоспособным, необходимо привнести в сферу нечто новое. Например, создание уникальных фигурок и композиций в отличие от просто распечатанного 3D-скана. Для клиента это возможность создать свой персонаж в образе любимого героя и изготовить коллекционную фигурку со своим лицом. Возможно также применение нестандартных материалов и/или добавления подсветки, часов, скрытого USB-флеш-накопителя и других дополнений по пожеланиям заказчика.

Методика позволит получать прибыль не только с создания аватаров и фигурок, а также открывает возможности для сотрудничества со студиями и компаниями в различных областях деятельности: студии создания игр, фитнес, мода, а также она может быть применима к уже существующим проектам компании.

Также модели, созданные по предполагаемой методике, могут послужить для увеличения базы данных 3D-сканов людей для обучения алгоритмов (например, нейросетей): из одного реального 3D-скана можно воссоздать большое количество проекций в разных позах, одежде, симулировать движение и т.д. Также в перспективе можно обучать нейросети на ручной работе дизайнеров, чтобы иметь возможность автоматической генерации аватаров с нужными свойствами. Модели с хорошей сеткой также можно использовать в исследованиях по созданию и улучшению параметрических моделей тела человека.

Исходя из оценки экономической эффективности проекта, основанного на применении разработанной методики в обработке сканов, можно сделать вывод, что методика не только оправдывает свои вложения, принесет прибыль, но и поможет получить потенциальный прирост в доходах на 259 % за счет оптимизации рабочего процесса.

Многие пользователи Интернета давно заинтересованы возможностью получения собственного трехмерного аватара в полный рост для различных игр, приложений и общения на расстоянии. Использование аватара делает любую игру более реалистичной, дает ощущение значительно большего погружения в виртуальный мир.

В данный момент все серьезнее развивается сфера виртуальной реальности (VR), одним из ее применений является проведение виртуальных конференций и мероприятий.

Организация и участие в конференциях требуют немалых расходов, поэтому создание виртуальных аналогов является оптимальным решением. Форматом таких конференций являются виртуальные 3D-конференции, объединяющие преимущества реальных и видео-конференций. Такие мероприятия проходят в виртуальном зале, а участники представлены своими аватарами и имеют возможность общаться с аудиторией и взаимодействовать с предметами или выставочными павильонами.

За рубежом конференции с использованием виртуальной трехмерной среды становятся все популярнее.

Уже в течение долгого времени не перестаёт набирать популярность создание любительских сюжетных видеороликов на игровых движках. Особенно в последнее время, когда всё большему количеству людей стали доступны производительные игровые компьютеры. Подобный формат кинопроизводства является бюджетным и доступным, поэтому любительские студии заинтересованы в доступных по цене 3D-моделях персонажей со скелетом. Стоимость снижается за счет отказа от дорогих систем захвата движения или съемки с использованием технологии хромакей. Это также открывает возможность создания персонализированной рекламы на основе 3D-сканов и видеозаписей.

Раньше дизайнеры и модельеры использовали двухмерные чертежи для каждого ракурса, что требовало массу времени и ресурсов. Сейчас сотни тысяч самых разных компаний в мире используют технологии компьютерного моделирования для проектирования и дизайна. Производители одежды и обуви всех ценовых категорий спешат перестроить свои производственные процессы в соответствии с новыми технологиями.

Дизайнеры итальянской марки Gucci используют единую цифровую платформу ENOVIA для создания разных категорий товаров – от платьев до сумок. Коллекции prêt-à-porter и изделия из кожи теперь проектируются исключительно в 3D, также в компании постепенно начинают аналогичным образом создавать изделия из шелка.

Создание коллекции в формате 3D позволит не только существенно сэкономить средства и время, но и быстро проводить эксперименты с тканями, материалами и текстурами.

Отсканировав клиента, обратившегося за услугой по пошиву одежды, с помощью 3D можно создать уникальную, идеально сидящую одежду, быстро оценить и собрать весь образ клиента.

Для молодых дизайнеров 3D-моделирование для создания собственных показов является бюджетным вариантом пошива реальной коллекции. Созданные модели также могут быть продемонстрированы в интернет-магазинах.

Работа над моделью состояла из различных этапов: сканирование с использованием 3D-сканера Texel Portal и определение его оптимальных параметров; анализ концепта персонажа; работа над геометрией скана и определение инструментария и шагов обработки с использованием программы ZBrush; создание одежды с помощью Marvelous Designer и последующая её детализация; оптимизация модели с учетом требований; текстурирование в Substance Painter 2 и создание карт*.

Разработанная методика в дальнейшем будет востребована в различных областях, начиная с применения моделей в любительских играх, виртуальной реальности и заканчивая индустрией моды.

Сведения об авторе

Никитиных Елена Игоревна – кандидат технических наук, доцент Российского государственного университета им. А.Н. Косыгина, Москва, e-mail: elenanik_67@mail.ru

About the author

Nikitinyh Elena Igorevna – Ph.D. of Technical Sciences Associate Professor Russian State University named after A.N. Kosygina, Moscow, e-mail: elenanik_67@mail.ru

* Никитиных Е.И., Шехирева В.И. Создание 3D-модели персонажа по концепту на основе BODY-скана // Молодые ученые – инновационному развитию общества (МИР-2017): тез. докл. 69-й внутривуз. науч. студ. конф. Ч. 3. – М.: Изд-во РГУ им. А.Н. Косыгина, 2017. – 212 с.

НАВИГАЦИЯ АВТОНОМНОГО МОБИЛЬНОГО РОБОТА С ПОМОЩЬЮ СИСТЕМЫ ПОЗИЦИОНИРОВАНИЯ MARVELMIND

М.И. Харламов, О.В. Гончаровский
Пермский национальный исследовательский
политехнический университет, Пермь

В работе рассмотрена проблематика навигационных систем внутри помещения. Была приведена структура разработки системы позиционирования внутри помещения для автономного мобильного робота на основе системы позиционирования Marvelmind.

Ключевые слова: системы позиционирования, автономный мобильный робот, мобильный маяк.

NAVIGATION OF THE AUTONOMOUS MOBILE ROBOT BY THE MARVELMIND POSITIONING SYSTEM

M.I. Kharlamov, O.V. Goncharovsky
Perm National Research Polytechnic University, Perm

In the work the problems of indoor positioning system are considered. A structure for the development of an indoor positioning system for autonomous mobile robot based on the Marvelmind positioning system was presented.

Keywords: positioning systems, Marvelmind, autonomous mobile robot, beacon.

Глобальная спутниковая навигационная система (ГСНС) состоит из сети или совокупности спутников на околоземной орбите, передающих сигналы, использующиеся наземными приемниками в целях навигации. Наиболее развитой и широко используемой системой ГСНС в настоящее время является система GPS, функционирование которой обеспечивается Соединенными Штатами Америки. К другим системам ГСНС относятся российская система ГЛОНАСС и находящиеся в процессе создания навигационные системы Galileo (Европа) и Compass (Китай). Один из аспектов основанной на использовании ГСНС навигации заключается в том, что такая навигация не может осуществляться в помещении, так как стены и крыши зданий действуют как препятствия, которые не пропускают или ослабляют спутниковые сигналы. При таких условиях передаваемые спутниками сообщения или недоступны, или обладают очень низкими уровнями мощности сигнала, меньшими, чем уровень мощности фонового шума, так что они не пригодны к использованию стандартным приемником GPS.

В настоящее время существует несколько популярных систем позиционирования для помещений. Все они нужны для того, чтобы осуществлять навигацию в замкнутом пространстве, в котором невозможна работа систем спутниковой навигации. Все технологии можно разделить на несколько видов позиционирования:

- радиочастотное позиционирование (Wifi, Bluetooth, сотовая связь, NFER, UWB, CSS и SDS-TWR);
- локальное позиционирование (инфракрасное, ультразвуковое);
- активные, пассивные RFID.

Применение систем идентификации и позиционирования (определения местонахождения) материальных объектов – людей, транспортных средств, подвижных механизмов и различных предметов – актуальное направление оптимизации технологических и бизнес-процессов. Такие системы уже применяются в самых разных сферах деятельности: от мониторинга пациентов, персонала, лекарств и оборудования в клиниках до контроля местонахождения инструментов, сборочных единиц и рабочих на конвейере, от поиска пострадавших при чрезвычайных ситуациях до наблюдения за животными при свободном содержании для выявления заболевших. Разнообразие областей и направлений использования породило разнообразие технологий.

В данной работе рассматривается наиболее подходящая для нас система Marvelmind, основанная на стационарных ультразвуковых маяках. Навигационная система Marvelmind для помещений предназначена для обеспечения передачи данных о местоположении автономных роботов и транспортных средств, но она также может быть использована для отслеживания других объектов, где можно установить мобильный маяк.

Система основана на стационарных ультразвуковых маяках, объединенных радиointерфейсом в нелицензируемом диапазоне. Местонахождение мобильного маяка, установленного на роботе (автомобиле, вертолете, человеке), рассчитывается на основе задержки распространения ультразвукового сигнала к набору стационарных ультразвуковых маяков с использованием трилатерации*.

Ключевым требованием системы для функционирования должным образом является беспрепятственная передача сигнала на мобильный маяк, состоящий из трех или более стационарных маяков

* Marvelmind Indoor Navigation System.

одновременно. Для интеграции навигационной системы для помещений Marvelmind в систему автономного мобильного робота необходимо построить карту «рабочей» местности и настроить ее на корректное отображение желаемого объекта в пространстве.

Для примера предположим, что наша «рабочая» площадь имеет форму квадратной комнаты. Первым делом необходимо расставить стационарные маяки навигационной системы Marvelmind в местах с наибольшей зоной покрытия сигнала, т.е. разместить их на всех четырех стенах в верхних точках, как показано на рис. 1.

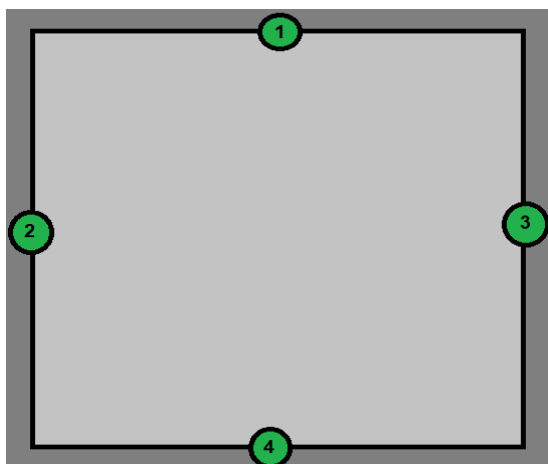


Рис. 1. Расположение стационарных маяков на «рабочей» площади: 1–4 – номера используемых стационарных маяков

Маяки навигационной системы Marvelmind обладают достаточно высокой точностью ± 2 см и дальностью действия до соседних маяков 50 м, что позволяет располагать их на большом расстоянии друг от друга. Все маяки связываются и находят друг друга при помощи установленного USB-роутера/модема и питаются от Li-polymer-аккумуляторов. Далее необходимо установить мобильный маяк на автономного мобильного робота. Этот маяк и будет основным маяком, на который будет нацелена навигационная система. Расположение маяка (робота) на импровизированной карте представлено на рис. 2.

После установки маяков в помещении необходимо определять, пересчитывать координаты из системы позиционирования в координаты карты и наоборот (для задания цели). Для привязки координат

системы позиционирования к координатам карты помещения на автономного мобильного робота установлен компас. Сначала с помощью компаса определяется азимут базовой стены помещения, на которой устанавливается маяк 1, сопоставленный координате (0,0) системы позиционирования.

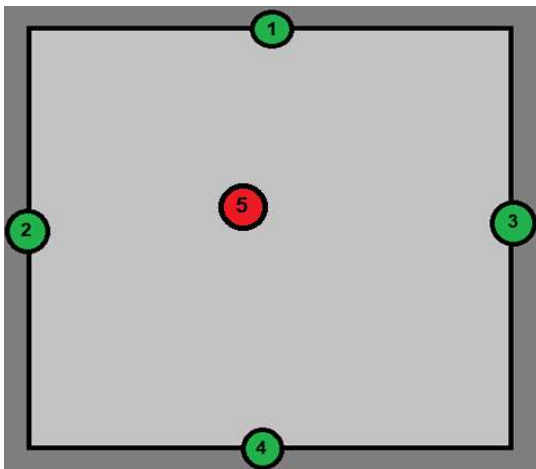


Рис. 2. Пример расположение маяков системы позиционирования на карте помещения: 1-4 – расположение стационарных маяков, 5 – расположение мобильного маяка

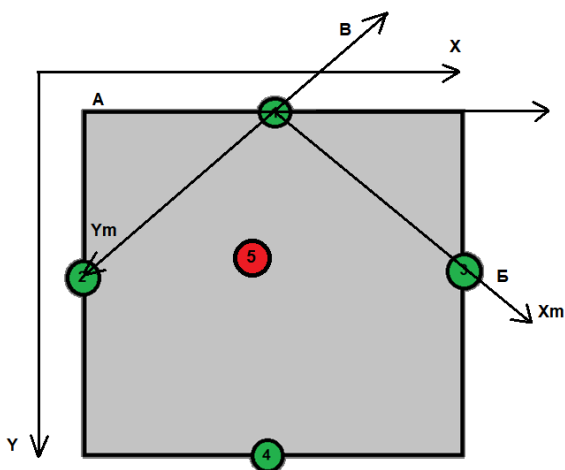


Рис. 3. Зависимость системы координат Marvelmind от условий

Установка мобильного маяка в точку A с координатой $(0,0)$ на карте помещения, определение его координат в системе позиционирования и знание азимута базовой стены позволяют определить угол между соответствующими осями карты помещения и карты системы позиционирования (рис. 3). Это позволит пересчитывать координаты карты помещения в координаты системы позиционирования.

На рис. 3 стрелками X_m и Y_m обозначены координаты навигационной системы Marvelmind, а стрелками X и Y – системы координат карты помещения.

Сведения об авторах

Харламов Максим Игоревич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: g1.awbg@gmail.com

Гончаровский Олег Владленович – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: 35911953@mail.ru

About the authors

Kharlamov Maxim Igorevich – Student Perm National Research Polytechnic University, Perm, e-mail: g1.awbg@gmail.com

Goncharovsky Oleg Vladlenovich – Ph.D. in Technical Sciences, Associate Professor of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: 35911953@mail.ru

SLAM-НАВИГАЦИЯ АВТОНОМНОГО МОБИЛЬНОГО РОБОТА С КАМЕРОЙ ВОСПРИЯТИЯ ГЛУБИНЫ ЦВЕТА

А.А. Чащин, О.В. Гончаровский

Пермский национальный исследовательский
политехнический университет, Пермь

В работе рассмотрен способ локализации мобильного робота с использованием датчика RGB-D Kinect. Использование RGB-D Kinect-датчика вместе с использованными ориентирами в целях локализации заставляют робота следовать за желаемым путем точно.

Ключевые слова: локализация, RGB-D Kinect-датчик, автономный мобильный робот, ориентиры.

SLAM NAVIGATION OF THE AUTONOMOUS MOBILE WITH A COLOR DEPTH PERCEPTION CAMERA

A.A. Chashchin, O.V. Goncharovsky

Perm National Research Polytechnic University, Perm

A method for localizing a mobile robot using a RGB-D Kinect sensor is discussed. Using the RGB-D Kinect sensor, along with the used landmarks, for localization purposes, forcing the robot to follow the desired path exactly.

Keywords: localization, RGB-D Kinect sensor, autonomous mobile robot, landmarks.

Чтобы мобильный робот мог быть использован для какой-либо значительной цели в реальной жизни, ему нужно точно знать свою позицию и ориентацию в системе координат карты во время его работы.

Традиционно робот пытается вычислить свою позицию от количества вращений его колес. Этот метод называют одометрия. Колеса оснащены кодерами, которые преобразовывают вращения колес в электрические импульсы. Но информация из одометрии подвержена различным ошибкам. Есть два типа ошибок одометрии: систематические и несистематические ошибки. Оба влияют на ориентацию мобильного робота в пространстве и поэтому приводят к изменению его траектории в нежелательный вид.

Источники систематических ошибок: колеса разного диаметра, среднее число обоих диаметров колеса отличается от номинального диаметра, неточное совмещение колес, ограниченная частота дискретизации кодера.

Источники несистематических ошибок: перемещение по неровным этажам, перемещение по неожиданному объекту на полу, уменьшение колес из-за скользких этажей, ускорения, быстрый поворот колес (скольжение), действие внешних сил (взаимодействие), действие внутренних сил (колесо солонки), неодноточечный контакт колеса с полом.

Вышеупомянутые источники ошибок в одометрии влияют на управление движением робота. Следовательно, робот должен дополнительно обращаться к ориентирам в среде, чтобы определить его позицию точно. Процесс, в котором мобильный робот в состоянии обнаружить свою истинную позицию точно в системе координат карты, назван локализацией.

Для обращения к различным объектам ориентиров в среде роботом используются различные датчики как гидролокаторы, лазеры и т.д. Один из таких датчиков RGB-D Kinect, который и рассматривается в данной работе.

Новый датчик – датчик Kinect RGB-D, придуманный в Microsoft в недавнем прошлом, хотя и для другой цели, находит обширное применение в области робототехники. Он состоит из инфракрасного лазерного излучателя, инфракрасной камеры и RGB-камеры. Таким образом, мы получаем трехмерное цветное изображение окружающей среды с использованием Kinect RGB-D-датчика (рис. 1).



Рис. 1. Датчик Kinect RGB-D

Сочетание цвета и глубины изображения имеет свои собственные преимущества (например, объект может быть идентифицирован по его цвету, а затем его диапазон глубины изображения дает свое положение относительно датчика).

Мы используем идентичные (по форме, размеру и цвету) ориентиры. Их поместили в произвольных расположениях в рабочей среде робота. В нашем методе мы выбрали цилиндрические ориентиры, которые отличаются цветом от остальных объектов в рабочей среде. Ориентиры расположены так, что при движении робота, как минимум, один или два ориентира появятся в диапазоне видимости датчика Kinect. Робот пытается извлечь местоположение этих ориентиров, основанных на их цвете и форме. Следовательно, предложенный метод оценивает позиции робота в системе координат карты, используя алгоритм локализации Монте–Карло, который убождает шумным измерительным вводам.

Традиционные подходы локализации используют карты рабочей среды. В нашем случае нам нужно поместить ориентиры в известных местоположениях и сделать доступным для робота общее количество используемых ориентиров, а также отдельные местоположения каждого ориентира с точки зрения их координат (x, y) в системе координат карты.

У этого метода очень низкие требования к ресурсам для достижения цели. Кроме того, этот подход улучшает гибкость и скорость запуска робота в новых неизвестных средах. Для того чтобы понять, куда нам расположить наши ориентиры, нужно построить карту рабочей среды, в которой будет двигаться робот.

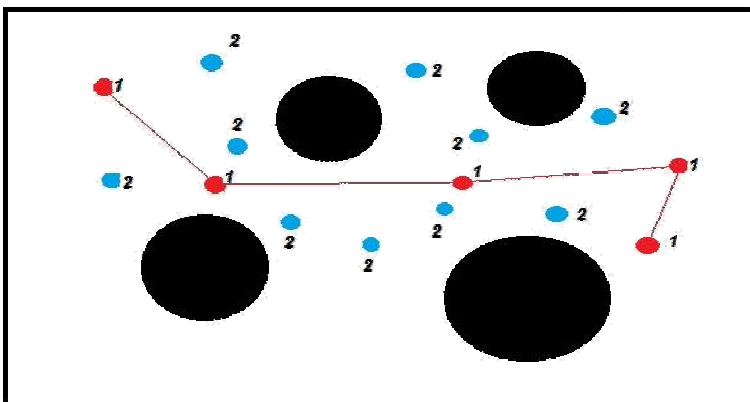


Рис. 2. Примерная карта рабочей среды: кружки с цифрой 1 – это вспомогательные ориентиры, которые показывают идеальный путь движения робота; кружки с цифрой 2 – это ориентиры для датчика Kinect RGB-D; большие кружки – это препятствия в рабочей среде

Когда робот начинает движение, благодаря компасу мы знаем его направление движения, а благодаря кодеру – его скорость. Изначально мы добавляем роботу отклонение в направлении его движения. Он начинает двигаться в определенном направлении, и мы только примерно знаем его местоположение на карте из-за компаса и кодера.

Когда на роботе датчик Kinect RGB-D засекает в своей видимости наши расположенные ориентиры, он считывает до них расстояние и тем самым уточняет свое местоположение на карте, выбирает новый азимут, поворачивает на него и двигается вперед до следующего вспомогательного ориентира. Этот цикл не заканчивается, пока робот не доедет до конечной точки на карте, которую мы выбрали.

Библиографический список

1. Eliazar A., Parr R. DPSLAM: Fast, Robust Simultaneous Localization and Mapping Without Predetermined Landmarks // IJCAI'03. – 2003. – P. 1135–1142.

2. Kai M., Wurm C., Stachniss G. Grisetti. Bridging the Gap Between Feature and Gridbased SLAM. // Robotics and Autonomous Systems. – 2010. – Т. 58. – № 2. – P 140–148.

3. Stachniss C. Gridbased FastSLAM. – URL: <http://ais.informatik.unifreiburg.de/teaching/ws12/mapping/pdf/slam12gridfastslam4.pdf>

Сведения об авторах

Чашин Андрей Андреевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: hardweiser@gmail.com

Гончаровский Олег Владленович – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: 35911953@mail.ru

About the authors

Chashchin Andrey Andreevich – Student Perm National Research Polytechnic University, Perm, e-mail: hardweiser@gmail.com

Goncharovsky Oleg Vladlenovich – Ph.D. in Technical Sciences, Associate Professor of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: 35911953@mail.ru

Секция 2

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

УСТРОЙСТВО ДЛЯ ОТОБРАЖЕНИЯ ИНФОРМАЦИИ С МЕХАНИЧЕСКОЙ РАЗВЕРТКОЙ

И.Г. Агибалов, Д.А. Тупикин

Ливенский филиал Орловского государственного
университета им. И.С. Тургенева, Ливны

Рассмотрена возможность создания действующего прототипа устройства с альтернативным методом отображения информации, с целью уменьшить площадь неактивного прибора.

Ключевые слова: визуализация, отображение информации, механическая развертка.

DEVICE FOR DISPLAYING INFORMATION WITH A MECHANICAL SCANNER

I.G. Agibalov, D.A. Tupikin

Livny's branch of Oryol State University
named after I.S. Turgeneva, Livny

The possibility of creating an active prototype of a device with an alternative method of displaying information is considered in order to reduce the area of the inactive device.

Keywords: visualization, display of information, mechanical scanning.

Разработанное устройство основано на эффекте Боба Блика – иллюзия «висящего» в воздухе изображения с помощью быстро перемещающихся источников света. Применение этого эффекта не получило широкого распространения.

Задача разрабатываемого устройства состоит в том, чтобы уменьшить площадь, занимаемую индикатором в неактивном состоянии. Альтернативой разработанному устройству является светодиодное табло в неактивном состоянии, в то время, когда она ничего не отображает, такая матрица занимает значительное пространство. Если применить механическую развертку, то занимаемая в неактивном состоянии площадь резко сокращается. Так же резко сокращается число необходимых источников света.

Устройство использует инерцию зрения и за счет синхронизации вращения и переключения светодиодов определенным образом в разные моменты времени способно при минимальном количестве индикаторов создавать достаточно четкие статические и динамические изображения с произвольным информационным наполнением.

В качестве аппаратной основы системы управления устройством использован микроконтроллер Atmel ATmega16. Устройство состоит из печатной платы и компонентов, представленных на рис. 1.

Электрическая схема устройства достаточно проста и хорошо видна на изображении печатной платы. Питание подается при помощи щетки под платой. Рядом с контроллером находятся: конденсатор для стабилизации напряжения, кварцевый резонатор частотой 16 МГц для тактирования контроллера, балансировочные конденсаторы по 22 пФ на выводах резонатора, датчик Холла и выводы для программирования. Вращение происходит при помощи бесколлекторного двигателя. Разводка печатной платы представлена на рис. 2.

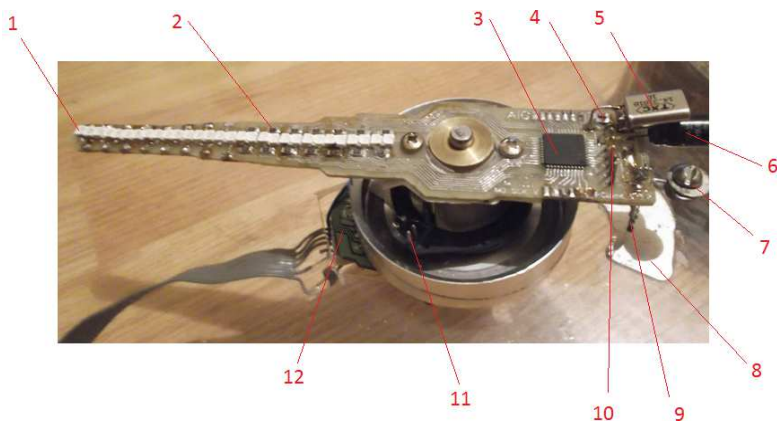


Рис. 1. Разводка печатной платы представлена: 1 – светодиоды, 2 – сопротивления 300 Ом, 3 – микроконтроллер, 4 – балансировочные конденсаторы 22 пФ, 5 – кварцевый резонатор с частотой 16 МГц, 6 – конденсатор 10 мкФ, 7 – грузик для балансировки, 8 – неодимовый магнит, 9 – датчик Холла, 10 – интерфейс программирования, 11 – вывод щетки питания, плата управления двигателем

Изображение печатной платы представлено на рис. 2.

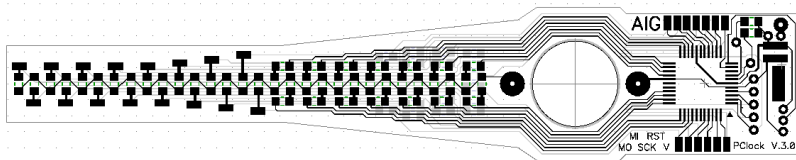


Рис. 2. Изображение печатной платы

Программа контроллера состоит из нескольких блоков:

- блок констант содержит информацию о создаваемых изображениях в виде шестнадцатеричных кодов портов микросхемы на каждый из 360 градусов;

- блок переменных, где переменные обрабатываются в оперативной памяти микросхемы. Они отвечают за отсчет времени, вычисление угла наклона, режим работы, автоподстройку при изменении скорости вращения, сдвиг бегущей строки;

- блок прерываний обрабатывает событие при срабатывании датчика Холла. Часть исходного кода блока представлена на рис. 3.



Рис. 3. Работа устройства

Прерывание наступает по возрастающему фронту сигнала. Здесь происходит автоподстройка частоты отображения для синхронизации с двигателем. Также здесь происходит сдвиг бегущей строки на одну позицию. Дабы не выходить за пределы массива, реализовано обновление указателя сдвига. Счетчики автоподстройки при этом обнуляются. Блок прерываний также содержит обработку прерывания по таймеру.

При совпадении количества прерываний по таймеру со значением автоподстройки происходят переключение градуса угла поворота, установка новых значений управляющих выводов микросхемы. Для автоподстройки используется счетчик количества смен градуса угла. Значение автоподстройки изменяется так, чтобы на момент срабатывания прерывания от датчика счетчик показывал число примерно 180.

Блок инициализации задействуется при включении устройства – микросхема выполняет инициализацию, необходимую для настройки и нормальной работы таймеров, прерываний, регистров вводов/вы-

водов и тактирования. Устройство работает с небольшими отклонениями при отображении, это вызвано тем, что частота вращения постоянно изменяется из-за внешних факторов.

Возможно настроить не только отображение статичных картинок, но и анимации. Для удобства кодирования изображения также было написано отдельное приложение, выполняющее конвертацию изображений из декартовой системы в радиальную в соответствии с разверткой. Частота вращения может плавно регулироваться посредством делителя напряжения на управляющем выводе микросхемы-драйвера двигателя.

Испытания показывают, что при снижении частоты вращения устройства качество создаваемого изображения практически не снижается до достижения нижнего предела частоты, зависящего от инерционности зрения.

Библиографический список

1. SUNISS. Первый этап завершен [Электронный ресурс] // Chip O'K!, 2011. – URL: <http://chipok.ru/archives/803> (дата обращения: 22.09.2017).

2. ATmega16 [Электронный ресурс] // Amtel, 2011. – URL: <http://www.atmel.com/devices/ATMEGA16.aspx> (дата обращения: 22.09.2017).

Сведения об авторах

Агибалов Иван Геннадьевич – студент Ливенского филиала Орловского государственного университета им. И.С. Тургенева, Ливны.

Тупикин Дмитрий Александрович – кандидат технических наук, доцент кафедры «Инженерное образование» Ливенского филиала Орловского государственного университета имени И.С. Тургенева, Ливны, e-mail: tupidim@mail.ru

About the authors

Agibalov Ivan Gennadievich – Student Livny's branch of Oryol State University named after I.S. Turgenev, Livny.

Tupikin Dmitry Alexandrovich – Ph.D. in Technical Sciences, Associate Professor of the department of engineering education Livny's branch of Oryol State University named after I.S. Turgeneva, Livny, e-mail: tupidim@mail.ru

РАЗРАБОТКА СИСТЕМЫ ПОДГОТОВКИ ПОПУТНОГО НЕФТЯНОГО ГАЗА

А.В. Арефьева, В.В. Тугов

Оренбургский государственный университет, Оренбург

В данной статье рассматривается проблема повышения эффективности переработки такого важного стратегического нефтехимического ресурса, как попутный нефтяной газ. Представлены новая разработанная технологическая схема для процесса его подготовки, а также результаты оценки процесса с помощью разработанного программного средства.

Ключевые слова: попутный нефтяной газ, подготовка газа, технологическая схема, программное обеспечение.

DEVELOPMENT OF PREPARING ASSOCIATED PETROLEUM GAS SYSTEM

A.V. Arefeva, V.V. Tugov

Orenburg State University, Orenburg

This article considers the problem of efficiency gains for important strategic petrochemical resource such as associated petroleum gas. New developed technological scheme for gas preparation process and results of the process evaluation with developed software are presented.

Keywords: associated petroleum gas, gas preparation, technological scheme, software.

Вопрос эффективной переработки продуктов нефте- и газодобычи (в том числе сопутствующих) актуален для современных предприятий этой отрасли. В разрезе остро стоящей проблемы обеспечения непрерывного и устойчивого развития общества на основе энергетической стабильности России в области недропользования на первый план выходят не такие гиганты энергетической безопасности, как нефть и газ, а другие стратегически важные энергетические и нефтехимические ресурсы, такие как попутный нефтяной газ (ПНГ). В связи с этим невосполнимый многокомпонентный природный ресурс ПНГ и его эффективное использование в настоящее время имеют не только высокую стратегическую, но и экономическую, социальную значимость [1].

Также этот вопрос тесно переплетается с проблемой независимости предприятий от объектов энергообеспечения. Очевидные перспек-

тивы в данной теме открывает применение поршневых газовых двигателей внутреннего сгорания для комбинированной выработки электрической и тепловой энергии, неоспоримыми преимуществами которых являются высокий коэффициент полезного действия (КПД), полная независимость от региональных энергосетей, а следовательно, и от роста тарифов, надежность, отсутствие затрат на строительство подводящих и распределительных сетей. Подобный подход представляется более простым и экономически выгодным в отличие от классических подходов. Например, сжигание попутного нефтяного газа на факела приводит к выбросу в атмосферу огромного количества разнообразных загрязняющих веществ, таких как диоксид серы, сажевые частицы, окислы азоты, углекислый газ (факельное сжигание ПНГ дает около двух процентов его мировых выбросов [2]). Создание новых технологий подготовки ПНГ для его использования в различных целях (в качестве самостоятельного топливного газа или сырья для химических и нефтехимических производств) – один из вариантов решения проблемы рационального использования ресурсов ПНГ [3].

В качестве основы для новой технологии используется процесс конверсии газа в объемных проницаемых матрицах с сжиганием попутного нефтяного газа в реакторе с добавлением кислородсодержащего газа [4]. Параллельно в настоящее время ведется работа по разработке технологии на основе фильтрационного горения газа с использованием тлеющего разряда.

Поверхностное горение, которое используется в подобных устройствах, позволяет осуществлять процесс горения с температурой ниже температуры факельного горения, но с высокой температурой поверхности самой объемной матрицы – до 800 °С. При этом параллельно проходит несколько процессов – горение в узкой зоне фронта пламени у внутренней поверхности матрицы (образование продуктов горения происходит там же), а также теплообмен между поверхностью матрицы и продуктами сгорания.

Подобный обмен значительно увеличивает скорости протекания реакции – продукты, поступающие в фронт пламени, подогреваются за счет рекуперации тепла продуктов сгорания. Все это повышает степень полноты конверсии горючего в целом, а также снижает процент выброса продуктов неполного сгорания (монооксид углерода и др.).

Технологическая схема разработанного процесса представлена на рис. 1.

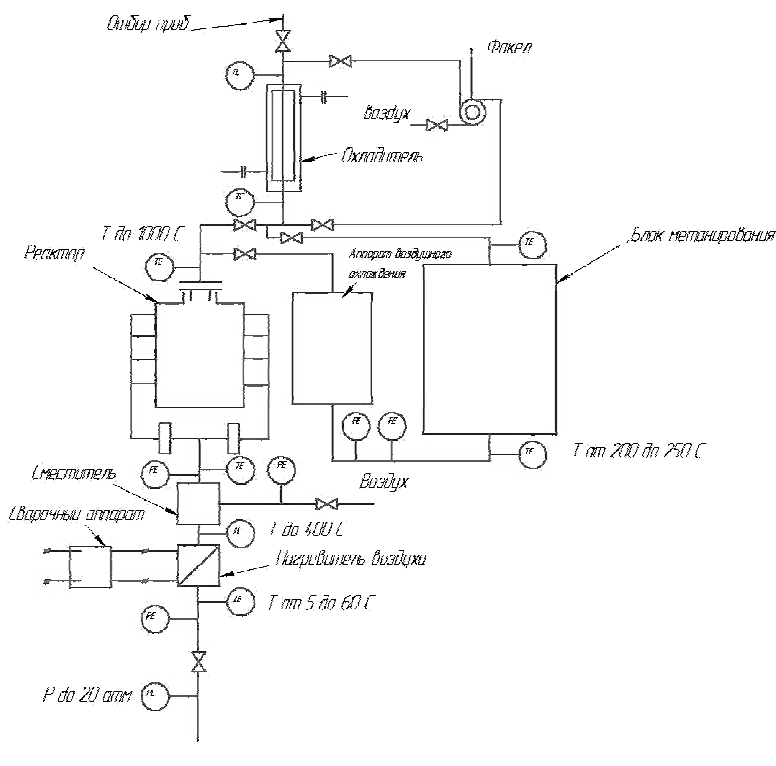


Рис. 1. Технологическая схема процесса

Промежуточным продуктом подготовки является синтез-газ, обычно используемый в качестве сырья для химической промышленности. Конечным продуктом является метан. После подготовки он поступает в двигатель внутреннего сгорания в качестве топливного газа.

Преимущества разработанной технологии – возможность замены попутного нефтяного газа на альтернативные источники, а также возможность использования промежуточного продукта – синтез-газа – в других целях.

Для оценки процессов подготовки и последующего использования топливного газа было разработано программное средство, состоящее из двух модулей. Экранная форма модуля программы для оценки эффективности работы двигателя внутреннего сгорания на полученном топливном газе представлена на рис. 2.

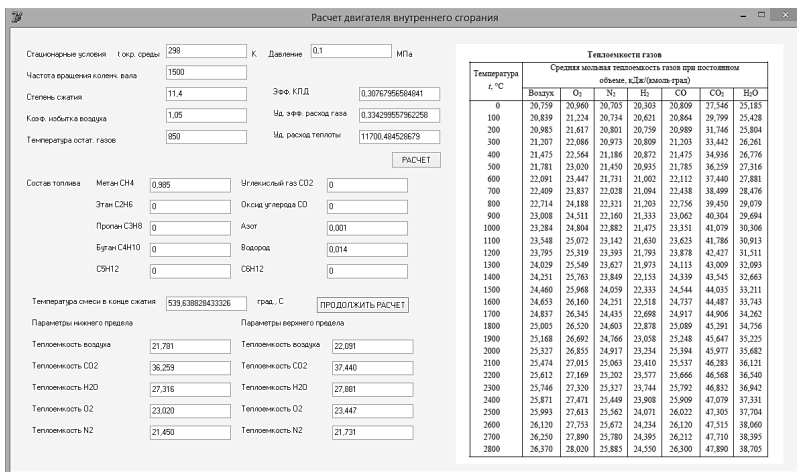


Рис. 2. Экранная форма программы расчета двигателя внутреннего сгорания, работающего на полученном топливном газе

На рис. 3 представлена экранная форма модуля программы для расчета температуры поверхности матрицы, позволяющая анализировать процесс горения на поверхности проницаемой матрицы в горелочных устройствах.

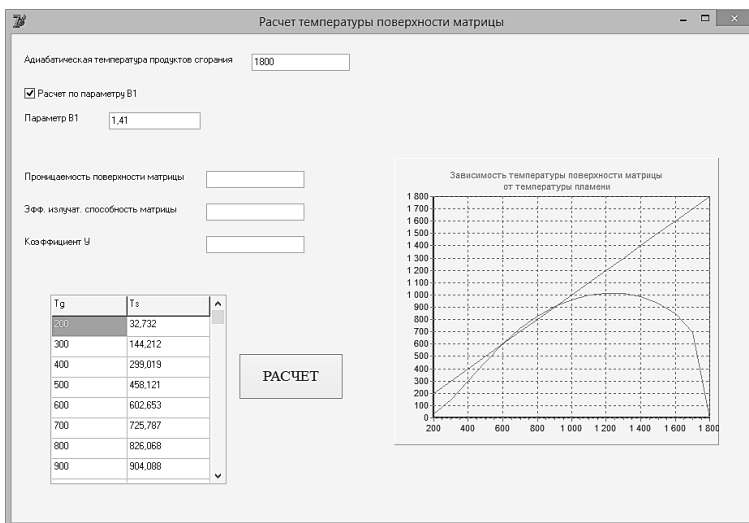


Рис. 3. Экранная форма программы для расчета температуры поверхности матрицы

Результаты проведенного анализа эффективности двигателя внутреннего сгорания, который проводился с помощью разработанного программного средства, показал рост эффективного КПД двигателя на 10–15 %.

Таким образом, разработанная технология переработки попутного нефтяного газа за счет использования процессов матричного горения позволяет эффективно использовать попутный нефтяной газ в качестве топлива для газопоршневых установок.

Библиографический список

1. Ильина М.Н. Подготовка попутного нефтяного газа к сжиганию в условиях автономного энергообеспечения нефтепромыслов: автореф. дис. ... канд. техн. наук. – Томск, 2009.

2. Аксенов А.Н. Экономический механизм рационального использования попутного нефтяного газа: автореф. дис. ... канд. экон. наук. – СПб., 2013.

3. Арефьева А.В., Тугов В.В. Исследование эффективности технологии подготовки попутного нефтяного газа // Компьютерная интеграция и ИПИ-технологии: материалы VIII Всерос. науч.-практ. конф. – Оренбург, 2017. – С. 586–589.

4. Способ переработки отходов, содержащих углеводороды: пат. 2116570 Рос. Федерация, МПК F23G 7/0 / Г.Б. Манелис, В.П. Фурсов, Л.Н. Стесик, Г.С. Яковлева, С.В. Глазов, Е.В. Полианчик, Н.Г. Альков; Институт химической физики в Черноголовке РАН. – № 96119443/03; заявл. 25.09.1996; опубл. 27.07.1998.

Сведения об авторах

Арефьева Александра Викторовна – студентка Оренбургского государственного университета, Оренбург, e-mail: Arefeva-a-v@mail.ru

Тугов Виталий Валерьевич – кандидат технических наук, доцент кафедры «Управление и информатика в технических системах» Оренбургского государственного университета, Оренбург, e-mail: sau@mail.osu.ru

About the authors

Arefeva Aleksandra Viktorovna – student Orenburg State University, Orenburg, e-mail: Arefeva-a-v@mail.ru

Tugov Vitalii Valerevich – Ph.D. in Technical Sciences, Associate Professor of the department of control and informatics in technical systems Orenburg State University, Orenburg, e-mail: sau@mail.osu.ru

НАВИГАЦИЯ И ПОЗИЦИОНИРОВАНИЕ

М.Н. Гатилова

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассмотрены Indoor-навигация, области её применения и реализации.

Ключевые слова: навигация, позиционирование, Beacon, Marvelmind.

NAVIGATION AND POSITIONING

M.N. Gatilova

Perm National Research Polytechnic University, Perm

In this article, we consider Indoor navigation, its application and implementation.

Keywords: navigation, positioning, Beacon, Marvelmind.

Indoor-навигация поможет ориентироваться человеку в здании, получить необходимую информацию, найти нужное место или даже автомобиль на парковке, и всё это займёт секунды. Это помогает сэкономить время посетителям и привлечь новых клиентов компании, необходимо всего лишь установить маяки. Сфера их применения практически не ограничена: конференции, музеи, выставки: возможность быстро найти нужный экспонат, получить о нём необходимую информацию. Спортивные залы, кафе, магазины, курорты: можно быстро находить и получать сведения о блюдах, представленной продукции, определить местонахождение тренажёра, различных аттракционов и получить информацию об их использовании. Больницы: пациент может легко найти нужный кабинет и получить информацию о враче, а врач при обходе в стационаре может получать электронную карточку пациента. Помощь слепым людям, возможность получать информацию о своём местоположении, определить путь, как пройти в нужное место, получить информацию о предложенных товарах с помощью голосовых уведомлений.

Маяк – это небольшой радиопередатчик Bluetooth, графически он представлен на рис. 1, состоит из процессора, радио и батареи, часто маяки используют небольшие батареи с литиевым аккумулятором или работают через USB-штекер. Маяк транслирует радиосигнал, состоящий из комбинации букв и цифр, графически представленных на рис. 2, с регулярным интервалом приблизительно 1/10 секунды.

iBeacon – это протокол-подмножество Bluetooth Low Energy, который позволяет узнать: UUID, Major, Minor для маячка, силу сигнала от маячка*.

Преамбула (4 байта) – префикс пакета, значение 4с000215 не меняется, обозначает маячок, состоит из 4 полей: идентификатор компании (2 байта, в данном примере – 4с00), тип (1 байт, в примере – 0х02) и длина данных (1 байт, значение – 0х15).

Proximity UUID (16 байт) – идентификатор группы Beacon-маяков. Например, есть несколько торговых залов, в которых требуется разместить маяки. В таком случае во всех этих залах маяки будут иметь один и тот же UUID, назначенный пользователем, и это позволит отличать свои маяки от других.

Major (2 байта) – позволяет различать небольшой набор маяков внутри одной группы. То есть внутри одной большой группы маяков, идентифицируемой UUID, может быть несколько подгрупп, каждая из которых идентифицируется по номеру мажора. Например, в примере каждому залу можно присвоить свой номер мажора. Если маяками требуется охватить несколько этажей здания, обычно с каждым этажом ассоциируют свой номер мажора.

Minor (2 байта) – номер, идентифицирующий сам маяк внутри мажора. Связка uuid + мажор + минор позволяет однозначно идентифицировать маяк и по этим данным определить по таблице соответствия маячков их координатам, координату самого маячка.

TX Power (параметр К на рисунке выше, 2 байта) – эталонное значение мощности маячка, представляющее собой силу сигнала на расстоянии в 1 м от маячка. Измеряется и записывается в маячок 1 раз при его производстве. Данная константа используется при определении расстояния от пользователя до маячка. Первый бит является знаковым (1 – «-», 0 – «+»).

Технология iBeacon отрывает невероятные возможности получения данных в общественных местах. Однако существуют и огромные минусы, например, низкая точность позиционирования, низкая степень защиты.

Indoor “GPS”. Сверхточная навигация (± 2 см) для автономных роботов и систем, представленная Marvelmind robotics. Идея идентичная: отслеживание положения внутри помещения объектов и людей,

* iBeacon – Frequently Asked Questions / Cisco and or its affiliates. – 2014.

снабжённых маячками, однако отличает её абсолютная точность, 1–3 % от положения до мобильного маяка. Радиус покрытия до 50 м, а площадь до 1000 м², при этом не требуется ничего измерять или вводить координаты, маяки сами автоматически сформируют систему. Покрытие больших территорий осуществляется аналогично сотовым сетям. Единственное замечание: необходимо обеспечить прямую видимость между мобильным и стационарными маяками или при необходимости установить дополнительные, тогда необходимая точность будет получена на объектах любой сложности. В комплект входят мобильный маяк, 4 стационарных, роутер и дополнительный софт.

Применение так же весьма обширно: автоматическая доставка, перемещение необходимых пакетов на предприятии, в офисах, развоз таблеток в больнице, доставка заказов в кафе, выдача отправок на складе, перемещение сумок на вокзалах и в аэропортах, развоз вещей и доставка питания в отелях; автоматическое патрулирование объекта или отслеживание; помощь аналитикам, получение данных для оптимизации, отслеживание положения груза. Современные системы навигации и позиционирования можно внедрять практически в любую сферу и получить пользу.

Сведения об авторе

Гатилова Марина Николаевна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: mng7@list.ru

About the author

Gatilova Marina Nikolayevna – Student Perm National Research Polytechnic University, Perm, e-mail: mng7@list.ru

ПРОБЛЕМЫ АВТОМАТИЗАЦИИ СИСТЕМ ОЧИСТКИ ОТРАБОТАННОГО МОТОРНОГО И ТРАНСМИССИОННОГО МАСЕЛ

О.М. Горбачева, А.С. Боровский

Оренбургский государственный университет, Оренбург

Рассматривается актуальность автоматизирования процессов очистки отработанных масел. Выбран наиболее целесообразный метод очистки моторных масел – очистка на центрифуге. В зависимости от основных параметров процесса очистки изучены зависимости влияния технологических параметров на степень очистки масла. Предложена установка, взятая за прототип, для ее дальнейшей автоматизации, с целью улучшения эффективности очистки масла.

Ключевые слова: методы очистки, параметры процесса, вязкость, установка для очистки, автоматизация.

PROBLEMS OF AUTOMATION OF SYSTEMS FOR CLEANING ENGINES AND TRANSMISSION OILS

O.M. Gorbacheva, A.S. Borovsky

Orenburg State University, Orenburg

In this article, the urgency of automating the processes for cleaning used oils is given. The most expedient method of cleaning motor oils is chosen – centrifuge cleaning. Depending on the main parameters of the purification process, the dependence of the influence of technological parameters on the degree of oil purification is studied. The installation, taken as a prototype, is proposed for its further automation, in order to improve the efficiency of oil purification.

Key words: cleaning methods, process parameters, viscosity, cleaning plant, automation.

В связи с высокими темпами роста источников образования отработанных масел встает вопрос о применении эффективных технологий по его регенерации для последующего повторного использования. Внедрение автоматизированных установок для восстановления первоначальных свойств масел является экологически и экономически целесообразным. Главным достоинством автоматизированных систем по очистке отработанного масла является повышение эффективности технологического процесса, а также повышение безопасности производственного процесса. Поэтому встает вопрос о необходимости использования в процессе очистки отработанных масел именно автоматизированных систем.

Как видно из рис. 1, главным источником образования отработанного масла является транспорт: автомобильный и железнодорожный [1].

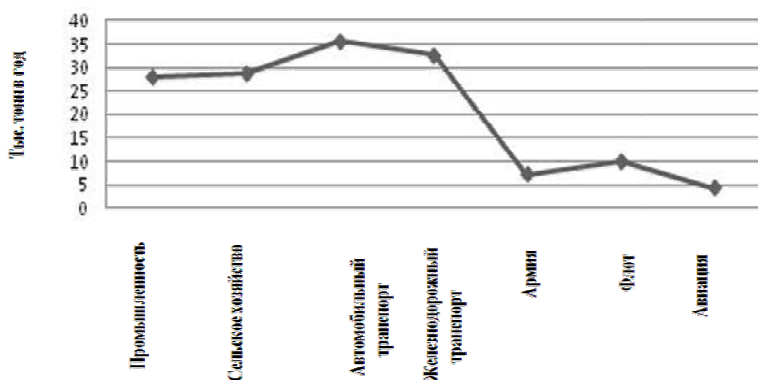


Рис. 1. Зависимость количества образованного масла от отрасли

На рис. 2 представлено количественное распределение отработанного масла по типам.

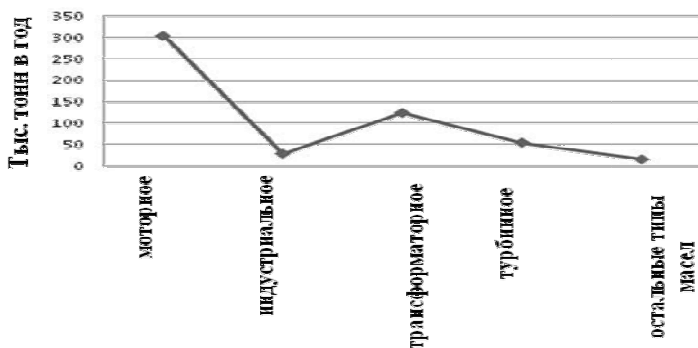


Рис. 2. Количество образованного масла в зависимости от типа

В связи с этим целесообразно изучить:

- существующие методы очистки отработанных моторных масел;
- основные параметры, влияющие на процесс очистки отработанного масла выбранным методом;
- принцип действия установки по очистке масла, принятой за прототип.

На сегодняшний день существуют три основных метода очистки отработанных масел: физико-химический, физический и химический (рис. 3).

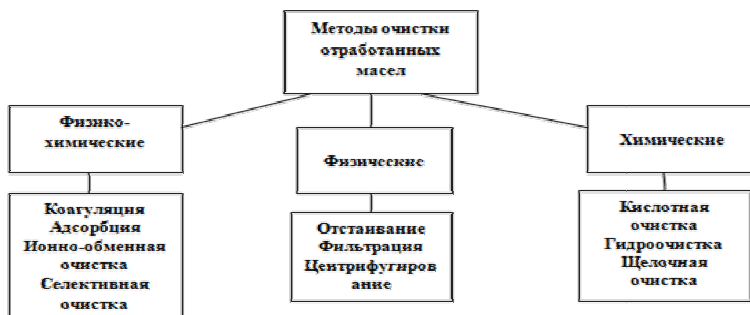


Рис. 3. Классификация методов очистки отработанных масел

К физико-химическим методам очистки отработанных масел относят: коагуляцию, метод адсорбции, метод ионно-обменной и селективной очистки.

Основными недостатками методов данного типа являются необходимость последующей обработки с целью нейтрализации кислых продуктов (метод коагуляции), контроль температуры при проведении процесса очистки (метод адсорбции) и недостаточно высокая степень очистки отработанного масла (ионно-обменный метод).

Химические методы очистки основаны на химическом взаимодействии привнесенных веществ с загрязняющими веществами, содержащимися в отработанном масле. К таким методам относят: метод кислотной очистки, щелочной метод, метод гидроочистки.

Недостатками методов данного типа являются образование побочных химически опасных веществ (кислый гудрон), а также высокая стоимость и сложность процесса очистки данным методом.

Физические методы очистки основаны на очистке отработанного масла при помощи физических сил. Такими методами являются: метод отстаивания, фильтрация, очистка при помощи центробежных сил.

Центробежная очистка масла является наиболее эффективным и высокопроизводительным методом удаления механических примесей и воды, при этом присадки, содержащиеся в масле, не удаляются.

Таким образом, проведя сравнительный анализ существующих методов очистки отработанного масла, можно сделать вывод о том,

что наиболее оптимальным по критериям эффективности очистки, стоимости и простоте является метод очистки отработанного масла при помощи центробежных сил (процесс центрифугирования).

Изучив сущность процесса осаждения при помощи центробежных сил, можно сказать о том, что скорость осаждения загрязняющих частиц зависит от интенсивности центробежного поля, а степень осаждения – от времени центрифугирования.

Осаждение мелких твердых частиц подчиняется закону Стокса [2]:

$$\omega = \frac{d^2(\rho_{\text{ТВ}} - \rho_{\text{Ж}})g}{18\mu}, \quad (1)$$

где ω – скорость осаждения; d – диаметр осаждаемой частицы; $(\rho_{\text{ТВ}} - \rho_{\text{Ж}})$ – разность между плотностью осаждаемой частицы и плотностью среды; μ – вязкость жидкости; g – ускорение силы тяжести.

Заменив ускорение силы тяжести g ускорением силы инерции a , получим:

$$\omega = \frac{d^2 \cdot (\rho_{\text{ТВ}} - \rho_{\text{Ж}}) \cdot a}{18 \cdot \mu}. \quad (2)$$

Выразим величину a :

$$a = \frac{\omega^2}{r} = \frac{(2 \cdot \pi \cdot r \cdot n)^2}{r} = 4 \cdot \pi^2 \cdot n^2 \cdot r, \quad (3)$$

где a – ускорение силы инерции; n – число оборотов в секунду.

Отсюда мгновенная скорость частицы, находящейся на расстоянии r от оси вращения,

$$\omega = \frac{dr}{dt} = \frac{2 \cdot \pi^2 \cdot d^2 \cdot (\rho_{\text{ТВ}} - \rho_{\text{Ж}}) \cdot n^2 \cdot r}{9 \cdot \mu}. \quad (4)$$

Время, необходимое для осаждения твердой частицы диаметром d на стенке,

$$\tau = \frac{9 \cdot \mu}{2 \cdot \pi^2 \cdot (\rho_{\text{ТВ}} - \rho_{\text{Ж}}) \cdot d^2 \cdot n^2} \cdot \ln\left(\frac{R}{r}\right), \quad (5)$$

где τ – время, необходимое для осаждения частицы; R – внешний радиус центрифуги; r – внутренний радиус центрифуги.

В течение этого времени частицы диаметром больше d будут удалены полностью, частицы меньшего размера осадут на стенке.

Как видно из формулы (5), время разделения жидких смесей от центробежной силы зависит от разностей плотностей и от вязкости жидкости.

Зависимость влияния температуры и давления на вязкость отработанного масла представлена на рис. 4 и 5 [2].

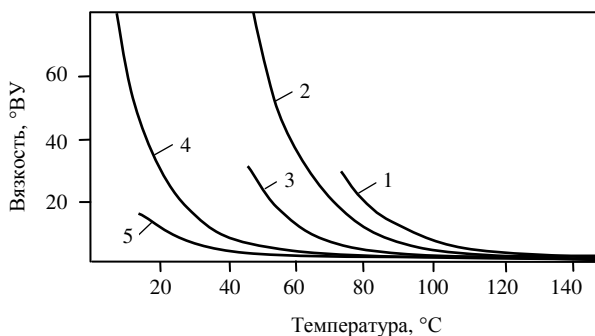


Рис. 4. Зависимость вязкости масла от температуры

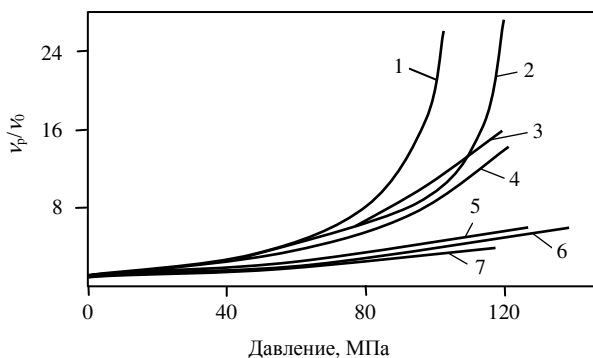


Рис. 5. Зависимость вязкости от давления

С понижением температуры и увеличением давления вязкость масла увеличивается [2].

Изучив существующие зависимости параметров, оказывающих влияние на процесс очистки, можно сделать вывод о необходимости автоматизирования процесса очистки отработанных масел методом центрифугирования, с учетом факторов, оказывающих влияние на степень очистки.

В качестве прототипа при создании автоматизированной системы очистки отработанного моторного масла была взята система турбокомпрессора для наддува дизельных двигателей, содержащего центрифугу для очистки масла (функциональная модель технологической схемы процесса очистки представлена с помощью диаграммы IDF0 на рис. 6).

Существует схема очистки моторного масла (патент №2550415) в турбокомпрессоре для наддува дизельных двигателей, содержащем центрифугу для очистки масла. Масло поступает непосредственно с двигателя в турбокомпрессор с центрифугой для очистки. После очистки масло поступает в двигатель. Центрифуга снабжена регулирующим устройством, позволяющим регулировать давление и скорость движения масла за счет изменения свободного сечения канала [3].

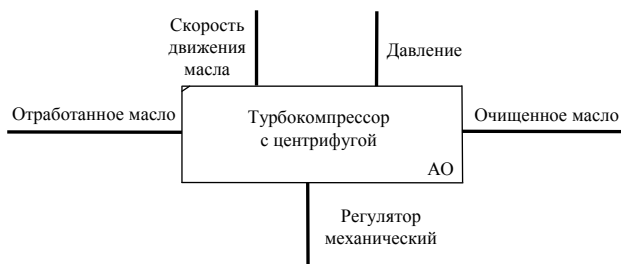


Рис. 6. Схема турбокомпрессора для наддува дизельных двигателей

Достоинством данного способа очистки является возможность очистки масла непосредственно в системе, а также возможность регулирования давления и скорости движения масла механическим регулятором.

В качестве недостатка установки можно отметить отсутствие автоматизации в системе.

Встает вопрос о необходимости автоматизации системы для повышения качества получаемого масла посредством контроля вязкости масла. В связи с тем, что вязкость напрямую зависит от таких технологических параметров, как температура и давление, изучив зависимости вязкости от этих параметров, можно при помощи постоянного контроля проводить очистку масла до тех пор, пока вязкость не приобретет необходимую величину. Это позволит проводить контроль качества очищаемого масла непосредственно в системе очистки, не проводя остановку центрифуги.

Таким образом, можно сделать следующие выводы:

- основными источниками образования масла является транспорт: железнодорожный и автомобильный;
- наиболее эффективным, применительно именно к моторному маслу, можно считать физический метод очистки центробежными силами, т.е. использование центрифуги;

– рассмотрев основные параметры и их влияние на степень очистки масла, можно сделать вывод о влиянии вязкости масла на степень очистки, а также температуры и давления на величину самой вязкости;

– изучив принцип действия известной технической системы для очистки отработанного моторного масла, можно сделать вывод об отсутствии автоматизации данной системы.

Библиографический список

1. Экологическая безопасность и особенности технического регулирования при обращении с отработанными нефтепродуктами на территории РФ. – URL: <http://www.myshared.ru/slide/923643/> (дата обращения: 15.11.2017).

2. Бойко Е.В. Химия нефти и топлив: учеб. пособие. – Ульяновск: Изд-во УлГТУ, 2007.

3. Турбокомпрессор для наддува дизельных двигателей: пат. №2550415 Рос. Федерация, F04D25 / Д.Ю. Кобзов, Г.Н. Плеханов, А.А. Трофимов, Н.Г. Плеханов; заявл. 25.04.2014, опубл.09.04.2015.

Сведения об авторах

Горбачева Ольга Михайловна – студентка Оренбургского государственного университета, Оренбург, e-mail: Ol.gorba4ewa2017@yandex.ru

Боровский Александр Сергеевич – доктор технических наук, доцент, заведующий кафедрой «Управление и информатика в технических системах» Оренбургского государственного университета, Оренбург, e-mail: borovski@mail.ru

About the authors

Gorbacheva Olga Mikhailovna – Student Orenburg State University, Orenburg, e-mail: Ol.gorba4ewa2017@yandex.ru

Borovsky Alexander Sergeevich – Doctor of Technical Sciences, Associate Professor, head of the department "Management and Informatics in Technical Systems", Orenburg State University, Orenburg, e-mail: borovski@mail.ru

АЛГОРИТМ ПРОГНОЗИРОВАНИЯ ПОВЕДЕНИЯ КОРРОЗИИ В НЕФТЕГАЗОВОМ ОБОРУДОВАНИИ

А.В. Докучаев

Оренбургский государственный университет, Оренбург

В данной статье рассматривается проблема выхода из строя нефтегазового оборудования связанного с появлением коррозии. Представлен разработанный алгоритм, который позволяет прогнозировать поведение коррозии при эксплуатации нефтегазового оборудования.

Ключевые слова: коррозия, алгоритм, нефтегазовое оборудование, погрешность, прогноз.

AN ALGORITHM FOR PREDICTING CORROSION IN OIL AND GAS EQUIPMENT

A.V. Dokuchaev

Orenburg State University, Orenburg

This article deals with the problem of failure of oil and gas equipment associated with the corrosion. Presents the developed algorithm that allows to predict the behavior of corrosion during the exploitation of oil and gas equipment.

Keywords: corrosion, algorithm, oil and gas equipment, error, forecast.

В связи с активным развитием нефтегазовой промышленности, созданием нового оборудования, усложнением технологических процессов возникает необходимость в мониторинге и прогнозировании технического состояния и в определении остаточного ресурса работоспособности нефтегазового оборудования. К нему относятся сосуды, работающие под давлением, без давления или под вакуумом, такие как колонны, емкости, теплообменники, испарители и другое. Это оборудование относится к опасным производственным объектам, и поэтому к нему предъявляются повышенные требования. Неисправности на таких объектах приводят к серьезным авариям и техногенным катастрофам, в том числе с человеческими жертвами [1]. Так как условия работы такого оборудования связаны с различными воздействиями: химическими, температурными, вибрационными и другими, то возникают коррозионные процессы, которые могут привести к появлению трещин внутри металла, изменению его толщины, потере свойств, что ведет к выходу из строя оборудования.

Проведенный анализ показал, что число отказов оборудования, связанных с «коррозионным дефектом», составляет 31 % от общего числа отказов [2].

Из-за дороговизны диагностических приборов, невозможности постоянного их применения активно развивается направление, связанное с созданием моделей, описывающих поведение («виртуальный» контроль) нефтегазового оборудования. Теоретические и прикладные аспекты данного направления исследовали ученые, такие как И.Г. Абдуллин, А.Г. Гареев, А.Г. Гумеров, Р.С. Зайнуллин и др.

Разработанные модели в основном связаны с «идеальным условием эксплуатации» (постоянное внутреннее давление, температура перекачиваемого газа и жидкости и т.п.), а это может вносить большие погрешности в расчеты, связанные с прогнозированием работы оборудования. Также существуют модели, которые связаны больше с теорией вопроса, а на практике их применить достаточно сложно, так как они основаны на большом количестве параметров, которые в условиях реального производства оценить невозможно, потому что использовать специфическое лабораторное оборудование достаточно затратно, как и привлекать кадры высшей квалификации. Работы, связанные с описанием действующих автоматизированных систем, оценивающие состояние нефтегазового оборудования, не приводят информацию об используемых математических моделях, заложенных в основу их работы. Поэтому необходимо составить математическое описание, на основе которого можно разработать алгоритм прогнозирования появления коррозии.

Коррозия возникает самопроизвольно и приводит к разрушению металла в результате взаимодействия с окружающей средой, при этом происходит выделение энергии и рассеивание вещества. В работе предложено представить скорость коррозии в зависимости от изменения массы металла, предела прочности, предела текучести или деформации. Учет изменения рассмотренных величин в единицу времени представим как скорость коррозии.

Для прогнозирования появления коррозии нефтегазового оборудования, эксплуатируемого в условиях механохимической коррозии, воспользуемся аналитической зависимостью, которая учитывает напряженное состояние и механохимическую активность металла в электролите [3]:

$$t = \frac{1 - \sigma_0 / \sigma_T}{a} \cdot \frac{S_0}{v_0}, \quad (1)$$

где σ_0 – начальное напряжение в стенке оборудования, МПа; σ_T – предел текучести, МПа; S_0 – начальная толщина стенки оборудования, мм; v_0 – скорость коррозии, мм/год;

$$a = \exp\left(\frac{\sigma_T V}{RT}\right), \quad (2)$$

где V – молярный объем металла, см³/моль; T – абсолютная температура, К; R – универсальная газовая постоянная, Дж/(моль·К).

Для определения скорости коррозии « $v_0 \cdot a$ » воспользуемся формулой:

$$v = v_0 \exp\left(\sigma_{\text{ср}} \frac{V}{RT}\right), \quad (3)$$

где $\sigma_{\text{ср}}$ – среднее напряжение, МПа.

В рассмотренное математическое описание не включаются изменения температуры, влажности, давления, задержка развития коррозии. Начальная скорость коррозии определяется на основе полной диагностики, однако на практике, как излагалось выше, может не быть необходимого оборудования, а заказ данной работы сторонней организации приведет к временным и экономическим затратам. Эту величину определим с использованием разработанного алгоритма представленного на рисунке.

Исходные данные о нефтегазовом оборудовании связаны с датой ввода в эксплуатацию, с датой замены изоляционного покрытия, с внутренним и наружным давлением ($p_{\text{в}}$, $p_{\text{н}}$), внутренним диаметром ($B_{\text{в}}$), пределом текучести (σ_T), с начальной толщиной стенки оборудования, а также со значением среднего напряжения в начальный и конечный момент исследования, абсолютной температурой, молярным объемом металла, типом и толщиной изоляционного слоя, параметрами катодной защиты. Кроме этого для осуществления полной диагностики и проведения прогнозирования необходимы также знания о глубине наружного и внутреннего коррозионного дефекта ($S_{\text{н.э}}$ и $S_{\text{в.э}}$), о текущей внутренней и наружной глубине дефекта ($S_{\text{в}}$ и $S_{\text{н}}$), о текущем времени ($t_{\text{тек}}$), о внутреннем и наружном радиусе оборудования ($r_{\text{в}}$, $r_{\text{н}}$).

Алгоритм осуществляется в несколько этапов.

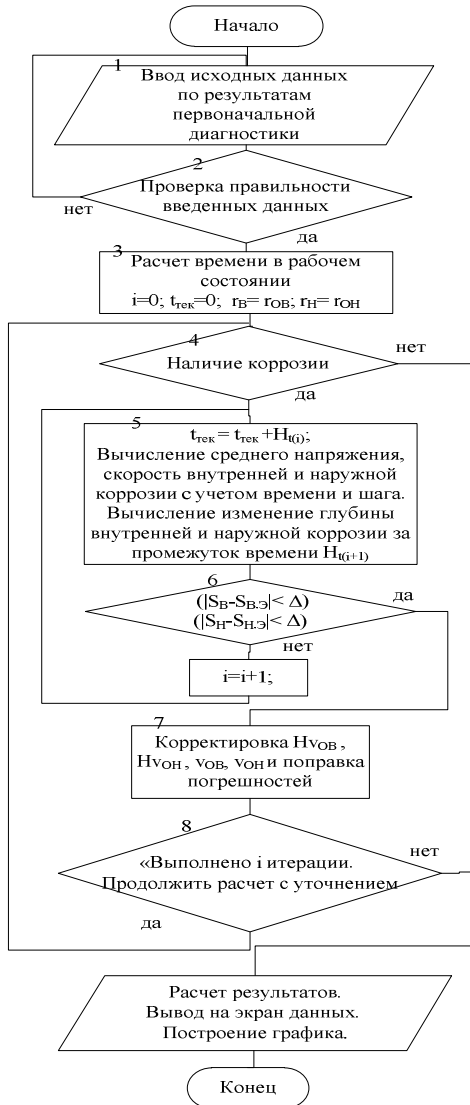


Рис. Алгоритм определения скорости коррозии

На первом этапе вводятся исходные данные по результатам технической диагностики, а также шаги увеличения/ уменьшения начальной внутренней и наружной скорости коррозии ($H_{Vов}$ и $H_{Vон}$)

и погрешность (Δ), определяющая допустимые отличия между реальными и вычисленными глубинами внутренних и наружных дефектов.

На втором этапе проверяют по ГОСТам введенные данные на правильность, адекватность. При определении ошибок необходимо данные ввести повторно.

На третьем этапе осуществляется вычисление первоначальных данных о существовании коррозии. Далее проверяется существование признаков коррозии в металле. При отсутствии коррозии необходимо перейти в блок расчета и вывода на экран данных. Иначе необходимо перейти на пятый блок.

На пятом этапе определяются характеристики коррозионных дефектов.

На шестом этапе осуществляется сравнение погрешности модуля разности расчетной и настоящей глубины дефекта. При разности глубины дефекта меньше заданной погрешности переходят к блоку 7 с целью корректировки данных. Иначе осуществляются вычисления в блоке 5, с изменением времени на $i + 1$, пока модуль разности расчетной и настоящей глубины дефекта не станет меньше Δ .

На седьмом этапе осуществляются корректировка $N_{V_{0в}}$, $N_{V_{0н}}$, $v_{0в}$, $v_{0н}$ и поправка погрешностей. Если расчетная глубина дефектов получается со знаком минус, то шаг увеличения/уменьшения начальной скорости коррозии уменьшается в два раза. Для увеличения процесса расчета первоначальные шаги увеличения/уменьшения начальной скорости коррозии задаются «более грубыми».

В зависимости от знака разности между расчетной и реальной глубиной дефекта выполняется изменение планируемой начальной скорости коррозии. Если модуль разности между предполагаемой и реальной глубиной внутреннего дефекта больше погрешности, а знак получаемой разности «отрицательный», то $v_{0в}$ уменьшается на $N_{V_{0в}}$, при этом, прежде чем поменять $v_{0в}$, проверяется разность $v_{0в} - N_{V_{0в}}$. Если разность меньше нуля, то выполняется исправление $N_{V_{0в}}$.

На последнем этапе осуществляется опрос оператора о необходимости продолжения расчета. Если его все удовлетворяет, то выводятся результаты расчета на экран, иначе переходим на пятый этап.

Таким образом, используя разработанный алгоритм, можно прогнозировать поведение коррозии при эксплуатации нефтегазового оборудования.

Библиографический список

1. Докучаев А.В. Тугов В.В. Разработка методики проведения диагностики нефтегазового оборудования на основе рентгеновского контроля // Компьютерная интеграция и ИПИ-технологии: материалы VIII Всерос. науч.-практ. конф. – Оренбург, 2017. – С. 208–211.

2. Старение труб нефтепроводов / А.Г. Гумеров [и др.]. – М.: Недра, 1995. – 218 с.

3. Абрамов О.В., Розенбаум А.П. Прогнозирование состояния технических систем. – М.: Наука, 1990. – 126 с.

Сведения об авторе

Докучаев Александр Владимирович – студент Оренбургского государственного университета, Оренбург, e-mail: xmanvel650@mail.ru

About the author

Dokuchaev Alexander Vladimirovich – Student Orenburg State University, Orenburg, e-mail: xmanvel650@mail.ru

ПЕРСПЕКТИВЫ РАЗВИТИЯ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ

А.В. Ерёмин, М.В. Чесноков, Р.Р. Сaitбатталов
Оренбургский государственный университет, Оренбург

В данной статье рассмотрены тенденции развития производства в направлении концентрации производства, механизации и автоматизации

Ключевые слова: автоматизация, технологические машины, системы.

PROSPECTS FOR DEVELOPMENT OF AUTOMATIC CONTROL

A.V. Eremin, M.V. Chesnokov, R.R. Saitbattalov
Orenburg state university, Orenburg

In this article, trends in the development of production towards concentration of production, mechanization and automation

Keywords: automation, technological machines, systems.

Объединение локальных систем автоматического управления (АСУ) служит основной тенденцией совершенствования и развития в автоматизации. Основная цель – это создания комплексных систем, которые сочетают в себе автоматизацию решения экономических задач и задач, связанных с управлением технологическими процессами, проектированием изделий и технологий.

Предпосылкой для разработки систем более высокого класса послужило повышение научно-технического уровня и эффективности автоматической системы управления. К таким системам относят многоуровневые интегрированные автоматизированные системы управления.

Интегрированные автоматизированные системы управления включают в себя:

- автоматическую систему управления производства – организационно-управленческую сторону производственной деятельности;
- автоматическую систему управления технологическими процессами – технико-технологическую сторону производственной деятельности;
- систему автоматического проектирования – конструкторско-технологическую сторону производственной деятельности.

Эти элементы не только связаны, но и образуют единый контур организационно-экономического управления.

Центром управления АСУ является система, состоящая из быстродействующих электронно-вычислительных машин. На них возлагаются справочные, информационные функции, а также функция контроля производственного процесса.

Внедрение автоматизированных систем управления способствует уменьшению непроизводственных расходов сырья, к тому же происходит увеличение качества продукции за счет точного регулирования параметров технологического процесса. Одновременно это также позволяет повысить производительность труда, эффективность производства и улучшить организацию и хранение информации.

Гибкие автоматизированные технологии, как и гибкие автоматизированные производства, хорошо сочетают в себе комплексную автоматизацию с экономией трудовых ресурсов.

Гибкая производственная система представляет совокупность технологического оборудования и систем, обеспечивающих его нормальное функционирование в автоматическом режиме, обладает свойством автоматизированной переналадки при производстве произвольной номенклатуры.

При создании гибких производственных систем используют отдельные модули, объединенные в гибкую производственную линию, либо участок, цех и т.д.

По степени автоматизации можно выделить:

- гибкий автоматизированный комплекс;
- гибкое автоматизированное производство.

Для того чтобы осуществить комплексную автоматизацию, нужно организовать производственные процессы, которые будут соответствовать технологиям производства и требованиям равномерного, непрерывного и интенсивного использования технологической системы без участия человека, при этом выпуская стабильно качественную продукцию.

Одновременно с комплексностью характера автоматизации автоматизированные системы должны обладать свойством гибкости как технологически, так и экономически. Под технологической гибкостью понимается возможность изменения производительности системы при

согласованной работе ее элементов. Экономическая гибкость – способность многократной смены номенклатуры выпускаемой продукции с наименьшими затратами при неизменности основного технологического оборудования. Основным звеном гибкого автоматизированного производства является гибкая производственная система.

При гибкой технологии система обладает способностью к структурным изменениям, быстрой адаптацией элементов производства в условиях динамизма и интенсификации. Гибкость может быть тактической и стратегической. Тактическая гибкость обеспечивается за счет эластичности внутренней организационно-технологической структуры производств при неизменных производственно-технологических функциях, а стратегическая связана с обеспечением работоспособности системы за счет ее многофункциональности.

Библиографический список

1. Асаль Р. Роботы и автоматизация производства / пер. с англ. М.Ю. Евстигнеева [и др.]. – М.: Машиностроение, 2001. – 448 с.

2. Промышленные роботы: Внедрение и эффективность: пер. с яп. / К. Асаи, С. Кигими, Т. Кодзима [и др.]. – М.: Мир, 2002. – 384 с.

3. Роботизированные производственные комплексы / Ю.А. Козырев, А.А. Кудинов, В.Э. Булатов [и др.]; под ред. Ю.Г. Козырева, А.А. Кудинова. – М.: Машиностроение, 2002. – 272 с.

4. ГОСТ 26228-90. Системы производственные гибкие. Термины и определения, номенклатура показателей // Доступ из справ.-правовой системы КонсультантПлюс.

5. Капустин Н.М. Автоматизация производственных процессов в машиностроении: учеб. для вузов / под ред. Н.М. Капустина. – М.: Высшая школа, 2004. – 415 с.

6. Юревич Е.И. Основы робототехники. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2005. – 416 с.

7. Воройский Ф.С. Информатика. Энциклопедический систематизированный словарь-справочник. (Введение в современные информационные и телекоммуникационные технологии в терминах и фактах). – М.: Физматлит, 2007. – 760 с.

8. Цыпкин Я.З. Основы теории автоматических систем. – М., Наука, 1977.

Сведения об авторах

Ерёмин Антон Вячеславович – студент Оренбургского государственного университета, Оренбург, e-mail: che1988@mail.ru

Чесноков Максим Васильевич – студент Оренбургского государственного университета, Оренбург, e-mail: gold.icon@mail.ru

Саитбатталов Рафаэль Рафикович – студент Оренбургского государственного университета, Оренбург, e-mail: shaidan4ik@mail.ru

About the authors

Eremin Anton Vyacheslavovich – Student Orenburg State University, e-mail: che1988@mail.ru

Chesnokov Maxim Vasilievich – Student Orenburg State University, e-mail: gold.icon@mail.ru

Saitbattalov Rafael Rafikovich – Student Orenburg State University, e-mail: shaidan4ik@mail.ru

ПОЛУЧЕНИЕ И ПРЕДОБРАБОТКА ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ ДЛЯ СОЗДАНИЯ ОБУЧАЮЩЕЙ ВЫБОРКИ ДЛЯ НЕЙРОННОЙ СЕТИ

Е.О. Ждановский, Г.А. Килин

Пермский национальный исследовательский
политехнический университет, Пермь

В статье рассматривается один из важных аспектов обучения нейронной сети, а именно создание обучающей выборки для нейросетевой модели газотурбинной электростанции. Данные были получены с помощью программного моделирующего комплекса «КМЭС».

Ключевые слова: газотурбинная установка, газотурбинная электростанция, система автоматического управления, синхронный генератор, нейронные сети, нейросетевая модель.

OBTAINING AND PREPROCESSING EXPERIMENTAL DATA TO CREATE A TRAINING SAMPLE FOR A NEURAL NETWORK

E.O. Zhdanovsky, G.A. Kilin

Perm National Research Polytechnic University, Perm

The article considers one of the most important aspects of training a neural network, namely the preparation of experimental data, in other words, the creation of a training and test sample for training a neural network model of a gas turbine power plant. The data were obtained using the software modeling complex "KMES".

Keywords: gas turbine plant, gas turbine power station, automatic control system, synchronous generator, neural network, neural network model.

В настоящее время нейронные сети находят огромное применение во многих задачах. Авторы статей [1, 2, 3] продемонстрировали, что они отлично проявляют себя в распознавании изображений, нашли широкое применение в финансовой сфере [4, 5]. Всё больший интерес к искусственным нейронным сетям проявляют специалисты различных отраслей промышленности. Благодаря их способности аппроксимировать любой вид нелинейности [6, 7, 8] они нашли применение в задачах идентификации газотурбинной установки (ГТУ) [9, 10]. Именно поэтому было решено использовать нейронные сети в создании модели газотурбинной электростанции (ГТЭС). Но для того чтобы нейросетевая модель адекватно работала, её необходимо обучить.

Обучение нейронной сети – это очень трудоемкая и объемная задача, она включает в себя получение и подготовку экспериментальных данных, выбор количества нейронов, выбор функции активации, архитектуры и метода обучения нейронной сети. В данной статье будет рассмотрен первый этап, т.е. получение и подготовка экспериментальных данных для обучения нейронной сети.

Получение и обработка экспериментальных данных. Выбор данных и обработка исходных данных являются довольно сложными этапами. В связи с отсутствием доступа к реальной установке данные получались с помощью сложной поэлементной математической модели ГТУ и электроэнергетической системы (ЭЭС), разработанной на авиадвигателестроительном предприятии в виде программно-моделирующего комплекса КМЭС (ПМК КМЭС) [11]. Данная программа имеет обширную область изменяемых параметров ГТЭС (рис. 1), настройка которых производилась с учетом поставленной задачи.

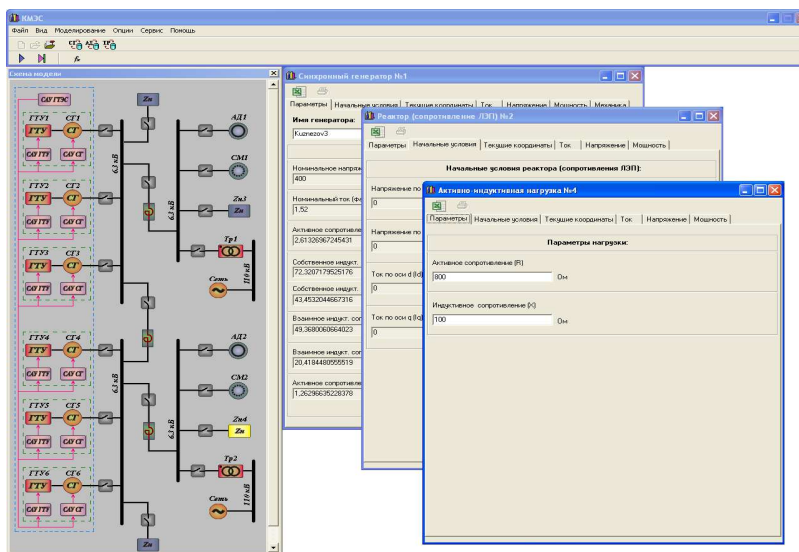


Рис. 1. Рабочая среда ПМК «КМЭС»

С помощью создаваемой нейросетевой модели планируется оптимизировать процесс настройки регуляторов реальной установки. В связи с этим все эксперименты проводились с отключенной системой автоматического управления (САУ) ГТУ. Это сделано для того,

чтобы нейронная сеть могла обучаться работе самой ГТЭС, а не системы управления. Далее рассмотрим методику проведения экспериментальных данных. Возмущающими воздействиями данной установки являются активное сопротивление и расход топлива. Активное сопротивление выставлялось единожды, а расход топлива был изменен в большую или меньшую сторону, в итоге сложная поэлементная модель строила следующие переходные характеристики (рис. 2).

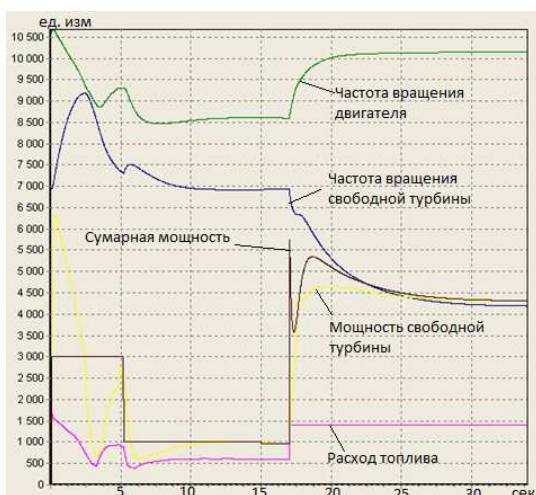


Рис. 2. Переходные характеристики газотурбинной установки

При каждом завершеном моделировании из ПМК «КМЭС» сохраняем таблицу данных с различными параметрами, такими как температура свободной турбины, давление за компрессором, момент генератора, ток фаз *A*, *B*, *C* и др. Подача всех данных на вход нейронной сети приведет лишь к увеличению времени обучения, поэтому было решено включать в обучающую выборку лишь интересующие нас параметры, а по данной выборке решать вопрос о количестве нейронов во входном слое. Один интересующий параметр будет соответствовать одному нейрону во входном слое. Также необходимо учесть, что сложная поэлементная модель строит и пусковой момент ГТЭС, но данная информация для поставленной задачи абсолютно не нужна, и необходимо вырезать начальные переходные данные до установившегося режима. Соответственно, интересовать будут значения, начинающиеся с 15-й секунды (рис. 3).



Рис. 3. Интересующие переходные характеристики ГТУ

Также интересовали и переходные характеристики синхронного генератора, такие как напряжение, ток, частота вращения синхронного генератора и напряжение обмотки возбуждения. Для лучшего обучения нейронной сети было произведено множество подобных экспериментов с различными нагрузками и расходами топлива, внесенных последовательно в одну большую базу данных переходных характеристик ГТУ и СГ, которая и является обучающей выборкой для нейросетевой модели газотурбинной электростанции.

Библиографический список

1. Дружи А.А. Применение сверточных нейронных сетей для выделения и распознавания автомобильных номерных знаков на изображениях со сложным фоном // Известия Томск. политехн. ун-та. – 2014. – Т. 324. – № 5.
2. Солдатова О.П., Гаршин А.А. Применение сверточной нейронной сети для распознавания рукописных цифр // Компьютерная оптика. – 2010. – Т. 34. – № 2.
3. Дорогой Я.Ю. Архитектура обобщенных сверточных нейронных сетей // Вісник Націон. техніч. університету України. – 2011. – №. 54. – С. 229–234.

4. Ефремова Е.А., Дунаев Е.В., Применение нейронных сетей для прогнозирования финансовых временных рядов // Автоматизированные системы обработки информации, управления и проектирования // Доклады ТУСУРа. – 2004. – С. 192.

5. Садовой А.В., Сотник С.Л. Алгоритмы обучения нейронных сетей будущего [Электронный ресурс]. – URL: <http://www.alicetele.com/~sergei/articles/algo/algo.htm> (дата обращения: 22.09.2017).

6. Хайкин С. Нейронные сети: полный курс. – 2-е изд. – М.: Вильямс, 2008.

7. Роберт К. Основные концепции нейронных сетей: пер. с англ. – М.: Вильямс, 2001.

8. Методы робастного, нейронечеткого и адаптивного управления / Н.Д. Егупов [и др.]. – М.: Изд-во МГТУ им. НЭ Баумана. – 2002.

9. Artificial neural network-based system identification for a single-shaft gas turbine / H. Asgari [et al.] // Journal of Engineering for Gas Turbines and Power. – 2013. – Т. 135. – № 9. – С. 092601.

10. Asgari H., Chen X. Q., Sainudiin R. Modelling and simulation of gas turbines // International Journal of Modelling, Identification and Control. – 2013. – Т. 20. – №. 3. – С. 253–270.

11. Св-во о гос. регистр. программы для ЭВМ № 2011611839 РФ. Программный комплекс «Комплекс математических моделей электрогенератора и электросети» «КМЭС» // А.Б. Петроченков, Б.В. Кавалеров, А.А. Шигапов, К.А. Один, А.И. Полулях, А.С. Ситников, И.Г. Лисовин, Е.Н. Ширинкина (дата регистр. 28.02.2011).

Сведения об авторах

Ждановский Евгений Олегович – аспирант Пермского национального исследовательского политехнического университета, Пермь, e-mail: Zhdanovskiy.e@gmail.com

Килин Григорий Александрович – старший преподаватель Пермского национального исследовательского политехнического университета, Пермь, e-mail: thisisforasm@rambler.ru

About the authors

Zhdanovsky Evgeny Olegovich – Student Perm National Research Polytechnic University, Perm, e-mail: Zhdanovskiy.e@gmail.com

Kilin Grigory Aleksandrovich – Senior Lecturer Perm National Research Polytechnic University, Perm, e-mail: thisisforasm@rambler.ru

О ВОЗМОЖНОСТЯХ КОРРЕКЦИИ НЕПРАВИЛЬНОЙ НАСТРОЙКИ СИСТЕМ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ СИНХРОННЫМ ГЕНЕРАТОРОМ ГАЗОТУРБИННЫХ ЭЛЕКТРОСТАНЦИЙ В РЕАЛЬНОМ ВРЕМЕНИ

И.Р. Зиятдинов, Б.В. Кавалеров

Пермский национальный исследовательский
политехнический университет, Пермь

Исследуются возможности исправления неправильной настройки САУ синхронным генератором (СГ) вблизи номинального режима для газотурбинной электростанции (ГТЭС). Рассматриваются способы парирования ошибки за счет подстройки САУ СГ, САУ газотурбинной установкой (ГТУ), введением адаптивного управления с эталонной моделью и с настраиваемой моделью. В качестве метода адаптации использован метод, основанный на функции Ляпунова. В качестве модели ГТУ используется сложная динамическая модель. Все модели выполняются совместно в составе программного моделирующего комплекса «КМЭС».

Ключевые слова: газотурбинная установка, система автоматического управления, синхронный генератор.

ON THE POSSIBILITIES OF GAS TURBINE POWER PLANTS AUTOMATIC CONTROL SYSTEMS CORRECTING THE MISCONFIGURATION FOR THE SYNCHRONOUS GENERATOR IN REAL TIME

I.R. Ziyatdinov, B.V. Kavalеров

Perm National Research Polytechnic University, Perm

The article explores the possibilities of correcting the incorrect adjustment of the automatic control system by a synchronous generator (SG) near the nominal mode for a gas turbine power plant (GTPP). The ways of parrying the error due to the adjustment of the SAU SG, the automatic control system with the gas turbine unit (GTU), the introduction of adaptive control with the reference model and with the adjustable model are considered. As a method of adaptation, a method based on the Lyapunov function was used. All models are performed jointly as part of the software modeling complex "KMES".

Keywords: gas turbine plant, automatic control system, synchronous generator.

Введение. Неустойчивый режим работы с возникновением колебаний был сымитирован на программном моделирующем комплексе «КМЭС» [5] для ГТГ-6. При этом использовалась наиболее распространенная структура микропроцессорного регулятора СГ типа КОСУР [6]:

$$U_{\text{пер}} = k_U \Delta U_r + k_{\text{и}} \int \Delta U_r dt + k'_U U'_r + k_f \Delta' f + k'_f f' + k'_I I'_B, \quad (1)$$

где Δf – сигнал об изменении частоты f_g напряжения генератора; U_g – напряжение генератора; $k_U, k'_U, k_n, k_f, k'_f, k'_i$ – коэффициенты пропорциональности: по отклонению напряжения генератора, его производной, интегральной функции, по изменению частоты, ее производной, по скорости изменения тока возбуждения генератора соответственно. Сигнал Δf существует только при переходном процессе изменения частоты, в установившемся режиме этот сигнал отсутствует.

1. Результаты настройки САУ ГТУ для парирования неправильной настройки САУ СГ вблизи номинального режима. Для проведения исследования преднамеренная неправильная настройка, вызывающая колебания, была получена при следующих значениях параметров: $k_U = 1$ о.е., $k'_U = 2$ о.е., $k_n = 2$ о.е., $k_f = 50$ о.е., $k'_f = 0$, $k'_i = 0$. Возмущающим воздействием является снижение потребляемой мощности с 6,0 до 5,7 МВт. Следует отметить, что на частичной мощности, например при 2500 кВт, при аналогичном возмущении колебания практически не заметны.

При перенастройке в момент времени $t = 75$ с коэффициентов в новые значения ($k_U = 3$ о.е., $k'_U = 2$ о.е., $k_n = 2$ о.е., $k_f = 30$ о.е., $k'_f = 0$, $k'_i = 0$) колебания затухают и режим становится устойчивым (рис. 1).

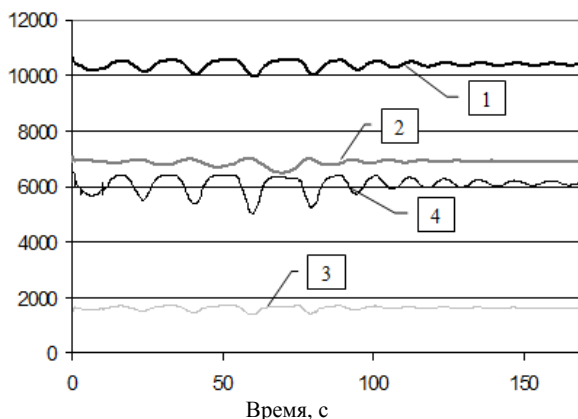


Рис. 1. Потеря устойчивости САУ ГТУ вследствие неправильной настройки САУ электрогенератора и восстановление устойчивости за счет подстройки САУ СГ: 1 – частота вращения двигателя, об/мин; 2 – частота вращения свободной турбины, об/мин; 3 – расход топлива, кг/ч; 4 – суммарная мощность нагрузки, кВт

Вслед за этим было решено проверить, возможно ли добиться устойчивого режима работы без воздействия на неправильно настроенную САУ СГ. Иными словами, сможет ли подстройка САУ ГТУ парировать вредное влияние неправильно настроенной САУ СГ.

Для проверки был повторно проведен рассмотренный ранее эксперимент с неправильной настройкой САУ СГ: $k_U = 1$ о.е., $k'_U = 2$ о.е., $k_n = 2$ о.е., $k_f = 50$ о.е., $k'_f = 0$, $k'_i = 0$.

Но в момент времени $t = 75$ с были изменены настройки не регулятора САУ СГ, а регулятора свободной турбины САУ ГТУ. Первоначальная (стандартная) настройка регулятора свободной турбины САУ ГТУ (рис. 2) следующая: $StK1 = k_i = 2,5$, $StK2 = k_f = 17$, $StK3 = k_n = 1$.

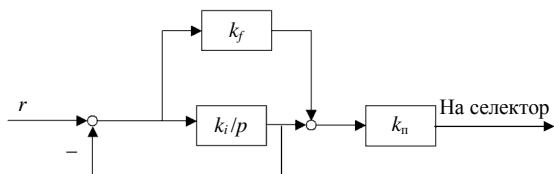


Рис. 2. Регулятор СТ САУ ГТУ

В момент времени $t = 75$ с была произведена перенастройка регулятора свободной турбины (СТ): $StK1 = k_i = 1,5$, $StK2 = k_f = 17$, $StK3 = k_n = 1$. Переходный процесс быстро устанавливается (см. рис. 1).

На рис. 3 показано сравнение восстановления устойчивости за счет подстройки САУ ГТУ и САУ СГ.

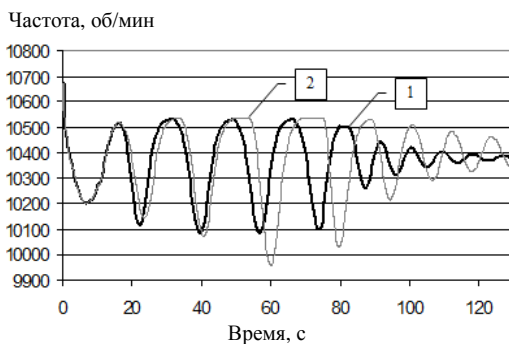


Рис. 3. Потеря устойчивости САУ ГТУ вследствие неправильной настройки САУ электрогенератора и восстановление устойчивости: 1 – за счет подстройки САУ ГТУ; 2 – за счет подстройки САУ СГ

В результате частота вращения свободной турбины без колебаний плавно устанавливается в заданное значение. Более того, как показывает компьютерный эксперимент, при использовании с самого начала новой настройки регулятора САУ ГТУ обеспечивает отсутствие колебаний при том же возмущении нагрузки (рис. 4).

За счет настройки САУ ГТУ возможно парировать неправильную настройку САУ СГ и обеспечить требуемый характер переходного процесса. Если сравнить графики на рис. 3, то можно видеть, что настройка САУ ГТУ дает в данном случае даже лучший результат, чем подстройка САУ СГ.

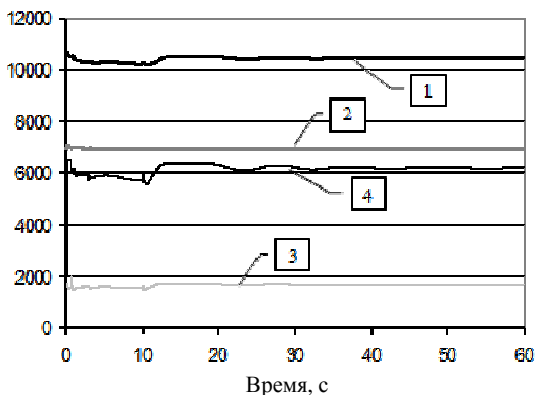


Рис. 4. Сброс мощности с 6,0 до 5,7 МВт при новой настройке регулятора СГ САУ ГТУ:
 1 – частота вращения двигателя, об/мин; 2 – частота вращения свободной турбины, об/мин; 3 – расход топлива, кг/ч; 4 – суммарная мощность нагрузки, кВт

Базовый компьютерный эксперимент проводился вблизи номинального режима (6 МВт), поэтому необходимо проверять новую настройку регулятора при частичной мощности. Но в любом случае результат является важным, поскольку способен в перспективе реализовать табличную настройку САУ ГТУ (коэффициенты являются функцией потребляемой активной мощности).

Автоматический поиск оптимальной настройки способен значительно сэкономить время на испытания и настройку САУ ГТУ при различных возмущениях со стороны синхронного генератора и нагрузки.

2. Результаты применения адаптивной САУ с эталонной моделью (ЭМ) для парирования неправильной настройки САУ СГ вблизи номинального режима. Убедимся в возможности САУ ГТУ

с адаптивным управлением [2, 3, 4] парировать вредное влияние неправильно настроенной САУ СГ. Проведем эксперимент, описанный выше, и сравним результаты (рис. 5).

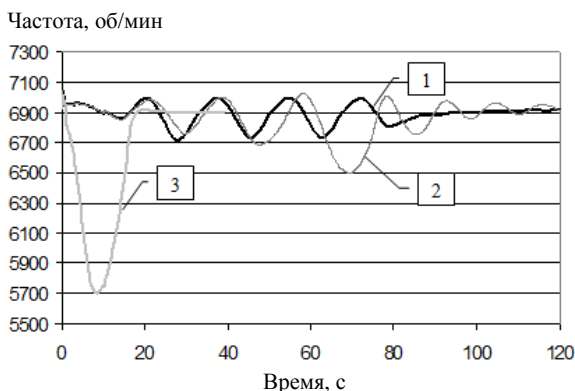


Рис. 5. Потеря устойчивости САУ ГТУ вследствие неправильной настройки САУ электрогенератора и восстановление устойчивости за счет подстройки: 1 – САУ ГТУ; 2 – САУ СГ; 3 – адаптивной системы (ЭМ)

Пока в системах с подстройкой САУ ГТУ и САУ СГ возникают и устраняются автоколебания, САУ ГТУ с адаптацией полностью установилась за 17 с, единственная проблема возникает в высоком скачке частоты вращения свободной турбины при пуске ГТУ, обусловленном рассогласованием начальных условий.

На основании рис. 7 можем сделать вывод о работоспособности и эффективности адаптивной САУ с ЭМ.

Заключение. Делаем вывод, что адаптивная САУ ГТУ с ЭМ не только парирует вредное влияние неправильно настроенной САУ СГ, но и показывает свою эффективность по сравнению с простой подстройкой САУ ГТУ. Скачок при пуске никак не связан с изменением нагрузки системы и появляется из-за рассогласования.

Библиографический список

1. Бахирев И.В. Управление электроэнергетической газотурбинной установкой с сигнальной настройкой и настраиваемой моделью // Наука сегодня: задачи и пути их решения: материалы междунар. науч.-практ. конф. – Вологда: Маркер, 2016. – С. 13–15

2. Зиятдинов И.Р., Кавалеров Б.В., Крылова И.А. Исследование адаптивного алгоритма управления с газотурбинными установками учетом динамики синхронного генератора // *Фундаментальные исследования*. – 2016. – № 6–2. – С. 235–240.

3. Зиятдинов И.Р., Кавалеров Б.В., Бахирев И.В. Исследование системы управления с эталонной моделью и сигнальной настройкой для электроэнергетической газотурбинной установки // *Фундаментальные исследования*. – 2015. – № 6–2. – С. 235–240.

4. Зиятдинов И.Р., Кавалеров Б.В. Исследование системы управления с эталонной моделью и параметрической настройкой для электроэнергетической газотурбинной установки // *Фундаментальные исследования*. – 2015. – № 12–6. – С. 1107–1111.

5. Св-во о гос. рег. программы для ЭВМ № 2011611839 РФ. Программный комплекс «Комплекс математических моделей электрогенератора и электросети» «КМЭС» / А.Б. Петроченков, Б.В. Кавалеров, А.А. Шигапов, К.А. Один, А.И. Полулях, А.С. Ситников, И.Г. Лисовин, Е.Н. Ширинкина (дата регистрации 28.02.2011).

6. Овчаренко Н.И. Автоматика энергосистем. – М.: Изд. дом МЭИ, 2007. – 476 с.

Сведения об авторах

Зиятдинов Илья Рудольфович – аспирант Пермского национального исследовательского политехнического университета, Пермь, e-mail: i.ziyatdinoff@mail.ru

Кавалеров Борис Владимирович – доктор технических наук, доцент, заведующий кафедрой «Электротехника и электромеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: kbv@pstu.ru

About the authors

Ziyatdinov Ilya Rudolfovich – Graduate Student Perm National Research Polytechnic University, Perm, e-mail: i.ziyatdinoff@mail.ru

Kavalerov Boris Vladimirovich – Doctor of Technical Sciences, Professor, Head of the department ETEM Perm National Research Polytechnic University, Perm, e-mail: kbv@pstu.ru

ИССЛЕДОВАНИЕ ГАРМОНИЧЕСКОГО СОСТАВА ОБУЧАЮЩЕЙ ВЫБОРКИ НЕЙРОСЕТОВОЙ МОДЕЛИ ДИНАМИЧЕСКОГО ОБЪЕКТА

Р.Р. Исламов, А.С. Александрова, А.Г. Шумихин

Пермский национальный исследовательский
политехнический университет, Пермь

В работе предложено исследование динамики простой имитационной модели технологического объекта путем идентификации каналов ее нейросетевого аналога частотным методом. Для проведения экспериментов на нейросетевой модели необходимо определить гармонический состав экспериментальных сигналов обучающей выборки. С этой целью рассмотрены два метода, один из которых заключается в подборе среднего значения экспериментальных сигналов, другой – в их разложении в ряд Фурье. В обоих методах используются результаты спектрального анализа испытательных сигналов. Представлены комплексные частотные характеристики нейросетевой модели, построенные на вычислениях двух методов. Их сходимость с комплексной частотной характеристикой имитационного объекта показала эффективность использования ряда Фурье.

Ключевые слова: динамический объект, нейросетевая модель, обучающая выборка, идентификация, комплексная частотная характеристика, спектральный анализ, ряд Фурье.

DETERMINATION OF THE HARMONIC COMPOSITION OF EXPERIMENTAL SIGNALS OF THE TRAINING SELECTION OF THE NEURAL NETWORK

R.R. Islamov, A.S. Aleksandrova, A.G. Shumikhin

Perm National Research Polytechnic University, Perm

The article offers the research of dynamics of a simple imitation model of a technological object by identification the channels of its neural network analogue by means of the frequency method. To perform experiments on the neural network model, it is necessary to determine the harmonic composition of test signals of the training selection. For this purpose two methods were considered, one of which is the selection of average value of the experimental signals, the other is its Fourier expansion. Both methods uses results of spectral analysis of test signals. Complex frequency characteristics of the neural network model based on calculations of two methods are presented. Its convergence with the complex frequency characteristic of the imitation object showed effectiveness of using the Fourier series.

Keywords: dynamic object, neural network model, training selection, identification, complex frequency characteristic, spectral analysis, Fourier series.

В последние годы в качестве инструментов моделирования динамических объектов применяются искусственные нейронные сети. Нейронные сети позволяют описать поведение объекта, используя информацию о входных и выходных переменных объекта. Нелинейная автокорреляционная нейронная сеть имеет в своем составе элементы в виде обратных связей, что дает возможность моделировать поведение динамических объектов [1]. Моделирование поведения инерционных объектов с чистым запаздыванием возможно благодаря временным задержкам входных сигналов и сигналов обратных связей [2].

Обученная нейросетевая модель позволяет провести на ней идентификацию каналов объекта на основе частотного метода, что предполагает последовательные воздействия на динамическую модель исследуемого объекта периодическими испытательными сигналами с различной частотой. Результатом подобных испытаний являются значения комплексной частотной характеристики для определенного набора частот [3–4].

Для нейросетевых моделей характерна способность – аппроксимировать поведение динамического объекта только для тех случаев, которые представлены в обучающей выборке. Например, при подаче на вход нейросетевой модели сигнала со значением вне диапазона значений данного сигнала в обучающей выборке выход нейросетевой модели будет неверным. Следовательно, для проведения вычислительного эксперимента на нейросетевой модели с подачей периодических испытательных сигналов необходимо определить допустимый диапазон частот и соответствующих им амплитуд испытательных сигналов по обучающей выборке. Спектральный анализ экспериментальных сигналов обучающей выборки позволяет определить их частотный состав. Определение амплитуды испытательных сигналов возможно путем разложения экспериментальных сигналов, обучающей выборки в ряд Фурье [5].

Пример определения гармонического состава экспериментальных сигналов обучающей выборки нейросетевой модели имитационного объекта. Проведено исследование предложенного подхода к определению допустимого диапазона частот и соответствующих амплитуд периодических испытательных сигналов в вычислительном эксперименте с нейросетевой моделью. Исследована простая имитационная модель динамического объекта, состоящего из двух каналов передачи, заданных аperiodическими звеньями второго порядка с запаздыванием (рис. 1).

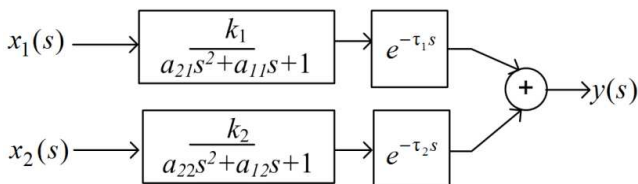


Рис. 1. Структурная схема имитационного объекта: $k_1 = -0,7$; $a_{21} = 0$;
 $a_{11} = 40$; $\tau_1 = 5$; $k_2 = 0,8$; $a_{22} = 50$; $a_{12} = 35$; $\tau_2 = 4$;
 размерность параметров a_{ij} , τ_j – единицы времени

В ходе вычислительного эксперимента на вход объекта сгенерированы два процесса $x_1(t)$, $x_2(t)$. По полученным входным сигналам на выходе объекта сформировался сигнал $y(t)$. Подаваемые на вход сигналы являются нормально распределенными случайными сигналами. Сигналы пропущены через высокочастотный фильтр в виде апериодического звена второго порядка, что позволяет получить на входе модели сигналы, близкие по характеру зашумленным низкочастотным сигналам промышленных объектов.

По полученным в результате вычислительного эксперимента на имитационной модели объекта данным была обучена динамическая нейронная сеть [6, 7]. В сети установлены задержки на 5 тактов, что обеспечивает влияние «исторических» данных с глубиной в 5 тактов на значение выходной величины объекта. Сеть имеет 20 нейронов в скрытом слое. Нейрон выходного слоя выдает значения выходного сигнала. Сеть была обучена на представителях, полученных в эксперименте, являющихся парами, включающими вектор значений внешних сигналов и выходной сигнал сети в соответствующие конфигурации сети дискретные моменты времени, начиная с текущего момента времени и далее в глубину «исторических данных». При тестировании на части экспериментальных данных, не вошедшей в обучающую выборку, нейросетевая модель имитационного объекта выдает значения выходной переменной с относительной погрешностью, не превышающей 0,24 %.

Проведены две серии вычислительных экспериментов, в которых на вход нейросетевой модели подавались периодические испытательные сигналы с различными амплитудами. В качестве частот испытательных сигналов выбирались частоты с наибольшей спектральной плотностью из результатов спектрального анализа входных сигналов обучающей выборки.

В первой серии экспериментов для выбранных частот они проводились с различными амплитудами испытательных сигналов. Выбраны были три уровня амплитуды сигналов: половина от диапазона изменения сигналов обучающей выборки, среднее значение отклонения сигналов обучающей выборки от среднего значения сигнала и пятая часть диапазона изменения сигналов обучающей выборки. В качестве среднего значения испытательного сигнала и значения застabilизированного сигнала рассмотрены три случая: близкие к средним значениям обучающей выборки значения сигналов, близкие к максимальным значениям обучающей выборки значения сигналов, близкие к минимальным значениям обучающей выборки значения сигналов. Полученные в ходе экспериментов комплексные частотные характеристики первого канала объекта приведены на рис. 2, где также приведена реальная комплексная частотная характеристика, рассчитанная по известной передаточной функции канала объекта.

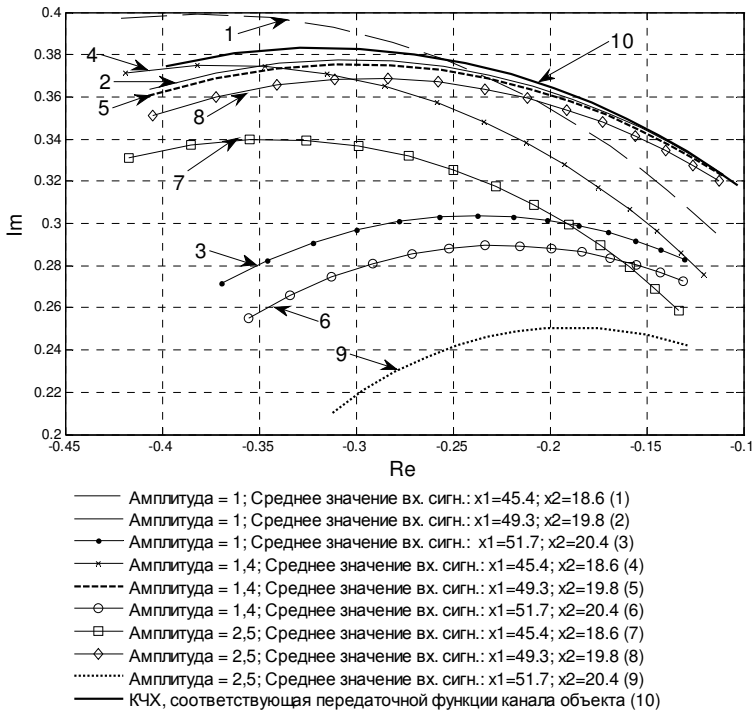


Рис. 2. Комплексные частотные характеристики, полученные в первой серии экспериментов

Результаты опыта показывают, что в качестве средних значений входных сигналов наилучший результат дают близкие к средним значениям сигналов обучающей выборки (кривые 2, 5, 8). Количественный критерий однозначного выбора амплитуды испытательных сигналов по результатам эксперимента сформулировать не удалось.

Во второй серии экспериментов амплитуды были определены путем разложения испытательных сигналов обучающей выборки в ряд Фурье. В результате разложения входного сигнала по каналу x_1 – у обучающей выборки в ряд Фурье в качестве испытательных выбраны гармоники:

$$\begin{array}{lll} -0,6202 \cdot \cos(0,0101 \cdot t); & 0,4052 \cdot \cos(0,0126 \cdot t); & -0,6258 \cdot \cos(0,0151 \cdot t); \\ -0,4157 \cdot \sin(0,0176 \cdot t); & 0,1569 \cdot \cos(0,0226 \cdot t); & -0,1881 \cdot \sin(0,0251 \cdot t); \\ -0,5149 \cdot \sin(0,0277 \cdot t); & 0,5219 \cdot \sin(0,0302 \cdot t); & -0,1529 \cdot \sin(0,0327 \cdot t); \\ 0,3453 \cdot \sin(0,0377 \cdot t); & -0,8254 \cdot \cos(0,0402 \cdot t); & 0,3856 \cdot \sin(0,0427 \cdot t); \\ 0,1339 \cdot \sin(0,0453 \cdot t); & -0,1998 \cdot \cos(0,0503 \cdot t). & \end{array}$$

Полученная экспериментальная и реальная комплексные частотные характеристики представлены на рис. 3.

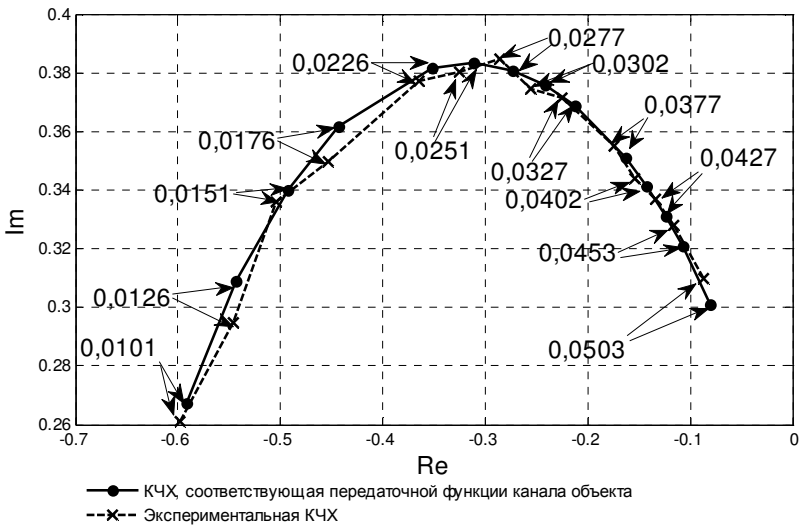


Рис. 3. Комплексные частотные характеристики, полученные во второй серии экспериментов

Полученная экспериментальная комплексная частотная характеристика близка к реальной.

Результаты эксперимента показывают, что метод, основанный на использовании ряда Фурье, позволяет определить оптимальные характеристики периодических испытательных сигналов для проведения опытов на нейросетевой модели динамического объекта.

Библиографический список

1. Giles C. Lee, Lawrance Steve, Ah Chung Tsoi. Noisy time series prediction using a recurrent neural network and grammatical interface // *Machine Learning*. – Vol. 44, no. 1 / 2. – P. 161–183.

2. Demuth Howard, Beale Mark, Hagan T. *Neural Network Toolbox. For use with Matlab. User's Guide*. – Natick, 2017. – 512 p.

3. Работников М.А., Бояршинова А.С., Шумихин А.Г. Автоматизация поиска значений параметров передаточной функции канала передачи по экспериментальной комплексной частотной характеристике // *Вестник Пермского национального исследовательского политехнического университета*. – 2017. – № 2. – С. 63–76.

4. Шумихин А.Г., Бояршинова А.С. Идентификация сложного объекта управления по частотным характеристикам, полученным экспериментально на его нейросетевой динамической модели // *Автоматика и телемеханика*. – 2015. – № 4. – С. 125–134.

5. Каханер Д., Моулер К., Нэш С. *Численные методы и программное обеспечение*: – М.: Мир, 2001. – 575 с.

6. Шумихин А.Г., Бояршинова А.С. Алгоритм выбора структурных параметров искусственной нейронной сети и объема обучающей выборки при аппроксимации поведения динамического объекта // *Компьютерные исследования и моделирование*. – 2015. – Т. 7. – № 2. – С. 243–251.

7. Пархоменко С.С., Леденёва Т.М. Обучение нейронных сетей методом Левенберга–Марквардта в условиях большого количества данных [Электронный ресурс] // *Вестник ВГУ*. – 2014. – № 2. – С. 98–104. – URL: <http://elibrary.ru/item.asp?id=21834126> (дата обращения: 27.02.2017).

Сведения об авторах

Исламов Рустам Рашидович – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: islamov.r.ra@yandex.ru

Александрова Анна Сергеевна – старший преподаватель кафедры «Автоматизация технологических процессов» Пермского национального исследовательского политехнического университета, Пермь, e-mail: boyarshinovaann@gmail.com

Шумихин Александр Георгиевич – доктор технических наук, профессор, заведующий кафедрой «Автоматизация технологических процессов» Пермского национального исследовательского политехнического университета, Пермь, e-mail: shumichin@gmail.com

About the authors

Islamov Rustam Rashidovich – Student Perm National Research Polytechnic University, Perm, e-mail: islamov.r.ra@yandex.ru

Alexandrova Anna Sergeevna – Senior Lecturer of the department automation of technological processes Perm National Research Polytechnic University, Perm, e-mail: boyarshinovaann@gmail.com

Shumikhin Alexander Georgievich – Doctor of Technical Sciences, professor, head of the department of automation of technological processes, Perm National Research Polytechnic University, Perm, e-mail: shumichin@gmail.com

МОДЕЛЬ СИНХРОННОГО ГЕНЕРАТОРА В СРЕДЕ MATLAB/SIMULINK С УЧЕТОМ НАСЫЩЕНИЯ МАГНИТНОЙ ЦЕПИ

И.А. Крылова, Б.В. Кавалеров

Пермский национальный исследовательский
политехнический университет, Пермь

Целью работы является совершенствование математической модели синхронного генератора, описанной уравнениями Парка–Горева для электрической идеализированной машины. Предложенная модель синхронного генератора построена в среде имитационного моделирования MatLab/Simulink.

Ключевые слова: синхронный генератор, газотурбинная установка, модель, насыщение.

MODEL OF SYNCHRONOUS GENERATOR WITH ACCOUNTING OF THE MAGNETIC CIRCUIT SATURATION IN THE MATLAB/SIMULINK ENVIRONMENT

I.A. Krylova, B.V. KavaleroV

Perm National Research Polytechnic University, Perm

The purpose of this article is to improve the mathematical model of a synchronous generator, described by the Park-Gorev equations for an electric idealized machine. The synchronous generator model in the MatLab / Simulink simulation environment was obtained.

Keywords: synchronous generator, gas turbine power plant, model, saturation.

Введение. Для исследования динамики синхронного генератора (СГ) применяются математические модели на основе уравнений Парка–Горева, однако такой тип математической модели СГ является моделью идеальной электрической машины. Для целей получения кривых переходных процессов, приближенных к реальным экспериментальным данным, важно учесть особенности протекания физических процессов в электрической машине и, прежде всего, явление насыщения магнитной цепи.

1. Порядок расчета параметров машины. Модель СГ составлена для явнополюсной синхронной машины [1]. Для учета насыщения используется характеристика холостого хода, в качестве примера ниже показаны данные для синхронного генератора ТК-4-2УХЛ.

Характеристика холостого хода генератора (ТК-4-2УХЛ)

$U, \text{кВ}$	3,0	3,5	4,0	4,5	5,0	5,5	6,0	6,3	7,0	7,5	8,2
$I_f, \text{А}$	48	55	64	76	82	93	107	116	143	172	240

Данные характеристики холостого хода позволяют найти зависимость индуктивности $L_{ад}$ от тока обмотки возбуждения i_f . Такую зависимость достаточно точно можно представить полином 3-й степени, полученным с помощью аппроксимации опытных данных (рис. 1).

Для рассматриваемой машины проекции тока намагничивания i_{μ} в осях ротора d, q определяются согласно выражениям:

$$I_{\mu d} = I_f + I_d \cdot \frac{I_{f\beta}}{I_H} + I_D \cdot \frac{I_{f\beta}}{I_H}, \quad (1)$$

$$I_{\mu q} = I_q \cdot \frac{I_{f\beta}}{I_H} + I_Q \cdot \frac{I_{f\beta}}{I_H}, \quad (2)$$

где $I_{\mu d}, I_{\mu q}$ – проекции тока намагничивания i_{μ} в осях ротора d, q ; I_d, I_q – проекции тока статора в осях ротора d, q ; I_f – ток возбуждения; $I_{f\beta}$ – ток возбуждения базовый; I_H – ток статора базовый; I_D, I_Q – проекции тока демпферных контуров в осях ротора d, q .

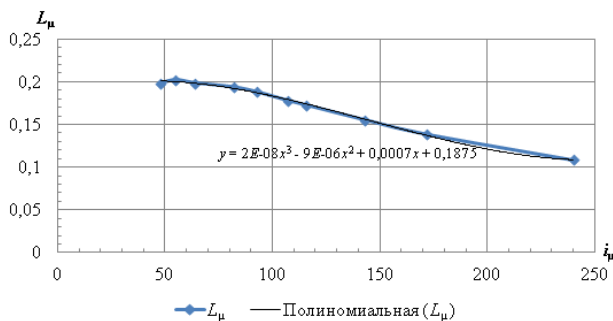


Рис. 1. Зависимость $L_{\mu} = F(i_{\mu})$ для ТК-4-2УХЛ

Из найденной выше зависимости $L_{\mu} = F(i_{\mu})$ определяются индуктивности $L_{\mu d}$ и $L_{\mu q}$ как функции $L_{\mu d}(q) = F[i_{\mu d}(q)]$.

Итоговый вид уравнений Парка–Горева в осях d, q для расчета потокосцеплений с учетом корректировки величин индуктивностей содержит систему дифференциальных уравнений с алгебраическим уравнением для расчета момента M (3) и систему алгебраических уравнений (4), записанную в векторно-матричном виде:

$$\begin{cases} u_d = -\Psi_q \omega + d\Psi_d / dt + i_d r; \\ u_q = \Psi_d \omega + d\Psi_q / dt + i_q r; \\ u_f = d\Psi_f / dt + i_f r_f; \\ 0 = d\Psi_D / dt + i_D r_D; \\ 0 = d\Psi_Q / dt + i_Q r_Q; \\ d\gamma/dt = \omega; \\ M = \Psi_d i_q - \Psi_q i_d; \end{cases} \quad (3)$$

$$\begin{pmatrix} \Psi_d(I_{\mu d}) \\ \Psi_D(I_{\mu d}) \\ \Psi_f(I_{\mu d}) \\ \Psi_q(I_{\mu q}) \\ \Psi_Q(I_{\mu q}) \end{pmatrix} = \begin{pmatrix} L_d(I_{\mu d}) & L_{ad}(I_{\mu d}) & L_{adf}(I_{\mu d}) & 0 & 0 \\ L_{ad}(I_{\mu d}) & L_D(I_{\mu d}) & L_{adf}(I_{\mu d}) & 0 & 0 \\ L_{fad}(I_{\mu d}) & L_{fad}(I_{\mu d}) & L_f(I_{\mu d}) & 0 & 0 \\ 0 & 0 & 0 & L_q(I_{\mu q}) & L_{aq}(I_{\mu q}) \\ 0 & 0 & 0 & L_{aq}(I_{\mu q}) & L_Q(I_{\mu q}) \end{pmatrix} \times \begin{pmatrix} I_d \\ I_D \\ I_f \\ I_q \\ I_Q \end{pmatrix}. \quad (4)$$

Модуль учета насыщения математической модели содержит в себе параметры индуктивностей, рассчитанных с применением известных методик [2, 3]:

$$L_{adf} = F(i_{\mu d}); \quad (5)$$

$$L_{ad} = \frac{L_{adf} \cdot I_{fB}}{I_H} [\Gamma_H], \quad x_{ad} = \frac{L_{ad} \cdot \omega}{z_B} [\text{o.e.}]; \quad (6)$$

$$L_d = \frac{x_d \cdot z_B}{\omega} [\Gamma_H], \quad x_d = x_{ad} + x_s [\text{o.e.}]; \quad (7)$$

$$L_{fad} = \frac{I_{fB} \cdot z_{fB} \cdot x_{ad}}{I_H \cdot \omega} [\Gamma_H]; \quad (8)$$

$$L_f = \frac{x_f \cdot z_{fB}}{\omega} [\Gamma_H], \quad x_f = \frac{x_{ad}^2}{x_d - x_d'} [\text{o.e.}]; \quad (9)$$

$$L_D = \frac{x_D \cdot z_B}{\omega} [\Gamma_H], \quad x_D = \frac{x_{ad}^2 \cdot (x_f - 2 \cdot x_{ad} + x_d - x_d'')}{x_f \cdot (x_d - x_d'') - x_{ad}^2} [\text{o.e.}], \quad (10)$$

где ω – синхронная угловая частота; zB – сопротивление статора базисное; x_s – индуктивное сопротивление рассеяния, $x_s = 0,0834$; z/B – сопротивление ротора базисное; $x'd$ – продольное переходное реактивное сопротивление для положительного следования фаз, $x'd = 0,2337$; $x''d$ – продольное сверхпереходное реактивное сопротивление для положительного следования фаз, $x''d = 0,139$, численные значения указаны для синхронного генератора ТК-4-2УХЛ.

Выражения (5)–(10) для расчета матрицы индуктивности справедливой и для поперечной оси, так как рассматриваемая машина является неявнополюсной, а значит, характеризуется магнитной симметрией.

2. Описание программного модуля учета насыщения. Программный модуль учета насыщения реализован в форме подмодели, показанной на рис. 2. Здесь входными параметрами являются токи статора I_d, I_q, I_D, I_Q , а также ток обмотки возбуждения I_f .

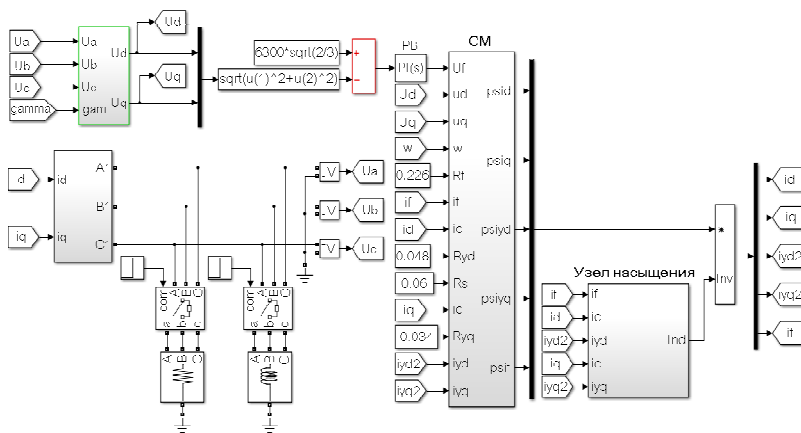


Рис. 2. Модуль учета насыщения в составе модели

Намагничивающие токи $I_{\mu d}$ и $I_{\mu q}$ и соответствующие им индуктивности $L_{\mu d}$, $L_{\mu q}$ определяются согласно (1), (2), (5) на каждом шаге расчета. По приведенным ранее выражениям (5)–(10) на каждом шаге интегрирования осуществляется расчет оставшихся индуктивностей матрицы индуктивностей (4) L_{ad} , L_{fad} , L_d , L_f , L_D , L_{aq} , L_q , L_Q .

Итоговый вид матрица индуктивностей (4) получает путем конкатенации векторов, состоящих из найденных индуктивностей (рис. 3).

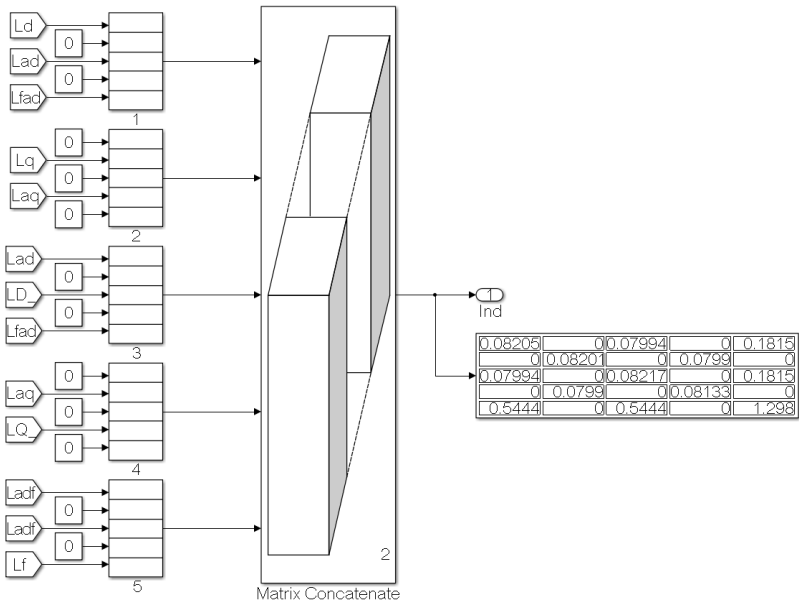


Рис. 3. Формирование итоговой матрицы индуктивностей (9)

3. Результаты моделирования. Результаты моделирования представлены на рис. 4–6.

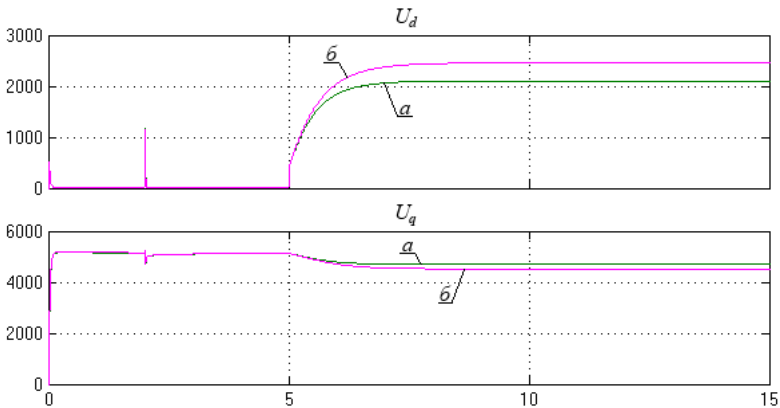


Рис. 4. Напряжение статора U_d и U_q (В): a – без учета насыщения магнитной цепи; b – с учетом насыщения магнитной цепи

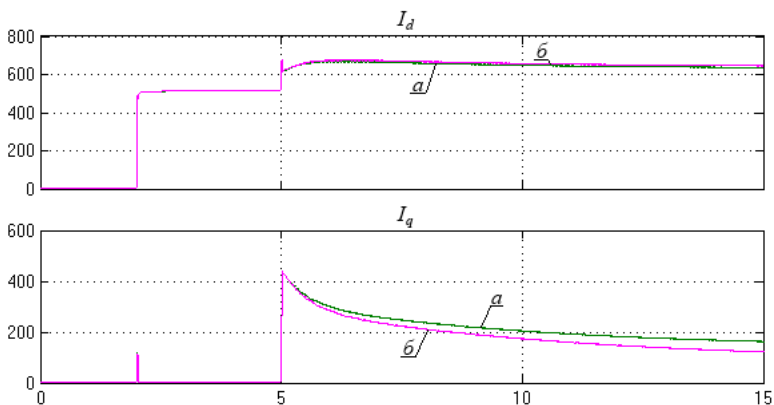


Рис. 5. Ток статора I_d и I_q (В): a – без учета насыщения магнитной цепи; b – с учетом насыщения магнитной цепи

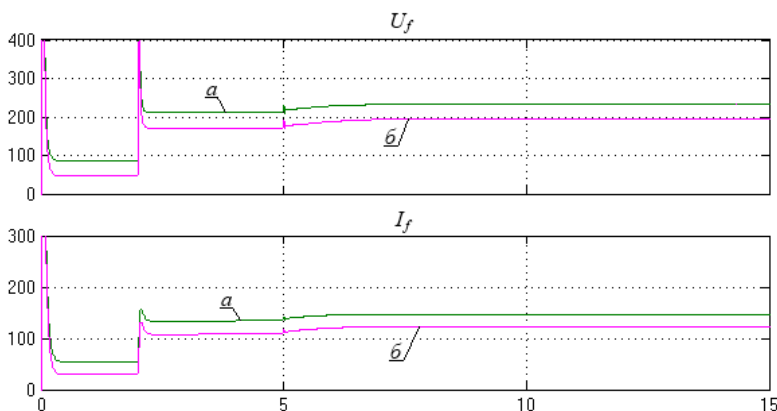


Рис. 6. Напряжение U_f (В) и ток I_f (А) обмотки возбуждения: a – без учета насыщения магнитной цепи; b – с учетом насыщения магнитной цепи

Время моделирования составляет 15 с, на протяжении первых 2 с осуществлен процесс пуска генератора на холостом ходу, нагрузка на силовых шинах отсутствует. С 2-й по 5-ю секунду моделирования подключается нагрузка в виде блока номинальной активной мощности 4 кВт. На оставшихся 10 с моделирования нагрузка генератора является активно-индуктивной, помимо активной номинальной мощности включается индуктивная номинальная нагрузка мощностью 3 кВт.

Как показывают результаты моделирования, при переходе к учету насыщения магнитной цепи путем коррекции индуктивностей взаимной индукции по продольной и поперечной осям в функции тока намагничивания на каждом шаге интегрирования статические параметры тока и напряжения статора, а также напряжения обмотки возбуждения претерпевают изменения.

Данный факт подтверждает необходимость учитывать насыщение магнитной цепи машины для более адекватного анализа работы систем автоматического управления (САУ) синхронным генератором.

Заключение. Как известно, в связи с упрощением объекта обычно возникает задача последующей настройки математической модели на реальный объект с целью более адекватного описания переходных процессов, иными словами, задача идентификации [4].

Для упрощения этой задачи целесообразно предварительно повысить точность математической модели объекта исследования. Именно с этой целью в данной статье предложена модель синхронного генератора, учитывающая насыщение магнитной цепи машины.

Данная модель может быть полезна при проектировании и настройке регуляторов САУ синхронного генератора.

Библиографический список

1. Крылова И.А., Тюленев М.Е. О моделировании синхронного генератора в среде Simulink для исследования автоматических регуляторов // Автоматизация в электроэнергетике и электротехнике: материалы II Междунар. науч.-техн. конф.; 21–22 апреля 2016 г. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2016, – С. 66–71.

2. Бернас С., Цек З. Математические модели элементов электроэнергетических систем / пер. с польск. Э.В. Турского, Н.Н. Шелухина. – М.: Энергоиздат, 1982. – 312 с.

3. Лютер Р.А. Расчёт синхронных машин. – Л.: Энергия, 1979. – 272 с.

4. Эйкхофф П. Основы идентификации систем управления. Оценка параметров и состояния. – М.: Мир, 1975. – 685 с.

Сведения об авторах

Крылова Ирина Андреевна – аспирантка Пермского национального исследовательского политехнического университета, Пермь, e-mail: krylova@eservice.perm.ru

Кавалеров Борис Владимирович – доктор технических наук, доцент, заведующий кафедрой «Электротехника и электромеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: kbv@pstu.ru

About the authors

Krylova Irina Andreevna – Graduate Student Perm National Research Polytechnic University, Perm, e-mail: krylova@eservice.perm.ru

Kavalerov Boris Vladimirovich – Doctor of Technical Sciences, Professor, head of the Electrotechnics and electromechanics department of Perm National Research Polytechnic University, Perm, e-mail: kbv@pstu.ru

ПРИМЕНЕНИЕ НЕЧЕТКОЙ ЛОГИКИ В ПРОЦЕССЕ УПРАВЛЕНИЯ РЕДУЦИРОВАНИЕМ ГАЗА В МАГИСТРАЛЬНЫХ ТРУБОПРОВОДАХ

В.В. Крюков

Оренбургский государственный университет, Оренбург

В данной статье рассматривается пример системы управления клапаном-регулятором высокого давления на базе нечеткой логики. Описываются принцип его управления, а также достоинства по сравнению с традиционным ПИД-регулированием.

Ключевые слова: газопровод, клапан-регулятор, износ деталей, нечеткая логика.

THE APPLICATION OF FUZZY LOGIC IN THE MANAGEMENT OF THE REDUCING GAS IN THE MAIN GASPIPELINES

V.V. Kryukov

Orenburg State University, Orenburg

This article describes an example control valve regulator high pressure on the basis of fuzzy logic. Describes the principle of its management, as well as advantages compared with the traditional PID-regulation.

Keywords: pipeline, regulator valve, wear parts, fuzzy logic.

Одной из основных задач газотранспортной системы является безопасное и безаварийное функционирование оборудования линейной части магистрального газопровода, одним из основных элементов которой является узел редуцирования газа. Узлы предназначены для понижения давления транспортируемого газа до заданного с целью перепуска газа из газопровода с более высоким давлением газа в газопровод с более низким [1]. Одной из главных составляющих любого узла редуцирования является регулирующий клапан. Именно от правильности его настройки в дальнейшем зависит работа всего магистрального газопровода.

Как показывает практика, настройка ПИД-регуляторов очень сложна и трудоемка. Она, как правило, включает в себя решение сложных систем дифференциальных уравнений, которое не всегда точное. Это свидетельствует о том, что на практике заданная величина (уставка) давления в таких системах достигаться не будет. К тому же все это ведет к автоколебаниям и перерегулированию в системе

и, как следствие, быстрому износу механически подвижных деталей регулирующего органа (клапана), таких как штоки, уплотнения, поршень, седло клапана и т.д. [2]. В связи с этим возникают различные аварийные ситуации, вплоть до разрыва газопровода при превышении максимально допустимого значения давления. Данные моменты ведут к ремонтно-восстановительным работам на участке газопровода, стравливаю газу в атмосферу (загрязнение экологии), в связи с чем происходят длительные простои в транспортировке газа и огромные финансовые потери для предприятия и общества в целом.

Однако в последнее время получил распространение новый принцип построения регуляторов, использующий правила нечеткой логики (fuzzy logic). Этот принцип соединяет в себе все преимущества существующих регуляторов и точность цифрового управления. Использование простых и недорогих контроллеров позволяет вести многопозиционное управление и в то же время не требует трудоемких вычислений, необходимых при непрерывном управлении.

Процесс регулирования в системе осуществляется по следующему принципу: время работы разбито на определенные интервалы, в течение каждого такого интервала происходит замер фактического давления на выходе регулятора. Показания измеренного давления с датчика фаззифицируются, т.е. переводятся в нечеткий формат и обрабатываются. Если по результату замера показания давления больше или меньше заданной величины, значит, система нуждается в регулировании. Данные с контроллера дефаззифицируются, и посылается соответствующий выходной управляющий сигнал (рис. 1).

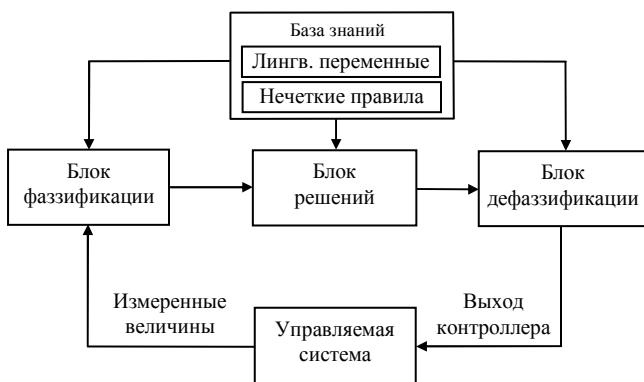


Рис. 1. Структурная схема регулятора на основе нечеткой логики

В регуляторах, основанных на правилах нечеткой логики (fuzzylogic), управляющее воздействие, так же как и при ПИД-регулировании, как уже говорилось, формируется на основе разности измеренного фактического давления в среде и задания (уставки) давления. Опишем подробнее принцип работы таких регуляторов. Область значений давления условно разделяется на промежутки (как правило, на три промежутка). Среди этих интервалов давления обязательно существует интервал, при попадании в который фактическое давление считается близким к заданию, не нуждающимся в регулировке (зона нечувствительности). В регуляторе реализованы простые условные правила, по которым в случае, когда давление попадает в один из промежутков, не являющихся зоной нечувствительности, подается регулирующий сигнал, соответствующий данному интервалу, переводящий значение давления в системе в зону нечувствительности. Эти условия принимают вид:

если $(P_{\max} \geq P - P_{\text{зад}} > N_{\text{верх}})$, то управляющее воздействие = Y_1 ;

если $(N_{\text{верх}} \geq P - P_{\text{зад}} \geq N_{\text{ниж}})$, то управляющее воздействие = 0;

если $(N_{\text{ниж}} > P - P_{\text{зад}} \geq P_{\min})$, то управляющее воздействие = Y_2 ,

где P_{\max} , P_{\min} – максимально возможное и минимально возможное значение давления в системе; P , $P_{\text{зад}}$ – фактическое давление и заданное соответственно; $N_{\text{верх}}$, $N_{\text{ниж}}$ – верхняя и нижняя границы зоны нечувствительности; Y_1 , Y_2 – величины управляющих сигналов.

Как зону нечувствительности правильно выбирать интервал давления газа, в диапазонах которого различия между фактическим давлением и заданным не влияют на технологический процесс.

Рассмотрим данный принцип управления на примере клапана регулятора, установленного на узле редуцирования магистрального газопровода № 1 с параметрами ДУ 1200 мм P_y 75 кг/см² в магистральный газопровод № 2 Ду 100 мм P_y 55 кг/см².

Давление пре перепуске газа из газопровода №1 в газопровод №2 должно осуществляется в пределах от 53 (+1...–1) кг/см². Следовательно, значения давления будут следующими:

$$P_{\max} = 55 \text{ кг/см}^2, P_{\min} = 0 \text{ кг/см}^2, N_{\text{верх}} = 54 \text{ кг/см}^2, N_{\text{ниж}} = 52 \text{ кг/см}^2.$$

Пусть уставка регулирования $P_{\text{зад}} = 53 \text{ кг/см}^2$.

Следовательно, функция принадлежности будет иметь следующий вид (рис. 2).

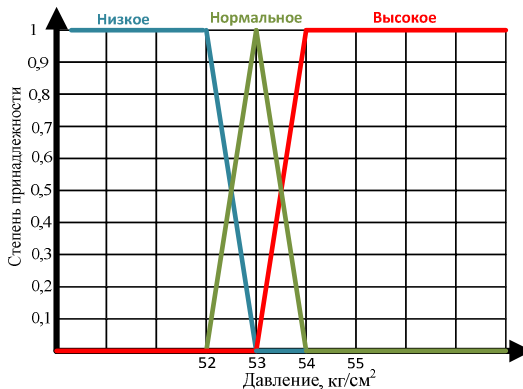


Рис. 2. Функция принадлежности

Управление клапаном будет осуществляться по следующему принципу:

если фактическое давление в газопроводе находится в пределах:

0–52 кг/см² – то «клапан открыть полностью»;

52–53 кг/см² – то «клапан частично открыть»;

53 кг/см² – то «клапан остается в текущем положении»;

53–54 кг/см² – то «клапан частично закрыть»;

более 54 кг/см² – то «клапан закрыть полностью».

Использование данного алгоритма управления значительно увеличит ресурс службы клапана в связи с минимальным воздействием на его механическую часть и, как следствие, позволит добиться безаварийного функционирования системы в целом.

Подводя итог, можно подытожить, что у нечетких систем возможности значительно шире, чем у ПИД-регуляторов. Нечеткие системы позволяют не только регулировать параметры объекта (т.е. заставляют их колебаться в некотором интервале от заданного значения), но и позволяют устанавливать взаимосвязь между ними и даже изменять задание в зависимости от ситуации.

Основная задача промышленной регулирующей трубопроводной арматуры – изменять расход газа в соответствии с производственным процессом. Успех применения нечеткой логики в других отраслях промышленности дает надежду, что и в управлении трубопроводной арматурой она займет достойное место.

Библиографический список

1. Козаченко А.Н. Эксплуатация компрессорных станций магистральных газопроводов. – М.: Нефть и газ, 1999. – 463 с.

2. Гостев В.И. Проектирование нечетких регуляторов для систем автоматического управления. – СПб.: БХВ-Петербург, 2011. – 416 с.

Сведения об авторах

Крюков Владимир Викторович – аспирант Оренбургского государственного университета, Оренбург, e-mail: krykov56@rambler.ru

About the authors

Vladimir Viktorovich Kryukov – Graduate Student Orenburg State University, Orenburg, e-mail: krykov56@rambler.ru

АВТОМАТИЗАЦИЯ ОПЕРАЦИИ ПО ЗАТЯЖКЕ ГАЙКИ ПОДШИПНИКА ВАЛА НЕСУЩЕГО ВИНТА ВЕРТОЛЕТНОГО РЕДУКТОРА ВР-8А

А.Ф. Наджафов

Оренбургский государственный университет, Оренбург

В данной статье рассмотрено проектирование станда, который позволит автоматизировать процесс затяжки гайки редуктора и обеспечить высокую точность момента затяжки.

Ключевые слова: автоматизация, станд, гайка.

AUTOMATION OF THE OPERATION FOR TIGHTENING THE ROTOR SHAFT BEARING OF THE ROTOR SHAFT OF THE HELICOPTER REDUCER VR-8A

A.F. Najafov

Orenburg State University, Orenburg

This article considers the design of the stand, which will automate the process of tightening the reducer nuts and ensure high accuracy of the tightening torque.

Keywords: automation, stand, nut.

В настоящее время на предприятии ремонт редуктора регламентируется руководящими документами: руководство по эксплуатации, перечень обязательных работ, технологические указания по монтажу и демонтажу агрегатов, технологические указания по ремонту отдельных агрегатов, РКР и т.д.

ТУ по ремонту редуктора адаптированы под конкретные условия проведения ремонта, т.е. под применяемые методы контроля технического состояния, имеющееся оборудование, применяемые методы восстановления покрытий и т.д.

На заводе используют различные прессы, ключи, съемники, электротельферы, механические подъемники и другие приспособления. Для сокращения продолжительности разборки редуктора и снижения трудозатрат работников заменены гаечные ключи, используемые при снятии отдельных деталей, на современные пневмопистолеты и шуруповерты с насадками различных диаметров для разворачивания гаек. Все детали и узлы редуктора раскладываются по сортовикам и телегам.

При проведении сборки редуктора используется различное технологическое оборудование, в том числе и различные станды. Операцию по затяжке гайки подшипников вала несущего винта редуктора ВР-8А производят с помощью динамометрического ключа. Недостатками данного оборудования и, как следствие, всего технологического процесса монтажа гайки являются:

- 1) измерение крутящего момента на входном валу редуктора. В процессе эксплуатации данного ключа происходит износ редуктора, что приводит к отклонению фактического момента затяжки от момента, заданного в ТУ. Данный недостаток приводит к уменьшению фактической долговечности подшипника 6-126236Б5 и, как правило, к его отказу и досрочному съему редуктора с эксплуатации;
- 2) невозможность обеспечить точность момента затяжки;
- 3) необходимо участие двух исполнителей.

Составление технического задания. Спроектировать станд по затяжке гайки подшипников вала несущего винта редуктора ВР-8А с контролем момента затяжки. Необходимо обеспечить момент затяжки в 10 кНм.

Проектируемый станд должен отвечать следующим требованиям:

- 1) момент затяжки должен осуществляться непосредственно на выходном валу устройства перед гайкой;
- 2) обеспечивается точность момента затяжки порядка ± 50 Н·м;
- 3) число исполнителей, работающих на станде, не более 1 человека;
- 4) возможность подключаться к пневмолинии с давлением 0,6...0,8 МПа;
- 5) изготавливается в условиях ремонтного предприятия, по возможности с использованием унифицированных элементов и агрегатов конструкции.

Выбор принципиальной схемы станда. На основании технического задания разрабатывается принципиальная схема (рисунок) проектируемого оборудования.

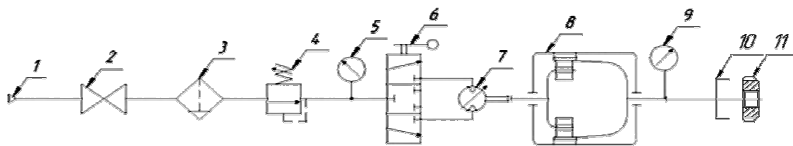


Рис. Принципиальная схема станда: 1 – штуцер; 2 – перекрывной кран; 3 – фильтр-влагодотделитель; 4 – редуктор; 5 – манометр; 6 – кран 3-ходовый; 7 – пневмомотор регулируемый реверсивный; 8 – волновой редуктор; 9 – индикатор часового типа; 10 – переходник; 11 – гайка

Для преобразования угловой скорости вращения входного вала в более низкую на выходном валу, повышая при этом вращающий момент, необходимо применять редуктор.

Типы рассматриваемых редукторов:

- 1) червячный редуктор,
- 2) планетарный редуктор,
- 3) волновой редуктор.

Волновой редуктор выбран, так как он обладает следующим рядом преимуществ:

- высокая кинематическая точность и плавность хода;
- большое передаточное отношение при малом количестве деталей;
- улучшенные массогабаритные характеристики по сравнению с обычными зубчатыми передачами;
- высокая нагрузочная способность.

Червячный редуктор не выбран из-за низкого КПД и склонности к заеданию, а планетарный – из-за большой массы.

Подбор стандартных элементов конструкции:

1. Индикатор ИЧ-05 кл.0 ГОСТ 577-68.
2. Кран шаровой.
3. Манометр ДМ-1001У2.
4. Пневмодвигатель Deprag 63-001F07, $T = 18$ Нм, расход 1200 л/мин.
5. Пневмоклапан редукционный ПКРМ 112-25.
6. Пневмораспределитель 12-21.
7. Фильтр-влагоотделитель П-ФВ-16-2

Техническое описание стенда

Стенд предназначен для затяжки гайки подшипников вала несущего винта редуктора ВР-8А с контролем момента затяжки. Момент затяжки может достигать 10 кНм. Стенд состоит из системы подготовки и преобразования энергии сжатого воздуха в механическую, блока передачи и контроля крутящего момента.

Для системы подготовки и преобразования энергии в качестве источника сжатого воздуха служит заводская пневмомагистраль с максимальным давлением 0,8 МПа и расходом 10 л/мин. Подача воздуха в систему подготовки воздуха осуществляется запорным краном. После подачи воздуха происходит его очистка в фильтровлагоотделителе.

Контроль за давлением осуществляется с помощью манометра. Направление вращения пневмодвигателя задается пневмораспределителем, установленным на лицевой панели. В пневмомоторе осуществляется непосредственно преобразование энергии сжатого воздуха в механическую, которая передается на волновой редуктор.

Блок передачи и контроля крутящего момента: состоит из накидного ключа с установленными на торцевой части двумя индикаторами часового типа и торсиона, через который осуществляется передача крутящего момента на накидной ключ. Крутящий момент замеряется по двум индикаторам во избежание погрешности.

При установке редуктора на станину устанавливается блок передачи и контроля крутящего момента. При выборе направления вращения крутящий момент через волновой редуктор передается на торсион с помощью шлицевого соединения, происходит затяжка/отворачивание гайки в зависимости от выбранного направления вращения. Торсион передает крутящий момент на накидной ключ также с помощью шлицевого соединения. С увеличением крутящего момента происходит скручивание торсиона, и через два поводка осуществляется замер угла скручивания торсиона, который линейно зависит от крутящего момента на гайке. Скорость закрутки регулируется с помощью дросселя, установленного на пневмодвигателе, и настраивается заранее, а также с помощью пневморедуктора и плавно изменяется в процессе монтажа или демонтажа.

Библиографический список

1. Данилов В.А. Вертолет Ми-8 (устройство и техническое обслуживание). – М.: Транспорт, 1988. – 278 с.
2. Редуктор ВР-8А: руководство по ремонту.
3. Орлов П.И. Основы конструирования: справочно-методическое пособие. – М.: Машиностроение, 1988. – 560 с.
4. Решетов Д.Н. Детали машин: учебник для студ. машиностроит. и механ. специальностей вузов. – М.: Машиностроение, 1989. – 496 с.
5. Игонин Н.Н., Новиков Г.А., Старостин И.Г. Исследование причин появления неисправностей авиационной техники: метод. указания. – Самара: Изд-во СГАУ, 2004. – 44 с.

6. Руденко, В.Н. Планетарные и волновые передачи: альбом конструкций. – М.: Машиностроение, 1980. – 148 с.

7. Анурьев В.И. Справочник конструктора-машиностроителя. – М.: Машиностроение, 2001. – 864 с.

Сведения об авторе

Наджафов Анар Фикретович – студент Оренбургского государственного университета, Оренбург, e-mail: Anarnadzhafov@yandex.ru

About the author

Najafov Anar Fikretovich – Student Orenburg State University, Orenburg, e-mail: Anarnadzhafov@yandex.ru

ПРИМЕНЕНИЕ МЕТОДА ФУНКЦИОНАЛЬНО-ВОКСЕЛЬНОГО МОДЕЛИРОВАНИЯ К ЗАДАЧАМ ПОИСКА ПУТИ С ПОМОЩЬЮ ОБЪЕКТОВ СЛОЖНОЙ КОНФИГУРАЦИИ

П.А. Петухов, С.В. Додонов, А.В. Толоч
Московский государственный технологический
университет «СТАНКИН», Москва

В данной работе рассматриваются задачи поиска возможных вариантов построения трассы с помощью функционально-воксельного моделирования с применением принципов метода потенциалов на примере сложных коммуникаций технических систем. На основе функционально-воксельного моделирования создается графическая среда трассировки, которая способствует формированию трассы от начальной до конечной точки, в обход статических препятствий. Принцип потенциальных полей позволяет динамически сканировать пространство с препятствиями для решения таких задач в слабодетерминированной среде.

Ключевые слова: функционально-воксельное моделирование, метод потенциалов, градиентный метод, локальные геометрические характеристики (ЛГХ), воксельный вычислитель.

APPLICATION OF THE FUNCTION-VOXEL MODELING METHOD TO THE PROBLEMS OF SEARCHING FOR THE ROUTE WITH THE OBJECTS OF THE COMPLEX CONFIGURATION

P.A. Petukhov, S.V. Dodonov, A.V. Tolok
Moscow State University of Technology «STANKIN», Moscow

In this study, we consider the problem of finding possible route variants with the help of functional-voxel modeling and the method of potential, in the case of complex communications in a technical system. On the basis of functional-voxel modeling, a graphic trace system is created, which forms the trace from the initial to the end point, bypassing obstacles, and also by the method of potential.

Keywords: functional-voxel modeling, method of potentials, gradient method, local geometric characteristics (LHC), voxel calculator.

На сегодняшний день существует множество подходов к решению задач, связанных с поиском пути в детерминированной (заранее определённой) среде. В большинстве случаев они сводятся к задачам управления объектом, движущимся к цели. Использование различных подходов при построении трассы (или группы трасс) в зависимости от

используемого метода предъявляет определённые требования. Так, к примеру, для построения оптимального маршрута мобильного робота можно использовать такие параметры, как «близость» к препятствию и величины, влияющие на выбор решения. Варьируя данными параметрами, можно оптимизировать варианты решения для каждой конкретной ситуации. Алгоритм основан на использовании «притягивающего» и «отталкивающих» полей, в результате чего на каждом шагу рассчитывается потенциальное поле в текущем положении координат, а затем рассчитывается сила, индуцированная этим полем. Полученная сила определяет направление движущегося объекта к назначенной цели. Метод характерен тем, что позволяет постоянно сканировать динамически изменяемую среду. Недостатком является временная зависимость работы алгоритма от количества препятствий в среде.

Методом, который позволяет более полно описать геометрические свойства объекта на компьютере, является метод функционально-воксельного моделирования (ФВМ).

Функционально-воксельное моделирование – графическое представление данных об объекте, которое использует аналитический способ описания моделей. ФВМ позволяет эффективно решать задачи, связанные с прокладкой трасс с использованием статического (аналитического) описания объектов-препятствий.

Добавление динамической составляющей метода потенциальных полей позволит эффективно строить маршрут для слабодетерминированных сред, когда доступны к использованию сильные стороны обоих методов. Реализация данного подхода позволит привести к синтезу двух методов: метода «потенциалов» и метода ФВМ (рис. 1).

Метод потенциальных полей. Вспомогательным средством для построения трассы в системе является метод потенциальных полей (potential fields). Традиционные подходы метода потенциальных полей создают притягивающее поле внутри цели. Потенциальное поле определяется через все свободное пространство, и на каждом временном шаге вычисляется потенциальное поле для текущего положения, а затем рассчитывается система индуцированных этим полем сил. Трасса прокладывается в соответствии с системой сил. Принцип работы метода представлен на рис. 2.



Рис. 1. Функциональная модель интерактивного редактора

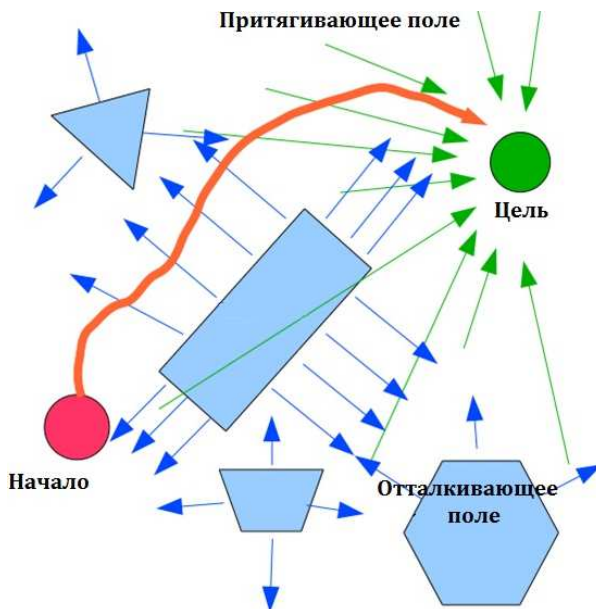


Рис. 2. Притягивающие и отталкивающие поля

Для того чтобы построить трассу, необходимо вычислить потенциал функции. Формула в общем виде для вычисления потенциала, как правило, представляется в виде:

$$U(q) = U_{\text{att}}(q) + U_{\text{rep}}(q). \quad (1)$$

«Притягивающий» потенциал $U_{\text{att}}(q)$ и его градиент определяют как функция от фактической конфигурации q и конфигурации цели q_{goal} :

$$U_{\text{att}}(q) = \begin{cases} \frac{1}{2} \zeta d^2(q, q_{\text{goal}}), & d(q, q_{\text{goal}}) \leq d_{\text{goal}}^*, \\ d_{\text{goal}}^* \zeta d(q, q_{\text{goal}}) - \frac{1}{2} \zeta (d_{\text{goal}}^*)^2, & d(q, q_{\text{goal}}) > d_{\text{goal}}^*, \end{cases} \quad (2)$$

$$\nabla U_{\text{att}}(q) = \begin{cases} \zeta(q - q_{\text{goal}}), & d(q, q_{\text{goal}}) \leq d_{\text{goal}}^* \\ \frac{d_{\text{goal}}^* \zeta (q - q_{\text{goal}})}{d(q, q_{\text{goal}})}, & d(q, q_{\text{goal}}) > d_{\text{goal}}^*, \end{cases} \quad (3)$$

где ζ – коэффициент притяжения; $d(q, q_{\text{goal}})$ – расстояние между текущим положением и положением цели; d_{goal}^* – пороговая функция, изменяющее свое значения для того, чтобы сбалансировать величину потенциала.

«Отталкивающий» потенциал $U_{\text{rep}}(q)$ и градиент определяются как функция расстояния $D(q)$ от фактической конфигурации q и ближайшим препятствием:

$$U_{\text{rep}}(q) = \begin{cases} \frac{1}{2} \eta \left(\frac{1}{D(q)} - \frac{1}{Q^*} \right)^2, & D(q) < Q^*, \\ 0, & D(q) > Q^*, \end{cases} \quad (4)$$

$$\nabla U_{\text{rep}}(q) = \begin{cases} \eta \left(\frac{1}{Q^*} - \frac{1}{D(q)} \right) \frac{1}{D^2(q)} \nabla D(q), & D(q) < Q^*, \\ 0, & D(q) > Q^*, \end{cases} \quad (5)$$

где η – отталкивающий коэффициент; $D(q)$ – расстояние между конфигурацией q и его ближайшим препятствием; Q^* – порог близости препятствий.

Описание программного обеспечения для прокладки пути.

Для динамичной работы системы в детерминированной среде применяется метод ФВМ [3]. Создан графический модуль для трассировки на двумерных функционально-воксельных моделях, который позволяет моделировать сцену, при этом автоматически формируя аналитическое описание модели. Для моделирования объектов-препятствий используется интерактивная графическая подсистема компоновки замкнутых контурных объектов [1]. Базовым примитивом, с которым работает пользователь, является плоское положительное

полупространство. Строится замкнутый контурный объект путем компоновки из нескольких полупространств [1]. Программа представляет собой среду для динамического и интерактивного построения пути к назначенной цели с учетом обхода препятствий. Разработка осуществлялась на основе метода функционально-воксельного моделирования [2]. Синтез двух методов (ФВМ и потенциальных полей) позволяет ускорить время расчёта динамического движения объекта к выбранной цели. При этом стационарные препятствия и цель описаны градиентной поверхностью, что позволяет двигаться к цели по градиентному спуску. Динамические же препятствия подлежат постоянному мониторингу методом потенциальных полей. Разница в построении трассы с использованием функционально-воксельного метода без учета потенциальных полей продемонстрирована на рис. 3, а, а с учетом потенциальных полей – в разработанном приложении на рис. 3, б.

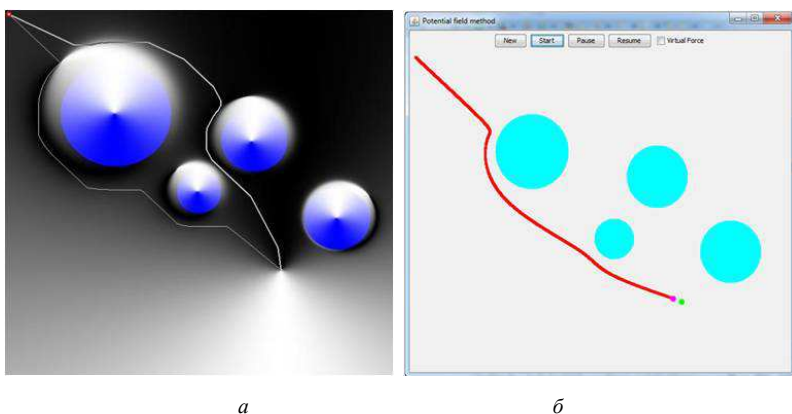


Рис. 3. Построение трассы с использованием: а – ФВМ; б – метода потенциалов

Задача поиска пути сводится к синтезу метода потенциалов и метода функционально-воксельного моделирования, использующему градиентный подход для обхода пути. Реализация нового подхода позволит решать все задачи, требующие максимальной готовности, чтобы обойти движущееся препятствие.

Идея создания воксельного вычислителя. Функционально-воксельный метод также позволяет разрабатывать альтернативные способы решения задач моделирования [3]. В чем же может прояв-

ляться эта альтернатива? Можно уйти от традиционных координатных методов и перейти к понятию локальных геометрических характеристик. Координаты (x, y, z) , которые несли свою геометрическую информацию о форме объекта в координатном методе, превращаются в обычную точку в пространстве, не несущую никакой информации о форме и лишь локализирующую геометрическую информацию в определенной точке пространства. При этом вся геометрическая информация о форме остается только в локальных геометрических характеристиках. Таким образом, как бы подменяется пространство «хуз» на пространство « $ABCD$ », которое должно подвергаться геометрическим преобразованиям. К геометрическим преобразованиям пространства относятся операции сдвига, поворота и масштабирования модели. Принципы и алгоритмы геометрических преобразований для координатного метода описаны в работе [4]. Данный шаг позволит отказаться от «хуз» на определенном уровне, и тогда работа будет проводиться только с локальными геометрическими характеристиками, которые позволят изменять как пространство функции, так и двигать вправо-влево, поворачивать, масштабировать функционально-воксельную модель в пространстве и т.д.

Для этого сначала потребуется создать математический аппарат, позволяющий определять локальные геометрические характеристики воксельной геометрической модели. Затем закодировать созданный математический аппарат и алгоритмы геометрических преобразований в процедуры автоматических вычислительных средств, коим и будет являться воксельный вычислитель. Разработка такого рода графического вычислителя позволит повысить эффективность обработки воксельных геометрических моделей за счет ускорения выполнения геометрических преобразований.

Библиографический список

1. Интерактивная система создания и компоновки функционально-воксельных моделей для решения задачи поиска пути градиентным методом / С.В. Додонов, М.А. Локтев, П.А. Петухов, А.В. Толок // Вестник МГТУ «Станкин». – 2016. – № 3(38). – С. 66–69.

2. Локтев М.А., Толок А.В. Функциональный принцип обхода препятствий с применением метода функционально-воксельного моделирования // Вестник МГТУ «Станкин». – 2016. – № 1(36). – С. 75–80.

3. Толок А.В. Функционально-воксельный метод в компьютерном моделировании / под ред. акад. РАН С.Н. Васильева. – М.: ФИЗМАТЛИТ, 2016. – 112 с.

4. Толок А.В., Лоторевич Е.А. Тройственность подхода к задачам преобразования пространства функционально-воксельной модели // Тр. 26-й Междунар. науч. конф. GraphiCon2016. – Н. Новгород: Изд-во ИФТИ, ННГАСУ, 2016. – С. 81–84.

Сведения об авторах

Петухов Павел Андреевич – аспирант Московского государственного технологического университета «Станкин», Москва, e-mail: petuxowpawel@yandex.ru

Додонов Сергей Валерьевич – аспирант Московского государственного технологического университета «Станкин», Москва, e-mail: dodonov15@yandex.ru

Толок Алексей Вячеславович – доктор технических наук, профессор Московского государственного технологического университета «Станкин», Москва, e-mail: a.tolok@stankin.ru

About the authors

Petukhov Pavel Andreevich – Graduate Student Moscow State University of Technology «STANKIN», Moscow, e-mail: petuxowpawel@yandex.ru

Dodonov Sergey Valer'evich – Graduate Student Moscow State University of Technology «STANKIN», Moscow, e-mail: dodonov15@yandex.ru

Tolok Alexey Vyacheslavovich – Doctor of Technical Sciences, Professor Moscow State University of Technology «STANKIN», Moscow, e-mail: a.tolok@stankin.ru

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ИДЕНТИФИКАЦИИ КАНАЛОВ УПРАВЛЯЕМОГО ОБЪЕКТА ПО ЭКСПЕРИМЕНТАЛЬНОЙ КОМПЛЕКСНОЙ ЧАСТОТНОЙ ХАРАКТЕРИСТИКЕ

М.А. Работников, А.С. Александрова, А.Г. Шумихин

Пермский национальный исследовательский
политехнический университет, Пермь

Представлены результаты разработки и тестирования программного приложения, позволяющего производить поиск значений параметров передаточной функции канала передачи исследуемого объекта по найденной экспериментально его комплексной частотной характеристике. Приложение протестировано на данных с реального управляемого лабораторного объекта – эмулятора печи. Реализованные в приложении оптимизационные методы позволяют идентифицировать параметры объекта управления, по которым в виде его передаточных функций можно получить имитационную модель объекта управления.

Ключевые слова: управляемый объект, комплексная частотная характеристика, передаточная функция, идентификация, метод наименьших квадратов, метод сканирования, метод Гаусса–Зейделя, симплекс-метод, метод наискорейшего спуска.

PROGRAM IMPLEMENTATION OF THE ALGORITHM FOR THE IDENTIFICATION TRANSFER FUNCTION OF THE CONTROL OBJECT ACCORDING TO EXPERIMENTAL COMPLEX FREQUENCY RESPONSE

M.A. Rabotnikov, A.S. Aleksandrova, A.G. Shumikhin

Perm National Research Polytechnic University, Perm

In this article the results of the development and testing of the software application that allows to search the values of the parameters of the transfer function of the controlled object based on the experimentally found its complex frequency response are presented. The application was tested on data from a controlled laboratory facility – an oven emulator. The optimization methods implemented in the application make possible to identify the parameters of the control object through which, in the form of transfer functions, it is possible to obtain a simulation model of the control object.

Keywords: controlled object, complex frequency response, transfer function, identification, least squares method, scan method. Gauss–Seidel method, simplex method, gradient method.

Существует множество способов исследования динамики технологических объектов, одним из них является идентификация каналов объекта с использованием частотных методов. Результатом таких испытаний является набор экспериментальных данных, а именно набор значений комплексной частотной характеристики для соответствующего им набора частот.

Для упрощения обработки результатов подобных измерений разработано приложение [1], позволяющее идентифицировать параметры передаточной функции исследуемого объекта управления по экспериментально полученной его комплексной частотной характеристике.

Решение задачи нелинейного программирования, использующей все степени свободы выборки экспериментальных значений $\text{Re}e(\omega_v)$ и $\text{Im}e(\omega_v)$, дает оценки по методу наименьших квадратов параметров передаточной функции:

$$\left\{ \begin{aligned} \Phi(\vec{b}, \vec{a}, k, \tau) &= \sum_{v=1}^N (\text{Re}^e(\omega_v) - \text{Re}^{ap}(\omega_v))^2 + \\ + \sum_{v=1}^N (\text{Im}^e(\omega_v) - \text{Im}^{ap}(\omega_v))^2 &\rightarrow \min_{\vec{b}, \vec{a}, k, \tau} \end{aligned} \right\} \rightarrow \vec{b}^0, \vec{a}^0, k^0, \tau^0, \quad (1)$$

где k – коэффициент передачи объекта, τ – чистое запаздывание, \vec{b}, \vec{a} – другие параметры передаточной функции объекта, $\vec{b}^0, \vec{a}^0, k^0, \tau^0$ – оценки параметров передаточной функции объекта.

В приложении решение задачи (1) предусмотрено методом сканирования, методом Гаусса–Зейделя, симплекс-методом и методом наискорейшего спуска.

В разработанном приложении исследуемый канал передачи в общем виде описан как последовательное соединение аperiodического звена первого порядка с интегрирующим звеном и звеном запаздывания:

$$W_y(s) = k_y \frac{bs + 1}{a_2 s^2 + a_1 s + 1} e^{-s\tau}. \quad (2)$$

Исследуемый канал передачи может быть описан также, как канал «возмущающее воздействие – управляемая величина» регулируемого объекта с одноконтурной системой управления (рис. 1).

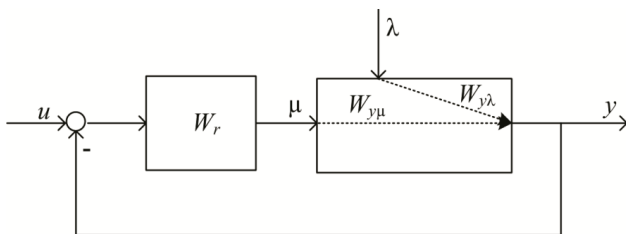


Рис. 1. Структура одноконтурной системы управления

Передаточную функцию канала «возмущающее воздействие – управляемая величина» системы управления можно представить в виде:

$$W_{y\lambda}^{sys}(s) = \frac{W_{y\lambda}(s)}{1 + W_{yu}(s)W_r(s)}, \quad (3)$$

где $W_{yu}(s)$ – передаточная функция технологического объекта по каналу «управляющее воздействие–управляемая величина», $W_r(s)$ – передаточная функция регулятора, $W_{y\lambda}(s)$ – передаточная функция технологического объекта по каналу «возмущающее воздействие – управляемая величина».

При подстановке передаточных функций регулятора и рассматриваемого объекта управления передаточная функция канала «возмущающее воздействие – управляемая величина» примет вид:

$$W_{y\lambda}^{sys}(s) = \frac{k_{y\lambda} \frac{b_\lambda s + 1}{a_{2\lambda} s^2 + a_{1\lambda} s + 1} e^{-s\tau_{y\lambda}}}{1 + k_{yu} \frac{b_\mu s + 1}{a_{2\mu} s^2 + a_{1\mu} s + 1} e^{-s\tau_{yu}} \left(k_r + \frac{k_r}{T_i s} + k_r T_d s \right)}.$$

Для тестирования разработанного программного приложения были получены данные с реального лабораторного объекта – эмулятора печи, схема которого представлена на рис. 2.

Эмулятор печи обдувается воздухом, который проходит через змеевик, помещенный на водяную баню и сужающее устройство. Температура печи регулируется изменением напряжения тока на нагревателе. Методом нейросетевого моделирования [2] получены экспериментальные комплексные частотные характеристики по каналам передачи «температура воздуха на обдув – температура печи» и «перепад давления на сужающем устройстве – температура печи».

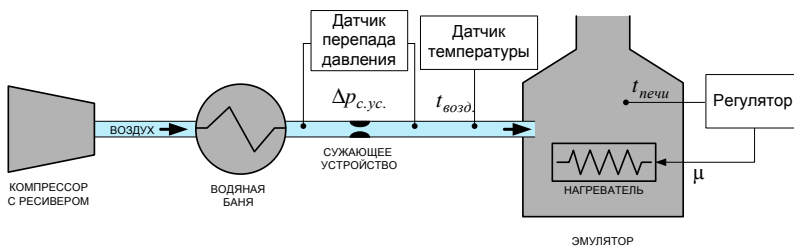


Рис. 2. Лабораторная установка

По полученным экспериментальным комплексным частотным характеристикам найдены параметры каналов передачи лабораторного объекта с использованием разработанного программного приложения методом сканирования, симплекс-методом и методом наискорейшего спуска. С целью оценки полученных результатов также найдены параметры каналов передачи методом последовательного квадратичного программирования (SQP) с помощью расширения MatLab – Optimization toolbox.

Результаты идентификации параметров передаточной функции объекта для комплексных частотных характеристик по каналам «перепад давления на сужающем устройстве – температура печи» и «температура воздуха на обдув – температура печи» представлены в табл. 1 и 2 соответственно.

Таблица 1

Результаты идентификации объекта по КЧХ канала «перепад давления на сужающем устройстве – температура печи»

КЧХ 1		Оптимизационные методы			
Канал	Параметр	Сканирование	Симплекс-метод	Метод наискорейшего спуска	SQP (MatLab)
Возмущения	кул	-0,14	-0,129	-0,132	-0,136
	аул	8	8,94	13,161	5,642
	тул	7	7,078	2,649	7,577
Управления	куц	0,12	0,111	0,111	0,11
	ауц	5	4,401	11,971	3,401
	туц	5	9,233	2,366	3,001

Результаты идентификации объекта по КЧХ канала
«температура воздуха на обдув – температура печи»

КЧХ 1		Оптимизационные методы			
Канал	Параметр	Сканирование	Симплекс-метод	Метод наискорейшего спуска	SQP (MatLab)
Возмущения	кул	0,44	0,405	0,397	0,426
	аул	14,5	11,532	13,896	15,792
	тул	4,5	5,207	5,468	2,689
Управления	кум	0,12	0,111	0,11	0,116
	аум	5	4,401	11,971	11,01
	тум	5	9,233	2,366	0

В графической среде моделирования Simulink составлены имитационные модели лабораторного объекта с параметрами, найденными программно реализованными методами оптимизации.

На рис. 3 представлена структура построенных моделей эмулятора печи.

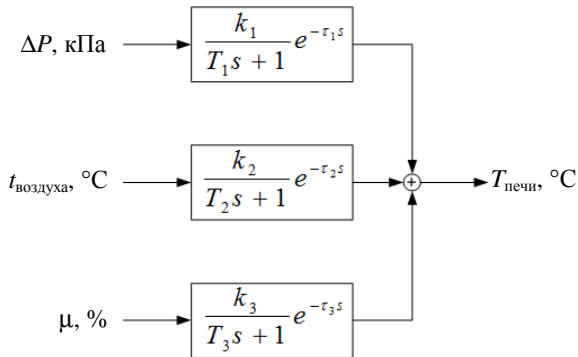


Рис. 3. Структура имитационной модели лабораторного объекта

Составленные имитационные модели были протестированы на данных, полученных экспериментально на лабораторном объекте. Входными сигналами являются изменения перепада давления на сужающем устройстве, температуры воздуха на обдув и напряжения тока на нагревателе. На выходе модели регистрируется изменение температуры печи. На рис. 4 представлены реальные значения температуры печи и значения температуры, полученные в имитационных

моделях, построенных по результатам идентификации объекта управления с помощью разработанного приложения методом сканирования, симплекс-методом и методом наискорейшего спуска, а также методом последовательного квадратичного программирования (SQP) в среде MatLab.

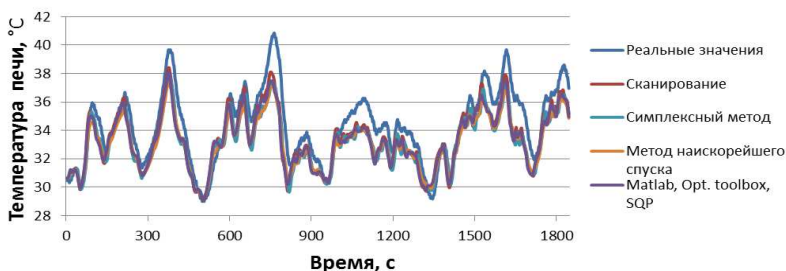


Рис. 4. Температура печи

Значение среднего квадратичного отклонения температуры печи, рассчитанной имитационной моделью, и ее реальное значение для имитационных моделей представлены в табл. 3.

Таблица 3

Среднее квадратичное отклонение температуры печи

Оптимизационный метод	Сканирование	Симплекс-метод	Метод наискорейшего спуска	SQP (MatLab)
СКО (σ), °C	1,341	1,464	1,443	1,497

Реализованные в приложении оптимизационные методы позволяют идентифицировать параметры эмулятора печи, по которым в виде её передаточных функций можно построить имитационную модель, выдающую значения температуры печи с СКО от её реальных значений, не превышающих 1,5 °C.

Библиографический список

1. Работников М.А., Бояршинова А.С., Шумихин А.Г. Автоматизация поиска значений параметров передаточной функции канала передачи по экспериментальной комплексной частотной характеристике // Вестник Пермского национального исследовательского поли-

технического университета. Химическая технология и биотехнология. – 2017. – № 2. – С. 63–76.

2. Шумихин А.Г., Бояршинова А.С. Идентификация сложного объекта управления по частотным характеристикам, полученным экспериментально на его нейросетевой динамической модели // Автоматика и телемеханика. – 2015. – № 4. – С. 125–134.

Сведения об авторах

Работников Михаил Алексеевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: rabotnikovma@gmail.com

Александрова Анна Сергеевна старший преподаватель Пермского национального исследовательского политехнического университета, Пермь, e-mail: boyarshinovaann@gmail.com

Шумихин Александр Георгиевич – доктор технических наук, профессор, заведующий кафедрой «Автоматизация технологических процессов» Пермского национального исследовательского политехнического университета, Пермь, e-mail: shumichin@gmail.com

About the authors

Rabotnikov Mikhail Alekseevich – Student Perm National Research Polytechnic University, Perm, e-mail: rabotnikovma@gmail.com

Aleksandrova Anna Sergeevna – Senior Lecturer Perm National Research Polytechnic University, Perm, e-mail: boyarshinovaann@gmail.com

Shumikhin Aleksandr Georgievich – Doctor of Technical Science, Professor, head of the ATP department Perm National Research Polytechnic University, Perm, e-mail: shumichin@gmail.com

СИСТЕМА УПРАВЛЕНИЯ ПРОЦЕССОМ ДОЗИРОВАНИЯ НА УСТАНОВКЕ КАРУСЕЛЬНОГО ТИПА

А.В. Сазонов, М.Б. Азимов, С.В. Захаркина, О.М. Власенко

Российский государственный университет
им. А.Н. Косыгина, Москва

В статье рассматривается система управления установкой дозирования, основанной на весовом методе и имеющей транспортирующее устройство карусельного типа. Приведен разработанный алгоритм работы программируемого логического контроллера (ПЛК) для реализации автоматического управления процессом дозирования.

Ключевые слова: система управления, система дозирования, поворотный столик, ПЛК, автоматическое управление, алгоритм работы.

CONTROL SYSTEM OF DOSAGE PROCESS AT THE CAROUSEL INSTALLATION

A.V. Sazonov, M.B. Azimov, S.V. Zakharkina, O.M. Vlasenok

Russian State University named after A.N. Kosygin, Moscow

The article includes a description of the control system of dosage process at the carousel installation. The machine uses the weight method of dosing. The algorithm for programmable logic controller (PLC) is given. It will allow realizing of automatic control of the dosing process.

Keywords: control system, dosing system, carousel installation, PLC, automatic control, algorithm.

Дозирование представляет собой операцию отмеривания выдачи порции вещества с использованием дозатора. Системы дозирования широко применяются в химической, пищевой и текстильной промышленности [1].

В данной работе описана разработанная установка для дозирования жидкости с карусельным транспортирующим механизмом. Жидкость наливается в исходный резервуар и в дальнейшем распределяется по нескольким емкостям небольшого объема, равномерно установленным на поворотном столике. Автоматическое дозирование осуществляется весовым методом с помощью датчика веса Scaime AAD-D. Функциональная схема, описывающая алгоритм работы установки, приведена на рис. 1.

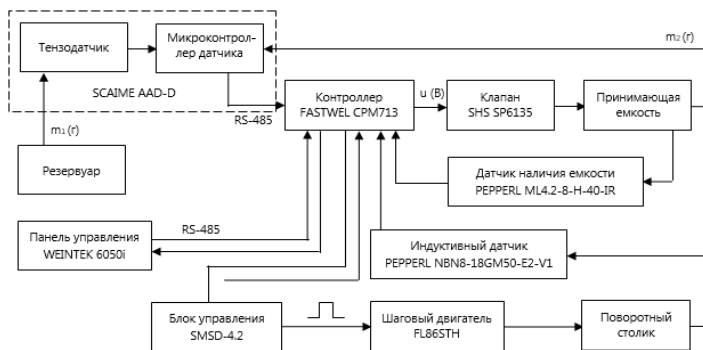


Рис. 1. Функциональная схема установки дозирования

В установку дозирования входят следующие устройства:

1. Одноточечный датчик тензометрического типа фирмы Scaime модели AAD-A, который можно разделить на 2 составляющие части: непосредственно сам тензометрический датчик веса и небольшой микроконтроллер, осуществляющий управление работой датчика [2]. Максимальный вес, который датчик способен измерить, – 5 килограмм. Датчик имеет четыре цифровых выхода, два цифровых входа и один разъем стандарта RS-485 для непосредственного управления процессом дозирования. Работа датчика происходит в режиме реального времени. Количество измерений, которые датчик способен производить, достигает восьмисот измерений в секунду, что позволяет произвести максимально точную дозировку.

2. Программируемый логический контроллер (ПЛК) модульного типа Fastwel CPM 713, который осуществляет управление всей работой системы дозирования [3]. Под управлением ПЛК на стенде находятся следующие модули:

- модуль дискретного ввода Fastwel DIM 717, на который поступают сигналы от оптического датчика и индуктивного датчика;
- модуль дискретного вывода Fastwel DIM 719, с помощью которого ПЛК осуществляет управление программируемым блоком шагового двигателя и электромагнитным дозирующим клапаном;
- интерфейсный модуль Fastwel NIM-741, предназначенный для получения и преобразования информации с сенсорной панели Weintek 6050i и датчика веса Scaime, поступающей в ПЛК посредством интерфейса RS-485;

– модуль ввода питания Fastwel OM-752, предназначен для подачи питания на ПЛК.

3. Электромагнитный клапан SP61355 компании «Приборы Урала», размещенный под исходным резервуаром. Это позволяет наливать жидкость под напором, создаваемым ее собственным весом. Дозирование происходит на основании непрерывно идущей с датчика веса информации, который находится под несущей резервуар частью каркаса. Тип клапана – нормально закрытый.

4. Принимающие емкости объемом 200 мл, расположенные на поворотном столике. Максимальное количество емкостей – семь штук.

5. Оптический датчик фирмы Pepperl+Fuchs модели ML4.2-8-N-40-IR для определения наличия принимающей емкости под клапаном дозирования.

6. Индуктивный датчик фирмы Pepperl+Fuchs модели NBN8-18GM50-E2-V1, установленный напротив ребра поворотного столика и предназначенный для нахождения меток на ребре столика. Эта функция была реализована для того, чтобы ПЛК смог определять, произошло вращение столика с принимающими емкостями или нет.

7. Сенсорная панель фирмы Weintek модели 6050i установлена на передней части стенда и предназначена для осуществления оператором контроля и управления работой стенда.

8. Шаговый двигатель отечественной фирмы «НПФ “Электропривод”» модели FL86STH, приводящий в движение карусельный механизм – столик с принимающими емкостями. Работа двигателя находится под управлением программируемого блока SMSD – 4.2 фирмы «НПФ Электропривод».

Блок-схема, описывающая алгоритм работы установки дозирования, приведена на рис. 2.

Предполагается, что перед началом работы установки исходный резервуар заполнен жидкостью. Вес жидкости $Y1$ измеряется тензодатчиком и поступает в программу контроллера. С панели управления оператор задает количество установленных в поворотном столике емкостей N (возможен вариант организации автоматического подсчета емкостей), а также максимальный объем емкости $Y2$.

Далее производится расчет необходимого объема жидкости $Y3$ для каждой принимающей емкости. Программа производит сравнение рассчитанного значения объема жидкости $Y3$ с заданным гранич-

ным значением $Y2$. Если $Y3$ больше $Y2$, на панель оператора выводится сообщение о необходимости установить еще одну принимающую емкость на столлик.

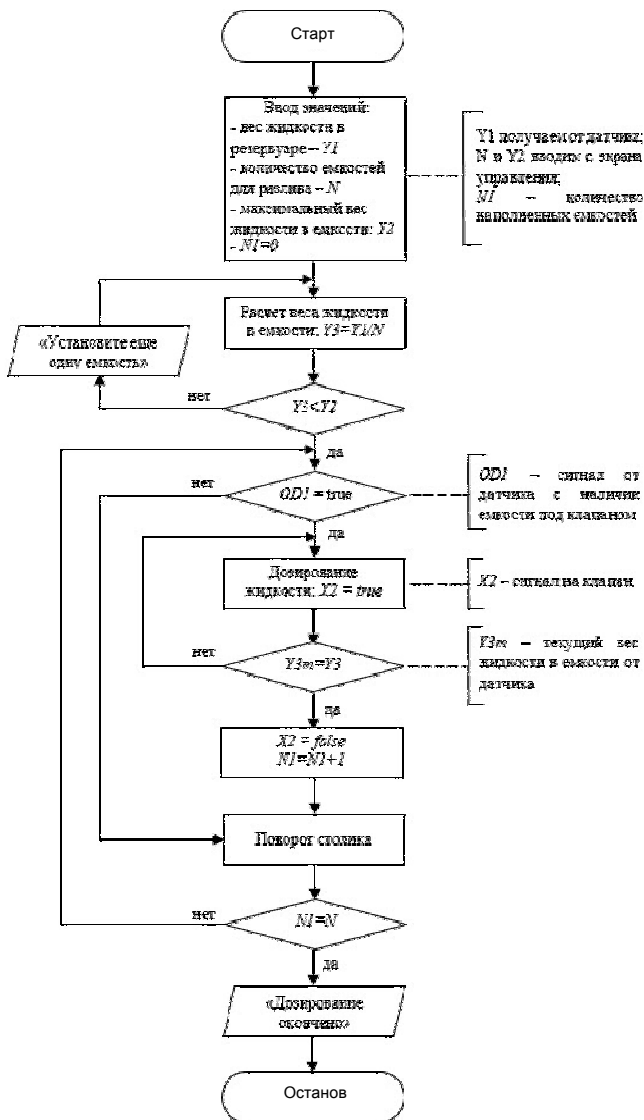


Рис. 2. Блок-схема алгоритма работы установки дозирования

При получении сигнала о наличии принимающей емкости под клапаном дозирования $ODI = true$ контроллер подает сигнал об открытии электромагнитного клапана $X2 = true$. Производится дозирование жидкости на основании данных от датчика веса $Y3m$. При достижении заданного веса $Y3m = Y3$ клапан подачи закрывается $X2 = false$ и подается сигнал на программируемый блок шагового двигателя $Ob1 = true$ о подаче напряжения на обмотки шагового двигателя; о поиске нулевой точки $Poisk0 = true$ и повороте столика $Step1 = true$ – подача импульсов от программируемого блока на шаговый двигатель. Датчик индуктивности подает сигнал $ID = true$ о нахождении следующей метки на поворотном столике.

Когда количество набранных емкостей $N1$ равно заданному значению установленных емкостей N , то выводится сообщение об окончании дозирования, и программа останавливается.

По разработанному алгоритму будет разработан код в программе CoDeSys, по которому ПЛК Fastwel будет осуществлять автоматическое управление установкой.

Библиографический список

1. Безменов В.С., Ефремов В.А., Руднев В.В. Автоматизация процессов дозирования жидкостей в условиях малых производств. – М.: URSS, 2010. – 216 с.

2. SCAIME AAD-D/ AXD-D. Digital dosing load-cell. User's Instructions. NU-AXD-D-E-0213_195702-C. Technosite Altea. Juvigny. – France, 2016. – 30 с.

3. Программируемый блок управления шаговыми двигателями SMSD-4.2. Паспорт SMSD.42.001.ПС / НПФ «Электропривод». – СПб., 2011. – 6 с. – URL: <http://electroprivod.ru/pdf/smsd-42-pasp.pdf>

Сведения об авторах

Сазонов Алексей Васильевич – студент Российского государственного университета им. А.Н. Косыгина, Москва, e-mail: h3c32x@yandex.ru

Азимов Мухаммаджон Боротович – студент Российского государственного университета им. А.Н. Косыгина, Москва, e-mail: azimovmb@gmail.com

Захаркина Светлана Валерьевна – кандидат технических наук, доцент Российского государственного университета им. А.Н. Косыгина, Москва, e-mail: kruglovas@mail.ru

Власенко Ольга Михайловна – кандидат технических наук, доцент Российского государственного университета им. А.Н. Косыгина, Москва, e-mail: o.m.vlasenko@gmail.com

About the authors

Sazonov Aleksey Vasilievich – Student Russian State University named after A.N. Kosygin, Moscow, e-mail: xhc32x@yandex.ru

Azimov Muhammadjon Borotovich – Student Russian State University named after A.N. Kosygin, Moscow, e-mail: azimovmb@gmail.com

Zakharkina Svetlana Valerievna – Ph.D. in Technical Sciences, Associate Professor Russian State University named after A.N. Kosygin, Moscow, e-mail: kruglovas@mail.ru

Vlasenko Olga Mikhailovna – Ph.D. in Technical Sciences, Associate Professor Russian State University named after A.N. Kosygin, Moscow, e-mail: o.m.vlasenko@gmail.com

РЕАЛИЗАЦИЯ ПРОЦЕССА СБОРКИ ПАКЕТА OPENSCADA НА ОСНОВЕ МОДИФИЦИРОВАННЫХ ИСХОДНЫХ ТЕКСТОВ

М.А. Чудинов

Пермский национальный исследовательский
политехнический университет, Пермь

Рассмотрены особенности процесса сборки пакета OpenSCADA на основе модифицированных исходных текстов – предварительная настройка системы Ubuntu, а также удовлетворение зависимостей проекта OpenSCADA. Проведена проверка функционирования системы после сборки.

Ключевые слова: SCADA-система, OpenSCADA, Ubuntu, Debian-пакет, пользовательский графический интерфейс.

IMPLEMENTATION OF BUILD PROCESS OF OPEN SOURCE SCADA SYSTEM OPENSCADA BASED ON THE MODIFIED SOURCES

M.A. Chudinov

Perm National Research Polytechnic University, Perm

The article gives some information about features of build process of open source SCADA-system OpenSCADA based on the modified sources – description of the opened SCADA-system OpenSCADA. The article describes pre-configure of OpenSCADA and Ubuntu, and testing of built system.

Keywords: SCADA-system, OpenSCADA, Ubuntu, Debian-package, graphical user interface.

SCADA-пакеты (или SCADA-системы) являются одним из инструментальных средств разработки программного обеспечения при проектировании систем автоматизации и управления (САиУ) [1].

Система OpenSCADA предназначена для сбора, архивирования, визуализации информации, выдачи управляющих воздействий, а также других родственных операций, характерных для полнофункциональной SCADA-системы [2].

Для установки системы предусмотрена как стандартная установка программы (загрузка и установка методом стандартной процедуры при помощи команды «sudo apt-get install»), так и сборка из исходных текстов, последовательность которой будет приведена далее.

Для сборки OpenSCADA из исходных текстов требуются опыт сборки свободного ПО, а также базовые знания в ОС Linux и исполь-

зуемого дистрибутива Linux, что позволит корректно удовлетворять зависимости и решать возможные проблемы сборки [3].

Предварительная настройка системы Ubuntu. Дистрибутивы, основанные на Debian, – это не только отличная система управления пакетами APT, которая сама разрешает зависимости, но и удобные инструменты для создания пакетов и своих репозиториев [4].

Для сборки Deb-пакетов OpenSCADA вам понадобятся архивы исходных текстов и ресурсов, которые можно загрузить с ftp или http-сервера проекта.

Сборка Deb-пакетов производится в директории "debian" со скриптами сборки, которая содержится в архивах исходных текстов OpenSCADA.

Для начала необходимо создать директорию для сборки проекта. В системе Ubuntu запустим «Терминал» (Ctrl + Alt + T) и пропишем туда следующие команды `mkdir ~/build; cd ~/build`

Далее, находясь в директории build, проводим загрузку и распаковку пакета с исходными текстами.

```
wget ftp://ftp.oscada.org/OpenSCADA/0.8.17/openscada-0.8.17.tar.lzma
wget ftp://ftp.oscada.org/OpenSCADA/0.8.17/openscada-res-0.8.17.tar.lzma
tar --lzma -xvf openscada-0.8.17.tar.lzma
```

В качестве типа сборки выберем бинарные файлы в одном пакете:
\$ `ln -s openscada-0.8.0/data/debian openscada-0.8.17/debian`

Система OpenSCADA, как и любое другое программное обеспечение, имеет свои аппаратные и программные требования для сборки ядра OpenSCADA и её модулей.

Удовлетворение зависимостей проекта OpenSCADA для сборки. Проверка на наличие необходимых пакетов для сборки OpenSCADA проводится при помощи запуска скрипта `./configure` в директории с распакованными исходниками: `~/build/openscada-0.8.17$./configure`

Удовлетворение зависимостей ядра системы OpenSCADA представляет собой стандартный набор библиотек, обычно уже доступных в установленном дистрибутиве Ubuntu. Проверка на установление зависимостей ядра представлена на рис. 1.

Когда все библиотеки, необходимые для работы системы OpenSCADA, установлены выводятся сводные данные об установленном необходимом ПО в системе, как показано на рис. 2.

```

===== Core libraries check =====
checking for stdlib.h... (cached) yes
checking for GNU libc compatible malloc... yes
checking for stdlib.h... (cached) yes
checking for GNU libc compatible realloc... yes
checking for sin in -lm... yes
configure: LibM: Pass global library using
checking for dlopen in -ldl... (cached) yes
configure: LibDL: Pass global library using
checking for crypt in -lcrypt... yes
configure: LibCrypt: Pass global library using
checking for deflate in -lz... yes
configure: LibZ: Pass global library using
checking pcre.h usability... yes
checking pcre.h presence... yes
checking for pcre.h... yes
checking for pcre_compile in -lpcre... yes
configure: PCRE: Pass global library using

```

Рис. 1. Зависимости ядра системы OpenSCADA

```

- Enable(yes)/disable(no) all modules = individual
- Crosscompile build = no
- Core lib build only static = no
* Generic features:
- Strings charset encode support (by iconv) = yes
- Interfaces internationalisation (I18N) support (by LibIntl) = yes
- Graphical library (LibGD2) use by core = no
- Subsystem modules build:
  "DB": DBF MySQL SQLite FireBird PostgreSQL
  "DAQ": System BlockCalc JavaLikeCalc LogicLev SNMP Siemens
ModBus DCON DAQGate SoundCard OPC-UA
  "Archive": FSArch DBArch
  "Transport": Sockets SSL Serial
  "Transport's protocol": HTTP SelfSystem UserProtocol
  "UI": VCAEngine Vision QTstarter QTCfg WebCfg WebCfgD WebC
ision WebUser
  "Special": SystemTests FLibComplex1 FLibMath FLibSYS
- Modules included to OpenSCADA core:
* Modules' features:
- FFTW3 for signal spectrum purchase: -lfftw3
- Linux sensors library use: -lsensors
- Media play engine: -lphonon -lQtGui -lQtDBus -lQtXml -lQtCo
re
admin1@admin1-VirtualBox:~/build/openscada-0.8.175

```

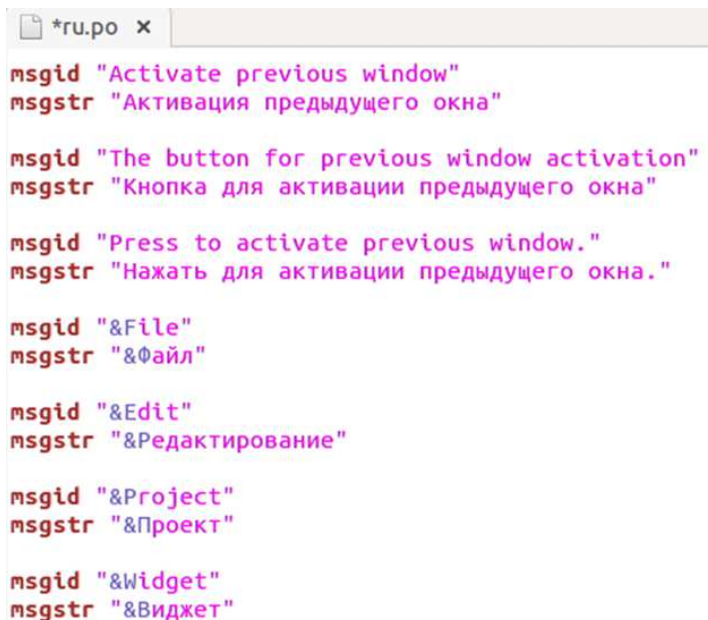
Рис. 2. Завершенная проверка на удовлетворение зависимостей проекта OpenSCADA

Далее совершим переход в директорию OpenSCADA и перейдем к модификации исходного кода.

Пример модификации исходного текста системы OpenSCADA. Проект OpenSCADA развивается уже достаточно дол-

гое время, имеет обширный круг пользователей. Системой предусмотрено переход на другие иностранные языки: английский, немецкий, русский, украинский.

Рассмотрим пример модификации исходных файлов локализации OpenSCADA. Для реализации данной задачи перейдем в директорию с файлами локализации {user}/build/openscada-0.8.17/src/moduls/ui/Vision/po и в файл ru.po. Как видно на рис. 3, файл содержит перевод пунктов меню с английского на русский язык.



```
*ru.po x
msgid "Activate previous window"
msgstr "Активация предыдущего окна"

msgid "The button for previous window activation"
msgstr "Кнопка для активации предыдущего окна"

msgid "Press to activate previous window."
msgstr "Нажать для активации предыдущего окна."

msgid "&File"
msgstr "&Файл"

msgid "&Edit"
msgstr "&Редактирование"

msgid "&Project"
msgstr "&Проект"

msgid "&Widget"
msgstr "&Виджет"
```

Рис. 3. Файл локализации ru.po

Необходимо внести изменения в файл. Поменяем слово «Файл» на слово «Проверка», и, если установка OpenSCADA из исходных текстов будет проведена должным образом, первый пункт меню будет обозначен словом «Проверка».

Приступим к процессу сборки OpenSCADA. Находясь в директории с исходными текстами OpenSCADA, при помощи команды `sudo checkinstall -D` создадим deb-пакет, использующийся в дистрибутивах, основанных на Debian, таких как используемая нами Ubuntu. Процесс создания deb-пакета представлен на рис. 4.

```
Устанавливается Debian-пакет...OK
Удаляются временные файлы...OK
Записывается пакет с резервной копией...OK
OK
Удаляется временный каталог...OK

*****

Done. The new package has been installed and saved to
/home/admin1/build/openscada-0.8.17/openscada_0.8.17-1_i386.deb
You can remove it from your system anytime using:

    dpkg -r openscada

*****

admin1@admin1-VirtualBox:~/build/openscada-0.8.17$ █
```

Рис. 4. Сборка установочного deb-пакета системы OpenSCADA

Теперь можно произвести установку данного deb-пакета, например, при помощи команды `sudo dpkg -i openscada_0.8.17-1_i386.deb`

После завершения установки запустим OpenSCADA, и, как видно на рис 5, название пункта меню «Файл» заменилось на слово «Проверка». Это также говорит нам о том, что сборка была проведена должным образом.

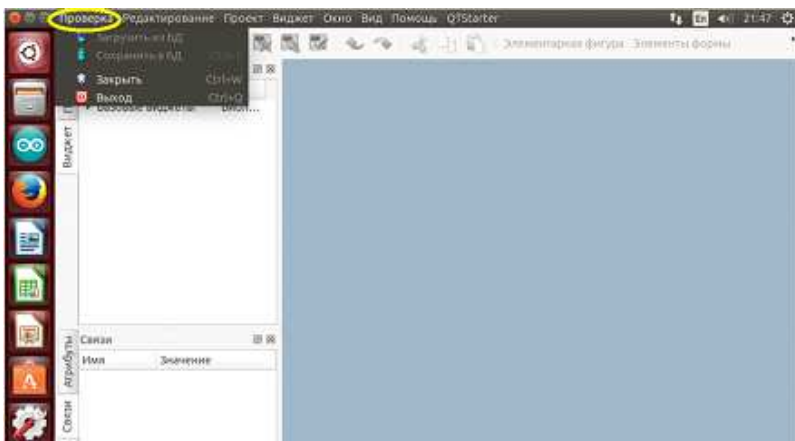


Рис. 5. Модифицированный вариант системы OpenSCADA

Заключение. В данной работе на примере были рассмотрены особенности процесса сборки и модификации пакета OpenSCADA на основе исходных текстов – проведена предварительная настройка системы Ubuntu, а также удовлетворены зависимости проекта OpenSCADA. В рамках данной работы была рассмотрена сборка из Debian-based дистрибутивов (deb-пакетов). Результаты, представленные на рис. 5, означают, что сборка была проведена правильно.

Модификация на уровне исходных текстов является большим преимуществом для данного SCADA-пакета, поскольку имеется возможность дополнить его в соответствии с потребностями разработки.

Библиографический список

1. Кавалеров М.В. К вопросу о термине «SCADA-система» // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2011. – № 5. – С. 205–209.

2. Савоченко Р.А. О проекте OpenSCADA [Электронный ресурс]. – URL: <http://oscada.org/ru/glavnaja/o-proekte/> (дата обращения: 02.11.2017).

3. Савоченко Р.А. Сборка OpenSCADA из исходных текстов [Электронный ресурс]. – URL: <http://wiki.oscada.org/Doc/SborkaIzIsxodnikov> (дата обращения: 05.11.2017).

4. Сборка пакетов. Русскоязычная документация по Ubuntu [Электронный ресурс] – URL: http://help.ubuntu.ru/wiki/сборка_пакетов (дата обращения: 05.11.2017).

Сведения об авторе

Чудинов Максим Андреевич – аспирант Пермского национального исследовательского политехнического университета, Пермь, e-mail: m-chudinov@list.ru

About the author

Chudinov Maksim Andreevich – Graduate Student Perm National Research Polytechnic University, e-mail: m-chudinov@list.ru

МОДИФИКАЦИЯ ИСХОДНЫХ ТЕКСТОВ ПАКЕТА OPENSCADA ДЛЯ РЕШЕНИЯ ЗАДАЧИ ВЗАИМОДЕЙСТВИЯ С МИКРОКОНТРОЛЛЕРОМ ARDUINO

М.А. Чудинов

Пермский национальный исследовательский
политехнический университет, Пермь

В статье рассмотрены особенности интеграции дополнительного модуля в систему OpenSCADA для реализации взаимодействия с микроконтроллером Arduino, а также особенности функционирования разработанного модуля под названием «Arduino client» на конкретном примере.

Ключевые слова: SCADA-система; OpenSCADA; Arduino; микроконтроллер.

MODIFICATION OF OPEN SOURCE SCADA SYSTEM OPENSCADA SOURCES TO SOLVE TASK OF INTERACTION WITH MICROCONTROLLER ARDUINO

M.A. Chudinov

Perm National Research Polytechnic University, Perm

The article gives some information about features of special module (called "Arduino client") integration to the OpenSCADA system to interact with microcontroller Arduino, and also features of its functioning as an example.

Keywords: SCADA-system; OpenSCADA; Arduino; microcontroller.

В процессе функционирования программного обеспечения возможно обнаружение ошибок в программах, и появляется необходимость их модификации и расширения функций [2].

Эти доработки, как правило, ведутся одновременно с эксплуатацией текущей версии программного изделия. После проверки подготовленных корректировок на одном из экземпляров программ очередная версия программного изделия заменяет ранее эксплуатировавшиеся или некоторые из них.

Современные SCADA-системы [3] не ограничивают выбора аппаратуры нижнего уровня (контроллеров), так как предоставляют большой набор драйверов или серверов ввода/вывода и имеют хорошо развитые средства создания собственных программных модулей или драйверов новых устройств нижнего уровня [4].

Общие рекомендации при модификации программного обеспечения для решения поставленной задачи

Встраиваемые разработчиками OpenSCADA модули подсистемы, к примеру для реализации взаимодействия по различным протоколам, в плане подключения к определенным моделям контроллеров носят универсальный, но, как правило, избыточный характер. Некоторые функции, задаваемые в исходном тексте данных модулей, могут вносить дополнительную, лишнюю нагрузку на вычислительную способность исполняющего устройства. С этой целью, обладая информацией о наилучшем, по мнению разработчика, методе взаимодействия, появляется возможность создания и интеграции модулей в дерево исходных текстов проекта OpenSCADA или как независимо проекта внешнего модуля к OpenSCADA.

Поскольку модуль не должен противоречить духу открытого проекта и лицензии, на основе которой разрабатывается и распространяется OpenSCADA, то лицензией нового модуля очевидно должна быть одна из свободных лицензий.

Продукты семейства Arduino могут использовать как любители, увлекающиеся компьютерной микроэлектроникой, так и профессионалы, разрабатывающие самые различные приборы с целью их промышленного применения. Наличие всей необходимой документации и ее свободная лицензия позволяют не только самостоятельно собирать Arduino из общедоступных компонентов, но и использовать его в качестве базы в собственных проектах [1].

Особенности интеграции разрабатываемого модуля в систему OpenSCADA для взаимодействия с микроконтроллером Arduino. В качестве основы для разработки используются шаблон модуля сбора данных «=TmpI=», а также опыт реализации взаимодействия по протоколу DCON.

В целом процедура создания нового модуля с включением в дерево исходных текстов на основе шаблона включает в себя шаги:

1. Получение дерева исходных текстов проекта OpenSCADA, к примеру, путем ввода в «Терминал» таких команд:

```
wget ftp://ftp.oscada.org/OpenSCADA/0.8.0/opencada-0.8.17.tar.lzma
wget ftp://ftp.oscada.org/OpenSCADA/0.8.0/opencada-res-0.8.17.tar.lzma
tar --lzma -xvf opencada-0.8.17.tar.lzma
cd opencada-0.8.17
```

2. Копирование директории шаблона с именем нового модуля "Arduino" (для подсистемы «Сбор данных»):

```
cd OpenSCADA/src/moduls/daq
cp -r =Tmpl= Arduino; cd Arduino
```

3. Редактирование файла "module.cpp". Изменить имена функций включения модуля согласно имени нового модуля:

```
"TModule::Sat daq_Tmpl_module( int n_mod )" ->
daq_Arduino_module
"TModule *daq_Tmpl_attach( const TModule::SAT
&AtMod, const string &source )" -
daq_Arduino_attach
```

4. Информация о модуле в файле «module.cpp», а именно участок:

```
/* *****
/* Modul info! *
#define MOD_ID           " Arduino client"
#define MOD_NAME         _("DAQ Arduino ")
#define MOD_TYPE         SDB_ID
#define VER_TYPE         SDB_VER
#define MOD_VER          "0.0.1"
#define AUTHORS          _("Name Surname")
#define DESCRIPTION      _("DAQ Arduino")
#define MOD_LICENSE      "GPL2"
```

5. Редактирование конфигурации сборки модуля в файле "Makefile.am" к такому виду:

```
EXTRA_DIST = *.h po/*
if ArduinoIncl
noinst_LTLIBRARIES = daq_Arduino_la
daq_Arduino_la_CXXFLAGS = -DMOD_INCL -fpic
daq_Arduino_la_LIBTOOLFLAGS = --tag=disable-
shared
daq_Arduino_la_LDFLAGS = -module
else
oscd_modul_LTLIBRARIES = daq_Arduino_la
daq_Arduino_la_CXXFLAGS =
daq_Arduino_la_LIBTOOLFLAGS = --tag=disable-
static
daq_Arduino_la_LDFLAGS = -module -avoid-
version $(top_builddir)/src/liboscada_la
```

```
endif

daq_Arduino_la_CXXFLAGS += $(Arduino_CFLAGS)
daq_Arduino_la_LDFLAGS += $(Arduino_LDLFLAGS)
daq_Arduino_la_SOURCES = module.cpp

I18N_mod = $(oscd_modulpref)Arduino
include ../../../../I18N.mk
```

6. Добавление записи нового модуля в конец секции подсистемы, конфигурационного файла (OpenSCADA/configure.ac) сборочной системы OpenSCADA:

```
AX_MOD_DAQ_EN(Arduino, [disable or enable[=incl] build module DAQ.Arduino], disable, incl,
[
    # Код проверки внешних библиотек модуля
])
```

7. Теперь новый модуль можно собрать в составе OpenSCADA после реформирования сборочной системы при помощи команд в «Терминале», находясь при этом в директории OpenSCADA (по умолчанию build/openscada-0.8.17/):

```
autoreconf -if
./configure --enable-Arduino
```

8. При помощи команды `sudo checkinstall -D` создадим deb-пакет.

9. Проведем установку `sudo dpkg -i openscada_0.8.17-1_i386.deb`

10. Осуществим запуск системы OpenSCADA. Как видно на рис. 1, также был произведен запуск встраиваемого нами модуля Arduino, что говорит о правильности выполнения необходимых действий.

Также еще одним фактом того, что сборка была проведена верно, говорит появление модуля «Arduino client» среди модулей сбора данных, как показано на рис. 2.

Особенности функционирования разработанного модуля на примере взаимодействия с микроконтроллером Arduino. В качестве примера взаимодействия настроим включение/отключение диода на Arduino путем нажатия кнопки в проекте OpenSCADA.

Включение светодиода будет осуществляться в зависимости от значения I/O в отправляемой от OpenSCADA строке.

```

admin1@admin1-VirtualBox: ~
2017-06-05T09:37:24 0[/WorkStation/sub_BD/mod_PostgreSQL/] Включение модуля.
2017-06-05T09:37:24 1[/WorkStation/sub_UI/] Work station > Интерфейсы Пользовате
ля: Подключение модуля 'WebCfg'!
2017-06-05T09:37:24 0[/WorkStation/sub_UI/mod_WebCfg/] Включение модуля.
2017-06-05T09:37:24 1[/WorkStation/sub_Protocol/] Work station > Транспортные Пр
отоколы: Подключение модуля 'UserProtocol'!
2017-06-05T09:37:24 0[/WorkStation/sub_Protocol/mod_UserProtocol/] Включение мод
уля.
2017-06-05T09:37:24 1[/WorkStation/sub_Special/] Work station > Специальные: Под
ключение модуля 'FLibSYS'!
2017-06-05T09:37:24 0[/WorkStation/sub_Special/mod_FLibSYS/] Включение модуля.
2017-06-05T09:37:24 1[/WorkStation/sub_Transport/] Work station > Транспорты: По
дключение модуля 'Sockets'!
2017-06-05T09:37:24 0[/WorkStation/sub_Transport/mod_Sockets/] Включение модуля.
2017-06-05T09:37:24 1[/WorkStation/sub_Protocol/] Work station > Транспортные Пр
отоколы: Подключение модуля 'HTTP'!
2017-06-05T09:37:24 0[/WorkStation/sub_Protocol/mod_HTTP/] Включение модуля.
2017-06-05T09:37:24 1[/WorkStation/sub_DAQ/] Work station > Сбор Данных: Подключ
ение модуля 'LogicLev'!
2017-06-05T09:37:24 0[/WorkStation/sub_DAQ/mod_LogicLev/] Включение модуля.
2017-06-05T09:37:24 1[/WorkStation/sub_DAQ/] Work station > Сбор Данных: Подключ
ение модуля 'Arduino'!
2017-06-05T09:37:24 0[/WorkStation/sub_DAQ/mod_Arduino/] Включение модуля.
2017-06-05T09:37:24 1[/WorkStation/sub_DAQ/] Work station > Сбор Данных: Подключ
ение модуля 'DCON'!

```

Рис. 1. Подключение модуля «Arduino»

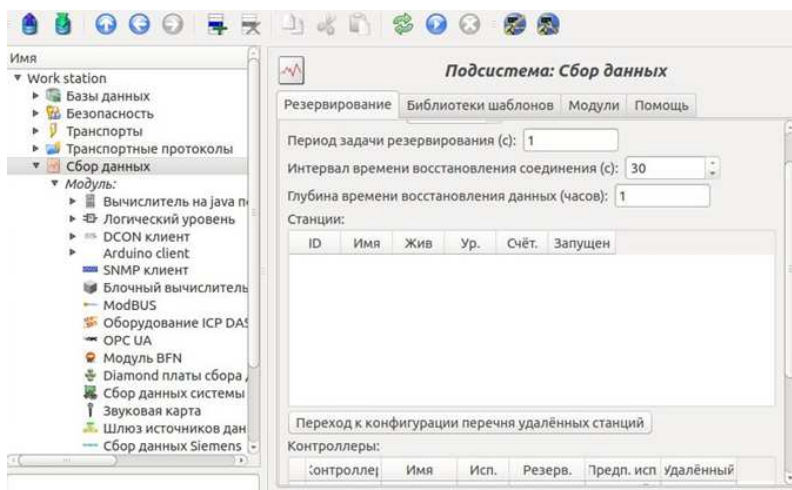


Рис. 2. Встроенный модуль «Arduino client»

В модуле Arduino для проверки модифицированного пакета OpenSCADA и проверки последующего взаимодействия с микроконтроллером Arduino используется только метод записи дискретных выходов (DO).

Теперь с данной командой в разработанном интерфейсе OpenSCADA нужно связать кнопку.

Перейдем к созданному для мнемосхемы логическому контроллеру, перейдем во вкладку «Параметры» и выберем созданный нами ранее параметр. Во вкладке «Конфигурация шаблона» находим переменную DO0. Теперь необходимо установить связь с переменными модуля Arduino. Таким образом, установленная связь для переменной DO: Arduino.название_контроллера.название_параметра.DO.

Если все сделано должным образом, то во вкладке параметра «Конфигурация шаблона» правильно установленная связь будет обозначена символом «(+)», как показано на рис. 3.



Рис. 3. Конфигурация параметра

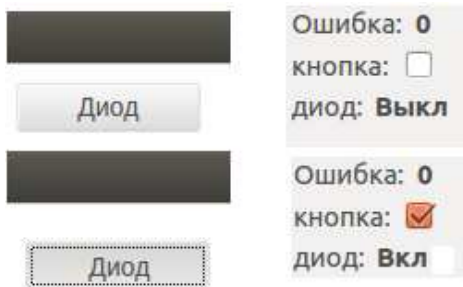


Рис. 4. Формирование команды «Включить диод»

При запуске проекта и нажатии кнопки включения диода в окне созданного модуля Arduino будет осуществляться передача параметра, что при правильной настройке модуля означает передачу команды на Arduino (рис. 4).

Заключение. В результате проделанной работы был разработан модуль «Arduino client» для взаимодействия с микроконтроллером Arduino, рассмотрены особенности его интеграции в систему OpenSCADA, а также особенности функционирования разработанного модуля на конкретном примере. Выполнив данную задачу, мы удостоверились в том, что с помощью разработанного модуля «Arduino client» можно настроить связь между микроконтроллером Arduino и OpenSCADA.

Библиографический список

1. Arduino приходит в Россию [Электронный ресурс]. – URL: <http://www.abber.org/arduino-prixodit-v-rossiyu> (дата обращения: 04.11.2017).
2. Жизненный цикл программного обеспечения [Электронный ресурс]. – URL: http://www.tehprog.ru/index.php_page=lecture15.html (дата обращения: 05.11.2017).
3. Кавалеров М.В. К вопросу о термине «SCADA-система» // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2011. – № 5. – С. 205–209.
4. Организация взаимодействия с контроллерами [Электронный ресурс]. – URL: <http://asutp.ru/?p=600462> (дата обращения: 02.11.2017).

Сведения об авторе

Чудинов Максим Андреевич – аспирант Пермского национального исследовательского политехнического университета, Пермь, e-mail: m-chudinov@list.ru

About the author

Chudinov Maksim Andreevich – Graduate Student Perm National Research Polytechnic University, e-mail: m-chudinov@list.ru

РАЗРАБОТКА АЛГОРИТМА УПРАВЛЕНИЯ НАПОРНОЙ СИСТЕМОЙ ВОДОПОДАЧИ С НАСОСНОЙ СТАНЦИЕЙ ВТОРОГО ПОДЪЕМА

Н.С. Шаров, В.В. Тугов

Оренбургский государственный университет, Оренбург

В данной статье рассмотрена проблема энергетической эффективности использования насосного оборудования и систем водоснабжения. Проанализированы существующие методы управления насосными станциями второго подъема. Выявлена и обоснована необходимость разработки алгоритма управления напорной системой водоподачи. На основе проведенного исследования автором представлены блок-схема разработанного алгоритма управления и его подробное описание.

Ключевые слова: энергетическая эффективность, алгоритм управления, КПД насосных систем, напорная система водоподачи, насосные станции второго подъема.

DEVELOPMENT OF THE CONTROL ALGORITHM FOR THE PRESSURE WATER SUPPLY SYSTEM WITH THE PUMP STATION OF THE SECOND LIFT

N.S. Sharov, V.V. Tugov

Orenburg State University, Orenburg

In this article the problem of energy efficiency of using pumping equipment and water supply systems is considered. The existing methods of controlling the pumping stations of the second ascent are analyzed. The necessity of developing an algorithm for controlling the pressure water supply system has been identified and justified. Based on the study, the author presents a block diagram of the developed control algorithm and its detailed description.

Keywords: energy efficiency, control algorithm, efficiency of pumping systems, pressurized water supply system, pumping stations of the second lifting.

На насосное оборудование по разным оценкам приходится до 25 % мирового потребления всей вырабатываемой электроэнергии. До 85 % затрат на эксплуатацию насосов составляют затраты на электроэнергию. Исследования показывают, что в среднем КПД насосных систем составляет 40 %, а 10 % насосов работают с КПД ниже 10 % [4].

Экономическая эффективность водопроводно-канализационного хозяйства в большой степени связана с эксплуатацией насосного оборудования, поэтому для организаций ЖКХ снижение энергопотребления

является приоритетной задачей. Основными источниками энергопотребления (более 90 %) в системах водоснабжения населенных мест и производственных объектов составляют насосные системы. В связи с растущими ценами на электричество, газ и нефть остро встают вопросы повышения энергетической эффективности систем водоснабжения, а также их элементов.

Водоснабжение представляет собой комплекс мероприятий по обеспечению водой различных ее потребителей. Системой водоснабжения называется комплекс сооружений, осуществляющих задачи водоснабжения, т.е. получение воды из природных источников, ее очистку, транспортирование и подачу потребителям.

В состав системы водоснабжения обычно входят следующие сооружения:

- водоприемные сооружения, осуществляющие прием воды из природных источников;
- водоподъемные сооружения, т.е. насосные станции, подающие воду к местам ее очистки, хранения или потребления;
- сооружения для очистки воды;
- водоводы и водопроводные сети (насосные станции 2-го подъема), служащие для транспортирования и подачи воды к местам ее потребления;
- башни и резервуары, являющиеся регулирующими и запасными емкостями в системе водоснабжения.

Режим расходования воды потребителями является основным фактором, определяющим режим работы всех элементов системы водоснабжения. В основу расчета водопроводных сетей и сооружений кладутся принятые графики режима водопотребления, которые определяют в значительной степени стоимость системы и расходы на ее эксплуатацию [1].

В рамках данного исследования рассматривается напорная система водоподачи с насосной станцией 2-го подъема, при этом учитывается подача воды только на хозяйственно-питьевые нужды.

График работы напорной системы водоподачи определяется режимом водопотребления, который изменяется в течение суток. Обычно график подачи насосной станции не совпадает в точности с графиком водопотребления, поэтому предусматриваются регулирующие емкости: водонапорные башни, напорные баки. При этом за счет приближения графика подачи к графику водопотребления обес-

печивается их минимальная вместимость. Поэтому обычно назначают 2 – 3-ступенчатый график подачи.

Уменьшение ступеней графика водоподачи, как правило, приводит к увеличению объема резервуара воды, что приводит к росту его стоимости. Увеличение ступеней графика водоподачи и приближение его к графику водопотребления требуют установления большего количества насосных агрегатов, что увеличивает стоимость как самой насосной станции, так и стоимость ее эксплуатации. Поэтому основной задачей системы управления здесь является увеличение ступеней графика водоподачи для снижения стоимости резервуара, при этом без увеличения количества насосных агрегатов в напорной системе.

Одним из основных требований к системе управления напорной системой водоподачи с насосной станцией второго подъема является требование поддержания КПД насосных агрегатов на высоком уровне. Целью управления в этом случае является оптимальный запуск насосных агрегатов с использованием допустимой мощности одного перед запуском другого насосного агрегата.

При помощи теории массового обслуживания (ТМО) возможно построение точных графиков водопотребления, на основании которых работает алгоритм управления напорной системой водоподачи с насосной станцией 2-го подъема. Исследование по применению ТМО для напорной системы водоподачи было рассмотрено в другой публикации автора [4].

Работа алгоритма управления начинается с формирования графика водопотребления, который описывается входящим потоком заявок системы массового обслуживания (СМО). Здесь это марковский поток, где $\nu(t)$ – число заявок, поступивших в интервале времени $[0, \infty)$, а $\tau_1, \tau_k, \dots, \tau_k, \dots, \tau_1 \geq 0$ – моменты их поступления. Таким образом, формируется график водоподачи [2].

Расчет характеристик ожидаемого потока заявок на обслуживание и закономерностей взаимодействия системы с обслуживающим потоком необходим для оценки требуемых характеристик быстрого действия системы обслуживания. В связи с этим рассмотрены закономерности и факторы взаимодействия потока заявок на обслуживание λ и системы со средней интенсивностью μ потока обслуживания заявок. Рассмотрим эксплуатационные свойства СМО, обозначив через $\alpha = \lambda/\mu$ относительную интенсивность исходного потока заявок по отношению к интенсивности потока обслуживания.

Интенсивность исходного потока заявок

$$\lambda_c = \frac{1}{\tau_c}, \quad (1)$$

где τ_c – среднее время между моментами поступления заявок на обслуживание.

Потенциальная интенсивность потока обслуживания заявок

$$\mu_{об} = \frac{1}{\tau_{об}}, \quad (2)$$

где $\tau_{об}$ – среднее время обслуживания одной заявки системой обслуживания.

Взаимодействие одноканальной системы обслуживания с потенциальной интенсивностью $\mu_{об}$ потока обслуживания и потока заявок с интенсивностью λ_c заключается в том, что при поступлении каждой заявки на обслуживание через интервал времени τ_c начинается ее обработка в течение времени $\tau_{об}$, где среднее время совместной занятости системы обслуживания потока заявок составит $\tau_c + \tau_{об}$. Это значит, что в целом СМО работает с интенсивностью $\lambda_{смо} = 1 / \tau_c + \tau_{об}$ [3].

Для обеспечения надежности системы проводится оценка наработки насосных агрегатов (НА). Первоочередным насосом для запуска выбирается НА с наименьшим показателем наработки.

КПД насосных агрегатов определяется по следующей формуле:

$$\eta = S \cdot H \cdot \rho / 3670 \cdot P, \quad (3)$$

где S – водоподача; H – напор; ρ – плотность жидкости; 3670 – постоянный коэффициент; P – мощность насоса.

Графическое представление разработанного алгоритма управления напорной системой водоподачи с насосной станцией 2-го подъема представлено на рис. 1.

После запуска насосного агрегата развивается и поддерживается мощность, соответствующая водоподаче. Через 30 с происходит сравнение показателя требуемой водоподачи и текущей мощности НА, здесь возможны два варианта развития событий: в случае, если мощность насоса выше водоподачи, то мощность НА уменьшается на требуемую величину, вплоть до отключения насоса. Если мощность не выше водоподачи, то через 5 с происходит следующее сравнение мощности и водоподачи. Здесь возможны два варианта событий: в случае, если мощность ниже водоподачи, то задается вопрос, развилась ли максимальная мощность работающего НА, в случае положительного ответа проводится оценка наработки незапущенных НА, происходит

выбор и запуск оптимального варианта. В случае отрицательного ответа мощность НА увеличивается на требуемую величину. Если мощность не ниже водоподачи, то через 5 с происходит проверка на аварию в системе.

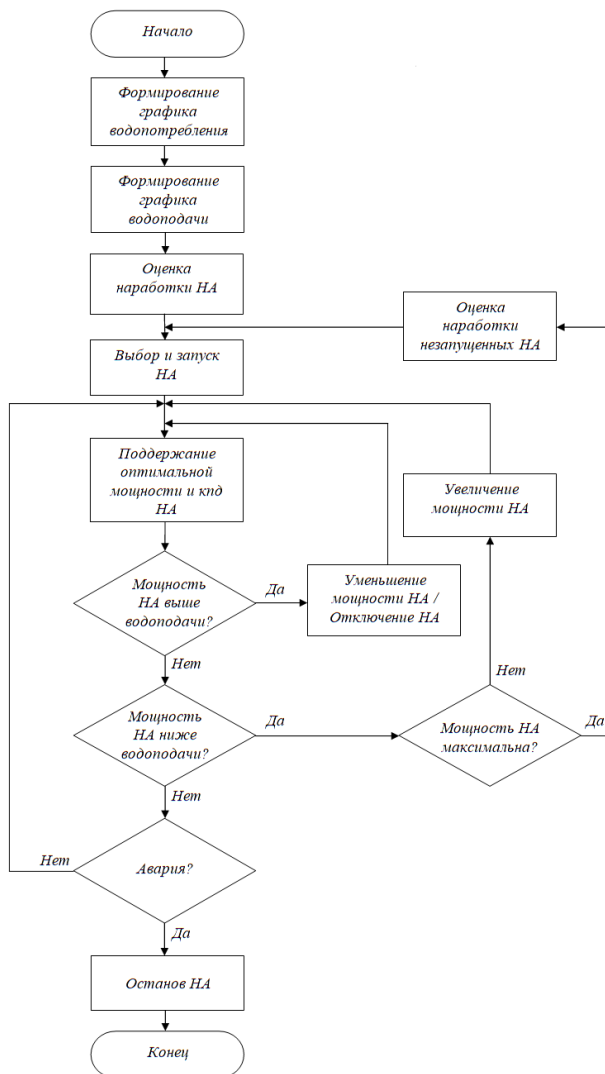


Рис. 1. Алгоритм управления напорной системой водоподачи с насосной станцией 2-го подъема

Если аварии нет, то система продолжает работать в штатном режиме, и через 30 с повторится первое сравнение мощности НА и водоподачи. В случае аварии происходит аварийный останов насосов и оповещение в АСУ ТП верхнего уровня.

Таким образом, с помощью разработанного алгоритма поддерживаются оптимальная мощность и КПД насосных агрегатов, в результате чего повышается энергетическая эффективность работы напорной системы водоподачи с насосной станцией второго подъема.

Библиографический список

1. Абрамов Н.Н. Водоснабжение: учеб. для вузов. – 2-е изд., перераб. и доп. – М.: Стройиздат, 1974. – 480 с.
2. Бочаров П.П., Печинкин А.В. Теория массового обслуживания: учебник. – М.: Изд-во РУДН, 1995. – 529 с.
3. Вентцель Е.С. Теория вероятностей. – М.: Наука, 1969. – 576 с.
4. Шаров Н. С., Тугов В.В. Исследование напорной системы водоподачи с применением теории массового обслуживания // Компьютерная интеграция и ИПИ-технологии: материалы VIII Всерос науч.-практ. конф. – Оренбург, 2017. – С. 360–363.

Сведения об авторах

Шаров Никита Сергеевич – студент Оренбургского государственного университета, Оренбург, e-mail: www.nixon.ru@mail.ru

Тугов Виталий Валерьевич – кандидат технических наук, доцент кафедры «Управление и информатика в технических системах», Оренбургского государственного университета, Оренбург, e-mail: sau@mail.osu.ru

About the authors

Sharov Nikita Sergeevich – Student Orenburg State University, Orenburg, e-mail: www.nixon.ru@mail.ru

Tugov Vitaliy Valerevich – Ph.D. in Technical Sciences, Associate Professor of the department of management and informatics in technical systems Orenburg State University, Orenburg, e-mail: sau@mail.osu.ru

Секция 3

**ИННОВАЦИОННЫЕ НАПРАВЛЕНИЯ В ЭНЕРГЕТИКЕ.
ЭНЕРГОРЕСУРСОСБЕРЕЖЕНИЕ**

ДЕЯТЕЛЬНОСТЬ ИНЖЕНЕРА Р.А. КОРЕЙВО ПО ПРОДВИЖЕНИЮ ДИЗЕЛИЗАЦИИ РОССИЙСКОГО РЕЧНОГО ФЛОТА В НАЧАЛЕ XX ВЕКА

С.Н. Киселев, С.П. Столяров

Санкт-Петербургский государственный морской
технический университет, Санкт-Петербург

Рассмотрено влияние деятельности главного инженера Коломенского завода Р.А. Корейво на процесс становления теплоходостроения в первой четверти прошлого века. Дается краткий обзор внедренных им конструктивных решений, позволивших занять заводу ведущие позиции в отрасли.

Ключевые слова: дизельные двигатели, пневматическая муфта, двигатель со встречным движением поршней, Р.А. Корейво, Коломенский завод.

ACTIVITY OF ENGINEER R.A. KOREYVO FOR THE PROMOTION OF DIESELIZATION OF THE RUSSIAN RIVER FLEET AT THE BEGINNING OF THE XX CENTURY

S.N. Kiselev, S.P. Stolyarov

Saint-Petersburg State Marine Technical
University, Saint-Petersburg

This article examines the influence of the activities of the chief engineer of the Kolomna plant, R.A. Koreyvo on the process of formation of diesel shipbuilding in the first quarter of the last century. Briefed the review of the constructive solutions implemented by him, which allowed the plant to take the leading positions in the industry.

Keywords: diesel engines, pneumatic clutch, opposed-piston engine, R.A. Koreyvo, Kolomna plant.

О биографии талантливого русского инженера Р.А. Корейво известно немного. Окончив Петербургский технологический институт, он занимался вопросами снижения ударных нагрузок в механизмах при пуске машин (его первые изобретения относятся к 1880 г. [5]). Тогда, решая эту проблему, он разработал специальную упругую муфту переменной жесткости, получившую впоследствии широкое применение во многих отраслях машиностроения. Но перед тем, как рассмотреть его деятельность в качестве главного инженера Коломенского завода, рассмотрим кратко исторический контекст событий.

Дизельный двигатель появился в России в 1898 г., когда Эммануилом Нобелем был приобретен патент, чертежи и рабочая доку-

ментация на одноцилиндровый вертикальный двигатель Р. Дизеля мощностью 20 л.с. для Петербургского чугунолитейного и механического завода «Людвиг Нобель» [4]. В 1903 г. лицензия на право производства дизеля была получена от Нобеля Коломенским машиностроительным заводом. В этом же 1903 г. завод «Л. Нобель» начал опыты по применению дизельных двигателей в качестве главных судовых установок на судах внутреннего плавания. Для этого на один из трех построенных Сормовским заводом корпусов однотипных наливных барж, получивший имя «Вандал», были установлены три дизельных двигателя собственного производства завода Л. Нобеля. Двигатели на судне не имели механической связи с гребными валами: использовалось полное электродвижение. Большие потери при преобразовании энергии вынудили использовать на построенном в 1904 г. «Сармате» электрический двигатель только для движения назад.

Хотя «Вандал» и «Сармат» показали возможность работы двигателей Дизеля в судовых условиях, интереса к ним не последовало. Как написал Е. Силин, «за промежуток времени с 1904 по 1908 г. наблюдалось затишье, то это обстоятельство, несомненно, должно быть отнесено за счет того, что существовавшие в то время приспособления для изменения направления движения судна не могли считаться рациональными» [2].

Проблема реверсирования судовых дизелей встала и перед Коломенским заводом. По завершении разработки собственного судового дизельного двигателя коломенцы, имея за плечами богатый опыт постройки паровых судов, при участии инженера завода «Людвиг Нобель» К.В. Хагелина [6] начали работу над своим первым теплоходом. Для обеспечения заднего хода заведующий бюро общего машиностроения (главный инженер Коломенского завода) Р.А. Корейво разработал оригинальную передачу, основу которой составляла фрикционно-пневматическая муфта, показанная на рис. 1, на которую 14 июля 1906 г. он получил патент № 29794 [1].

Разработанная муфта получила применение в 1907 г. на первом в мире дизельном колесном буксире «Мысль» (ранее «Коломенский Дизель»). Кроме реверса, понижая или повышая давление воздуха и тем самым варьируя степень проскальзывания дисков, можно было плавно менять обороты движителя, не изменяя при этом существенно обороты самого двигателя. Отрицательной стороной этого решения были значительные потери тепла с охлаждающей водой, снижавшие

ее КПД при работе на частичных режимах. Конструкция позволяла избавиться от электрической части, так что для ее привода и работы нужны были только охлаждение трущихся поверхностей и сжатый воздух.

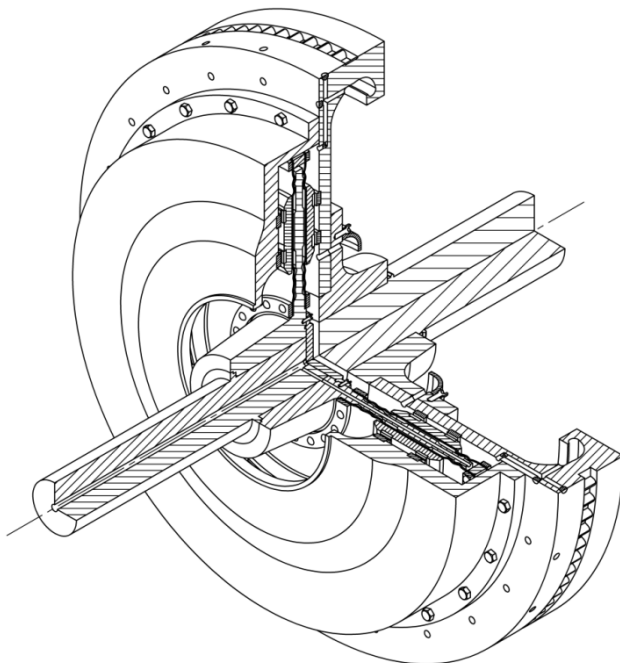


Рис. 1. Объемная модель пневматической муфты Р.А. Корейво

В процессе эксплуатации муфта хорошо себя зарекомендовала, что позволило применять ее для различных типов судов (особенно колесных) и после появления в 1910 г. у Коломенского завода реверсивных двигателей.

Принимая участие в работе над первыми дизельными судами, Р.А. Корейво стал известен не только благодаря специальной реверсивной передаче: по его проекту на Коломенском заводе был изготовлен оригинальный двухтактный дизель с противоположно движущимися поршнями (ПДП). После участия на нескольких специализированных международных выставках двигатель был замечен и скопирован Г. Юнкерсом. Руководство Коломенского завода, осте-

регаясь конфликта, не стало поддерживать претензию Р.А. Корейво и, таким образом, прекратило развитие этого направления.

Продолжая решать возникающие на заводе практические задачи, Р.А. Корейво для устранения ударов в передачах колесных судов применил свои предыдущие наработки, создал и запатентовал (в 1910 г. две российские привелегии №21008, 24325 и в 1911 г. один германский патент №285373 (класс 47 с, группа 5)) судовой вариант упругой муфты [3], о применении которой он написал свою работу «Удары и их устранение в зубчатых передачах колесных теплоходов», напечатанную в журнале «Теплоход» за 1912 г. Муфта изображена на рис. 2.

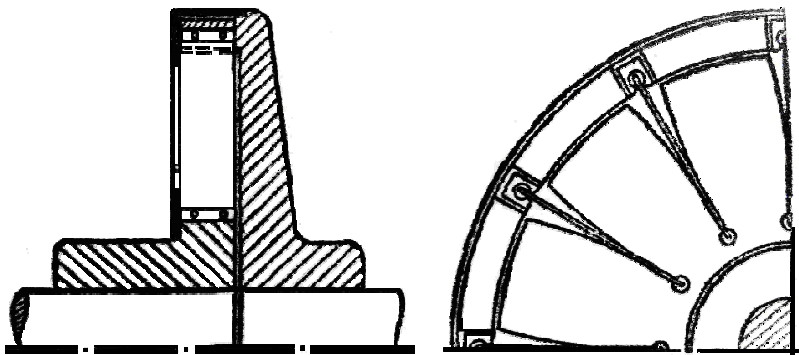


Рис. 2. Упругая муфта Р.А. Корейво с нелинейным уровнем жесткости звеньев

Расширяя сферу применения дизельных двигателей, на Коломенском заводе в 1911 г. создается колесный пассажирский теплоход «Урал». Получившаяся излишне сложная установка судна часто ломалась, а в 1916 г. «Урал» и вовсе погибает от взрыва в машинном отделении. Таким образом, негативный результат послужил толчком к созданию принципиально нового типа судна: под руководством Корейво был разработан проект винтовых грузо-пассажирских теплоходов «Бородино». В 1914 г. Российская Империя вступила в войну, и мощности Коломенского завода стали постепенно работать для военной промышленности. Обобщая опыт по постройке дизельных судов, в журнале «Теплоход» за 1914–1915 гг. Р.А. Корейво публикует свою вторую статью «По вопросу об устройстве машинных подкреплений в речных теплоходах».

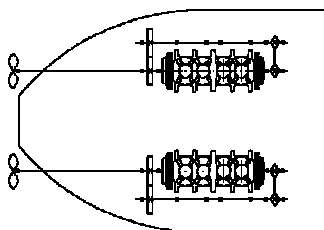


Схема 1. Судно с гребными винтами, нереверсивный двигатель, реверсивная передача

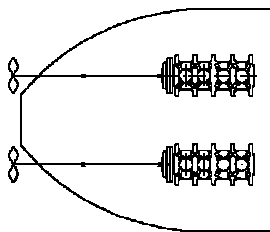


Схема 2. Судно с гребными винтами, реверсивный двигатель, разобщительная муфта Р.А. Корейво

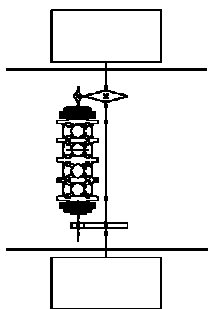


Схема 3. Судно с бортовыми гребными колесами, нереверсивный двигатель, реверс-редукторная передача Р.А. Корейво

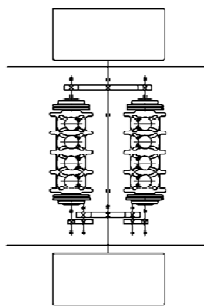


Схема 4. Судно с бортовыми гребными колесами, 2 нереверсивных двигателя, реверс-редукторная передача Р.А. Корейво

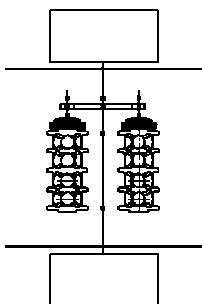


Схема 5. Судно с бортовыми гребными колесами, 2 реверсивных двигателя, редукторная передача Р.А. Корейво

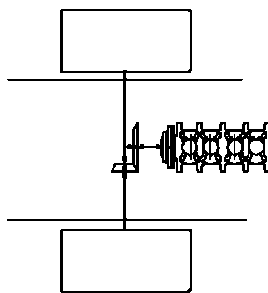


Схема 6. Судно с бортовыми гребными колесами, реверсивный 1 двигатель, редукторная передача Р.А. Корейво

Рис. 3. Схемы передач, разработанные Р.А. Корейво на основе изобретенной пневматической муфты

За несколько лет, предшествующих революции, завершается строительство последних судов типа «Бородино», «Байрам-Али». В сложной экономической ситуации создаются еще два новых дизельных судна – колесный буксир «Философ Платон» и винтовой буксир «Матвей Башкиров».

Таким образом, при непосредственном участии Р.А. Корейво в должности главного инженера Коломенского завода было создано новое направление в деятельности предприятия – теплоходостроение. Коломенский завод стал ведущим дизелестроительным предприятием, выпустившим в период с 1907 по 1916 г. около 33 дизельных судов на различных типах, на более чем половине из которых были установлены передачи с применением пневматической муфты Р.А. Корейво (все схемы разработанных передач показаны на рис. 3).

Но тем не менее при всех имеющихся заслугах об этом выдающемся инженерно-механике осталось крайне мало упоминаний, а большая часть достоверной информации была найдена в исторических источниках.

Библиографический список

1. Ефремов Г.П. История Коломенского завода. – М.: Мысль, 1973. – 366 с.
2. Силин Е. Судовые двигатели Дизеля в России. – Петроград (Издание журнала «Теплоход»), 1918. – 36 с.
3. Сулькин А.Г. Муфта Корейво // Вестник машиностроения. – 1949. – № 11. – С. 56–59.
4. Теплоход. – СПб. (Издание журнала «Теплоход»), 1911–1915.
5. Чудаков Е.А. Машиностроение: энциклопедический справочник: в 15 т. (Раздел 3: Технология производства машин). – М.: Гос. науч.-техн. изд-во машиностроит. лит-ры, 1947. – Т. 3. – 712 с.
6. Шубин И.А. Волга и Волжское судоходство. – М.: Транспечать, 1927. – 908 с.

Сведения об авторах

Киселев Степан Николаевич – магистрант Санкт-Петербургского государственного морского технического университета, Санкт-Петербург, e-mail: stak93@rambler.ru

Столяров Сергей Павлович – кандидат технических наук, доцент Санкт-Петербургского государственного морского технического университета, Санкт-Петербург, e-mail: stsp56@ya.ru

About the authors

Kiselev Stepan Nikolaevich – Master Student Saint-Petersburg State Marine Technical University, Saint-Petersburg, e-mail: stak93@rambler.ru

Stolyarov Sergey Pavlovich – Ph.D. in Technical Sciences, Associate Professor Saint-Petersburg State Marine Technical University, Saint-Petersburg, e-mail: stsp56@ya.ru

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ГАЗОТУРБИННЫХ ЭЛЕКТРОСТАНЦИЙ

И.А. Мальцев, Г.А. Килин

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассмотрены перспективы использования газотурбинных электростанций. Приведены преимущества и недостатки использования газотурбинных электростанций. Приведен общий вид работы газотурбинной электростанции.

Ключевые слова: газотурбинная установка; газотурбинная электростанция; газотурбинный двигатель; мобильность; комбинированность.

PROSPECTS FOR THE USE OF GAS TURBINE POWER PLANTS

I.A. Maltsev, G.A. Kilin

Perm National Research Polytechnic University, Perm

The prospects of using gas turbine power stations are considered in this article. The advantages and shortcomings of the use of gas turbine power stations are given. The general view of the operation of gas turbine power stations is given.

Keywords: gas turbine installation; gas turbine power station; gas turbine engine; mobility; kombinirovannoi.

Введение. Газотурбинная электростанция – это энергетическая установка, которая способна преобразовывать сжиженное топливо в электроэнергию. Мощность электростанции может иметь от 20 кВт до сотен МВт. Основной частью газотурбинной электростанции является газотурбинный двигатель (ГТД), число их варьируется от одного до нескольких в зависимости от требований, предъявляемых ГЭС.

ГТД – это тепловой двигатель, в котором газ сжимается и нагревается, а затем энергия сжатого и нагретого газа преобразуется в механическую работу на валу газовой турбины. Если верить источнику [9], то газотурбинная установка является самым мощным двигателем внутреннего сгорания. Источник [3] утверждает, что ее удельная мощность может составлять 6 кВт/кг.

Принцип действия. Большинство современных газотурбинных электростанций работают по схеме непрерывного сгорания топлива по открытому, другими словами, разомкнутому или закрытому (замкнутому) циклу в зависимости от вида сжигаемого топлива. Газотурбинные электростанции замкнутого цикла позволяют использовать как твёрдое, так и высокосернистое жидкое топливо (мазут), сжигаемое в камере сгорания, где установлен подогреватель рабочего тела, обычно воздуха. В схему газотурбинных электростанций замкнутого цикла включены воздухоохладитель, который уменьшает работу сжатия в компрессоре, и регенератор, что приводит к повышению экономичности.

Источник [11] гласит, что в газотурбинных электростанциях открытого цикла используется сжиженный природный газ (рис. 1), необходимый для работы двигателя, который подается под давлением в теплообменный контур, там происходит повышение температуры и его регазификация. Для работы газотурбинного двигателя необходимо, чтобы в его камере сгорания поступила смесь газа и воздуха.

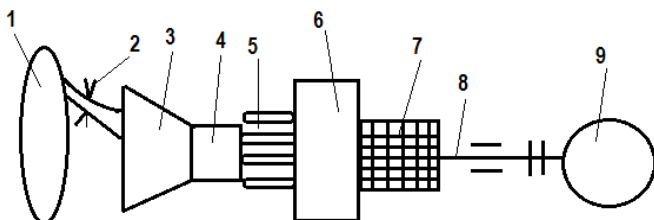


Рис. 1. Схематическое изображение газотурбинной электростанции:
1 – теплообменный контур, 2 – улитка, 3 – компрессор низкого давления,
4 – компрессор высокого давления, 5 – лопатки компрессора, 6 – камера
сгорания, 7 – лопасти силовой турбины, 8 – вал генератора, 9 – генератор

Атмосферный воздух втягивается через улитку, поступая в компрессор низкого, а затем и в компрессор высокого давления. Вращающиеся лопатки компрессора повышают давление, и воздух подается в камеру сгорания вместе с газом и воспламеняется. Струя продуктов сгорания вращает силовые турбины, которые передают вращающийся момент валу генератора. Продукты сгорания выводятся через выхлопную систему. В результате вращения турбины и ротора в генераторе вырабатывается ток.

Преимущества и недостатки. Как показывает источник [1], у любых электростанций есть свои плюсы и минусы, ГТЭС не является исключением.

Преимущества:

- ГТЭС весьма надежны. В среднем длительность работы основных узлов без капитального ремонта составляет до 100–130 тыс. ч;
- КПД самой газотурбинной установки составляет порядка 51 %, а при утилизации уходящих газов достигает 93 %;
- возможность выбора разных мощностей, экономичность работы, доступность топлива;
- небольшой размер, что уменьшает срок строительства и расхода строительных средств и позволяет быстрее окупаться;
- газотурбинные электростанции экологичны;
- такие установки могут работать как на промышленном газе: пропан-бутан, кокса, биогазе, так и на природном: магистральном сжатом и сниженном;
- ГТЭС могут работать полностью в автономном режиме, это облегчает диагностику состояния оборудования и основных узлов станции, простота управления, минимальное количество обслуживающего персонала делают их наиболее оптимальными в самых различных ситуациях.

Недостатки:

- в работе газовых турбоагрегатов используется газ с весьма высокой начальной температурой – более 550 град. Это вызывает трудности при практическом исполнении газовых турбин, так как требуются специальные жаростойкие материалы и особые системы охлаждения для наиболее нагреваемых частей;
- около половины развиваемой турбиной мощности расходуется на привод компрессора;
- ГТЭС принимает нагрузку через 15–17 мин после пуска;
- требуется высокое давление газа, порядка 4–10 атм.

Места эксплуатации. Использование газотурбинных установок целесообразно для удаленных от централизованных линий электро-снабжения потребителей, а также для сезонно функционирующих объектов. В таком случае затраты на обеспечение предприятия электричеством будут ниже, чем на подключение к ЛЭП. Конструктивно газотурбинные электростанции могут быть размещены на полупри-

цепях-фургонах или на железнодорожных платформах и использованы в местах новых разрабатываемых месторождений полезных ископаемых, особенно в районах месторождений нефти, где газотурбинные электростанции могут работать на попутном газе, или в районах строительства в качестве временных электростанций, это подтверждают источники [2, 4].

При этом удается сэкономить и на обогреве помещений. Эти обстоятельства определили и наиболее рациональную область использования газотурбинных электростанций в энергосистеме в качестве пиковых и обычно автономно запускаемых установок. В последнее время мобильная газотурбинная электростанция стала широко применяться и в городских условиях благодаря низкому уровню производимого шума, вибрации и токсичности выхлопных газов. Ее целесообразно использовать в случаях, когда подключение к энергосети города затруднено или стоимость последней слишком высока.

Перспективы развития. Развитие ГТЭС продолжается, это утверждает источник [12]. С каждым годом совершенствуются газотурбинные двигатели, позволяющие увеличить КПД электростанции. В настоящее время основным типом являются электростанции комбинированного цикла. Это парогазовые установки STAG (рис. 2).

Парогазовые электростанции представляют собой сочетание газовой и паровой турбины [13]. Электростанции комбинированного типа на базе парогазовых установок обладают очень высоким КПД – 58 %, а также они более экологически чистые, так как производят гораздо меньше выбросов парниковых газов.

Парогазовые установки могут работать на природном газе или на жидких видах топлива, это, как правило, дизельное топливо, солярка, мазут [10], а комбинированность достигается в результате утилизации отработанных газов. Газы, образующиеся в результате горения топлива, не только приводят в действие основную турбину, но и поступают в специальный котел-утилизатор. Здесь они нагревают водяной пар, и в результате высокого давления последнего приводится в действие паровая турбина, передающая энергию на второй генератор.

Именно благодаря такой совокупности выработки энергии и достигается высокая эффективность работы электростанции комбинированного типа на базе парогазовой установки.

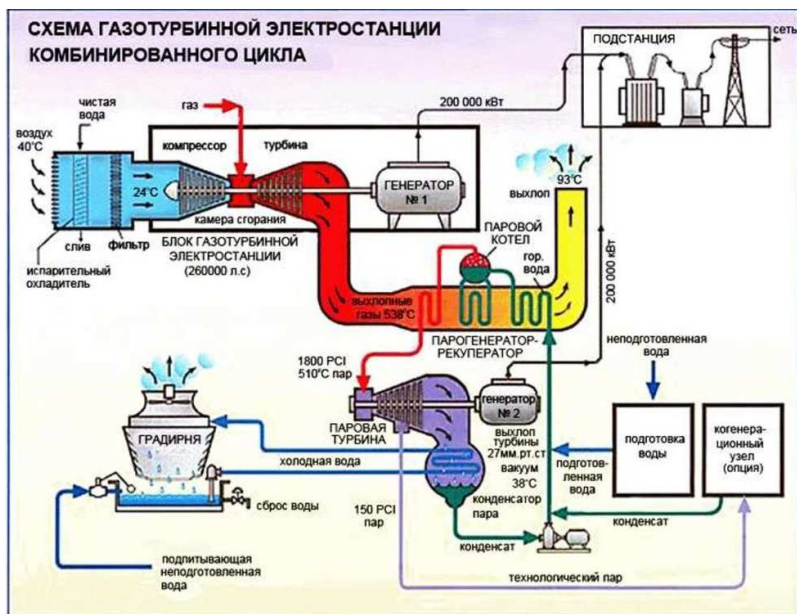


Рис. 2. Схема газотурбинной электростанции комбинированного цикла

Появляются инновации в системе автономного управления (САУ) газотурбинных установок [5, 6], она совершенствуется с каждым годом. Разрабатываются новые модели ГТУ на основе нейронных сетей [8], а в [7] изложено, что быстрорешаемые модели системы «ГТУ – синхронный генератор» можно получать с помощью идентификации.

Заключение. Из всего вышеизложенного, ввиду неоспоримых преимуществ, имеющих широкие перспективы для дальнейшего использования и развития ГТЭС, можно сделать вывод: газотурбинные электростанции – перспективное направление для развития электроэнергетики. Это самый оптимальный выход для нефтегазовых месторождений, где требуется бесперебойное поступление электроэнергии, и к тому же на таких месторождениях не будет проблем с поставкой топлива для ГТЭС, что обеспечит бесперебойное поступление электричества. Газотурбинные электростанции комбинированного цикла способны не только к выработке электроэнергии, но и обогреть помещения на добываемых месторождениях.

Библиографический список

1. Брюхань Ф.Ф. Оценка экологичности проекта строительства мобильной пиковой газотурбинной электростанции в республике Тыва // Вестник МГСУ. – 2011. – № 2. – С. 10–12.
2. Брюхань Ф.Ф., Коськин И.О. Предпроектное геоэкологическое обоснование выбора площадок размещения мобильных газотурбинных электростанций на рекреационных территориях // Вестник МГСУ. – 2012. – № 5.
3. Газотурбинная электростанция [Электронный ресурс] // Материал из Википедия. – URL: https://ru.wikipedia.org/wiki/Газотурбинная_электростанция (дата обращения: 18.11.2017).
4. Газотурбинные установки малой мощности в энергетике: пути повышения эффективности и масштабов внедрения / А.С. Косой, О.С. Попель, В.Н. Бесчатных, Ю.А. Зейгарник, М.В. Синкович // Теплоэнергетика. – 2017. – № 10. – С. 25–32.
5. Килин Г.А., Кавалеров Б.В., Бахирев И.В. Адаптивное управление автономными и неавтономными газотурбинными электростанциями с учетом электрической нагрузки // Автоматизация в электроэнергетике и электротехнике: материалы II Междунар. науч.-техн. конф.; 21–22 апреля 2016 г. / Перм. нац. исслед. политехн. ун-т. – Пермь: ИП Серегина О.Н., 2016. – С. 15–23.
6. О задачах исследования адаптивного управления электростанциями на базе конвертирования авиационных ГТУ / Г.А. Килин, Б.В. Кавалеров, И.В. Бахирев, Е.А. Маталасова // Вестник Пермского национального исследовательского политехнического университета. Электротехника. – 2014. – № 10. – С. 12–15
7. Килин Г.А., Ждановский Е.О. Получение быстрорешаемой модели системы «ГТУ – синхронный генератор» с помощью идентификации // Энергетика. Инновационные направления в энергетике. CALS-технологии в энергетике : материалы VI Междунар. интернет-конф.; г. Пермь, 1–30 ноября 2012 г. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2012. – С. 225–236.
8. Килин Г.А., Ждановский Е.О., Кавалеров Б.В. Разработка тематической модели газотурбинной электростанции на основе технологии нейронных сетей // Фундаментальные исследования. – 2016. – № 12–3. – С. 479–485.
9. Лебедев А.С., Костенко С.В. Тенденции повышения эффективности ГТУ // Теплоэнергетика. – 2008. – № 6. – С. 11–18.

10. Филиппов С.П., Дильман М.Д., Ионов М.С. Потребности электроэнергетики России в газовых турбинах: текущее состояние и перспективы // Теплоэнергетика. – 2017. – № 11. – С. 53–65.

11. Принцип работы газотурбинного двигателя. Видеоматериал [Электронный ресурс]. – URL: https://vk.com/video169387304_169838519 (дата обращения: 18.11.2017).

12. Тауд Р. Перспективы развития тепловых электростанций на органическом топливе // Теплоэнергетика. – 2013. – № 2. – С. 68–72.

13. Цанев С.В., Бурев В.Д., Ремезов А.Н. Газотурбинные и парогазовые установки тепловых электростанций. – М: Изд-во МЭИ, 2002.

Сведения об авторах

Мальцев Илья Анатольевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: iliamalcev18.08.1997@mail.ru

Килин Григорий Александрович – магистр, старший преподаватель Пермского национального исследовательского политехнического университета, Пермь, e-mail: thisisforasm@rambler.ru

About the authors

Maltsev Ilya Anatolyevich – Student Perm National Research Polytechnic University, Perm, e-mail: iliamalcev18.08.1997@mail.ru

Kilin Grigory Alexandrovich – Master, Senior Lecturer Perm National Research Polytechnic University, Perm, e-mail: thisisforasm@rambler.ru

ВОЗОБНОВЛЯЕМЫЕ ИСТОЧНИКИ ЭНЕРГИИ И ПЕРСПЕКТИВЫ ИХ ИСПОЛЬЗОВАНИЯ

Ю.В. Озерец, А.Д. Полухович

Белорусский национальный технический
университет, Минск

В статье рассмотрены основные аспекты развития возобновляемых источников энергии (ВИЭ). Главной причиной распространения ВИЭ является снижение нагрузки на окружающую среду. Также были рассмотрены существующие на данный момент технологии эксплуатации различных видов энергии, а именно: солнечной, ветряной, биоэнергии и гидроэнергии.

Ключевые слова: возобновляемая энергия, солнечная энергия, солнечные батареи, ветроэнергетика, ветрогенератор, гидроэнергетика, биотопливо.

RENEWABLE ENERGY SOURCES AND PROSPECTS OF THEIR USE

Yu.V. Aziarets, A.D. Paliukhovich

Belarusian National Technical University, Minsk

In this article the main aspects of renewable energy sources (RES) development are considered. The main reason for the spread of RES is to reduce the burden on the environment. Currently existing technologies of operation of various types of energy, namely, solar and wind energy, bioenergy and hydropower were also considered.

Keywords: renewable energy, solar power, solar panels, wind power, wind turbine, hydropower, biofuel.

Энергетика является важнейшей отраслью в стране, определяя стабильность экономического развития и прогресс общественного производства.

На данный момент в качестве основных источников энергии используется органическое топливо, а именно: нефть, газ, уголь, урановые руды.

Согласно исследованиям, если существующие тенденции использования органического топлива сохранятся, то годовое потребление нефти к 2018 г. достигнет 3 млрд т. Даже допуская, что промышленные запасы существенно возрастут, геологи приходят к выводу, что к 2030 г. будет исчерпано 80 % разведанных мировых запасов нефти. В связи с этим необходимо задуматься о поиске замены традиционных источников энергии.

На сегодняшний день использование возобновляемых источников энергии является одним из решений данной проблемы.

Возобновляемая энергия – энергия из источников, которые по человеческим масштабам являются неисчерпаемыми. Основной принцип использования возобновляемой энергии заключается в её извлечении из постоянно происходящих в окружающей среде процессов и предоставлении для технического применения [4]. Возобновляемые источники энергии представляют интерес из-за выгоды их использования, как правило, при низком риске причинения вреда окружающей среде. В таблице представлены сравнительные характеристики работы различных типов электростанций [7].

Сравнительные экологические характеристики работы электростанций

Тип электростанции	Объем вредных выбросов в атмосферу, м ³ /МВт·ч	Потребление свежей воды, м ³ /МВт·ч	Сброс загрязненных сточных вод, м ³ /МВт·ч	Объем твердых отходов, кг/МВт·ч	Изъятие земель, га/МВт·ч	Затраты на охрану природы, % от общих затрат
СЭС (солнечная)	–	–	0,02	–	2-3	–
ВЭС (ветровая)	–	–	0,01	–	1–10	до 1
ГеоТЭС (геотермальная)	Менее 1	–	–	–	0,2	до 1
Энергия биомассы	2–10	20	0,2	0,2	0,2–0,3	–
Угольные ТЭС		40–60	0,5	200–500	1,5	30
Газомазутные ТЭС	2–15	2–5	0,2	0,2	0,5–0,8	10
ГЭС	–	–	–	–	100	2
АЭС	–	70-90	До 0,5	0,2	0,2	50

На сегодняшний день основными источниками возобновляемой энергии являются: солнечная энергия, энергия ветра, гидроэнергия, биотопливо.

Первым рассматриваемым нами источником является энергия солнечного света. Солнечная энергия – это преобразование солнечного света в электричество либо непосредственно с использованием фотогальваники (PV), либо косвенно с использованием солнечных систем концентрирующего типа (CSP). Системы CSP используют

линзы и зеркала, чтобы фокусировать энергию солнечных лучей в концентрированный луч света. Этот луч используется как источник тепловой энергии для нагрева рабочей жидкости.

В 2016 г. солнечная энергия произвела 1,3 % глобальной мощности, превысив 300 ГВт. На рис. 1 представлено распределение рынка солнечной энергии по странам на 2016 г.

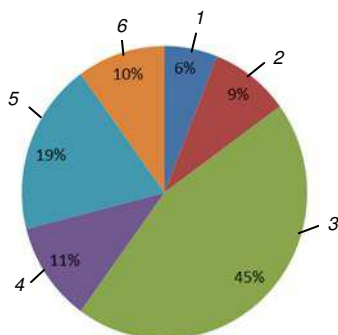


Рис. 1. Распределение рынка солнечной энергии по странам на 2016 г.: 1 – Индия; 2 – Европа; 3 – Китай; 4 – Япония; 5 – США; 6 – другие страны

Как полагают эксперты Международного энергетического агентства, уже через 40 лет при соответствующем уровне распространения передовых технологий данный источник будет вырабатывать около 9 тыс. ТВт/ч, или 20–25 % всего необходимого электричества. Это обеспечит сокращение выбросов углекислого газа на 6 млрд т ежегодно [6].

Основными достоинствами использования энергии солнечного света являются доступность энергоресурса, его постоянство, минимальное влияние на экосистему в процессе ее преобразования. Однако, несмотря на перечисленные преимущества, существует ряд сопутствующих недостатков. Так, после отработки оборудования резко встает вопрос его утилизации. На сегодняшний день не существует технологий безопасной переработки солнечных элементов, вследствие чего возникает риск загрязнения окружающей среды.

Следующим рассматриваемым нами источником является энергия ветра. Ветроэнергетика – отрасль энергетики, специализирующаяся на преобразовании кинетической энергии воздушных масс в атмосфере в электрическую, механическую, тепловую или в любую другую форму энергии, удобную для использования в народном хозяйстве [3]. Ветроэнергетика является активно развивающейся отрас-

лью. К началу 2016 г. общая установленная мощность всех ветрогенераторов составила 432 ГВт и превзошла суммарную установленную мощность атомной энергетики.

Ветровая энергия как альтернатива сжиганию ископаемого топлива является возобновляемой, широко распространенной, чистой, не производит выбросов парниковых газов во время эксплуатации, не потребляет воды. Чистое воздействие на окружающую среду по сравнению с нетрадиционными источниками энергии.

Электрическую энергию из ветра получают посредством использования ветрогенераторов. Ветрогенераторы – это устройства, которые позволяют нам использовать силу ветра и преобразовывать ее в электрическую энергию. Когда ветер дует, лопасти турбины вращаются, приводя в движение основной вал, соединенный с генератором, который производит электричество. Затем электричество перемещается вниз по башне к трансформатору, где уровни напряжения регулируются в соответствии с сеткой.

По состоянию на 2015 г. Дания генерирует 40 % своей электроэнергии от ветра [8], и по меньшей мере 83 страны по всему миру используют ветроэнергетику для питания своих электрических сетей. В 2014 г. глобальная мощность ветроэнергетики увеличилась на 16 % до 369 553 МВт. Ежегодное производство энергии ветра быстро растет и достигает около 4 % от общего потребления электроэнергии в мире.

Хотя ветряные электростанции относительно мало влияют на окружающую среду по сравнению с электростанциями на ископаемом топливе, существует ряд проблем, связанных с шумом, создаваемым лопастями ротора. Большая часть этих вопросов была решена или значительно сокращена благодаря технологическому развитию и правильному размещению ветровых установок.

Несмотря на то, что стоимость ветроэнергетики за последние 10 лет резко снизилась, технология требует более высоких первоначальных инвестиций, чем генераторы, работающие на ископаемом топливе. Примерно 80 % стоимости – это оборудование, требующееся для подготовки и установки площадки. Тем не менее, если ветрогенераторы сравниваются с системами с ископаемым топливом на основе «жизненного цикла» (с учетом топлива и эксплуатационных расходов на срок службы генератора), затраты на ветер намного более конкурентоспособны с другими генерирующими технологиями.

Еще одним крупнейшим источником возобновляемой энергии является гидроэнергетика. Гидроэнергетика – область хозяйственно-экономической деятельности человека, совокупность больших естественных и искусственных подсистем, служащих для преобразования энергии водного потока в электрическую энергию [5]. Типичная гидроэлектростанция представляет собой систему с тремя частями: электростанцией, где производится электричество, плотиной, которая может открываться или закрываться для контроля потока воды, и резервуаром, в котором может храниться вода. Вода за плотиной течет через впуск и толкает лопасти в турбине, заставляя их вращаться. Турбина вращает генератор для производства электроэнергии. Количество электричества, которое может генерироваться, зависит от того, насколько сильно падает вода и сколько воды проходит через систему. Электричество может транспортироваться по междугородним электрическим линиям в дома, заводы и предприятия.

Гидроэнергетика – самый дешевый способ производства электроэнергии на сегодняшний день. Это чистый источник топлива, который ежегодно возобновляется снегом и осадками. Гидроэнергетика также легко доступна; инженеры могут контролировать поток воды через турбины для производства электроэнергии по требованию. За 2015 г. гидроэнергетика обеспечила производство 63 % возобновляемой и 16,6 % всей электроэнергии в мире

Последним рассматриваемым нами источником является биотопливо. В настоящее время технологии переработки биологического сырья нашли широкое применение для решения проблемы экологически безопасной утилизации органических отходов, уменьшения загрязнения окружающей среды, а также получения альтернативной энергии.

Биотопливо – топливо из растительного или животного сырья, из продуктов жизнедеятельности организмов или органических промышленных отходов [2].

На сегодняшний день существует тенденция использования водорослей для получения биотоплива. Водорослевое топливо является альтернативой общеизвестным источникам биотоплива, таким как кукуруза и сахарный тростник. Как и ископаемое топливо, водоросли выделяют CO_2 при сжигании, но в отличие от него водорослевое топливо выпускает только CO_2 , недавно удаленный из атмосферы с помощью фотосинтеза по мере своего роста.

Энергетический и мировой продовольственный кризис вызвал интерес к использованию водорослей для производства биотоплива

с использованием земли, не пригодной для сельского хозяйства. Большим плюсом является то, что их можно выращивать с минимальным воздействием на ресурсы пресной воды. Во Франции предложили следующую разработку: использование сточных вод для выращивания особых видов водорослей. В них вводятся определенного вида бактерии, которые способствуют их росту.

Ученые утверждают, что водоросли могут быть от 10 до 100 раз более производительными, чем традиционные источники биоэнергии. По оценкам Министерства энергетики Соединенных Штатов Америки, если бы водорослевое топливо заменило все нефтяное топливо в стране, для этого потребовалось бы 39 000 км², что составляет всего 0,42 % от карты США.

По данным Международного энергетического агентства, к 2050 г. биотопливо должно удовлетворить более четверти мирового спроса на транспортные топлива для снижения зависимости от нефти и угля.

На сегодняшний день развитие возобновляемых источников энергии является одной из первостепенных задач энергетики. Системы ВИЭ быстро становятся более эффективными и дешевыми. На рис. 2 представлены темпы роста ВИЭ в мировом производстве электроэнергии за период с 1990 по 2016 г.

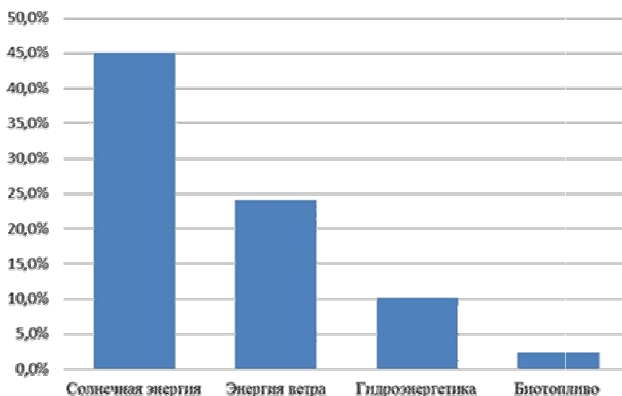


Рис. 2. Темпы роста ВИЭ в мировом производстве электроэнергии за период с 1990 по 2016 г.

В то же время рост потребления угля и нефти может завершиться к 2020 г. в связи с увеличением доли возобновляемых источников энергии в общем потреблении энергии [1].

Библиографический список

1. Electric cars and cheap solar could halt fossil fuel growth by 2020 [Электронный ресурс]. – URL: <https://www.theguardian.com/environment/2017/feb/02/electric-cars-cheap-solar-power-halt-fossil-fuel-growth-2020> (дата обращения: 09.12.2017).
2. Биотопливо [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D1%82%D0%BE%D0%BF%D0%BB%D0%B8%D0%B2%D0%BE> (дата обращения: 09.12.2017).
3. Ветроэнергетика [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D1%82%D1%80%D0%BE%D1%8D%D0%BD%D0%B5%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D0%BA%D0%B0> (дата обращения: 09.12.2017).
4. Возобновляемая энергия [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%B7%D0%BE%D0%B1%D0%BD%D0%BE%D0%B2%D0%BB%D1%8F%D0%B5%D0%BC%D0%B0%D1%8F_%D1%8D%D0%BD%D0%B5%D1%80%D0%B3%D0%B8%D1%8F (дата обращения: 09.12.2017).
5. Гидроэнергетика [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%B4%D1%80%D0%BE%D1%8D%D0%BD%D0%B5%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D0%BA%D0%B0> (дата обращения: 09.12.2017).
6. Российский деловой интернет-портал [Электронный ресурс]. – 2008. – URL: <https://www.bfm.ru/> (дата обращения: 09.12.2017).

Сведения об авторах

Озерец Юлия Вячеславовна – студентка Белорусского национального технического университета, Минск, e-mail: ms.ozerec@mail.ru

Полухович Александра Денисовна – студентка Белорусского национального технического университета, Минск, e-mail: aleksandra-poluhovich@tut.by

About the authors

Aziarets Yulia Vyacheslavovna – Student Belarusian National Technical University, Minsk, e-mail: ms.ozerec@mail.ru

Paliukhovich Aliaksandra Dianisovna – Student Belarusian National Technical University, Minsk, e-mail: aleksandra-poluhovich@tut.by

БЛОКЧЕЙН – НОВЫЙ УРОВЕНЬ ЭНЕРГЕТИКИ

М.И. Русецкая, Я.А. Стасула

Белорусский национальный технический университет, Минск

В данной статье рассмотрены перспективы внедрения технологии блокчейн в систему энергетики. Особое внимание уделяется внедрению децентрализованной системы. Показано, что применение данной технологии удешевит процесс передачи электроэнергии, что, в свою очередь, обеспечит более приемлемые цены на электроэнергию для населения. На основе уже внедрённых проектов исследованы другие варианты применения технологии блокчейн в энергетике.

Ключевые слова: блокчейн, энергетика, электроснабжение, транзакция, умные контракты, модель счетов, децентрализованная система.

BLOCKCHAIN – NEW ENERGY LEVEL

M.I. Rusetskaya, Ya.A. Stasula

Belarusian National Technical University, Minsk

This article examines the prospects for implementation of blockchain-technology in the energy system. Special attention is paid to the introduction of a decentralized system. It is shown that the use of this technology reduces the transfer of electricity, which in turn will provide a more reasonable electricity prices for the population. On the basis of already implemented projects other applications of blockchain-technology in the energy sector are investigated.

Keywords: blockchain, power engineering, power supply system. Transaction, clever contracts, model of accounts, the decentralized system.

Технология блокчейн, представляющая собой выстроенную по определенным правилам цепочку из формируемых блоков транзакций, впервые нашла своё применение ещё в 1990-х гг., но на тот момент она являлась централизованной системы транзакций. Биткоин же как первое применение децентрализованной технологии блокчейн-на появился осенью 2008 г. благодаря Сатоши Накомото. На сегодняшний день данная технология нашла намного больше сфер для применения.

Довольно ярким примером может послужить применение блокчейн-технологии в финансовой отрасли. В первую очередь, этой технологией интересуются представители банковской сферы и различных платёжных компаний. Это обусловлено тем, что блокчейн может решить множество проблем финансовой отрасли и в целом улучшить

её. Здесь речь идёт о трудностях, таких как проблема скорости и безопасности транзакций, проблема количества совершаемых платежей за единицу времени, проблема транзита «чёрных денег» и т.д.

Однако на этом развитие блокчейна не остановилось, и технологию начали использовать в других сферах жизни. Например, для операций с товарами и сырьём. Уже стало возможным безопасно и эффективно покупать золотые и серебряные слитки. Огромный вклад эта технология внесла в решение проблем с цифровой идентичностью, проверкой подлинности и подтверждением прав доступа. Сейчас также активно разрабатывается на основе технологии блокчейн безопасная и открытая платформа для онлайн-голосований (таблица).

Мировой опыт использования технологии блокчейн

Страна	Области применения
Германия	Сфера культуры и искусства (авторство и право владения произведением)
Швейцария	Финансовые технологии и услуги; сфера инновационного бизнеса
Россия	Банковская сфера; системы регулирования и государственного управления
Англия	Алмазная индустрия
США	Область финансов и банковского дела; системы хранения личных данных

Как оказалось, некоторые варианты применения блокчейн в финансовой сфере возможны и в энергетической отрасли:

- децентрализованное хранение данных по транзакциям (повышает уровень их защиты и обеспечивает более высокую степень независимости);
- цепочки блоков (упрощают совершение платежей с использованием криптовалют, исполнение торговых операций, обеспечивают их безопасность);
- децентрализованные бизнес-модели (позволяют сократить число посредников).

Однако следует учитывать, что сфера энергетики отличается от финансовой наличием самого продукта, а именно электроэнергии. Следовательно, следует акцентировать внимание на торговле энергией с помощью объектов сетевой инфраструктуры.

Отсюда следуют возможные варианты внедрения блокчейн-проектов в энергетике.

- Децентрализованная система энергетики.

При использовании уже известных технологий блокчейн финансового сектора можно с их помощью сделать систему энергетики децентрализованной, так как в будущем система распределения электроэнергии будет состоять из миллиардов точек, взаимодействующих друг с другом, в которую будут включены и солнечная энергия, и энергия ветра, и т.д. Важно создать надежную систему, которую можно контролировать, но которая позволит проводить своего рода автономные транзакции. Что обеспечит введение децентрализованной системы?

1. Контроль электросетей с помощью «умных контрактов». Именно умные контракты будут подавать сигнал, когда нужно проводить транзакцию, а когда нет. Например, каждый раз, когда объемы произведенной электроэнергии превышают существующие потребности, можно использовать «умные контракты» для того, чтобы данные излишки электроэнергии автоматически направлялись в хранилище. И наоборот, электроэнергию из хранилища можно использовать тогда, когда произведенного объема электроэнергии оказывается недостаточно.

2. Безопасное хранение и достоверное отражения всех транзакций, проведенных за всё время благодаря использованию распределенного реестра.

3. Надёжное хранение записей о праве собственности. История перехода прав по каждому сертификату будет точно отражена в цепочке блоков.

4. Возможность интеграции криптовалюты.

Объединив всё вышеизложенное, можно организовать энергоснабжение без привлечения посредников (энергетических компаний, брокеров). При действующей системе электроэнергия производится на генерирующих объектах с централизованным управлением и поставляется промышленным и бытовым потребителям по распределительным сетям, операторами которых являются электроэнергетические компании. Трейдеры покупают и продают электроэнергию на биржах, а банки выступают в роли поставщиков платежных услуг, занимаясь обработкой транзакций, осуществленных участвующими сторонами. Для процессов, основанных на применении блокчейна, уже не будут требоваться электроэнергетические компании, трейдеры и банки (для проведения платежей). Вместо этого появится децентрализованная система

энергетических транзакций и энергоснабжения, в рамках которой приложения «умные контракты», работающие на основе блокчейн-технологии, позволят потребителям управлять своими договорами на электроснабжение и данными об объеме потребленной ими электроэнергии.

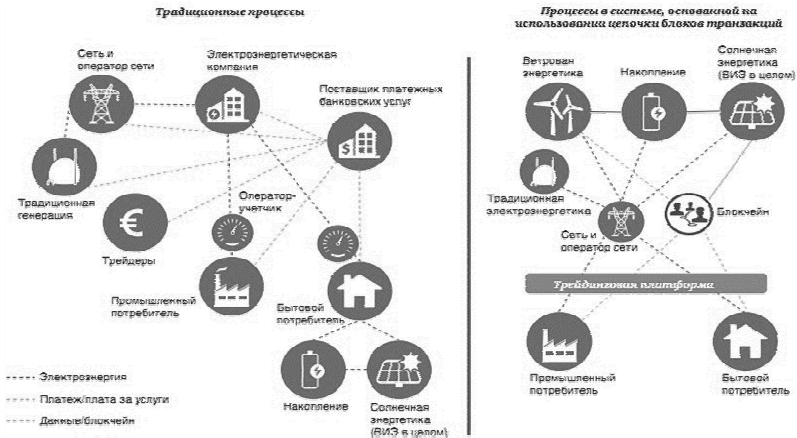


Рис. Сравнение централизованной и децентрализованной систем

- **Модель счетов.**

Данная технология найдёт своё применение при подзарядке электромобилей, так как сам процесс подзарядки занимает очень длительное время в основном из-за выставления счетов, а технология блокчейн позволит это исправить. Например, водитель электромобиля припарковывает свой электромобиль и идёт по своим делам, а в это время его автомобиль самостоятельно регистрируется в системе станции подзарядки и заряжается автоматически. После того как водитель уедет с парковки, станция подзарядки автоматически выставит ему счет за потребленную электроэнергию, используя при этом технологию «блокчейн».

- **Хранение информации по счетам.**

В будущем, когда все устройства начнут друг с другом взаимодействовать, именно благодаря использованию «умных контрактов» можно будет создать не только полный архив данных, но и с внедрением «умных счётчиков» можно будет считывать показания и направлять их для выставления счетов по электроэнергии.

Если говорить о внедрении блокчейн-проектов на практике, то можно привести несколько примеров из мирового опыта:

- Brooklyn Microgrid.

Проект BrooklynMicrogrid на данный момент разрабатывается в Бруклине компанией TransactiveGrid. Суть заключается в следующем: на 5 зданиях установили фотоэлектрические энергетические системы, которые преобразовывают солнечную энергию в электроэнергию. Все объёмы электроэнергии, которые не используются самим зданием, передаются пяти другим. Все здания объединены в обычную электросеть. В будущем планируется, что всю систему можно будет контролировать посредством приложения, т.е. благодаря этой технологии даже один человек, имея одну солнечную батарею или ветровую установку, сможет стать частью рынка. Следовательно, энергию можно будет продавать в индивидуальном порядке.

Над подобным проектом также работает нидерландская компания Vattenfall и Oneup.

- Blockcharge.

Немецкие компании Slock.it и RWE запустили пилотный проект, который позволит ускорить процесс подзарядки электромобилей. Согласно концепции проекта электромобили будут взаимодействовать со станциями подзарядки в автоматическом режиме, обеспечивая управление процессом выставления счетов за электроэнергию, полученную за время подзарядки. Предполагается, что в конечном итоге в каждый автомобиль будет вмонтирован чип с криптовалютой, что позволит автомобилю самостоятельно управлять процессом оплаты потребленной электроэнергии.

На данный момент проекты блокчейн находятся только на стадии разработки и поиске концепции, которая будет удовлетворять все стороны. Однако уже реализованные проекты показывают, что перспектива есть, и внедрение блокчейн в энергетику носит многообещающий характер.

Говоря же о Беларуси, на данный момент уже реализован проект с применением блокчейна в финансовой сфере. Технология позволяет хранить распределенные списки реестра выданных банковских гарантий и создана в рамках программы по изучению новых банковских технологий. Это поможет снизить риски при заключении международных контрактов и предотвратить фальсификацию банковских гарантий.

В перспективе рассматривается дальнейшее внедрение блокчейн в банковскую систему. Это и внедрение в систему ЕРИП, что обеспечит полную безопасность в обмене информации, и рынок ценных бумаг, что сделает этот рынок более прозрачным и поспособствует его развитию. Также рассматривается технология блокчейн со стороны финансирования (InitialCoinOffering), однако законодательство РБ пока не позволяет это сделать.

Что касается энергетики, то согласно плану развития энергетической отрасли Республики Беларусь планируется переход энергетики к децентрализованной системе. Блокчейн же может быть одним из способов достижения этой цели. Первоначально это можно сделать на более локальном уровне, последовать примеру Бруклина, а впоследствии расширить применение данной технологии. Также в связи со строительством АЭС в Республике Беларусь будет ощущаться избыток электроэнергии, что позволит использовать электромобили, а следовательно, можно последовать примеру проекта Blockcharge.

В заключение хотелось бы отметить, что финансовые приложения в сфере «блокчейн» уже достигли внушительного уровня. По части блокчейн-проектов в сфере энергетики на данный момент ещё рано делать какие-либо выводы. Однако согласно пилотным проектам можно сказать, что технология имеет огромный потенциал, включая и преимущества для потребителей, и участников рынка. Для того же, чтобы блокчейн-системы обеспечивали преимущества для потребителей (включая и обычных потребителей электроэнергии, и потребителей, являющихся одновременно и производителями электроэнергии), потребуется уделять огромное внимание вопросам защиты прав потребителей. Также стоит уделить внимание нормативно-правовой базе, так как на данный момент главной проблемой внедрения технологии блокчейн является несовершенство законодательства многих стран.

Библиографический список

1. Блокчейн – новые возможности для производителей и потребителей электроэнергии? [Электронный ресурс]. – 2017 – URL: https://www.pwc.ru/ru/publications/blockchain/blockchain_opportunity-for-energy-producers%20and-consumers_RUS.pdf (дата обращения: 11.12.2017).

2. Blockchain может способствовать развитию энергетики будущего [Электронный ресурс]. – 2017. – URL: <https://rodovid.me/energy/blockchain-mozhet-sposobstvovat-razvitiyu-energetiki-buduschego.html> (дата обращения: 11.12.2017).

Сведения об авторах

Руцкая Мария Игоревна – студентка Белорусского национального технического университета, Минск, e-mail: mari.rusetskaya.1@mail.ru

Стасула Яна Андреевна – студентка Белорусского национального технического университета, Минск, e-mail: stasula_yana@mail.ru

About the authors

Rusetskaya Maria Igorevna – Student Belarusian National Technical University, Minsk, e-mail: mari.rusetskaya.1@mail.ru

Stasula Yana Andreevna – Student Belarusian National Technical University, Minsk, e-mail: stasula_yana@mail.ru

ОСОБЕННОСТИ ФОРМИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ЗАТРАТАМИ НА ПРЕДПРИЯТИЯХ ЭНЕРГЕТИКИ РЕСПУБЛИКИ БЕЛАРУСЬ

Н.А. Самосюк

Белорусский национальный технический
университет, Минск, Республика Беларусь

В данной статье рассмотрена система управления затратами на предприятии. Изучены структура и динамика затрат РУП «Облэнерго». Предложено провести реструктуризацию энергетических предприятий Республики Беларусь на соответствующие центры ответственности и места возникновения затрат. Данное мероприятие позволит получать информацию, которая будет способствовать принятию оперативных, тактических и стратегических решений для регулирования хозяйственных процессов, изыскания внутренних резервов и повышению эффективности деятельности предприятия.

Ключевые слова: энергосбережение, энергетика, затраты, система управления затратами.

FEATURES OF FORMATION OF THE COST MANAGEMENT SYSTEM AT THE ENTERPRISES OF POWER OF THE REPUBLIC OF BELARUS

N.A. Samasiuk

Belarusian National Technical University,
Minsk, Republic of Belarus

In this article the cost management system at the enterprise is considered. The structure and dynamics of expenses of RUP Oblenergo is studied. It is offered to carry out restructuring of the power enterprises of Republic of Belarus on the relevant centers of responsibility and the place of emergence of expenses. This action will allow to obtain information which will promote adoption of operational, tactical and strategic decisions, for regulation of economic processes, research of internal reserves and to increase in efficiency of activity of the enterprise.

Keywords: energy saving, power industry, cost, cost management system.

Повышение конкурентоспособности экономики, обеспечение энергетической безопасности и энергетической независимости за счет повышения энергоэффективности и увеличения использования собственных топливно-энергетических ресурсов (ТЭР), в том числе и возобновляемых источников энергии (ВИЭ), является приоритетным направлением страны.

Однако энергоёмкость ВВП Республики Беларусь остается в 1,5 раза выше, чем в среднем в странах Организации экономического сотрудничества и развития, и в 1,2 раза выше мирового среднего уровня этого показателя. Ежегодная реализация в 2011–2015 гг. региональных и отраслевых программ энергосбережения позволила обеспечить в Белорусской энергетической системе устойчивую тенденцию к снижению удельного расхода условного топлива на отпуск электроэнергии с 268,9 г у.т./кВт·ч в 2010 г. до 235,5 г у.т./кВт·ч в 2015 г. Это было достигнуто за счет ввода в эксплуатацию высокоэффективного энергетического оборудования и наращивания комбинированного производства электрической и тепловой энергии, являющегося одним из наиболее эффективных направлений использования топлива [1].

Проведя анализ энергетического баланса Республики Беларусь, можно сделать следующий вывод, что наблюдается тенденция к уменьшению потребления электро- и тепловой энергии (рис. 1) [2].

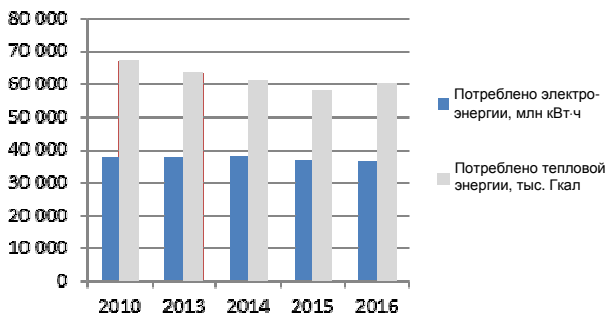


Рис. 1. Динамика потребления электро- и тепловой энергии за 2010–2016 гг.

Но, несмотря на снижение показателей потребления энергии в республике, экономия ТЭР в результате реализации энергосберегающих мероприятий в 2011–2015 гг. составила 7,79 млн т у.т. при задании 7,1–8,85 млн т у.т. Полученные результаты позволяют говорить о том, что в Республике Беларусь существует резерв по снижению расходов ТЭР. Поэтому на предприятиях энергетики Республики Беларусь остро встает вопрос эффективного управления затратами.

Система управления затратами на производство и реализацию продукции как составная часть системы управления деятельностью предприятия должна быть подчинена задаче достижения стратегической цели – обеспечение устойчивого и эффективного развития деятельности предприятия [6].

Эффективное управление затратами предполагает построение на предприятии системы обеспечения этого управления, которое, опираясь на использование современных методов планирования, нормирования, бюджетирования, учета и анализа затрат, позволяет принимать эффективные управленческие решения. Центральное место в решении этой проблемы связано с разработкой научно-обоснованной системы управления затратами на производство и реализацию продукции и определения условий эффективного применения. Комплексная система управления затратами обеспечивает взаимосвязанные действия по рациональному использованию материальных, трудовых, финансовых и других ресурсов на постоянной основе [3].

В современной теории управления затратами выделяют две основные группы инструментов. К первой можно отнести стратегические меры, направленные на оптимизацию затрат, такие как реструктуризация деятельности организации, выделение непрофильных активов и видов деятельности, поглощение конкурентов, поставщиков и тому подобное. Во вторую группу относят механизмы регулярного управления затратами. Механизм управления затратами состоит из следующих этапов, перед каждым из которых стоят определенные задачи:

- 1) определение цели и критериев управления;
- 2) планирование;
- 3) организация;
- 4) мотивация;
- 5) контроль.

Таким образом, система управления затратами на энергетическом предприятии с учётом распределения функциональных обязанностей между отделами включает в себя:

- 1) разработку (принятие) решений (прогнозирование и планирование: планово-экономический отдел);
- 2) реализацию решений (организация – заместитель директора по экономике и финансам; координация и регулирование; активизация и стимулирование – заместитель директора по экономике и финансам);
- 3) контроль (мониторинг): учет – бухгалтерия; анализ – планово-экономический отдел.

Оценивая структуру затрат на производство электроэнергии РУП «Облэнерго» можно заключить, сказать, что наибольшую часть в них занимают материальные затраты (более 70 %). На рис. 2 рассмотрим динамику затрат на выработку электроэнергии.

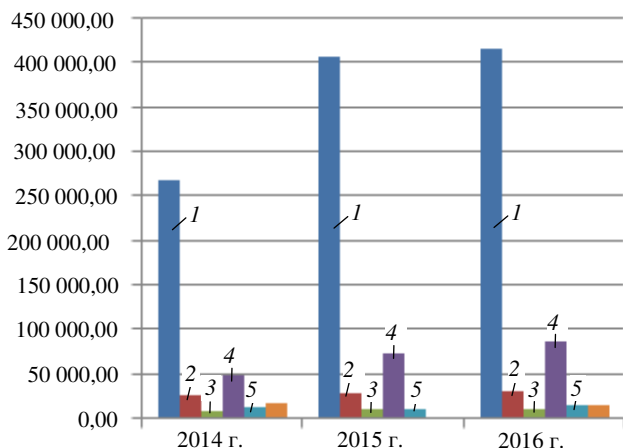


Рис. 2. Динамика затрат на выработку электроэнергии РУП «Облэнерго», тыс. руб.:
 1 – материальные затраты; 2 – затраты на оплату труда; 3 – отчисления на социальные нужды; 4 – амортизация ОС и НА; 5 – прочие затраты

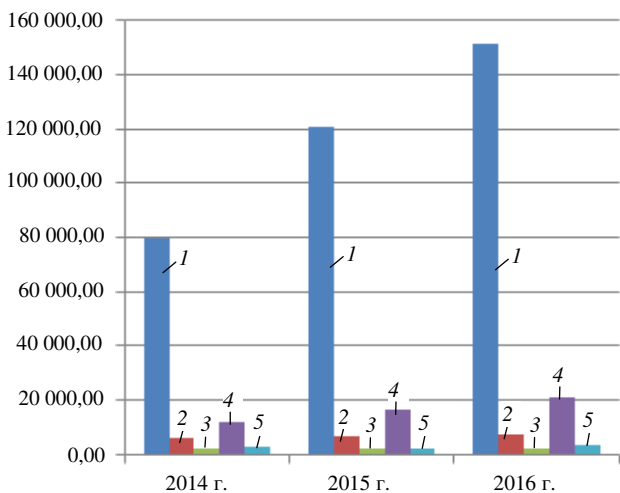


Рис. 3. Динамика затрат на отпуск тепловой энергии РУП «Облэнерго», тыс. руб.:
 1 – материальные затраты; 2 – затраты на оплату труда; 3 – отчисления на социальные нужды; 4 – амортизация ОС и НА; 5 – прочие затраты

Изучив динамику затрат на выработку электроэнергии РУП «Облэнерго», можно сказать что материальные затраты в 2016 г. значительно увеличились по сравнению с 2014 г. Перерасход наблюдается

практически по всем показателям за все три года, кроме прочих затрат и покупной энергии.

В структуре затрат на отпуск тепловой энергии наибольшую долю так же, как и в структуре затрат на выработку электроэнергии, составляют материальные затраты (около 80 %). На рис. 3 рассмотрим динамику затрат на отпуск тепловой энергии РУП «Облэнерго».

Анализируя рис. 3, можно сделать выводы о том, что наблюдается перерасход по всем статьям затрат, кроме прочих затрат. Однако в 2015 г. отпуск тепловой энергии был ниже по сравнению с 2014 г., а затраты продолжили увеличиваться, что является негативным моментом. В настоящее время раздельный учет затрат в энергетике Республики Беларусь осуществляется по следующим видам деятельности: производство электроэнергии; передача электроэнергии; распределение электроэнергии; производство теплоэнергии; передача и распределение теплоэнергии (таблица).

Разделение технологических стадий при выработке электро- и тепловой энергии на текущий момент

Статья затрат	Электроэнергия, удельный вес, %			Тепловая энергия, удельный вес, %	
	Производство	Передача	Распределение	Производство	Передача и распределение
Материальные затраты	84,2	8,7	17,9	85,0	67,2
Затраты на оплату труда	1,4	13,7	33,8	3,8	4,7
Отчисления на социальные нужды	0,5	4,6	11,6	1,2	2,0
Амортизация основных средств и нематериальных активов	13,1	50,9	26,4	8,6	22,8
Прочие затраты	0,8	22,1	10,3	1,4	3,3
ИТОГО	100,0	100,0	100,0	100,0	100,0

По данным таблицы видно, как меняется структура затрат по разным технологическим стадиям. Если на передачу электрической энергии наибольший удельный вес занимает амортизация (50,9 %), то на ее производство – материальные затраты (84,2 %), в частности стоимость условного топлива, а на распределение – затраты на оплату труда (33,8 %) и амортизация (26,4 %).

Если же рассмотреть структуру затрат по разным технологическим стадиям по отпуску теплоэнергии, то можно сделать следующие выводы: наибольший удельный вес как по производству теплоэнергии,

так и по передаче и распределению занимают материальные затраты (85,0 и 67,2 % соответственно). Но в структуре материальных затрат на производство наибольший удельный вес занимают затраты на топливо на технологические цели (96,2 %), а по передаче и распределению – затраты на транспортировку тепловой энергии по сетям других юридических лиц (74,2 %).

Общая сумма затрат на производство может измениться из-за объема производства; структуры продукции; уровня переменных затрат на единицу продукции каждого вида; общей суммы постоянных затрат. Таким образом, менеджерам необходимо активнее признавать значение фактора затрат и управления ими. Система управления затратами на предприятиях энергетики должна способствовать повышению эффективности предприятия и его конкурентоспособности за счет более рационального использования ресурсов и возможности постоянного снижения себестоимости.

Для повышения эффективности и конкурентоспособности энергетического предприятия необходима информация, которая должна обладать определенными свойствами и качественными характеристиками. Для этих целей на энергетических предприятиях Республики Беларусь необходимо провести реструктуризацию организации на соответствующие центры ответственности и места возникновения затрат. Деление предприятия на центры ответственности зависит от особенностей технологии и организации производственных процессов, методов управления производством, состава продукции или выполненных работ (услуг), уровня технической оснащенности производства и обеспеченности квалифицированным кадровым персоналом. Можно формировать следующие центры ответственности: центр затрат; центр доходов; центр прибыли; центр инвестиций [3].

С учетом специфики энергетических предприятий, а также по уровню полномочий руководителей подразделений в рамках существующей организационной структуры можно выделить на ТЭЦ следующие центры ответственности:

- центры затрат: цеха основного производства (топливно-транспортный цех, химический цех, котельный цех, турбинный цех электрический цех); цеха вспомогательного производства (механический цех, ремонтно-строительный цех, цех (или лаборатория) тепловой автоматики и измерений, электроремонтная мастерская);
- центры доходов: бухгалтерия, финансовый отдел, планово-экономический отдел, производственно-технический отдел [5].

Благодаря спецификации делегирования полномочий подразделению, собственно и определяющих его статус как центра ответственности, любые отклонения от плановых показателей будут фиксироваться не только по месту возникновения, но и по ответственному лицу (подразделению). Полученная информация о затратах и их отклонениях будет способствовать принятию оперативных, тактических и стратегических решений, для регулирования хозяйственных процессов, изыскания внутренних резервов и повышению эффективности деятельности предприятия энергетических предприятий Республики Беларусь.

Библиографический список

1. Государственная программа «Энергосбережение» на 2016–2020 годы (утв. Постановлением Совета министров Республики Беларусь 28 марта 2016 г., № 248) [Электронный ресурс]. – URL: http://www.economy.gov.by/ru/gp_energ-ru (дата обращения: 05.10.2017).

2. Энергетический баланс Республики Беларусь, 2017 [Электронный ресурс]. – URL: http://www.belstat.gov.by/ofitsialnaya-statistika/realny-sector-ekonomiki/energeticheskaya-statistika/statisticheskie-izdaniya/index_7869/ (дата обращения: 05.10.2017).

3. Глазов М.М. Управление затратами: новые подходы: монография. – СПб: Изд-во РГГМУ, 2009. – 169 с.

4. Иванов В.В., Хан О.К. Управленческий учет для эффективного менеджмента. – М.: ИНФРА-М, 2012. – 208 с.

5. Ламакин Г.Н. Основы менеджмента в электроэнергетике: учеб. пособие. Ч.1. – 1-е изд. – Тверь: Изд-во ТГТУ, 2006. – 208 с.

6. Управление затратами предприятия / В.Г. Лебедев, Т.Г. Дроздова, В.П. Кустарев, А.Н. Асаул, Т.А. Фомина. – СПб.: Изд. дом «Бизнес-пресса», 2003. – С. 16–17.

Сведения об авторе

Самосюк Наталья Александровна – магистр экономических наук, старший преподаватель Белорусского национального технического университета, Минск, Республика Беларусь, e-mail: Tasha712@tut.by

About the author

Samasiuk Natallia Aleksandrovna – Master of economics, teacher Belarusian National Technical University, Minsk, Republic of Belarus, e-mail: Tasha712@tut.by

Секция 4

**ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

ПРИМЕНЕНИЕ CRYPTOAPI ДЛЯ ШИФРОВАНИЯ НА ЯЗЫКЕ C#

К.А. Батуев, А.И. Тур, А.Н. Кокоулин
Пермский национальный исследовательский
политехнический университет, Пермь

В связи с постоянным развитием информационных технологий весьма актуальной продолжает оставаться проблема обеспечения информационной безопасности компьютерных систем и сетей. Основными видами нарушений защищенности информации в таких системах являются неправомерный доступ к конфиденциальной информации и несанкционированное изменение, подмена, уничтожение важной информации. Одним из наиболее эффективных механизмов защиты является использование современных криптографических средств. Благодаря CryptoAPI имеется возможность самостоятельной реализации такой защиты.

Ключевые слова: CryptoAPI, информационная безопасность, Windows.

APPLICATION OF CRYPTOAPI FOR ENCIIPHERING IN THE C#

K.A. Batuyev, A.I. Tur, A.N. Kokoulin
Perm National Research Polytechnic University, Perm

Due to the constant information technology development of very relevant the problem of ensuring information security of computer systems and networks continues to remain. Main types of violations of security of information in such systems are illegal access to confidential information and unauthorized change, substitution, destruction of important information. One of the most effective mechanisms of protection is use of modern cryptographic means. CryptoAPI is a possibility of independent realization of such protection.

Keywords: CryptoAPI, Information Security, Windows.

Цель работы – изучить применение CryptoAPI на языке программирования C# и реализация приложения, использующего алгоритмы шифрования криптопровайдеров, входящих в состав Windows.

CryptoAPI – это интерфейс программирования приложений, который обеспечивает разработчиков Windows-приложений стандартным набором функций для работы с криптопровайдером. Он поддерживает работу с асимметричными и симметричными ключами, т.е. позволяет шифровать и расшифровывать данные, а также работать с электронными сертификатами. Набор поддерживаемых криптографических алгоритмов зависит от конкретного криптопровайдера [1].

Реализация всех алгоритмов (шифрования, цифровой подписи и т.п.) полностью выведена из состава самого Crypto API и реализуется в отдельных независимых динамических библиотеках – «криптопровайдерах» (Cryptographic Service Provider – CSP). Сам же Crypto API просто предъявляет определенные требования к набору функций (интерфейсу) криптопровайдера и предоставляет конечному пользователю интерфейс работы с CSP [2].

Класс AesCryptoServiceProvider представляет реализацию криптоалгоритма блочного симметричного шифрования AES с помощью криптографического интерфейса приложений Windows (CryptoAPI), функции которого обеспечивают доступ приложений к ресурсам криптопровайдеров Windows. Конструктор, вызываемый при создании объектов этого класса, параметров не содержит. Если значение длины секретного ключа не равно одному из трех допустимых значений (128, 192 или 256 бит), то генерируется исключение PlatformNotSupportedException.

Класс AesManaged представляет реализацию алгоритма симметричного шифрования AES в управляемом коде. Его конструктор не содержит параметров. При использовании объектов этого класса могут возникать исключения классов CryptographicException и InvalidOperationException (если данный класс не поддерживается платформой .Net в компьютерной системе пользователя).

Класс DESCryptoServiceProvider представляет реализацию криптоалгоритма блочного симметричного шифрования DES с помощью CryptoAPI. Конструктор этого класса не содержит параметров. Длина блока, ключа и обратной связи устанавливается в 64 бита. Если криптопровайдер не поддерживает алгоритм DES, то генерируется исключение класса CryptographicException.

Класс RC2CryptoServiceProvider представляет реализацию криптоалгоритма блочного симметричного шифрования RC2 с помощью CryptoAPI. Его конструктор не содержит параметров. Поддерживаются ключи длиной от 40 до 128 бит с шагом 8 бит. При использовании объектов этого класса могут возникать исключения классов CryptographicException и InvalidOperationException.

Класс RijndaelManaged содержит реализацию в управляемом коде алгоритма блочного симметричного шифрования Rijndael (оригинального варианта криптоалгоритма AES). Конструктор класса параметров не содержит. При использовании объектов этого класса возможна генерация исключения InvalidOperationException.

Класс `TripleDESCryptoServiceProvider` содержит реализацию криптоалгоритма блочного симметричного шифрования `TripleDES` («тройного» `DES`) с помощью `CryptoAPI`. Конструктор класса параметров не содержит. Значения длины ключа, длины блока и длины обратной связи устанавливаются соответственно в 192, 64 и 64 бита. Если криптопровайдер не поддерживает алгоритм `TripleDES`, то генерируется исключение класса `CryptographicException`.

Класс `DSACryptoServiceProvider` содержит свойства и методы для вычисления и проверки электронной цифровой подписи (ЭЦП). Этот класс имеет конструктор без параметров и конструкторы с параметрами:

- 1) `CspParameters parameters` (создание объекта с заданными параметрами для криптопровайдера);
- 2) `int dwKeySize` (создание объекта с ключом заданной длины);
- 3) `int dwKeySize, CspParameters parameters` (создание объекта с ключом заданной длины и заданными параметрами для криптопровайдера).

Класс `RSACryptoServiceProvider` имеет конструктор без параметров, создающий объект с парой ключей по умолчанию для используемого криптопровайдера или с новой случайной парой ключей. Данный объект будет предназначен для обмена секретными ключами симметричного шифрования. Другие конструкторы данного класса имеют параметры:

- `CspParameters parameters` – создание объекта с указанными параметрами, передаваемыми криптопровайдеру;
- `int dwKeySize` – создание объекта с парой ключей по умолчанию (если она существует) или новой случайной парой ключей заданной длины, предназначенной для обмена ключами симметричного шифрования;
- `int dwKeySize, CspParameters parameters` – создание объекта с парой ключей длины `dwKeySize` бит и параметрами для криптопровайдера `parameters`.

При шифровании и расшифровании файлов в приложениях для платформы `.Net` применяются классы `FileStream` и `CryptoStream` [3, 4].

Основываясь на вышеназванной информации, было создано приложение на языке `C#`, содержащее 4 формы. В первой форме было реализовано шифрование файла по алгоритмам `DES`, `RC2`, `TripleDES` на ключе, генерируемом из парольной фразы, имеющей длину не ме-

нее 8 знаков (рис. 1). При генерации ключа будет также использована случайная примесь длиной 8 байт, которая сохраняется в начале зашифрованного файла.

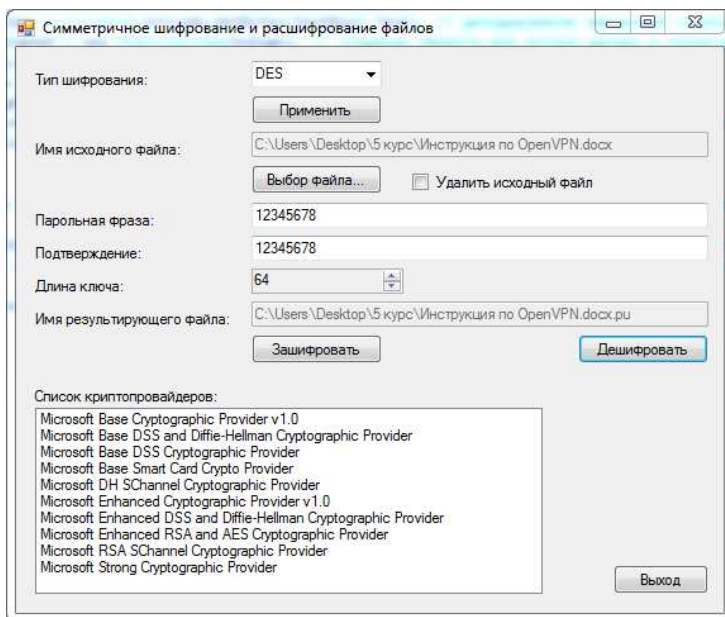


Рис. 1. Шифрование файлов на парольной фразе

Основным методом класса `OpenFileDialog` является `DialogResult ShowDialog()` – отображение диалогового окна и возвращение значения `DialogResult.OK`, если пользователь подтвердил выбор файла.

Класс `Encoding` из пространства имен `System.Text` используется для кодирования и декодирования текстовых строк.

Для вывода сообщений в программе используется класс `MessageBox` из пространства имен `System, Windows, Forms` и его статический метод `DialogResult Show (string text, string caption, MessageBoxButtons buttons, MessageBoxIcon icon)` – вывод сообщения с текстом `text` в окне с заголовком `caption`, кнопками `buttons` и пиктограммой `icon`.

Для получения пути к текущей папке в программе используется статический метод `string GetCurrentDirectory()` класса `Directory` из пространства имен `System.IO`.

Для удаления файла используется статический метод `void Delete(string path)` класса `File` из пространства имен `System. IO` (`path` – полный путь к удаляемому файлу).

Во второй форме – шифрование и расшифрование по алгоритму AES в режиме сцепления блоков шифра на случайно генерируемом секретном ключе введенного пользователем сообщения, длина которого не больше 20 символов (рис. 2).

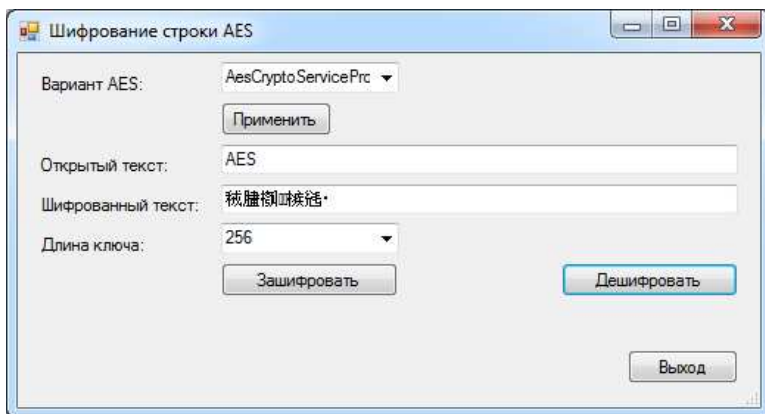


Рис. 2. Шифрование и расшифрование введенного сообщения

Здесь для работы с потоком данных в оперативной памяти в программе используется класс `MemoryStream` из пространства имен `System. IO`, имеющий конструктор без параметров и конструктор с параметром типа `byte[]`, который задает массив байт, связываемый с потоком данных в оперативной памяти. Метод `byte[] ToArray()` этого класса позволяет получить данные из потока в оперативной памяти.

Для кодирования шифротекста перед его отображением в окне используется метод класса `Encoding string GetString(byte[] bytes, int index, int count)`, позволяющий получить строку символов, соответствующую данным длиной `count` байт из массива `bytes`, начиная с элемента `index`.

В третьей форме была составлена программа вычисления и проверки электронной цифровой подписи по алгоритму DSA (рис. 3) для данных из выбираемого пользователем файла с сохранением ЭЦП и открытого ключа, необходимого для проверки подписи, в отдельных файлах в той же папке, что и исходный подписываемый файл.

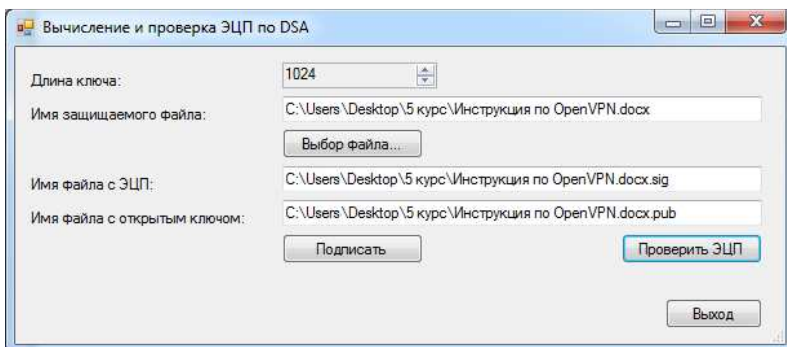


Рис. 3. Окно программы вычисления и проверки ЭЦП для файла

В программе использовался класс File из пространства имен System. IO, содержащий статические методы для действий с файлами, и один из таких методов bool Exists(string path) – проверка существования файла с полным именем path.

В четвертой форме – получение и проверка ЭЦП под сообщениями с помощью криптоалгоритм RSA (рис. 4).



Рис. 4. Окно программы для подписания сообщения

Использование стандартного набора функций для работы с криптопровайдерами позволило нам написать приложение, которое позволяет использовать симметричное и асимметричное шифрование, а также подписывать и проверять файлы и сообщения.

Библиографический список

1. Хабрахабр [Электронный ресурс] // CryptoApi и Криптопровайдер VipNet CSP. – URL: <https://habrahabr.ru/sandbox/22763/> (дата обращения: 19.11.2017).

2. MSDN [Электронный ресурс] // Пространство имен System.Security.Cryptography. – URL: [https://msdn.microsoft.com/ru-ru/library/system.security.cryptography\(v=vs.110\).aspx](https://msdn.microsoft.com/ru-ru/library/system.security.cryptography(v=vs.110).aspx) (дата обращения: 19.11.2017).

3. MSDN [Электронный ресурс] // Службы криптографии. – URL: [https://msdn.microsoft.com/ru-ru/library/92f9ye3s\(v=vs.110\).aspx](https://msdn.microsoft.com/ru-ru/library/92f9ye3s(v=vs.110).aspx) (дата обращения: 19.11.2017).

4. MSDN [Электронный ресурс] // Walkthrough: Creating a Cryptographic Application. – URL: [https://msdn.microsoft.com/ru-ru/library/bb397867\(v=vs.110\).aspx](https://msdn.microsoft.com/ru-ru/library/bb397867(v=vs.110).aspx) (дата обращения: 19.11.2017).

Сведения об авторах

Батуев Кирилл Александрович – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: batuev_kirill@mail.ru

Тур Александр Игоревич – аспирант Пермского национального исследовательского политехнического университета, Пермь, e-mail: tur.aleksandr93@mail.ru

Кокоулин Андрей Николаевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: liga_asu@mail.ru

About the authors

Batuev Kirill Aleksandrovich – Student Perm National Research Polytechnic University, e-mail: batuev_kirill@mail.ru

Tur Aleksandr Igorevich – Graduate Student Perm National Research Polytechnic University, e-mail: tur.aleksandr93@mail.ru

Kokoulin Andrey Nikolayevich – Ph.D. in Technical Sciences, Associate Professor of the department "Automation and telemechanics" Perm National Research Polytechnic University, Perm, e-mail: liga_asu@mail.ru

ОБЗОР ПРОГРАММНЫХ СРЕДСТВ ЗАЩИЩЕННОГО ХРАНЕНИЯ АУТЕНТИФИКАЦИОННЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ

И.А. Белый

Южный федеральный университет, Таганрог

Защищенность учетных записей пользователей во многом зависит от надежности формируемых паролей и используемых способов их защищенного хранения. В рамках студенческой исследовательской работы проводится разработка собственного менеджера паролей. В качестве первого этапа был проведен обзор современных программных менеджеров паролей и выделены основные функциональные свойства менеджеров паролей, которые лягут в основу разрабатываемого программного обеспечения.

Ключевые слова: менеджер паролей, аутентификация пользователей, защищенное хранение данных, мастер-пароль, генерация стойких паролей, KeePass.

PROTECTED STORAGE SOFTWARE FOR AUTHENTICATION USER'S DATA

I.A. Belyi

South Federal University, Taganrog

The security of user accounts largely depends on the reliability of the generated passwords and the methods used for their secure storage. Within the framework of student research work, I am developing my own password manager. As the first stage, a review was conducted of modern software password managers and identified the main functional properties of password managers that will form the basis of the developing software.

Keywords: password manager, user authentication, secure data storage, master password, generation of strong passwords, KeePass.

Защита аккаунтов пользователя зависит от надежности сформированных паролей учетных записей. Опираясь на аналитические исследования Positive Technologies [1], можно сделать вывод, что пользователи зачастую формируют слабые пароли (состоящие только из цифр или подходящие для перебора по словарям) по причине легкой запоминаемости (рис. 1).

При генерации паролей многие пользователи задают один тот же пароль (ограниченный набор паролей) на различные учетные записи либо сохраняют их в открытом виде на жестком диске. Данные

способы работы с паролем являются ненадежными и способствуют компрометации аккаунтов пользователей. Более надежным способом хранения паролей служит запись их в защищенное хранилище браузеров, но при этом усложняются редактирование, сортировка и доступ к учетным данным. Одним из самых надежных и удобных способов работы с паролями является использование менеджеров паролей, которому посвящена данная статья.

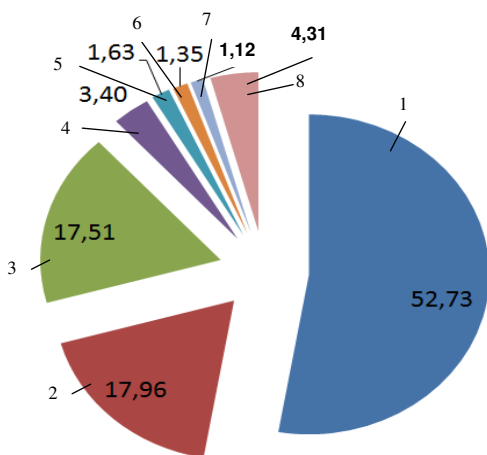


Рис. 1. Аналитика использования символов пользователями при формировании пароля: 1 – только цифры (numeric); 2 – символы английского алфавита в нижнем регистре (loweralpha); 3 – символы английского алфавита в нижнем регистре и цифры (loweralphanumeric); 4 – символы английского алфавита в разных регистрах и цифры (mixalphanumeric); 5 – символы английского алфавита в разных регистрах (mixalpha); 6 – символы английского алфавита в верхнем регистре и цифры (alpha-numeric); 7 – символы русского алфавита в нижнем регистре (loweralpha-rus); 8 – прочие наборы

В первую очередь следует выделить наиболее распространенные на сегодняшний день менеджеры паролей [2], в рамках работы были выбраны следующие программы:

- KeePass Password Safe (<https://keepass.info/>).
- SafeInCloud Password Manager (<https://www.safe-in-cloud.com/ru/>).
- True Key (<https://www.truekey.com/ru/>).
- Avira Password Manager (<https://www.avira.com/ru/avira-password-manager>).
- Trend Micro Password Manager (https://www.trendmicro.com/en_us/forHome/products/password-manager.html).

- LastPass Password Manager (<https://www.lastpass.com/ru>).
- Sticky Password (<https://www.stickypassword.com/ru/>).
- Dashlane (<https://www.dashlane.com/>).
- F-Secure KEY (https://www.f-secure.com/ru_RU/web/home_ru/products).
- Norton Identity Safe (<https://identitysafe.norton.com/>).
- Enpass (<https://www.enpass.io/>).
- Kaspersky Password Manager (<https://www.kaspersky.ru/password-manager>).
- RoboForm Everywhere (<https://www.roboform.com/ru/everywhere>).
- Splikity (<https://splikity.com/>).

После проведенного анализа удобства и надежности работы менеджеров паролей было принято решение взять за функциональную основу характеристики приложения KeePass [3]. В данном приложении есть множество возможностей безопасно хранить свои пароли, создавая базы данных учетных записей. Помимо всего прочего есть функционал по созданию собственного генератора паролей, который также можно обезопасить паролем. Данный генератор паролей способен присваивать один пароль множеству записей, только этот пароль будет перемешан и все символы для каждой записи будут составлены случайным образом. Это очень удобное свойство, когда речь идет о том, что пользователь не помнит, каким именно паролем защитил данные в хранилище менеджера KeePass.

Рабочий интерфейс KeePass приведен на рис. 2. Рассмотрим особенности работы с мастер-паролем для самой базы данных KeePass [4]. Мастер-пароль является главным для самой базы данных в менеджере паролей, и знание пользователем этого пароля открывает доступ к самим записям внутри базы данных. Проще говоря, знание такого пароля открывает пользователю способность прочесть все хранимые пароли. Мастер-пароль не сохраняется на устройстве (съёмном носителе) и известен только хозяину базы данных паролей.

Для защиты базы паролей пользователей в менеджерах паролей используются стойкие криптографические алгоритмы, например, Advanced Encryption Standard (AES) с 128 или 256-битным ключом, ГОСТ Р 34.12-2015 (алгоритмы «Магма» и «Кузнецик»), PRESENT и т.д. В случае работы с менеджером паролей KeePass разработчиками предусмотрено использование шифра AES-256. В этом случае защита 256-битного ключа, который необходим для расшифровки паролей, – это ключевой момент безопасности менеджера паролей. Если

злоумышленник узнает этот ключ, то легко взломает всё хранилище независимо от сложности алгоритма шифрования. Поэтому защита ключа шифрования основана на следующих базовых принципах:

- доступ к ключу шифрования блокируется мастер-паролем, который нигде не хранится;
- ключ шифрования не должен быть математически связан с мастер-паролем.

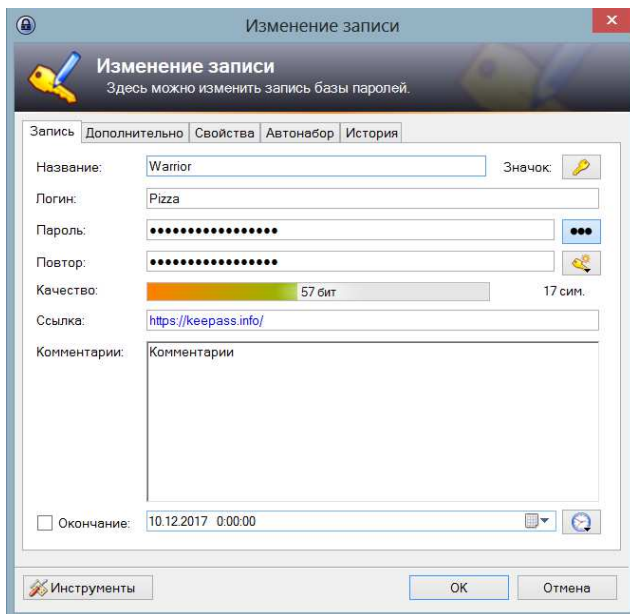


Рис. 2. Интерфейс программы KeePass

В разрабатываемом менеджере паролей были учтены эти аспекты, связанные с безопасностью мастер-паролей, и дополнительно функция сброса мастер-пароля (без понижения уровня доверия к надежности менеджера паролей). Если мастер-пароль просто удалять и создавать новый (с перешифрованием базы), то даже самый неквалифицированный пользователь сможет получить несанкционированный доступ к базе данных, создав новый мастер пароль. Поэтому были выделены способы реализации смены пароля на случай утери мастер-пароля:

- 1) создание самим пользователем при внесении мастера пароля в учетную запись подсказок (ассоциаций) для напоминания;
- 2) создание пароля для сброса мастер-пароля;

3) занесение мастер пароля в зашифрованный файл и привязка его к самой базе данных;

4) создание резервных копий на другой базе данных и в случае утери основного возможно удаление сохраненных паролей и использование резервной копии.

Также полезным свойством в разрабатываемом менеджере паролей будет такая функция, как привязка к определенным сайтам самих учетных записей, хранящихся в менеджере, т.е. при открытии сайта, например «ВКонтакте», пароль и логин вводятся автоматически в веб-форму сайта, и пользователь моментально авторизуется. Однако пароли могут быть скомпрометированы в случае открытой передачи их по сети на сервер, поэтому стоит устанавливать способ автоматического входа в учетную запись только для доверенных сайтов (поддерживающих протоколы шифрования канала передачи, Hyper-Text Transfer Protocol Secure, https).

Каким бы безопасным ни был используемый менеджер паролей, его популярность зависит от того, насколько просто им пользоваться [5]. Напомним, что популярный менеджер паролей KeePass даже в сумме используют не более 1 процента пользователей Интернета.

Наиболее часто пользователи сохраняют пароли в браузере [6]. При хранении логинов и паролей в хранилище браузера получить доступ к списку своих паролей не так уж и просто. Доступ к ним осуществляется через «Настройки» (следует перейти в «Дополнительные настройки» и найти «Управления паролями»). Таким образом, можно получить доступ к примитивному списку зарегистрированных аккаунтов, которые нельзя отсортировать по логину, а также нельзя добавить к ним текстовое примечание или отредактировать.

Важным критерием безопасности при создании менеджера паролей являются знания самих злоумышленников, т.е. разрабатываемая система безопасности паролей должна соответствовать принципу Керкгоффа. Согласно данному принципу криптосистема должна оставаться безопасной даже в том случае, когда злоумышленнику известно всё, кроме значений применяемых секретных ключей.

Были сформированы следующие требования к разрабатываемому программному обеспечению менеджера паролей:

- Итоговый продукт: Windows-приложение.
- Поддержка алгоритма создания стойких паролей.
- Поддержка многопользовательского режима для Windows-приложения (нескольких отдельных хранилищ паролей).

- Приложение не должно опираться на сторонние библиотеки (кроме стандартных библиотек ОС) и служебные программы.
- Хранилище паролей должно быть переносимым.
- Хранилище паролей должно быть зашифровано (в режиме контроля целостности).
- Пароли учетных записей должны быть зашифрованы внутри хранилища.
- Расшифровка пароля учетной записи происходит только по запросу.
- Контроль использования буфера обмена при работе с данными.
- Структура учетной записи в хранилище: «Имя учетной записи», «URL-адрес учетной записи», «Идентификатор имени пользователя», «Пароль проверки подлинности» (зашифрованное значение).
- (Опционально) Внесение данных из защищенного хранилища в веб-формы при аутентификации (плагин для браузера).

Библиографический список

1. Евтеев Д. Анализ проблем парольной защиты в российских компаниях. – URL: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-Metrics-Passwords-2009.pdf>
2. Менеджеры паролей – краткий обзор. – URL: <https://habrahabr.ru/post/225053/>
3. Официальная страница KeePass «KeePass Password Safe». – URL: <https://keepass.info/>
4. Security. Detailed information on the security of KeePass. – URL: <https://keepass.info/help/base/security.html>
5. Как пользователи воспринимают разные методы аутентификации. – URL: <https://habrahabr.ru/post/344406/>
6. «Как мы создавали менеджер паролей со стойкой криптографией и мастер-паролем. Опыт команды Яндекс.Браузера». – URL: <https://habrahabr.ru/company/yandex/blog/344382/>

Сведения об авторе

Белый Илья Андреевич – студент Южного федерального университета, Таганрог, e-mail: beliinikita.2015@yandex.ru

About the author

Beliy Ilya Andreevich – Student South Federal University, Taganrog, e-mail: beliinikita.2015@yandex.ru

МЕТОДЫ И АЛГОРИТМЫ НАДЕЖНОГО УДАЛЕНИЯ ДАННЫХ С ФИЗИЧЕСКИХ НОСИТЕЛЕЙ

Д.А. Бурылов, А.Н. Кокоулин

Пермский национальный исследовательский
политехнический университет, Пермь

Рассмотрены основные методы и алгоритмы удаления данных с цифровых носителей. Проанализированы нормативная база Российской Федерации и рекомендации стандартов других стран. Проведено исследование удаления информации разными методами и алгоритмами. Выявлены закономерности для разных видов устройств хранения. Выявлены некоторые уязвимости, связанные с особенностями работы твердотельных накопителей.

Ключевые слова: алгоритмы; удаление; затирание; носители информации.

METHODS AND ALGORITHMS OF RELIABLE DELETION OF DATA FROM PHYSICAL CARRIERS

D.A. Burylov, A.N. Kokoulin

Perm National Research Polytechnic University, Perm

In this article, the main methods and algorithms for data deletion from digital media are considered. The regulatory framework of the Russian Federation and the recommendations of the standards of other countries are analyzed. The study of information removal by different methods and algorithms is carried out. The patterns for different types of storage devices are revealed. Some vulnerabilities associated with the features of the operation of solid state drives have been revealed.

Keywords: algorithms; removal; mashing; information carriers.

Сейчас все больше и больше места занимает электронный документооборот. В связи с этим возникает вопрос безопасного уничтожения информации, а особенно остро он встает, если речь идет об информации ограниченного доступа.

В исследовании рассматривается уничтожение информации с физических цифровых носителей информации. В организациях такие носители часто называются отчуждаемыми носителями информации. Такие носители могут быть как частью оборудования, используемого непосредственно для обработки информации, так и отчуждаемыми в прямом смысле слова, т.е. использоваться для переноса информации. После того как информацию перенесли, она вновь сохраняется уже на носитель, на котором будет обрабатываться.

Немаловажен и вопрос носителей, которые вышли из строя или их срок службы закончен и их необходимо вывести из работы.

Объектом исследования можно назвать электронные носители информации.

Предметом исследования будут методы и алгоритмы надежного удаления информации ограниченного доступа с физических носителей в коммерческих организациях.

Проблема исследования заключается в выборе наиболее эффективного алгоритма для разных типов накопителей.

Актуальность этой темы обусловлена тем, что современные организации так или иначе используют систему электронного документооборота (СЭД), а следовательно, используют устройства хранения данных. В условиях предприятия могут возникать ситуации, когда передача документов от одного компьютера к другому невозможна без применения переносного устройства хранения информации. Чаще всего это бывают Flash-карты памяти. Возникают и ситуации, когда необходимо вывести из эксплуатации средства хранения информации, такие как жесткие диски разных типов. С точки зрения безопасности использование устройств хранения информации для переноса – это возникновение целого ряда новых угроз безопасности информации.

Анализ проблемы с точки зрения требований государственной политики РФ показывает, что существует неопределенность в законах. В России существует 3 документа, в которых определяется необходимость очистки памяти:

– В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» определяется, что очистка внешней памяти при ее освобождении должна производиться путем записи в нее маскирующей информации. Количество и содержание проходов не уточняются [1];

– РД ФСТЭК «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» определяет, что СЗИ НСД, сертифицированные по 3-му классу защищенности, должны производить очистку внешней памяти путем записи в нее маскирующей информации. Количество и содержание проходов также не уточняются [2];

– РД ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» определяет, что в автоматизированных системах, аттестованных по классам защищенности 3А, 2А, 1А, 1Б, 1В и 1Г, должна производиться очистка внешней памяти путем двукратной произвольной записи. Содержание проходов не уточняется [3].

В этой области также имеются стандарты других стран, описывающие основные стандарты удаления:

- Dod 5220.22M (США);
- NAVSO P-5239-26 (США);
- VSITR (Германия).

В качестве практической части исследования было произведено рассмотрение разных вариантов удаления информации с HDD и Flash-накопителя. В качестве исследуемых объектов будем использовать flash-накопитель объемом 4 Гб и интерфейсом подключения USB 2.0, локальный том на HDD диске объемом 100 Мб. Flash-накопитель имеет файловую систему FAT32 и размер единицы распределения 16 Кб. Вторым этапом попытаемся восстановить информацию с тома HDD жесткого диска. Том имеет файловую систему NTFS с размером единицы распределения 32 Кб. Принципы работы файловых систем были взяты из [4].

Форматирование производилось средствами проводника операционной системы (ОС) Windows 10. Утилитами для надежного удаления будут выступать: Ccleaner, Eraser. Для проверки результатов использовались утилиты восстановления утраченных файлов Recuva и Hetman Partition Recovery поочередно.

Путем многократного проведения эксперимента для Flash-накопителя с разными условиями было выяснено, что форматирование Flash-накопителя без установленной галочки «Быстрое форматирование» достаточно, чтобы удалить файлы без возможности восстановления простыми бесплатными утилитами. Установлено, что быстрое форматирование с изменением величины единицы распределения на значение больше того, которое было изначально, также удаляет файл без последующей возможности восстановления простыми программами. При форматировании с изменением единицы блока

распределения на величину меньше исходной файл восстанавливается без потерь, но с искаженным именем. Возможно, это объясняется тем, что в случае, когда блок становится больше, к полезной информации добавляется мусор, который дополняет блок до конца, и программа не может выделить полезную информацию среди мусора. Было выяснено, что затирание всего свободного пространства и затирание лишь используемого пространства дают одинаковый эффект – файл не найден. Способ форматирования с изменением размера единицы распределения наиболее подходит для использования с Flash-носителями, так как в этом случае мы не перезаписываем весь накопитель, а изменяем лишь его таблицу размещения, что позволяет продлить его срок службы.

Для HDD жестких дисков с файловой системой NTFS утилиты не находят файл уже после быстрого форматирования. Но, как мы видим, имеет место аналогичная ситуация при изменении размера единицы распределения.

Также выявляется такая особенность, при которой после того как файл был удален в проводнике и мы затираем свободное место на жестком диске, файл восстанавливается, и утилита восстановления помечает данный файл, как «Не удален», но при этом его название изменяется. После того как мы указываем на конкретный файл, и утилита затирает только то место, где хранится файл, в этом случае восстановления файла не происходит.

Из всего этого можно сделать вывод, что должны применяться разные методы и алгоритмы надежного удаления для разных типов устройств хранения. То, что подходит для одного, не всегда подходит для другого. Также нужно брать в расчет срок службы устройств, ведь частое изменение состояния памяти может плохо повлиять на работоспособность.

Анализ проблемы bad blocks или «плохих блоков» для отчуждаемых Flash-носителей показывает, что существует угроза, связанная со старением устройств или механическим воздействием на них. Старение или повреждения могут приводить к увеличению числа таких блоков с остаточной информацией в них. Вся полезная информация в таких блоках сохраняется в них, так как к блоку невозможен доступ из-за его заголовка. Такая угроза актуальна для маленьких

файлов, которые могут целиком поместиться в один блок. В этом случае к злоумышленнику попадает находящаяся в блоке информация (например, текстовый документ целиком). Для тех файлов, которые не помещаются в один блок, такая угроза менее актуальна, так как часть файла, которая расположена в других блоках (неповрежденных), может быть удалена, и тогда утечка не представляется возможной. Значение объема памяти одного блока выбирается самим пользователем при форматировании (разметке) устройства хранения и может изменяться в любой момент.

Задачей администратора будет проверка списываемых носителей на наличие блоков с остаточной информацией и в случае, если таких блоков будет значительное количество, физическое уничтожение носителя. Только физическим уничтожением возможно полное и безвозвратное уничтожение данных с носителей. Методов и технологий физического разрушения носителей так же довольно большое количество.

Библиографический список

1. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (введ. 1996-01-01). – М.: Изд-во стандартов, 1995.

2. РД ФСТЭК «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» (введ. 1992-03-30): сб. руководящих докум. по защите информации от несанкционир. доступа. – М., 1998.

3. РД ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (введ. 1992-03-30): сб. руководящих докум. по защите информации от несанкционир. доступа. – М., 1998.

4. Гордеев А.В. Операционные системы: учебник для вузов. – 2-е изд. – СПб.: Питер, 2007. – 416 с.

5. Supriya Kulkarni Jisha Study of bad block management and wear leveling in nand flash memories // IJRET: International Journal of Research in Engineering and Technology.

Сведения об авторах

Бурьлов Дмитрий Анатольевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: burylov.dmitriy@gmail.com

Кокоулин Андрей Николаевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail:liga_asu@mail.ru

About the authors

Burylov Dmitry Anatolyevich – Student Perm National Research Polytechnic University, Perm, e-mail: burylov.dmitriy@gmail.com

Kokoulin Andrey Nikolayevich – Ph.D. in Technical Sciences, Associate Professor of the department "Automation and telemechanics" Perm National Research Polytechnic University, Perm, e-mail:liga_asu@mail.ru

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В ИНФРАСТРУКТУРЕ ОТКРЫТЫХ КЛЮЧЕЙ

П.Д. Веселицкая, Е.Л. Кротова

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье представлен анализ существующих технологий реализации инфраструктуры открытых ключей: удостоверяющие центры и сети доверия. Показаны их достоинства и недостатки. Также сделан обзор нового подхода к реализации, а именно технология *Certcoin*. Данная технология решает многие проблемы, присущие текущим *PKI*, такие как потребность в доверенной третьей стороне, централизация и ограниченная доступность.

Ключевые слова: инфраструктура открытого ключа, удостоверяющий центр, сети доверия, блокчейн, *Certoin*.

APPLICATION OF BLOKCHAIN TECHNOLOGY IN PKI

P.D. Veselitskaya, E.L. Krotova

Perm National Research Polytechnic University, Perm

This article presents an analysis of existing technologies for implementing the public key infrastructure: Certificate Authority and Webs of Trust. Their advantages and disadvantages are shown. Also reviewed is a new approach to implementation – *Certcoin*. This technology solves many of the problems inherent in current PKIs, such as the need for a trusted third party, centralization and limited availability.

Keywords: PKI, Certificate Authority, Webs of Trust, blockchain, *Certoin*.

Инфраструктура открытых ключей, *PKI* – набор средств (технических, материальных, людских и т.д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей [1]. В данной работе рассматриваются два подхода реализации: централизованные, сторонние удостоверяющие центры (УЦ) и децентрализованные сети доверия.

Удостоверяющий центр действует доверенной третьей стороной, которая отвечает за доставку и управление цифровыми сертификатами для сети пользователей. Для этого УЦ должен иметь процесс регистрации, в соответствии с которым удостоверяется личность пользователя, им присваивается уникальное имя (например, *Google* или *Facebook*), и их открытые ключи записываются вместе с их уникальным именем. Эти записи содержат дату истечения срока действия, а также указание цели ключа: шифрование данных или проверка под-

писи. УЦ выполняет две цели: упрощает проверку того, что пользователь имеет определенный открытый ключ, и облегчает поиск открытых ключей, соответствующих пользователям [1].

В сетях доверия аутентификация полностью децентрализована; пользователи могут обозначать других как заслуживающих доверия, подписывая их открытые ключи. Таким образом, пользователь накапливает сертификат, содержащий его открытый ключ и цифровые подписи от лиц, которые считают его заслуживающим доверия. Сертификат затем доверяется стороной, если они могут проверить, что сертификат содержит подпись того, кому он доверяет [2].

В таблице представлено сравнение реализаций *PKI*. У каждого вида реализации есть свои достоинства и недостатки. Исходя из того, что инфраструктура открытых ключей в данное время является достаточно распространённой, а существующие технологии не удовлетворяют всем необходимым требованиям безопасности, требуется создание альтернативного подхода к реализации.

Сравнение реализаций *PKI*

№	Параметр для сравнения	УЦ	Сети доверия
1	Централизация	+	–
2	Сложность добавления нового клиента	–	+
3	Возможность восстановления ключа	+	–
4	<i>Open Source</i>	–	+

Группа разработчиков из Массачусетского технологического института (МТИ, *Massachusetts Institute of Technology, MIT*) представила проект *Certcoin*. Это децентрализованная альтернативная инфраструктура открытого ключа, основанная на технологии блокчейн. Она предоставляет возможность публиковать открытый ключ, соответствующий данному идентификатору или домену, надежным, постоянным способом. *Certcoin* – это жизнеспособная *PKI*, способная заменить УЦ и *Webs of Trust*. Такая конструкция имеет преимущества – полностью децентрализованная архитектура, отказоустойчивость, избыточность и прозрачность. Несмотря на это, *Certcoin* поддерживает ожидаемые функции полнофункционального УЦ, включая создание сертификатов, аннулирование, сцепление (формирование цепочки) и восстановление. Доменные покупки и переводы осуществляются с помощью простых транзакций *Bitcoin* для стимулирования майнеров [2].

Разработчики выявили проблему необходимости хранения каждым пользователем всей цепочки блоков. Предлагается использовать криптографические аккумуляторы для хранения хранилища постоянного размера для аутентификации доменов [3].

Конструкция *Certcoin* имеет преимущества от полностью децентрализованной архитектуры, предлагающей присущую отказоустойчивость, избыточность и прозрачность, а также решает многие проблемы, присущие текущим *PKI*, такие как потребность в доверенной третьей стороне и ограниченная доступность.

Библиографический список

1. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. – М.: Горячая линия-Телеком, 2004.
2. Fromknecht C., Velicanu D., Yakoubov S. CertCoin: A NameCoin Based Decentralized Authentication System [Электронный ресурс]. – URL: <https://courses.csail.mit.edu/6.857/2014/files/19-fromknechtvelicann-yakoubov-certcoin.pdf> (дата обращения: 12.11.2017).
3. Nelly Fazio, Antonio Nicolosi. Cryptographic accumulators: Definitions, constructions and applications [Электронный ресурс]. – URL: <https://www.cs.stevens.edu/~nicolosi/tech-reports/FaNi03.pdf> (дата обращения: 12.11.2017).

Сведения об авторах

Веселицкая Полина Дмитриевна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: polyuch@gmail.com

Кротова Елена Львовна – кандидат физико-математических наук, доцент кафедры «Высшая математика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: lenkakrotova@yandex.ru

About the authors

Veselitskaya Polina Dmitrievna – Student Perm National Research Polytechnic University, Perm, e-mail: polyuch@gmail.com

Krotova Elena Lvovna – Ph.D. in Physic-Mathematic Sciences, Associate Professor of the department "Higher mathematics" Perm National Research Polytechnic University, Perm, e-mail: lenkakrotova@yandex.ru

МОДЕЛИРОВАНИЕ GRE OVER IPSEC VPN СЕТИ ПРЕДПРИЯТИЯ В СРЕДЕ CISCO PACKET TRACER

Е.А. Губарев

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассмотрено моделирование технологии VPN (Virtual Private Network), решающей проблему удаленного доступа корпоративной сети предприятия. Для создания частной виртуальной сети были выбраны протокол безопасности IPsec (Internet Protocol Security) и туннелирования GRE (Generic Routing Encapsulation). Зашифровав GRE с помощью IPsec, гарантируется безопасность данных и решается проблема масштабируемости VPN.

Ключевые слова: VPN, IPsec, GRE, корпоративная сеть.

SIMULATION GRE OVER IPSEC VPN ENTERPRISE NETWORK BASED ON CISCO PACKET TRACER

E.A. Gubarev

Perm National Research Polytechnic University, Perm

This article describes simulation VPN (Virtual Private Network) technology provides a solution of economic remote access for the enterprise. To create a virtual private network, were selected protocols, Internet Protocol Security (IPsec) and Generic Routing Encapsulation (GRE). By encrypting the GRE with IPsec, the data security is guaranteed and the problem of VPN scalability is solved.

Keywords: VPN, IPsec, GRE, enterprise network.

Информатизация предприятий является единственным способом их развития. Предприятия характеризуются большим масштабом, с более чем одним подразделением или филиалом. Возникает необходимость в обмене информацией между филиалами, часть из которой связана с коммерческой тайной предприятия. Если данные предприятия передавать через Интернет, то появляются вопросы по защите информации. Да, Интернет имеет преимущество в дешевизне, но это небезопасно. В то время как, напротив, арендуемая линия безопасна, но принесёт дополнительные затраты предприятию. Для обеспечения конфиденциальности и целостности обмена информацией между штаб-квартирой и подразделениями на предприятии появилась технология виртуальных частных сетей VPN. Она позволяет сделать стоимость подключения не такой высокой, как стоимость аренды линии.

VPN (Virtual Private Network) – это технология, которая использует публичную сеть для построения специальной частной сети. В основном VPN использует две технологии: технологию туннелирования и технологию безопасности. Примеры используемых технологий туннелирования: PPTP, L2TP, IPsec. Для обеспечения безопасности передачи данных следует использовать безопасные средства шифрования. Технологии безопасности включают в себя MPPE, IPsec и другие алгоритмы шифрования [1].

IPsec – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. IPsec включает в себя три главных протокола безопасности: Authentication Header (AH) обеспечивает целостность передаваемых данных, аутентификацию источника информации и функцию по предотвращению повторной передачи пакетов; Encapsulating Security Payload (ESP) обеспечивает шифрование передаваемой информации, ограничение потока конфиденциального трафика; Internet Security Association and Key Management Protocol (ISAKMP) – протокол, используемый для первичной настройки соединения, взаимной аутентификации конечными узлами друг друга и обмена секретными ключами. Также одним из ключевых понятий является Security Association (SA). По сути, SA является набором параметров, характеризующих соединение. IPsec может функционировать в двух режимах: транспортном и туннельном. В транспортном режиме шифруются только данные IP-пакета, исходный заголовок сохраняется. В туннельном режиме шифруется весь исходный IP-пакет: данные, заголовок, маршрутная информация, а затем он вставляется в поле данных нового пакета, т.е. происходит инкапсуляция [2].

Протокол туннелирования сетевых пакетов GRE позволяет инкапсулировать пакеты сетевого уровня модели OSI в IP-пакеты. Однако сам GRE-туннель не поддерживает шифрование данных. Для реализации шифрования передачи данных используется IPSec. GRE-туннель определяется IP-адресом источника и IP-адресом назначения на обоих концах туннеля, поддерживает различные протоколы маршрутизации, такие как RIP, OSPF, IGRP и т.д.

Преимущества сети VPN с поддержкой IPSec очевидны. IPSec VPN использует зашифрованный туннель для передачи информации

внутренней частной сети через открытую сеть, и в то же время он гарантирует безопасность внутренних данных.

Представим, что компания имеет главный офис в городе Москве, а филиал в городе Перми. Создадим VPN между структурами компании. Установив GRE-туннель, офисы смогут передавать информацию друг другу. Поскольку сам протокол GRE не может шифровать и упаковывать данные, мы настраиваем IPSec для защиты сообщения GRE.

Структура сети разделена на три части: сеть головного офиса в Москве, сеть Пермского филиала и Интернет. Две сети предприятия подключены к Интернету. На рис. 1 показана топология сети. Роутер 1 является выходным маршрутизатором головного офиса в Москве, роутер 4 – это маршрутизатор выхода из Пермского филиала, роутер 2 и роутер 3 – это маршрутизаторы, используемые для имитации Интернета. Рабочие станции подключены во внутренней сети головного офиса и филиала, чтобы проверить подключение к сети.

Внутренние адреса сети устанавливаются как IP-адрес класса С. Головной офис – 222.17.244.0/24. IP-адрес PC1 – 222.17.244.2, маска подсети PC1 – 255.255.255.0 и адрес шлюза – 222.17.244.1.

Филиал – 222.17.245.0/24. IP-адрес PC2 имеет значение: 222.17.245.2, маска подсети – 255.255.255.0, а шлюз – 222.17.245.1.

Сеть между роутером 1 и роутером 2 – 188.128.5.0/24. Между роутером 3 и роутером 4 – 52.1.1.0/24. Сеть между двумя внешними маршрутизаторами – 198.96.6.0/24. Конфигурация роутеров представлена на рис. 2–4.

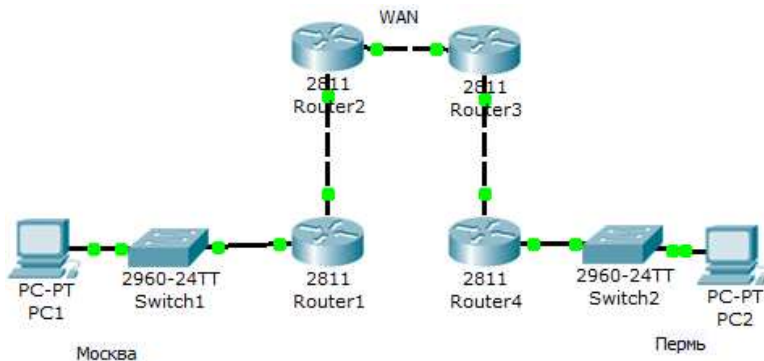


Рис. 1. Модель корпоративной сети

Роутер 1

```
1) Конфигурация IP-адресов
Router(config)#hostname R1
R1(config)#int f0/1
R1(config-if)#ip address 188.128.5.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#interface f0/0
R1(config-if)#ip address 222.17.244.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 188.128.5.2
2) Создание стратегии
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
3) Конфигурация первичного ключа и параметров
R1(config)#crypto isakmp key 13876694751 address
52.1.1.2
R1(config)#access-list 110 permit ip 222.17.244.0
0.0.255.222.17.245.0 0.0.0.255
```

4) IPsec параметры

```
R1(config)#crypto ipsec transform-set test esp-3des espmd5-
hmac
5) Конфигурация карты
R1(config)#crypto map gub-map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 52.1.1.2
R1(config-crypto-map)#set transform-set test
R1(config-crypto-map)#match address 110
6) Применение карты к интерфейсу
R1(config)#int f0/1
R1(config-if)#crypto map gub-map
7) Конфигурация туннеля
R1(config)#int tunnel0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#tunnel source f0/1
R1(config-if)#tunnel destination 52.1.1.2
R1(config-if)#exit
R1(config)#access-list 110 permit gre host 188.128.5.1
host 52.1.1.2
```

Рис. 2. Конфигурация маршрутизатора 1

Роутер 4

```
1) Конфигурация IP-адресов
Router(config)#hostname R4
R4(config)#int f0/1
R4(config-if)#ip address 52.1.1.2 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#int f0/0
R4(config-if)#ip address 222.17.245.1 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#ip route 0.0.0.0 0.0.0.0 52.1.1.1
2) Создание стратегии
R4(config)#crypto isakmp enable
R4(config)#crypto isakmp policy 10
R4(config-isakmp)#hash md5
R4(config-isakmp)#authentication pre-share
R4(config-isakmp)#lifetime 86400
R4(config-isakmp)#group 5
R4(config-isakmp)#exit
3) Конфигурация первичного ключа и параметров
R4(config)#crypto isakmp key 13876694751 address
188.128.5.1
R4(config)#access-list 110 permit ip 222.17.245.0
0.0.255.222.17.244.0 0.0.0.255
```

4) IPsec параметры

```
R4(config)#crypto ipsec transform-set test esp-3des espmd5-
hmac
5) Конфигурация карты
R4(config)#crypto map gub-map 10 ipsec-isakmp
R4(config-crypto-map)#set peer 188.128.5.1
R4(config-crypto-map)#set transform-set test
R4(config-crypto-map)#match address 110
6) Применение карты к интерфейсу
R4(config)#int f0/1
R4(config-if)#crypto map gub-map
7) Конфигурация туннеля
R4(config-if)#ip add 192.168.1.2 255.255.255.0
R4(config-if)#tunnel source f0/1
R4(config-if)#tunnel destination 188.128.5.1
R4(config-if)#exit
R4(config)#access-list 110 permit gre host 52.1.1.2 host
188.128.5.1
```

Рис. 3 Конфигурация маршрутизатора 4

Роутер 2

```
Router(config)#hostname R2
R2(config)#int f0/1
R2(config-if)#ip add 198.96.6.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#int f0/0
R2(config-if)#ip add 188.128.5.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 52.1.1.0 255.255.255.0 198.96.6.2
```

Роутер 3

```
Router(config)#hostname R3
R3(config)#int f0/1
R3(config-if)#ip add 198.96.6.2 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#int f0/0
R3(config-if)#ip add 52.1.1.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 188.128.5.0 255.255.255.0 198.96.6.1
```

Рис. 4. Конфигурация маршрутизаторов 2 и 3

По завершении настроек, используя команду ping между PC1 и PC2, т.е. между частными сетями, убеждаемся в работоспособности модели. Введем команды на роутере 1 для проверки конфигурации (рис. 5).

```
R1#show ip route
C   188.128.5.0 is directly connected, FastEthernet0/1
C   192.168.1.0/24 is directly connected, Tunnel0
C   222.17.244.0/24 is directly connected, FastEthernet0/0
S*  0.0.0.0 [1/0] via 188.128.5.2
R1#show int tunnel0
Tunnel0 is up, line protocol is up (connected)
Hardware is Tunnel
Internet address is 192.168.1.1/24
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 188.128.5.1 (FastEthernet0/1), destination 52.1.1.2
Tunnel protocol/transport GRE/IP
```

Рис. 5. Команды на роутере 1 для проверки конфигурации

С развитием современных предприятий, созданием филиалов, формированием удаленных клиентов всё большим и большим пользователям необходимо установить связь с корпоративной сетью. Виртуальная частная сеть IPsec, объединенная с GRE, может предоставлять предприятиям безопасные, недорогие и расширяемые сетевые сервисы, не затрагивая существующие коммуникации.

Библиографический список

1. Chong Wang. Implementation of GRE Over IPsec VPN. – International Conference on on Soft Computing in Information Communication Technology (SCICT 2014).
2. VPN [Электронный ресурс]. – URL: <http://linkmeup.ru/blog/50.html> (дата обращения: 02.12.2017).

Сведения об авторе

Губарев Евгений Андреевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: eugenegubarev@gmail.com

About the author

Gubarev Evgeniy Andreevich – Student Perm National Research Polytechnic University, Perm, e-mail: eugenegubarev@gmail.com

АНАЛИЗ ГЕНЕРАТОРОВ ШУМА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ПО КАНАЛУ ПЭМИ

Е.А. Гушчарин

Закрытое акционерное общество «Бионт», Пермь

С.А. Оборин, Ю.С. Фоминых

Пермский национальный исследовательский
политехнический университет, Пермь

Рассмотрен активный метод защиты информации конфиденциального характера от утечки по каналу ПЭМИ (побочные электромагнитные излучения). Он предполагает метод зашумления (радиомаскировки) путем использования генераторов шума. Проведем анализ существующих на рынке средств защиты информации по каналу ПЭМИ, рассмотрим их технические характеристики и уровни создаваемых помех.

Ключевые слова: ПЭМИ, средства защиты информации, информационная безопасность.

ANALYSIS OF NOISE GENERATORS OF INFORMATION PROTECTION ON THE CHANNEL TEMPEST

E.A. Gushcharin

Close joint-stock company «Biont», Perm,

S.A. Oborin, Yu.S. Fominykh

Perm National Research Polytechnic University, Perm

In this article, we consider an active method of protecting confidential information from leaking through the channel TEMPEST (Side electromagnetic radiation). It's suggests a method of noise (radiometric) by the use of noise generators. Will analyze existing means of protection of information according to channel TEMPEST, consider their characteristics and levels of interference they generate.

Keywords: TEMPEST, means of information protection, information security.

Побочные электромагнитные излучения (ПЭМИ) – это паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными.

В современном обществе трудно представить обработку информации без использования ПЭВМ, все большую популярность приобретает электронный документооборот. В последние годы промышленный шпионаж превращается в весьма доходную разновидность бизнеса. Современные средства разведки имеют миниатюрное

исполнение, доступность которых в определенных кругах велика. Как показывают исследования, масштабы промышленного шпионажа постоянно растут. По оценкам ФСБ России, каждая вторая российская фирма занимается промышленным шпионажем, а конкуренты занимаются против нее тем же самым. По экспертным оценкам на долю экономического шпионажа приходится 60 % потерь предприятия от недобросовестной конкуренции.

Традиционная ПЭМИН – атака возможна только тогда, когда компьютер обрабатывает данные. Но часто интерес для шпиона представляет информация, хранящаяся на HDD и используемая относительно редко. При этом ПК, ставший объектом атаки, заражается программой-трояном любым из известных способов (через CD с презентацией или ПО, через сеть, Flash-накопители). Программа ищет необходимую информацию на диске и путем обращения к различным устройствам вызывает появление побочных излучений. Подобный троян может встраивать сообщение в композитный сигнал монитора, и пользователь даже не подозревает, что в стандартное изображение рабочего стола вставлены секретные сообщения. С помощью разведывательного приемника обеспечиваются перехват паразитного излучения монитора и выделение требуемого полезного сигнала. Опасность подобной атаки заключается в том, что специалист по информационной безопасности или системный администратор часто мыслят штампами: «если ПК отключен от сети, то никакой троян ничего никому не передаст». Между тем сидящий за стенкой или под окнами шпион спокойно получает нужную ему информацию. При этом программа-троян не портит данные, не нарушает работу ПК, не производит несанкционированную рассылку по сети, а потому долго не обнаруживается антивирусным программным обеспечением. Как показывает практика, вирусы, использующие ПЭМИН для передачи данных, могут работать годами, не обнаруживая себя.

Несмотря на то, что данный метод был впервые использован в интересах армии США в начале XX века, открыто описан в марте 1985 г. Вимом ван Эйком в статье «Электромагнитное излучение видеодисплейных модулей: Риск перехвата?», проблема перехвата по каналу ПЭМИН актуальна до сих пор.

В настоящее время большинство организаций при построении системы защиты конфиденциальных данных уверено, что шифрование передаваемой информации между сетевыми узлами обеспечивает

полную безопасность защищаемой информации. Применение при передаче данных стойкого шифрования не оставляет шансов прочесть перехваченное сообщение. В этих условиях ПЭМИН-атака становится единственным способом получения информации до того, как она будет зашифрована.

В данной статье рассмотрим активный метод защиты информации конфиденциального характера от утечки по каналу ПЭМИ (побочные электромагнитные излучения). Он предполагает метод зашумления (радиомаскировки) путем использования генераторов шума, задачей которого является постановка помех, перекрывающих информативный сигнал. Проведем анализ существующих на рынке средств защиты информации по каналу ПЭМИ, рассмотрим их технические характеристики и уровни создаваемых помех.

Рассмотрим объект информатизации, расположенный в рабочем кабинете предприятия. Минимальное расстояние до границ контролируемой зоны (далее – КЗ) составляет 2,5 м, на этаже расположены сторонние организации (рис. 1).

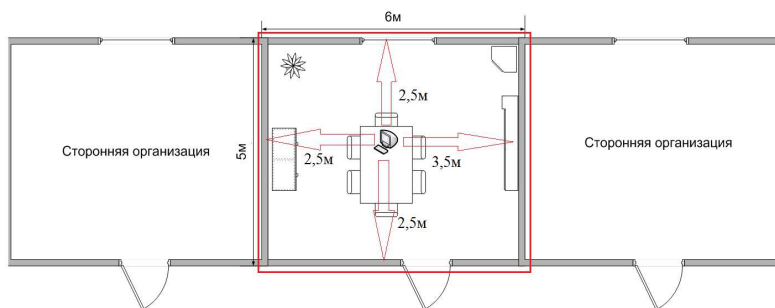


Рис. 1. Размещение объекта информатизации относительно границ контролируемой зоны

В рамках исследования рассматривалось излучение монитора Viewsonic VA1916W, использовался кабель с разъемом VGA, измерения проводились с помощью сборника тестовых программ при разрешении экрана 1600×900 с частотой 60 Гц. Замеры проводились в диапазоне частот от 0,09 до 1000 МГц.

При исследовании монитора на расстоянии 1 м были найдены сигналы, реагирующие на тест, запущенный на дисплее (рис. 2). Первая гармоника была найдена на частоте 32,5 МГц.



Рис. 2. Размещение антенны и источника ПЭМИ

Сигналы были различимы на фоне помех. Была четко различима «информативная» составляющая, например, при запущенном на мониторе тесте с полосами (чередование черных полос и полос с заполнением «точка-через точку»). Определив частоты, измерили значения «сигнал+шум», «шум» и путем расчета выяснили для каждой частоты расстояния распространения информативного сигнала. Сравнив полученные значения с реальным минимальным расстоянием до границ контролируемой зоны (необходимо выполнение условия $R_i < R_{кз}$), видно, что на большинстве частот условия не выполняются (рис. 3). Следовательно, необходимо применение средства защиты информации по каналу ПЭМИ (далее – СЗИ).

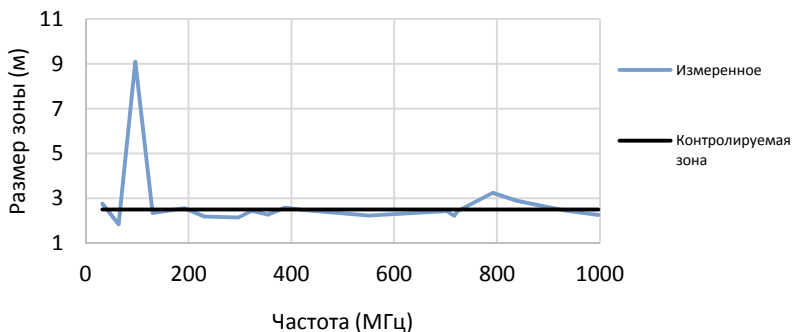


Рис. 3. Измеренное излучение монитора относительно границ КЗ

Для исследования были выбраны 2 (два) СЗИ по каналу ПЭМИН, имеющие действующие сертификаты соответствия ФСТЭК России. Все они имели разное исполнение и производителей. Замеры проводились на найденных частотах на расстоянии 1 м. Наша задача – перекрыть информативный сигнал от данного монитора на всех найденных частотах, создаваемый уровень шумов должен быть выше.

При рассмотрении СЗИ по каналу ПЭМИН видно, в исследуемом диапазоне на интересующих нас частотах постановка маскирующих помех не осуществляется сплошным спектром. На определенных частотах существуют как провалы, так и скачки. Также отличается средний уровень создаваемых помех. На нашем объекте допустимо использовать любой из исследуемых СЗИ, так как уровни помех, создаваемых всеми СЗИ, перекрывают информативный сигнал от данного монитора (рис. 4).

Можно сделать вывод, с использованием любого из рассматриваемых СЗИ съем информации по каналу ПЭМИН на границе контролируемой зоны невозможен.

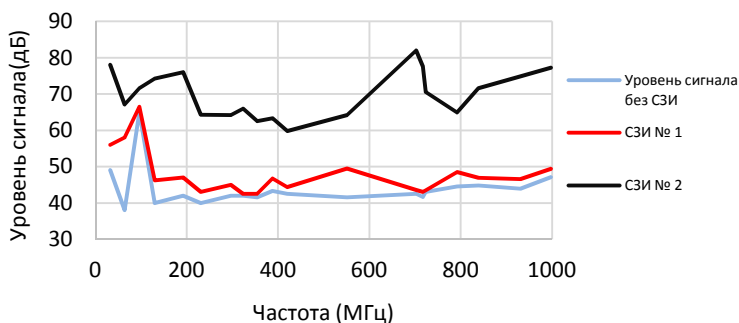


Рис. 4. Сравнение уровней сигналов от монитора и исследуемых СЗИ

Таким образом, СЗИ №1–2 подходят для защиты, но при выборе СЗИ №1 надо учитывать низкий уровень постановки помех, что может не перекрыть информативный сигнал на некоторых частотах. Также мощность излучаемых помех не подходит для создания распределенных объектов информатизации и защиты автоматизированных рабочих мест (далее – АРМ), состоящих из нескольких персональных электронно-вычислительных машин (ПЭВМ) (рис. 5). В свою очередь, их излучение оптимально для защиты одного АРМ и не создает избыточных шумовых помех в эфире.

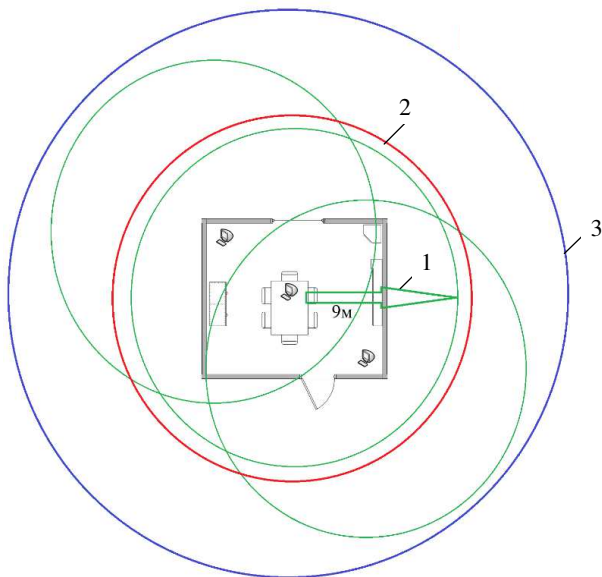


Рис. 5. Радиус действия СЗИ: 1 – максимальное распространение информативного сигнала; 2 – СЗИ № 1; 3 – СЗИ № 2

Проанализировав радиус распространения помех СЗИ № 2, делаем следующий вывод: установка данного СЗИ в центре помещения позволяет размещать АРМ в любом месте в пределах КЗ (границы помещения), что дает предпосылки для создания распределенного объекта информатизации, а также размещения нескольких АРМ (см. рис. 5).

Библиографический список

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 13.07.2015) «Об информации, информационных технологиях и о защите информации» // Доступ из справ.-правовой системы КонсультантПлюс.
2. Руководящий документ ФСТЭК России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» (Гостехкомиссия России, 2002 г.) // Доступ из справ.-правовой системы КонсультантПлюс.
3. Ярочкин В.И. Информационная безопасность: учебник для студ. вузов. – 2-е изд. – М.: Академический Проект: Гаудеамус, 2004. – 544 с.

4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации: учебник для вузов. – М.: Машиностроение, 2009. – 508 с.

5. Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 – ФСТЭК России [Электронный ресурс] // ФСТЭК России. – URL: <http://fstec.ru/normotvorcheskaya/sertifikatsiya/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00/> (дата обращения: 08.11.17).

Сведения об авторах

Гушарин Евгений Александрович – ведущий специалист по защите информации отдела информационной безопасности ЗАО «Бионт», Пермь, e-mail: egushcharin@biont.ru

Оборин Сергей Александрович – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: iceman-07@mail.ru

Фоминых Юрий Сергеевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: yfom@mail.ru

About the authors

Gushcharin Evgeny Aleksandrovich – Close joint-stock company «Biont», information security leading specialist, Perm, e-mail: egushcharin@biont.ru

Oborin Sergey Aleksandrovich – Student Perm National Research Polytechnic University, e-mail: iceman-07@mail.ru

Fominykh Yuriy Sergeevich – Student Perm National Research Polytechnic University, e-mail: yfom@mail.ru

ИССЛЕДОВАНИЕ НЕТРАДИЦИОННЫХ МЕТОДОВ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ ПОСРЕДСТВОМ СКРЫТЫХ КАНАЛОВ

А.В. Дробинина, И.И. Безукладников
Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассматриваются нетрадиционные методы атакующих воздействий посредством скрытых каналов для корпоративной ЛВС, условия существования скрытых каналов, а также принципы борьбы со скрытыми каналами на основе разрушения необходимых условий их существования.

Ключевые слова: скрытый канал, таргетированная атака, недоиспользованный ресурс.

RESEARCH OF NON-TRADITIONAL METHODS OF ATTACKING EFFECTS BY COVERED CHANNELS

A.V. Drobina, I.I. Bezukladnikov
Perm National Research Polytechnic University, Perm

In this article discuss about non-traditional methods of attacking effects through hidden channels for the corporate LAN, the conditions for the existence of hidden channels, as well as the principles of combating hidden channels based on the destruction of the necessary conditions for their existence.

Keywords: hidden channel, targeted attack, underutilized resource.

На данный момент существует проблема информационной безопасности – исследование нетрадиционных методов атакующих воздействий посредством скрытых каналов. Этой проблемой безопасности занимались Грушо, Тимонина, Конахович, Безукладников и др. Выбран объект исследования в виде информационной системы, подверженной таргетированным атакам – корпоративная ЛВС, а также предмет исследования – это методы защиты от таргетированных атак посредством скрытых каналов. Целью работы является разработка рекомендаций для защиты скрытых каналов.

Рассмотрим типовую модель ЛВС. На рисунке представлен наиболее распространенный вариант построения корпоративной сети, но даже такой уровень защиты не работает против таргетированных атак.

Скрытый канал будем рассматривать как средство передачи нелегальной (атакующей) или легальной информации. Заметим, что скрытый канал сам по себе представляет собой лишь альтернативный

способ передачи дополнительных объемов информации. В изученной литературе предлагается считать, что скрытые каналы – разновидность стеганографии.

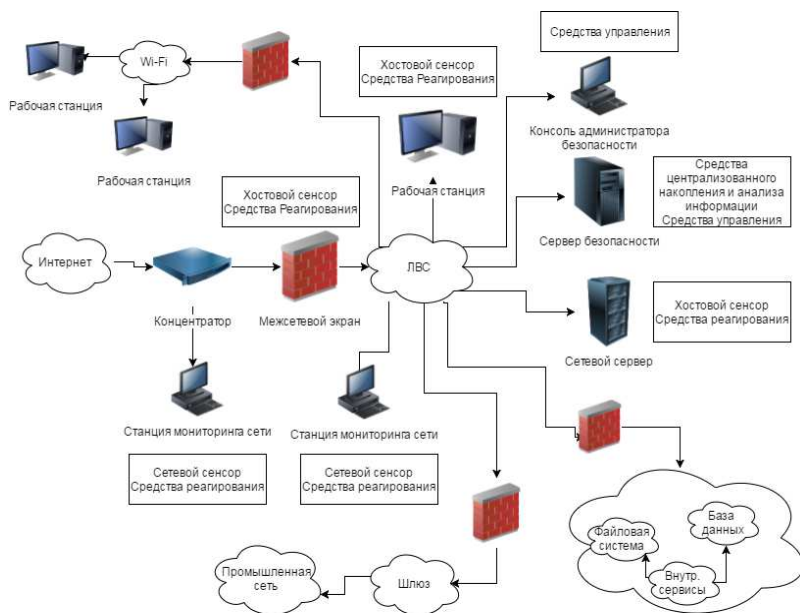


Рис. Модель корпоративной ЛВС

При этом для выделения скрытых каналов в отдельный класс будем считать, что стеганография рассматривает вопросы скрытой передачи информации в пользовательских сообщениях, скрытые каналы – вопросы скрытой передачи с использованием особенностей всей подлежащей транспортной инфраструктуры. Принцип функционирования скрытого канала заключается в передаче дополнительных объемов информации параллельно открытому каналу за счет эксплуатации тех или иных недоиспользованных ресурсов последнего.

Основной особенностью, отличающей скрытый канал от иных каналов передачи информации, является то, что скрытый канал не является самостоятельным, и передача информации в нем возможна только в моменты времени, так или иначе связанные с передачей информации в открытом канале. В случае с нелегальным использованием скрытого канала также появляется дополнительное условие – его

«незаметность», которая трактуется как непротиворечивость скрытого канала действующей в системе политике информационной безопасности и, как следствие, невозможность его выявления действующими фильтрами такой политики.

Рассмотрим условия существования скрытого канала. Введем определение недоиспользованного ресурса: под *недоиспользованным ресурсом* понимается произвольный информационный ресурс открытого канала, степень использования которого в процессе открытой передачи информации допускает внесение дополнительных модификаций в определенных пределах без вреда для передаваемой по открытому каналу пользовательской информации, а также без выхода за рамки иных действующих в системе ограничений.

Недоиспользованные ресурсы различных уровней ЭМВОС как основа существования скрытых каналов. В общем виде передача любых дополнительных объемов информации совместно с уже существующим в канале связи информационном потоком возможна только при наличии в этом канале так называемых «недоиспользованных информационных ресурсов». Для объяснения вводимого термина «недоиспользованный информационный ресурс» (НИР – в дальнейшем для краткости «недоиспользованный ресурс») воспользуемся следующими примерами:

1. Недоиспользованные ресурсы физического канала связи;
2. Недоиспользованные ресурсы в многоуровневой системе связи;
 - а) Передача информации путем воздействия на информационный поток специальным образом сформированной помехи. Неразрушаемость легальных данных в этом случае может обеспечиваться за счет корректирующей способности кодов.
3. Недоиспользованность временных ресурсов;
4. Недоиспользованность ресурса упорядоченности;
5. Структурная недоиспользованность (логическая избыточность структуры);
 - а) Недоиспользованные поля в протоколе;
6. Недоиспользованность ресурса физических параметров (амплитуда, частота, фаза).

Рассмотрим необходимые условия существования скрытого канала.

Условие 1: В системе должен существовать недоиспользуемый ресурс (НИР), отвечающий следующим требованиям, вытекающим из представления скрытого канала как дискретного канала связи.

Определим достаточное условие существования скрытого канала. Формулировка достаточного условия существования скрытого канала зависит в первую очередь от цели его применения. Так, в случае применения скрытого канала с целью осуществления злоумышленных воздействий требуется внесение, по меньшей мере, одного дополнительного условия, отражающего непротиворечивость скрытого канала действующей в системе политики информационной безопасности:

- условие непротиворечивости действующей ПИБ: скрытый канал должен являться непротиворечивым по отношению к действующей в системе политике информационной безопасности, либо время его компрометации/разрушения должно превышать время, необходимое для совершения требуемых вредоносных действий согласно выбранным сценариям атаки;

- условие удовлетворения ресурсных ограничений: создание и эксплуатация скрытого канала не должны выводить систему в целом и конкретные ее узлы за рамки существующих в ней аппаратных и программных ограничений.

Приведенное условие существования недоиспользованного ресурса (условие №1) в совокупности с введенными в работе условием непротиворечивости скрытого канала действующей политики безопасности и условием удовлетворения ресурсных ограничений (условия №2–3) составляют достаточное условие существования СК. Следует отметить что одной из основных проблем, возникающих в ходе проверки выполнимости условия №1, является необходимость не только выявления самого факта недоиспользованности того или иного ресурса, но и предложения способа, позволяющего применить эту недоиспользованность для скрытой передачи информации.

В результате с помощью скрытого канала может произойти:

- загрузка удаленного кода;
- активация Time Bomb;
- канал утечки информации (малый или большой).

Рассмотрим принципы борьбы со скрытыми каналами на основе разрушения необходимых условий их существования.

Используя полученные ранее необходимые условия существования скрытых каналов, можно подойти с формальной точки зрения также и к проблеме борьбы со скрытыми каналами. Это возможно по причине того, что невыполнение любого из приведенных условий

автоматически делает скрытый канал нереализуемым. Соответственно на основании анализа необходимых условий можно выделить следующие основанные на их нарушении методы борьбы.

Нарушение условия №1 (существования недоиспользованного ресурса с требуемыми характеристиками). Это может быть осуществлено при помощи введения дополнительных ограничений, препятствующих созданию или выделению требуемых состояний недоиспользованного ресурса, что приведет к разрушению скрытого канала, эксплуатирующего соответствующий вид недоиспользованности.

Заметим, что нарушение условий управляемости и наблюдаемости также может быть осуществлено альтернативным методом, использование которого в известных работах ранее замечено не было. Основой метода является создание легального скрытого канала, использующего для своего функционирования ту же недоиспользованность открытого ресурса. Сам факт передачи информации по такому легальному скрытому каналу уже существенно уменьшает недоиспользованность, доступную создателю злоумышленного скрытого канала, за счет чего ухудшает характеристики такого канала либо делает его реализацию невозможной. Кроме того, использование злоумышленником той же недоиспользованности неизбежно порождает конфликт, вызванный отсутствием координации доступа к общему ресурсу и, как следствие, к порче информации, передаваемой как по скрытому каналу злоумышленника, так и по легальному скрытому каналу. Этот факт может быть легко отслежен и, соответственно, использован для компрометации злоумышленного скрытого канала.

Нарушение одного из дополнительных условий (условия непротиворечивости действующей ПИБ, условия удовлетворения ресурсным ограничениям) может быть достигнуто путем усиления соответствующих фильтров ПИБ и, как следствие, уменьшения временных затрат на компрометацию злоумышленного скрытого канала, либо введения дополнительных фильтров, анализирующих необходимые для обнаружения скрытого канала параметры.

Для систем с ограниченными ресурсами также возможен вариант с противодействием реализации скрытому каналу путем уменьшения доступных для злоумышленника аппаратных и программных ресурсов. Так, например, в случае с устройствами полевого уровня существенная ограниченность их аппаратных ресурсов позволяет исключить или значительно уменьшить вероятность либо существенные харак-

теристики злоумышленного скрытого канала за счет введения дополнительной легальной задачи, по возможности использующей все свободные ресурсы.

Библиографический список

1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996. – 73 с.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – М.: МК-Пресс, 2006. – 288 с.
3. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. – М.: Професионал, 2005. – 490 с.
4. Безукладников И.И., Кон Е.Л. Анализ и классификация скрытых каналов // Системы мониторинга и управления: сб. науч. тр. – Пермь: Изд-во Перм. гос. техн. ун-та, 2009. – С. 32–41.
5. Безукладников И.И., Кон Е.Л. Скрытые каналы в распределенных автоматизированных системах // Вестник УГАТУ. – 2010. – Т. 14, № 2. – С. 245–250.

Сведения об авторах

Дробинина Александра Викторовна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: 999s5@mail.ru

Безукладников Игорь Игоревич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: corrector@at.pstu.ru

About the authors

Drobinina Aleksandra Viktorovna – Student Perm National Research Polytechnic University, Perm, e-mail: 999s5@mail.ru

Bezukladnikov Igor Igorevich – Ph.D. in Technical Sciences, Associate Professor of the department Automatics and telemechanics, Perm, e-mail: corrector@at.pstu.ru

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ ОПЕРАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ СКАНЕРОВ БЕЗОПАСНОСТИ

В.Г. Лесникова, А.Н. Кокоулин

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассмотрены проблемы информационной безопасности современных компьютерных систем, которые обусловлены наличием уязвимостей в операционных системах. Проанализированы угрозы, атаки, уязвимости. Выявлена и обоснована необходимость использовать инструменты, которые помогают обеспечить защищенность и целостность операционной системы. На основе проведенного теоретического исследования автор решает подробнее изучить проблему поиска уязвимостей операционных систем с использованием сканеров безопасности.

Ключевые слова: уязвимость; операционная система.

RESEARCH OF VULNERABILITY OF OPERATING SYSTEMS WITH USE OF SCANNERS OF SAFETY

V.G. Lesnikova, A.N. Kokoulin

Perm National Research Polytechnic University, Perm

In this article problems of information security of the modern computer systems which are caused by existence of vulnerabilities in operating systems are considered. Threats, the attacks, vulnerabilities are analyzed. Need to use tools which help to provide security and integrity of an operating system is revealed and justified. On the basis of the conducted theoretical research the author decides to study in more detail a problem of search of vulnerabilities of operating systems with use of scanners of safety.

Keywords: vulnerability; operating system.

На сегодняшний день вопросы конфиденциальности, целостности, доступности являются ключевыми не только для разработчиков, но и для пользователей разных информационно-коммуникационных систем и услуг. В этом общем вопросе выделяется проблема информационной безопасности современных компьютерных систем, которые обусловлены наличием уязвимостей в операционных системах.

Недавними примерами являются WannaCry, Petya – вредоносные программы, вымогатели денежных средств, поражающие компьютеры операционной системы Microsoft Windows [6, 7].

Безопасность операционной системы – состояние защищенности, при котором невозможно случайное или преднамеренное нарушение функционирования системы [1].

1. Угрозы по цели атаки (несанкционированное чтение информации; изменение; уничтожение; полное или частичное разрушение системы).

2. Угрозы по принципу воздействия (использование известных каналов получения информации; скрытых каналов; создание новых каналов).

3. Угрозы по характеру воздействия (активное – несанкционированные действия злоумышленника в системе; пассивное – несанкционированное наблюдение злоумышленника за процессами, происходящими в системе).

4. Угрозы по типу используемой уязвимости защиты (ошибки администратора системы; ошибки и недокументированные возможности ПО; ранее внедренная программная закладка) [2].

Распространенные типы уязвимостей представлены на рис. 1 [5]:

1. Отождествление прав с правами системы
2. Получение имени и пароля других служб и приложений
3. Дезинформация пользователя
4. Использование некорректных настроек безопасности реестра
5. Получение имени и пароля ОС или БД
6. Разрушение системы
7. Использование некорректных настроек файловой системы
8. Запуск произвольной программы
9. Подмена адреса программы
10. Использование ошибок программирования
11. Использование ошибки каталога ".." (две точки)
12. Удаление и перезапись
13. Определение имени пользователя
14. Получение доступа к временным файлам
15. Перехват информации пользователя

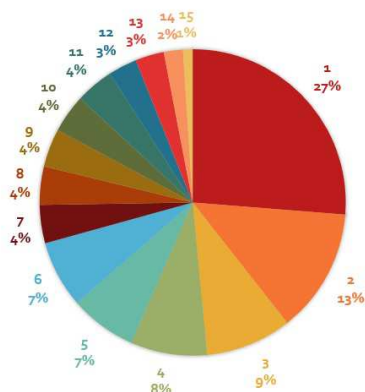


Рис. 1. Статистика уязвимостей

Компьютерные атаки: сканирование файловой информации; кража ключевой информации; подбор пароля; сборка мусора; превышение полномочий; программные закладки; «жадные программы» [2].

Таким образом, установлено, что уровень безопасности ОС низкий, имеются угрозы, уязвимости, атаки. Их нужно своевременно обнаруживать и устранять.

По данным компании NetMarketShare, представленным на рис. 2, во всем мире 91,59 % жителей используют в качестве ОС Microsoft Windows, macOS 6,27 % и Linux 2,14 % [4].

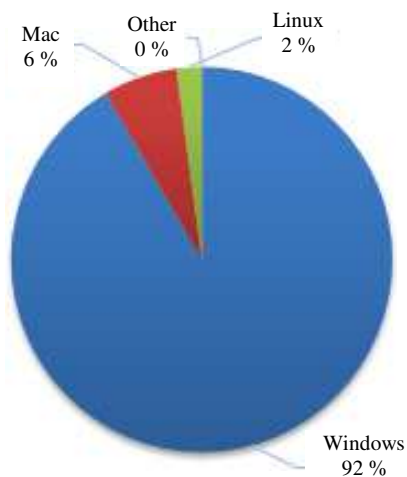


Рис. 2. Данные компании

Какие ОС Microsoft Windows входят в эти 91,59 % [4], представлено на рис. 3.

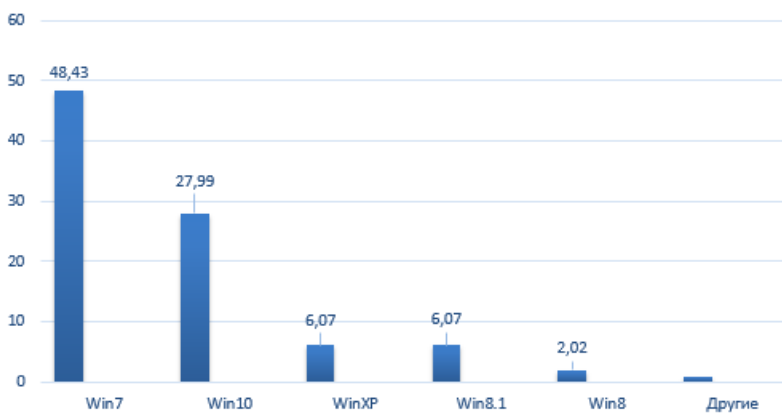


Рис. 3. ОС Microsoft Windows

Таким образом, принято решение исследовать уязвимости ОС Microsoft Windows 7, 10, XP.

Сканеры безопасности – это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющие сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости [3].

По данным опроса портала Securitylab.ru (рис. 4), большинство организаций предпочитают использовать продукт Positive Technologies XSpider или MaxPatrol (34 %) и Nessus Security Scanner (19 %) [3].

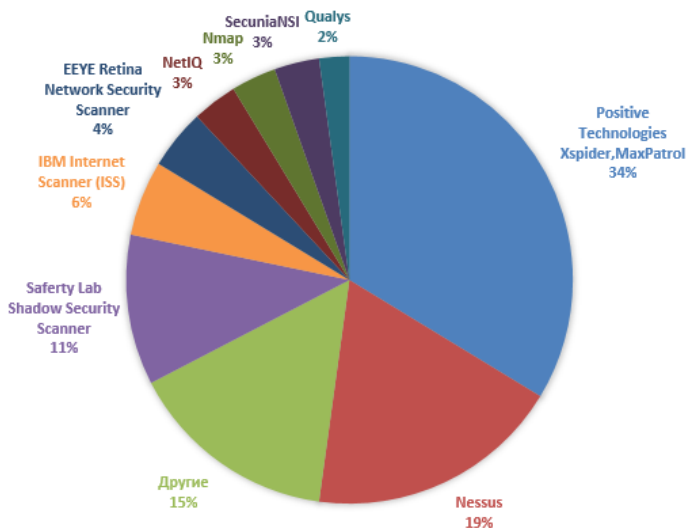


Рис. 4. Сканеры безопасности

Таким образом, принято решение использовать сканеры безопасности XSpider, MaxPatrol, Nessus для исследования уязвимости ОС Microsoft Windows 7, 10, XP.

Установлен VirtualBox на локальную машину, созданы виртуальные машины: Windows XP, Windows 7, Windows 10, Kali Linux (рис. 5).

На версии Windows установлены XSpider, MaxPatrol, а на Kali Linux – Nessus.

Исследование проводилось по каждой операционной системе в двух последовательных действиях: сначала при включенном брандмауэре, а затем с выключенным брандмауэром.

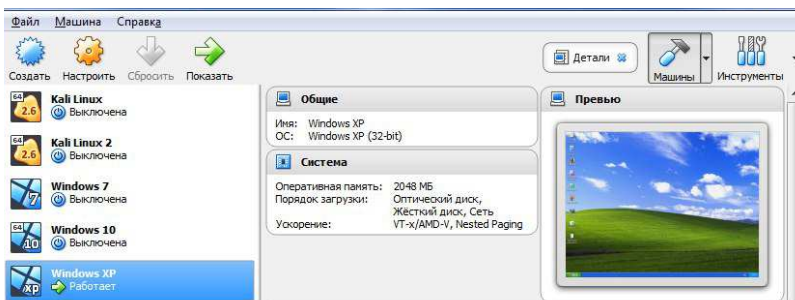


Рис. 5. Интерфейс программы

Чтобы осмыслить результаты и прийти к какому-либо выводу, была предложена следующая система подсчета баллов: за каждую найденную уязвимость добавляется определенное количество баллов в зависимости от степени опасности уязвимости:

- серьезная уязвимость (+3 балла);
- уязвимость средней тяжести (+2 балла);
- информация (+1 балл);

Результаты представлены в табл. 1, 2.

Таблица 1

Включенный брандмауэр

ОС / Сканер	MaxPatrol	XSpider	Nessus
Windows XP	3+2+7	3+3+2+7	3
Windows 7	2+2+8	2+3	3+5
Windows 10	3+2+2+2+6	2+1	3

Таблица 2

Выключенный брандмауэр

ОС/Сканер	MaxPatrol	XSpider	Nessus
Windows XP	3+3+2+2+7	3+3+2+2+7	3+3+3+3+2+2+2+2+2+2+2+2+29
Windows 7	2+2+8	2+3	3+3+2+2+30
Windows 10	3+2+2+2+6	3+2+1	3+22

Результаты по операционным систем с включенным брандмауэром представлены на рис. 6, а с выключенным – на рис. 7.

Лидер по защищенности – Windows 10, затем Windows 7 и Windows XP. Результаты по сканерам безопасности с включенным брандмауэром представлены на рис. 8, с выключенным – на рис. 9.

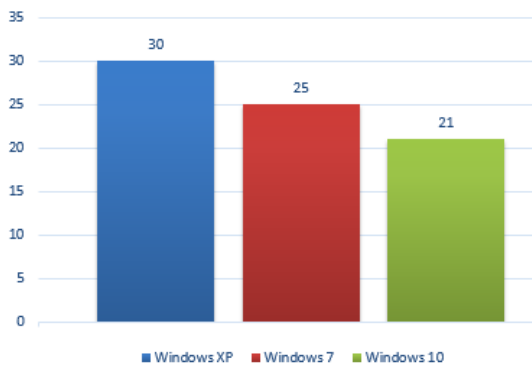


Рис. 6. Результаты с включенным брандмауэром

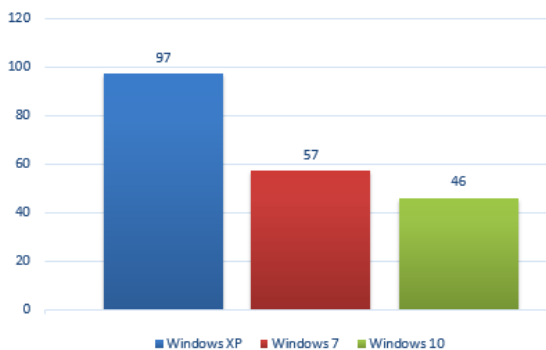


Рис. 7. Результаты с выключенным брандмауэром

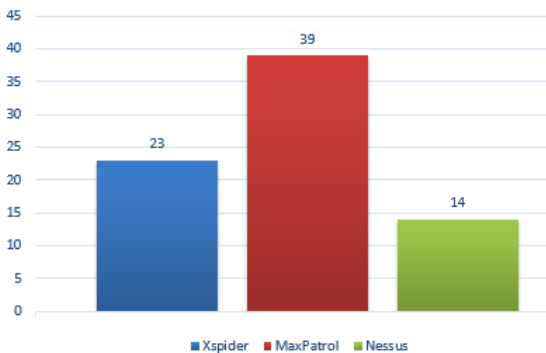


Рис. 8. Сканеры с включенным брандмауэром

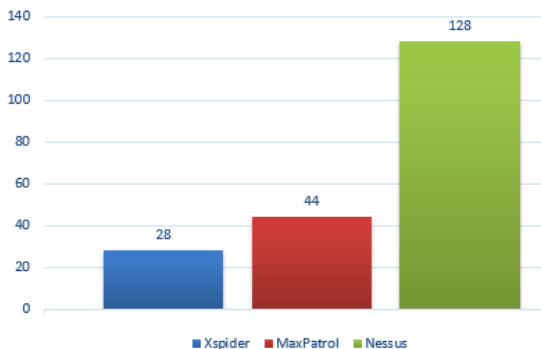


Рис. 9. Сканеры с выключенным брандмауэром

При включенном брандмауэре эффективнее MaxPatrol, при выключенном брандмауэре – Nessus.

Исследование показало, что защищенность выше у Windows 10, эффективнее с включенным брандмауэром сканер MaxPatrol, с выключенным брандмауэром – Nessus.

Текст доклада для XI Международной интернет-конференции молодых ученых, аспирантов и студентов «Инновационные технологии: теория, инструменты, практика».

Библиографический список

1. Безопасность операционных систем [Электронный ресурс]. – URL: <http://works.doklad.ru/view/d-U9G-zPi2g/all.html> (дата обращения: 30.11.2017).

2. Проблемы безопасности информации [Электронный ресурс]. – URL: http://infoprotect.net/protect_pk/problems-bezopasnosti-os (дата обращения: 30.12.2017).

3. Сканеры безопасности [Электронный ресурс]. – URL: <http://www.securitylab.ru/analytics/365241.php> (дата обращения: 1.12.2017).

4. Статистика операционных систем за август 2017 [Электронный ресурс]. – URL: <http://pyatilistnik.org/statistika-operatsionnyih-sistem-i-brauzerov-za-aprel-2017/> (дата обращения: 1.12.2017).

5. Уязвимости операционных систем [Электронный ресурс]. – URL: <http://www.cnews.ru/reviews/free/security2005/articles/vulnerability.shtml> (дата обращения: 30.12.2017).

6. Ретуа [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/Ретуа> (дата обращения: 30.11.2017).

7. WannaCry [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/WannaCry> (дата обращения: 30.11.2017).

Сведения об авторах

Лесникова Виктория Германовна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: bragina951993@yandex.ru

Кокоулин Андрей Николаевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: a.n.kokoulin@gmail.com

About the authors

Lesnikova Viktoria Germanovna – Student Perm National Research Polytechnic University, Perm, e-mail: bragina951993@yandex.ru

Kokoulin Andrei Nikolaevich – Ph.D. in Technical Sciences, Associate Professor of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: a.n.kokoulin@gmail.com

ОЦЕНКА ЭНЕРГОЭФФЕКТИВНОСТИ ПРОТОКОЛОВ LEACH И PEGASIS ДЛЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Ю.В. Лихачева

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье описываются основные характеристики протоколов LEACH и PEGASIS для беспроводных сенсорных сетей, разработка имитационной модели и результаты сравнительного анализа рассматриваемых протоколов с точки зрения энергоэффективности.

Ключевые слова: беспроводные сенсорные сети, протокол маршрутизации, LEACH, PEGASIS, оценка энергоэффективности.

ENERGY EFFICIENCY EVALUATION OF LEACH AND PEGASIS PROTOCOLS FOR WIRELESS SENSOR NETWORKS

Yu.V. Likhacheva

Perm National Research Polytechnic University, Perm

This article describes the main characteristics of LEACH and PEGASIS protocols for wireless sensor networks, the development of a simulation model and the results of a comparative analysis of the protocols in the context of energy efficiency.

Keywords: wireless sensor network, routing protocols, LEACH, PEGASIS, energy efficiency evaluation.

Недавние достижения в области радиоэлектроники с низким энергопотреблением позволили создать относительно недорогие маломощные беспроводные датчики. В сетях таких датчиков информация собирается и передается на базовую станцию. Датчики сильно ограничены мощностью своего аккумулятора, что ограничивает срок службы и качество передачи информации. Поэтому к сетевым протоколам передачи, в том числе маршрутизации, в таких сетях предъявляют жесткие требования по энергоэффективности, сроку службы и отказоустойчивости системы, величине задержки [1, 2]. В настоящей работе выполняется количественный анализ двух распространенных протоколов маршрутизации LEACH и PEGASIS.

В протоколе LEACH, представленном в [3], узлы самоорганизуются в кластеры. Назначенный узел в каждом кластере собирает данные с узлов в своем кластере и передает базовой станции. Протокол PEGASIS [1] формирует цепочку узлов таким образом, что каждый узел

будет получать и передавать данные ближайшему соседу. Собранные данные перемещаются от узла к узлу, объединяются, и, в конечном итоге, назначенный узел передает данные базовой станции. Узлы поочередно передают данные базовой станции таким образом, что средняя энергия, затрачиваемая каждым узлом за раунд, уменьшается.

LEACH – протокол, в котором глава кластера собирает данные с узлов, принадлежащих кластеру, и после агрегации отправляет данные в так называемый узел стока (рис. 1) [3].

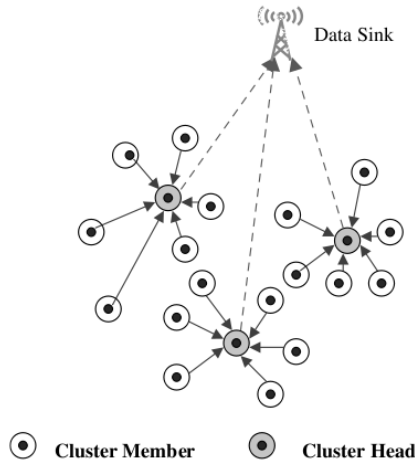


Рис. 1. Кластерный подход протокола LEACH

Чтобы все узлы в сети одинаково потребляли энергию, чтобы продлить срок службы сети, алгоритм случайным образом изменяет главу кластера, так как он потребляет в каждый период времени больше энергии, чем любой другой узел, принадлежащий кластеру. Чтобы снизить общие затраты на передачу, глава кластера выполняет агрегацию данных, а затем отправляет данные на узел стока. Каждый из узлов сети вычисляет пороговую величину $T(n)$, которая соответствует заранее заданному числу глав кластеров в сети. Пороговая величина $T(n)$ определяется следующим образом:

$$T(n) = \left\{ \begin{array}{ll} \frac{P}{1 - P \left(r \cdot \text{mod} \frac{1}{P} \right)} & \text{if } n \in G \\ 0 & \text{if } n \notin G \end{array} \right\},$$

где P – необходимый процент глав кластера, – текущий номер раунда, G – набор узлов, которые не были главами кластера в последних $1/P$ раундах.

Раунд состоит из двух фаз: фазы настройки и фазы устойчивого состояния. Первый этап – этап настройки кластера и главы кластера, второй – этап передачи данных с временным разделением (TDMA). Когда начинается новый раунд, каждый узел генерирует случайное число в диапазоне от 0 до 1, вычисляет пороговое значение с помощью выражения (1) и сравнивает эти два числа. Если сгенерированное число меньше порогового значения, узел назначается главой кластера. Назначенный глава кластера передает анонсы соседним узлам. Соседний узел, принимая анонс, выбирает тот из узлов, который передает самый мощный широкополосный сигнал, чтобы присоединиться к его кластеру, и отправляет ему сообщение «Join-REQ». После получения сообщения «Join-REQ» глава кластера регистрирует узел в своей таблице узлов-членов кластера. Глава кластера генерирует расписание TDMA для передачи данных внутри кластера и передает расписание узлам-членам.

В фазе устойчивого состояния каждый узел в кластерной сети отправляет данные главе своего кластера по расписанию. Глава кластера объединяет их и отправляет агрегированные данные в узел стока. Чтобы уменьшить расходы на выбор главы кластера, после выбора главы выполняется несколько раундов передачи данных, а затем вновь выполняется процедура реконфигурации кластера.

При использовании протокола PEGASIS узлы формируют цепочку таким образом, что каждый узел передает/принимает данные к/от соседнего узла [1]. Этот подход распределяет энергетическую нагрузку равномерно между узлами в сети и уменьшает количество энергии, затрачиваемой на передачу данных. Поскольку расчет цепочки выполняется один раз, а далее следует несколько раундов обмена данными, объем затраченной энергии мал по сравнению с объемом, затраченным на этапе сбора данных. Процесс построения цепочки начинается с самого дальнего от базовой станции узла. Следующим узлом в цепочке становится его наиболее близко расположенный сосед. Далее соседи выбираются последовательно из узлов, еще не присоединенных к цепочке (рис. 2).

Когда узел «умирает» (т.е. утрачивает всю свою энергию), цепочка перестраивается таким образом, чтобы обходить «мертвый»

узел. На этапе сбора данных в каждом раунде узел получает данные от одного соседа, объединяет данные со своими собственными и передает следующему соседу по цепочке.

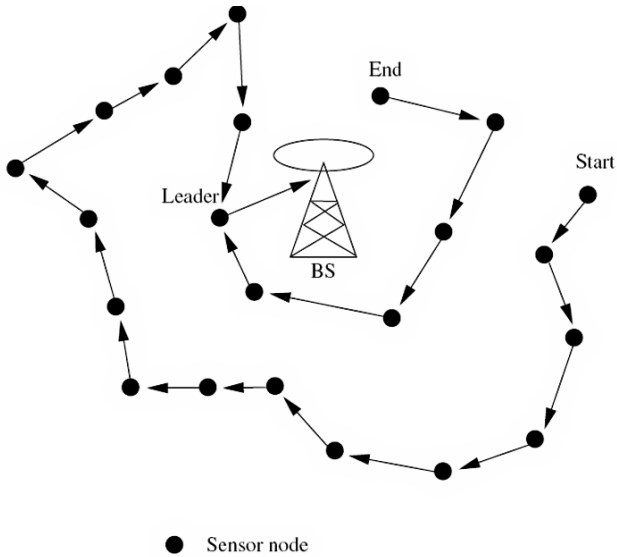


Рис. 2. Построение цепочки протоколом PEGASIS

Передача данных на базовую станцию осуществляется по алгоритму Round Robin, т.е. по очереди по кругу. Глава цепочки в каждом раунде – это случайный узел в любом месте в цепочке, что важно для того, чтобы узлы «умирали» равномерно внутри цепочки. Каждый цикл сбора данных инициируется базовой станцией с помощью сигнала-маячка, который синхронизирует все узлы. Поскольку все узлы знают свои позиции в цепочке, для передачи данных может использоваться временное разделение.

Для анализа характеристик протоколов LEACH и PEGASIS были разработаны имитационные модели с использованием системы MatLab. В данной работе в качестве модели используется сеть со 100 случайно распределенными узлами в области 100×100 м. Базовая станция находится в точке $x = 50, y = 100$. Длина каждого сигнала составляет 4000 бит, а энергия, необходимая для агрегации данных, составляет 5 нДж/бит [2, 3]. Время обработки данных на узле принимается за 5–10 мс [3]. Скорость радиосвязи считается равной

1 Мбит/с [2]. Рассматриваемая модель связи аналогична представленным в [3, 4]. В зависимости от расстояния между передатчиком и приемником для измерения потерь энергии из-за беспроводной передачи учитываются либо распространение волн в свободном пространстве, либо затухание вследствие многолучевого распространения в канале.

Для моделирования были использованы несколько сетей со 100 узлами, где каждый узел имеет 0,25 Дж начальной энергии. В качестве учитываемых параметров рассматривались количество раундов до «смерти» датчиков, энергия, потребляемая датчиками, и время, необходимое для завершения выбранного числа раундов. Узел считается «мертвым», когда его энергия становится нулевой, при этом узел исключается из последующих раундов. Как показано на рис. 3, фиксировалось число раундов, когда 1, 10, 20, 30, 40, 50, 60, 70 и 80 % узлов погибали. Был сделан вывод, что PEGASIS на 30 % эффективнее LEACH с точки зрения срока службы системы. Это достигается за счет сокращения количества сообщений до удаленной базовой станции до одного за раунд. Как показано на рис. 4, протокол PEGASIS потребляет меньше энергии, чем протокол LEACH.

PEGASIS образует одну цепочку узлов, тем самым вводя чрезмерную задержку. При использовании протокола LEACH задержка уменьшается. На рис. 5 можно заметить, что LEACH работает более эффективно, чем PEGASIS, с точки зрения задержки передачи информации.

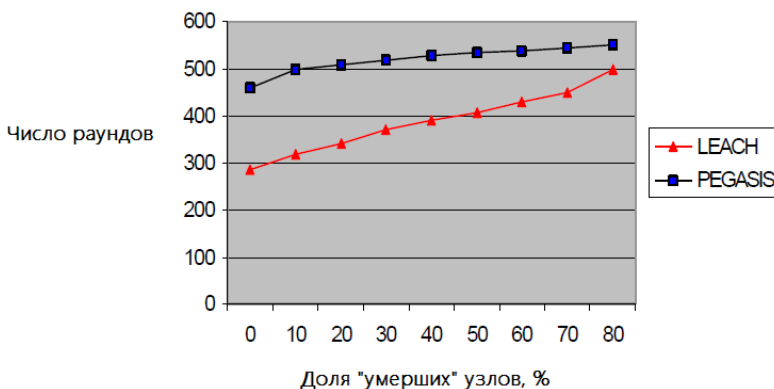


Рис. 3. Продолжительность жизни узлов в случайно сгенерированной сети из 100 узлов

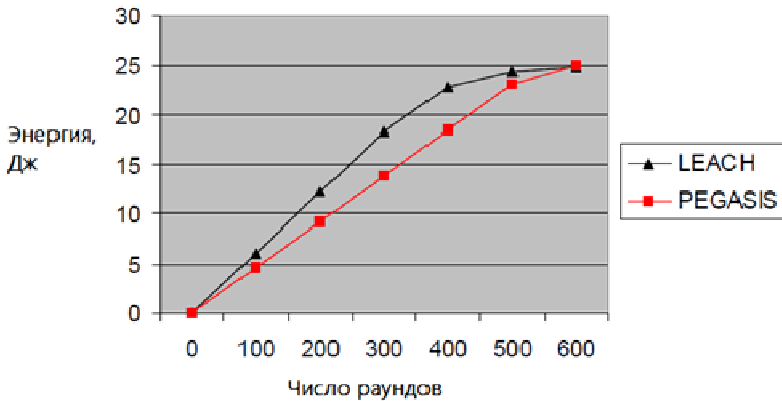


Рис. 4. Энергопотребление узлов в случайно сгенерированной сети из 100 узлов

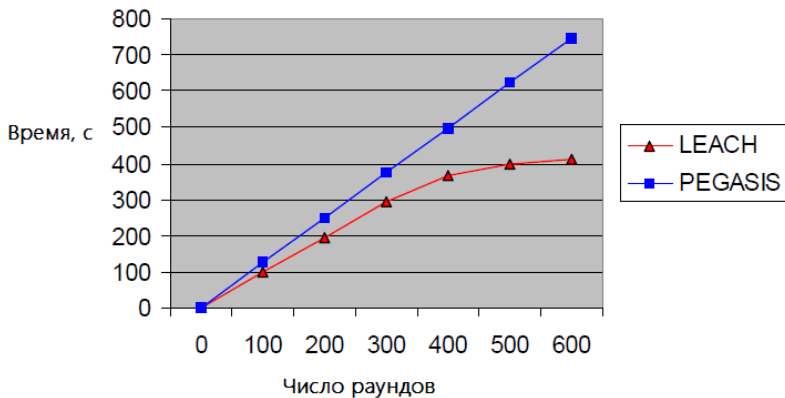


Рис. 5. Время, необходимое для завершения выбранного числа раундов

Благодаря полученным результатам появляется возможность разработки нового иерархического протокола маршрутизации, который компенсирует недостатки как LEACH, так и PEGASIS. Из результатов моделирования мы видим, что PEGASIS превосходит LEACH, устраняя накладные расходы на формирование динамического кластера, ограничивая количество передач и отправок и используя только одну передачу к базовой станции за раунд. Однако PEGASIS вводит чрезмерную задержку, которой при использовании LEACH удается избежать.

Библиографический список

1. Al-Karaki J.N., Kamal A.E. Routing techniques in wireless sensor networks: a survey // IEEE Wireless Communications Magazine. – 2004. – № 6. – С. 6–28.

2. Heinzelman W.B., Chandrakasan A., Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks // IEEE Trans. Wireless Communication. – 2002. – № 4. – С. 660–670.

3. Heinzelman W.R., Chandrakasa A., Balakrishnan H. Energy-efficient communication protocols for wireless microsensor networks // 33rd Hawaii International Conference on System Sciences. – 2000. – № 2.

4. Lindsay S., Raghavendra C. PEGASIS: Power-efficient gathering in sensor information systems // Proc. International Conference on Communications. – 2001.

Сведения об авторе

Лихачева Юлия Витальевна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: lijulia28@gmail.com

About the author

Likhacheva Yulia Vitalievna – Student Perm National Research Polytechnic University, Perm, e-mail: lijulia28@gmail.com

ЗАЩИТА СЕРВИСОВ ОТ DDOS-АТАК НА ПРИКЛАДНОМ УРОВНЕ

Е.С. Мазунина, И.И. Безукладников

Пермский национальный исследовательский
политехнический университет, Пермь

Распределенная атака отказа в обслуживании на сервера является актуальной проблемой в области информационной безопасности. В данной статье будет проанализирована данная атака на прикладном уровне модели OSI. А также приведены способы защиты сервисов от DDoS атак.

Ключевые слова: безопасность, атака, отказ в обслуживании, DDoS, защита сервисов.

PROTECTION SERVICES FROM DDOS-ATTACKS ON THE APPLICATION LAYER

E.S. Mazunina, I.I. Bezukladnikov

Perm National Research Polytechnic University, Perm

A distributed denial of service attack on the server is a topical problem in the field of information security. This article will analyze this attack on the application layer of the OSI model. And also provides ways to protect services from DDoS attacks.

Keywords: Security, Attack, Denial of Service, DDoS, Service Protection.

DDoS (distributed denial of service attack) – распределенная атака типа «отказ в обслуживании». Вследствие такой атаки сервис «жертва» получает лавинообразные запросы, влекущие за собой отказ в обслуживании. Злоумышленник в таком случае использует, например, так называемые зомби-сети, зараженные компьютеры пользователей вредоносным ПО, которые генерируют атакующие запросы (таблица).

Классификация DDoS-атак

Уровень модели OSI	Примеры технологий атак
Прикладной уровень	PDF GET запросы, HTTP GET, HTTP POST (формы веб-сайтов: логин, загрузка фото/видео, подтверждение обратной связи)
Представительский уровень	Подложные SSL запросы: проверка зашифрованных SSL пакетов очень ресурсоемка, злоумышленники используют SSL для HTTP-атак на сервер жертвы

Уровень модели OSI	Примеры технологий атак
Сеансовый уровень	Атака на протокол Telnet использует слабые места программного обеспечения Telnet-сервера на свитче, делая сервер недоступным
Транспортный уровень	SYN-флуд, Smurf-атака (атака ICMP-запросами с измененными адресами)
Сетевой уровень	ICMP-флуд — перегрузка пропускной способности целевой сети
Канальный уровень	MAC-флуд — переполнение пакетами данных сетевых коммутаторов
Физический уровень	Физическое разрушение, физическое препятствие работе или управлению физическими сетевыми активами

Чаще всего используются атаки на прикладном уровне из-за простой реализации и малой затраты ресурсов атакующего. Правда, такие атаки так же легко устраняются, но при бездействии приводят к простоям, который ведет за собой убытки.

Как происходят атаки на прикладном уровне? Самый простой способ для атаки – это «закидать» сервер HTTP-запросами. В основе запроса лежит HTTP-заголовок, к примеру, заголовком может быть URL-адрес, который запрашивает «жертва».

Запрашивающая сторона может использовать сколько угодно заголовков, придавая им нужные свойства. Проводящие DDoS-атаку злоумышленники могут изменять эти и многие другие HTTP-заголовки, делая их труднораспознаваемыми для выявления атаки. В добавок HTTP-заголовки могут быть написаны таким образом, чтобы управлять кэшированием и прокси-сервисами. Например, можно дать команду прокси-серверу не кэшировать информацию

HTTP-запросы делятся на два типа:

- HTTP GET

HTTP(S) GET-запрос – метод, который запрашивает информацию на сервере. Этот запрос может попросить у сервера передать какой-то файл, изображение, страницу или скрипт, чтобы отобразить их в браузере.

HTTP(S) GET-флуд – метод DDoS атаки прикладного уровня (7) модели OSI, при котором атакующий посылает мощный поток запросов на сервер с целью переполнения его ресурсов. В результате сервер не может отвечать не только на хакерские запросы, но и на запросы реальных клиентов.

- **HTTP POST**

HTTP(S) POST-запрос – метод, при котором данные помещаются в тело запроса для последующей обработки на сервере. HTTP POST-запрос кодирует передаваемую информацию и помещает на форму, а затем отправляет этот контент на сервер. Данный метод используется при необходимости передавать большие объемы информации или файлы.

HTTP(S) POST-флуд – это тип DDoS-атаки, при котором количество POST-запросов переполняют сервер так, что сервер не в состоянии ответить на все запросы. Это может привести к исключительно высокому использованию системных ресурсов и впоследствии к аварийной остановке сервера.

На первый квартал 2017 г. 10,71 % от всех DDoS атак приходится на HTTP-запросы

Защита от DDoS атак. К сожалению, за последние годы затраты на организацию DDoS-атак существенно снизились, а объем таких атак значительно возрос. Поэтому коммерческим предприятиям и государственным организациям необходимо иметь представление о возможных угрозах и принимать упреждающие меры для защиты от DDoS-атак.

56 % опрошенных представителей бизнеса высказали уверенность, что осуществленные на их компании DDoS-атаки использовались в качестве прикрытия других видов киберпреступлений. Порядка 26 % респондентов признались, что последовавшая за DDoS целевая атака привела к утечке данных.

Для должной защиты от DDoS-атак следует придерживаться следующего алгоритма:

1. Иметь отработанный план реагирования на DDoS, чтобы не расплывать внимание и не тратить время на координацию действий в случае атаки.

2. Максимальная автоматизация отражения DDoS-атак.

3. Мониторинг приложений – систематический мониторинг ПО, использующий определенный набор алгоритмов, технологий и подходов для выявления 0day-уязвимостей приложений. Идентифицировав такие атаки, их можно раз и навсегда остановить и отследить их источник.

4. Регулярный аудит безопасности ИТ-инфраструктуры и веб-приложения.

5. Устранение уязвимостей веб-приложений.

6. Проведение симуляции атак и проведение нагрузочных тестов. Это поможет найти слабые места в плане реагирования на атаки.

7. Оптимизация плана реагирования на атаки.

Одним хорошим способом защиты от DDoS-атак является использование CDN (Content Distribution Network)

Распределенные сетевые инфраструктуры оптимизируют загрузку сайтов и их содержимого, а также обеспечивают защиту от вредоносных ботов и блокируют угрозы.

Как работает технология CDN? CDN работает как reverse proxy (обратный прокси). Это значит, что если веб-сайт является частью инфраструктуры, то весь его трафик направляется через глобальную сеть, которую предоставляет провайдер CDN.

В сети хранятся копии статических файлов в географически близких к веб-посетителям местах, что означает быструю их загрузку. CDN кэширует такие ресурсы, как CSS, JavaScript и изображения. При этом с вашей стороны не требуется никаких дополнительных усилий – технология автоматически определяет, какие из файлов подлежат кэшированию, исходя из их расширений. Но динамический контент не кэшируется. Технология также применяет сжатие каждого запроса.

Сеть CDN также блокирует угрозы и разнообразных вредоносных ботов прежде, чем они наносят удар по вашему серверу, а это предотвращает потери трафика и ресурсов сервера.

В заключение можно подытожить, что защита от DDoS-атак должна быть комплексная, при этом используя не только программные средства защиты, но и организационные. При должной защите веб-ресурсы организации будут защищены от данной атаки.

Библиографический список

1. Шелухин О.И., Симонян А.Г., Иванов Ю.А. Особенности DDoS атак в беспроводных сетях // Т-Comm. – 2012. – № 11. – URL: <http://cyberleninka.ru/article/n/osobennosti-ddos-atak-v-besprovodnyh-setyah> (дата обращения: 15.09.2017).

2. Терновой О.С. Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности в результате ddos-атак // Известия АлтГУ. – 2013. – № 1(77). – URL:

<http://cyberleninka.ru/article/n/metodika-i-sredstva-rannego-vyyavleniya-i-protivodeystviya-ugrozam-narusheniya-informatsionnoy-bezopasnosti-v-rezultate-ddos-atak> (дата обращения: 15.09.2017).

Сведения об авторах

Мазунина Елизавета Сергеевна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: Muryshna@gmail.com

Безукладников Игорь Игоревич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: corrector@at.pstu.ru

About the authors

Mazunina Elizaveta Sergeevna – Student Perm National Research Polytechnic University, Perm, e-mail: Muryshna@gmail.com

Bezukladnikov Igor Igorevich – Ph.D. in Technical Sciences, Associate Professor of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: corrector@at.pstu.ru

О ШУМОПОДОБНЫХ СКРЫТЫХ КАНАЛАХ

А.А. Миронова, И.И. Безукладников

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассмотрена возможность построения шумоподобных скрытых каналов, работа которых может быть основана на принципах мимикрии под шум. Приведен пример подобного скрытого канала, принцип работы которого основан на плохой совместимости технологий Wi-Fi и LTE.

Ключевые слова: скрытые каналы, беспроводные технологии, Wi-Fi, LTE, канал связи, помехи.

ON THE PROBLEM OF NOISE-ALIKE COVERT CHANNELS

A.A. Mironova, I.I. Bezukladnikov

Perm National Research Polytechnic University, Perm

This article considers the possibility of constructing noise-like hidden channels, whose functioning can be maintained on the principles of noise mimicry. An example of such a covert channel is given, the operation principle of which is based on poor compatibility of Wi-Fi and LTE technologies.

Keywords: covert channels, wireless technologies, Wi-Fi, LTE, communication channel, noise.

В настоящее время в результате развития технологий связи в любой точке пространства может быть образовано скопление большого количества технологий, мешающих работе друг друга. Основываясь на этом принципе, злоумышленниками могут быть построены шумоподобные «скрытые каналы» связи, высокий уровень скрытности которых делает их обнаружение довольно проблематичным.

В общем случае «скрытыми каналами» (СК) связи называют методы НСД, основанные на передаче нелегальной информации незаметно для действующих средств ИБ. Принцип их функционирования основан на использовании ресурсов канала, позволяющих в процессе открытой передачи информации внести некоторые изменения, которые не повлекут за собой вред открытой передаче информации пользователя (недоиспользованный ресурс). Недоиспользованным ресурсом может служить, например, ресурс, выделенный под передачу служебной информации [1].

Работу любого СК можно представить следующим образом: существует легальный канал связи между пользователями U_1 - U_2 , который подвергается воздействию помехи E_1 , генерируемой пользователем СК А. В свою очередь, пользователь В – принимает информацию, передаваемую по СК (рис. 1).

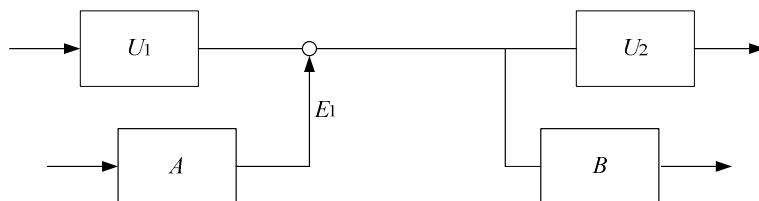


Рис. 1. Принцип работы СК-связи

В свою очередь, работа шумоподобных СК может основываться на принципах мимикрии под шум, и помехой E_1 в данном случае может служить работа другой технологии.

Например, СК, основанный на особенности динамического изменения скорости соединения беспроводной технологии Wi-Fi, может являться шумоподобным. Основа работы данного СК лежит в создании помехи, влияющей на уменьшение скорости соединения, тем самым конкретная скорость может служить единицей передачи данных. Для подобного СК метод мимикрии под шум может основываться на особенности плохого совмещения сетей Wi-Fi с сетями LTE (т.е. сотовыми сетями 4G) [2]. Так, на рис. 2 видно, что при существовании соты LTE с радиусом в x метров происходит подавление Wi-Fi точки доступа, при этом скорость соединения по сети Wi-Fi снижается с уменьшением радиуса соты LTE (красная линия на рис. 2).

Из вышеизложенного следует, что для повышения скрытности данного СК злоумышленнику достаточно осуществлять звонки по сети LTE, находясь вблизи точки Wi-Fi, тем самым изменяя скорость Wi-Fi-соединения, причем от дальности сотового абонента будет зависеть, насколько сильно уменьшается скорость. Этот метод может быть реализован посредством использования двух клиентов LTE, находящихся на разном расстоянии. Например, расстояния, соответствующие согласно рис. 2 скоростям 54 и 21 Мбит/с, – 125 м и 65 м (рис. 3).

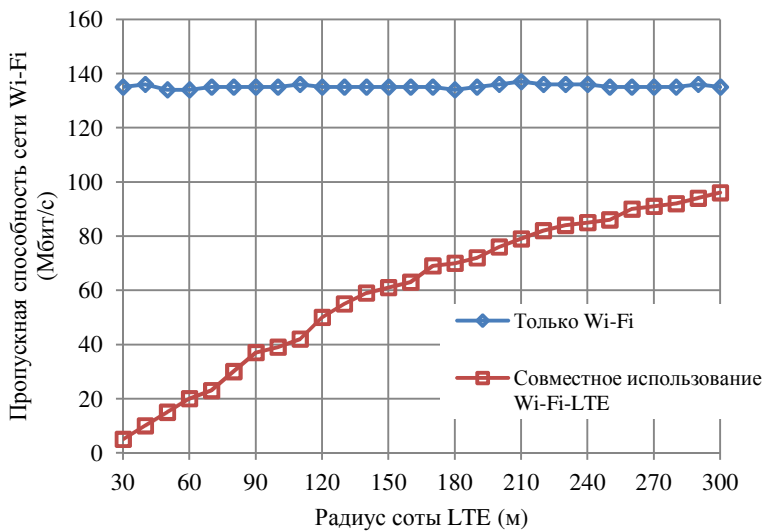


Рис. 2. Совмещение сетей Wi-Fi с сетями LTE

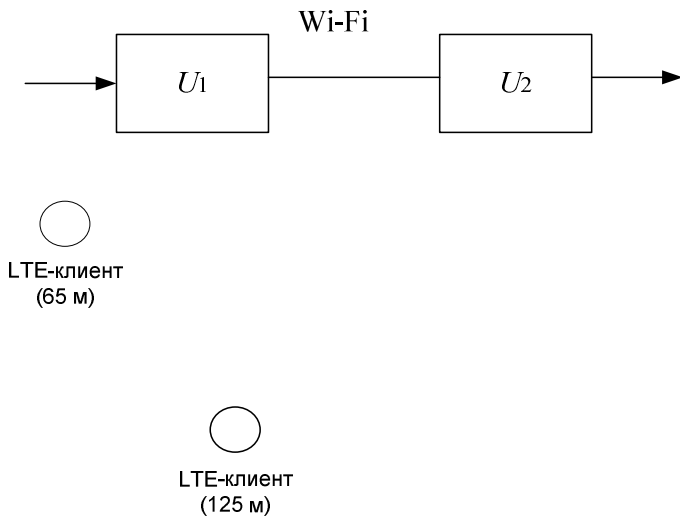


Рис. 3. Увеличение скрытности СК с использованием LTE-клиентов

Однако подобный СК может быть легко обнаружен, если звонки по сети LTE будут осуществляться с определенным интервалом (например, раз в 2 мин), так как реальные пользователи обычно так себя не ведут. В данном случае, чтобы улучшить возможности скрытности подобного канала, следует организовать трафик LTE сети в соответствии с нормальным законом распределения.

На рис. 4 изображен трафик LTE-сети в часы наибольшей нагрузки. Отсюда видно, что наибольшая активность пользователей наблюдается в середине дня, а в течение ночных часов активность использования LTE-сети снижается. Следовательно, используя СК, основанный на особенностях плохого совмещения технологий LTE и Wi-Fi, осуществлять звонки по сети LTE стоит согласно приведенному графику, чтобы повысить свойства скрытности и исключить возможность обнаружения подобного СК.

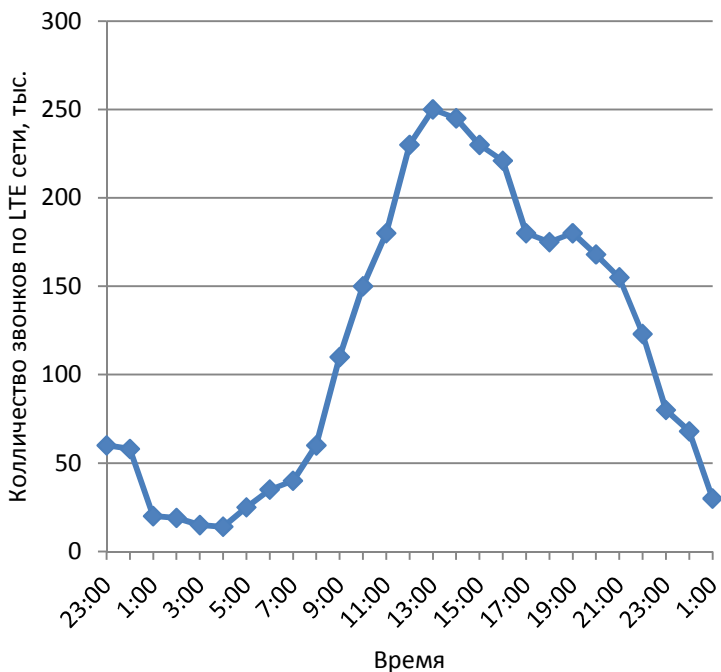


Рис. 4. Трафик сети в часы наибольшей нагрузки

Таким образом, в статье показана принципиальная возможность создания скрытого канала в рамках технологии WiFi, использующего для своего функционирования легальные передатчики другой технологии (LTE), обладающей плохой взаимной электромагнитной совместимостью. Это позволяет обеспечить дополнительную скрытность создаваемого канала и значительно затруднить принципиальную возможность его обнаружения.

Библиографический список

1. Безукладников И.И., Миронова А.А. Методы скрытой передачи информации на сетевом уровне телекоммуникационных систем // Вестник УрФО. Безопасность в информационной сфере. – 2016. – № 4(22). – С. 11–15.
2. Jeongho Jeon LTE in the Unlicensed Spectrum: A Novel Coexistence Analysis with WLAN Systems // Wireless Communications Symposium, Globecom. – 2014. – С. 3459–3464.

Сведения об авторах

Миронова Анна Алексеевна – студентка Пермского национального исследовательского политехнического университета, Пермь, e-mail: mir550@yandex.ru

Безукладников Игорь Игоревич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: corrector@at.pstu.ru

About the authors

Mironova Anna Alekseevna – Student Perm National Research Polytechnic University, Perm, e-mail: mir550@yandex.ru

Bezukladnikov Igor Igorevich – Ph.D. in Technical Sciences, Associate Professor of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: corrector@at.pstu.ru

СРАВНЕНИЕ СТАНДАРТОВ ШИФРОВАНИЯ

П.Е. Пьянков, О.С. Ведерникова, Е.Л. Кротова

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье произведен сравнительный анализ отечественного стандарта и вариантов зарубежных стандартов с целью выяснить, уступает ли традиционный подход более современному.

В 1990 г. вступил в силу отечественный стандарт симметричного шифрования «ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Рассмотрен стандарт симметричного шифрования данных Data Encryption Standard (DES), а также симметричный алгоритм блочного шифрования Advanced Encryption Standard (AES), который пришел на замену DES.

Ключевые слова: шифрование; стандарт; алгоритм; блок данных.

COMPARE ENCRYPTION STANDARTS

P.E. Pyankov, O.S. Vedernokova, E.L. Krotova

Perm National Research Polytechnic University, Perm

In this article the comparative analysis of the domestic standard and options foreign standards in order to determine whether inferior to the traditional approach is more modern.

In 1990 entered into force domestic standard symmetric cryptography "GOST 28147-89 System of information processing. Cryptographic protection. The algorithm of cryptographic transformation".

Considered the standard symmetric data encryption Data Encryption Standard (DES), a symmetric block cipher algorithm Advanced Encryption Standard (AES), which has replaced DES.

Keywords: encryption; standard; algorithm; data block.

В отличие от остальных стандартов размер шифруемого блока и размер ключа в алгоритме AES могут варьироваться, это стало возможным благодаря использованной в нем архитектуры «квадрат». Данное качество позволяет изменять криптостойкость и быстродействие алгоритма в зависимости от внешних требований к реализации. В алгоритме ГОСТ 28147-89 ключи шифрования берутся как составные части начального секретного ключа. В то же время в DES и AES используются значительно более сложные алгоритмы вычисления раундовых ключей. Эффективность криптоаналитических методов

зависит от количества циклов преобразования: чем больше циклов, тем труднее криптоанализ, как видим, у ГОСТа количество циклов больше, чем у DES и AES (таблица).

Ключевые характеристики

Характеристика	ГОСТ 28147-89	DES	AES
Размер блока, бит	64	64	128, 192, 256
Размер ключа, бит	256	56+8(для проверки)	128, 192, 256
Цикл преобразования	32	16	10, 12, 14
Архитектура	Сеть Фейстеля	Сеть Фейстеля	Square «Квадрат»
Операции в цикле	Подстановки, сдвиги, аддитивные операции	Подстановки, перестановки, аддитивные операции	Операции в конечных полях

Алгоритм ГОСТа 28147-89 и DESa основывается на архитектуре «сеть Фейстеля». Данная архитектура подразумевает разбиение исходного блока данных на две части. Одна из частей изменяется с помощью функции шифрования в зависимости от ключа раунда и далее складывается по модулю 2 с другой частью. После каждого раунда меняются местами, т.е. на следующем раунде текущий измененный блок становится неизменным [2, с. 73]. К достоинствам данной архитектуры можно отнести следующее:

- простота аппаратной реализации на современной электронной базе;
- простота программной реализации в силу того, что значительная часть функций поддерживается на аппаратном уровне в современных компьютерах (например, сложение по модулю 2 («xor»), сложение по модулю, умножение по модулю, и т.д.);
- хорошая изученность алгоритмов, построенных на основе сетей Фейстеля [3].

К недостаткам относится следующее:

- за один раунд шифруется только половина входного блока.

Алгоритм AES базируется на принципах новой сети подстановок-перестановок, который имеет новую архитектуру Squire «Квадрат», для которой характерно:

- представление шифруемого блока в виде двумерного байтового массива;
- шифрование за один раунд всего блока данных (байт-ориентированная структура);

– выполнение криптографических преобразований как над отдельными байтами массива, так и над его строками и столбцами [4].

Это обеспечивает диффузию данных одновременно в двух направлениях – по строкам и по столбцам [4].

Алгоритм ГОСТ 28147-89 (рис. 1.) шифрует информацию блоками по 64 бита, которые разбиваются на подблоки по 32 бита (N1 и N2) [1].

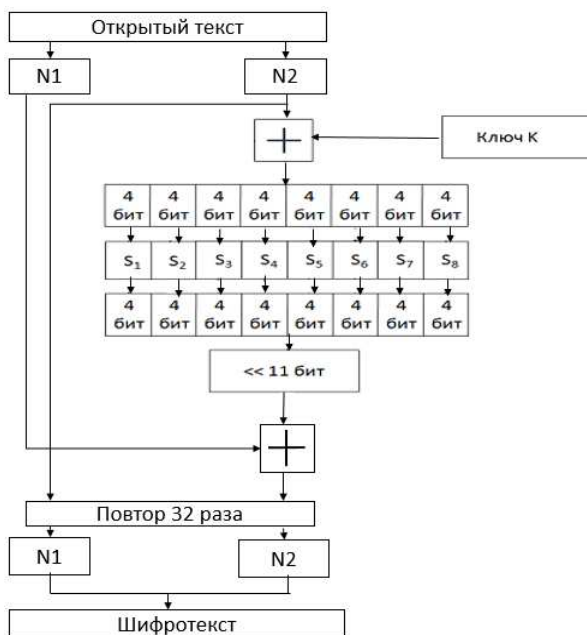


Рис. 1. Алгоритм шифрования ГОСТ 28147-89

Алгоритм состоит из следующих шагов:

- сложение по модулю 232 ключевого элемента и подблока N2 [1];
- табличная замена. Далее подблок разбивается на восемь 4-битовых частей, значения каждой из которых заменяются в соответствии с таблицей замены, называемой S-блоком. Количество S-блоков адекватно 4-битовым частям и представляют собой перестановку чисел от 0 до 15 [1];
- выходы S-блоков объединяются в 32-битную последовательность и циклически сдвигаются влево на 11 битов к старшему разряду [1];

– действия повторяются 32 раза.

DES работает с 64-битовыми блоками открытого текста. После первоначальной перестановки блок разбивается на правую и левую половины длиной по 32 бита [8, с. 36]. Алгоритм (рис. 2.) состоит из следующих шагов:

- 16 преобразований (данные объединяются с ключом);
- после последнего цикла левая и правая часть соединяются, алгоритм завершается заключительной перестановкой;
- на каждом цикле биты ключа сдвигаются, и затем из 56 битов ключа выбираются 48. Правая половина данных увеличивается до 48 с помощью перестановки с расширением, объединяются посредством XOR с 48 битами смещенного и перестановленного ключа, проходит через S-блоков, образуя 32 новых бита, и переставляется снова (перестановка с P-блоками). S-блоки выглядят как таблица, где каждый элемент представляется 4-битным числом с перестановкой от 0 до 15;
- результат объединяется с левой половиной с помощью другого XOR;
- действия повторяются 16 раз.

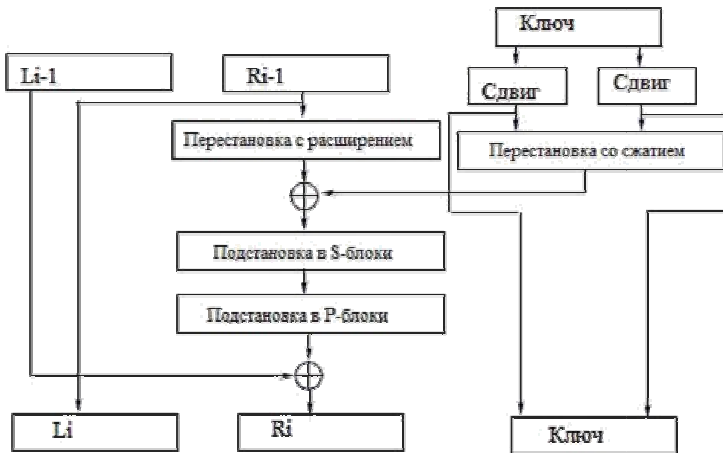


Рис. 2. Алгоритм шифрования DES

В AES шифруемый блок и его промежуточные состояния в ходе преобразования представляются в виде матрицы байтов $4 \times n$, где $n = 4, 6, 8$ в зависимости от размера блока. Функция нелинейного преобразования в алгоритме AES состоит из трех следующих элементарных преобразований, выполняемых последовательно [7]:

– байтовая подстановка – каждый байт преобразуемого блока заменяется новым значением, извлекаемым из общего для всех байтов матрицы вектора замены [7] – операция SubBytes;

– побайтовый циклический сдвиг в строках матрицы – первая строка остается неизменной, вторая строка циклически сдвигается влево на один байт, третья и четвертая строки циклически сдвигаются влево соответственно на 2 и 3 байта для $n = 4$ или 6 и на 3 и 4 байта для $n = 8$ [7] – операция ShiftRows;

– матричное умножение – полученная на предыдущем шаге матрица умножается слева на следующую матрицу–циркулянт размера 4×4 [7] – операция MixColumns. При этом операции с элементами матриц (сложение и умножение) выполняются в конечном поле GF(28), порождаемом полиномом $m(x) = x^8 + x^4 + x^3 + x + 1$ [7];

– побитовое суммирование байтов по модулю 2 – операция AddRoundKey.

Нетрудно заметить, что в каждом стандарте раунды шифрования аналогичны друг другу, это значительно упрощает их реализацию, делая ее компактной. ГОСТ не использует перестановку с расширением, как DES, что может отрицательно сказаться на его криптостойкости, так как отсутствие данной перестановки в DES уменьшает лавинный эффект. Лавинный эффект – зависимость битов результата от битов исходных данных [8, с. 37–38].

Последний раунд AES не содержит операции MixColumns, в последнем раунде ГОСТа отсутствует перестановка подблоков, в данном случае это сделано, чтобы обеспечить возможность расшифровки блока данных. Учитывая, что в ГОСТе используются 32 раунда шифрования, это позволяет противостоять существующим методам криптоанализа.

В алгоритме ГОСТ 28147-89 и DES, основанных на сети Фейстеля, процедура дешифрования использует те же основные элементы, но в обратном порядке.

В отечественном стандарте шифрования для генерации 32-битовых блоков из 256-битового ключа исходный ключ делят на 8 блоков: $k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8$. Каждый ключ используется 4 раза, т.е. 3 раза в прямом порядке (1...24 раунд) и 1 раз в обратном (25...32 раунда). Благодаря достаточной длине ключа сохраняется высокая криптостойкость алгоритма [5].

В DES преобразование ключей получается из начального 64-битового ключа. Далее ключ уменьшается путем отбрасывания каждого 8-го бита до 56 битов, и добавляются биты в позиции 8, 16, 24, 32, 40, 48, 56, 64 ключа таким образом, чтобы каждый байт содержал нечетное число единиц. Это используется для обнаружения ошибок при обмене и хранении ключей. Затем делают перестановку для расширенного ключа, кроме добавляемых.

В шифровании AES ключ и ключевая последовательность выглядят как векторы 4-байтовых слов, начальный участок последовательности заполняется словами из ключа. Следующие слова в ключевой последовательности вырабатываются группами, кратными размеру ключа. Первое 4-байтовое слово вырабатывается с использованием нелинейного преобразования, остальные – по простому линейному соотношению (рис. 3).

$$w_i = \begin{cases} w_{i-N_K} \oplus G(w_{i-1}), & \text{при } i \bmod N_K = 0 \\ w_{i-N_K} \oplus w_{i-1}, & \text{при } i \bmod N_K \neq 0 \end{cases}$$

Рис. 3. Линейное соотношение выработки слов: W – 4-байтовые слова, N_K – число 32-битовых слов в ключе

Функция G – это нелинейное преобразование 32-битовых слов, которые выглядят как:

- байтовый сдвиг;
- побайтовая подстановка по вектору замен;
- побитовое сложение по модулю 2 с вектором.

Можно заметить, алгоритм выработки ключей у AESa более сложный, чем у ГОСТа и DES, но, несмотря на это, он довольно простой и эффективный.

Силовая атака на ГОСТ абсолютно бесперспективна. ГОСТ использует 256-битовый ключ, а если учитывать секретные S-блоки, то длина ключа будет еще большей. ГОСТ более устойчив к дифференциальному и линейному криптоанализу, чем DES.

Библиографический список

1. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.

2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.
3. Панасенко С.П. Вые. – 2003. – № 8(60).
4. Сушко С.А. Практическая криптология, лекция 9 2014 [Электронный ресурс]. – URL: <http://bit.nmu.org.ua/ua/>
5. Сравнение симметричных стандартов шифрования РФ и США от 25.12.2014 [Электронный ресурс]. – URL: <https://allbest.ru/>
6. Панасенко С.П. Мифы и реальность криптографических алгоритмов [Электронный ресурс]. – URL: <http://www.panasenko.ru/>
7. Винокуров А., Применко Э. Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США // Системы безопасности. – М.: Гротэк, 2001. – № 1,2.
8. Чмора А.Л. Современная прикладная криптография. – М.: Гелиос АРВ, 2001. – 256 с.

Сведения об авторах

Пьянков Павел Евгеньевич – магистрант Пермского национального исследовательского политехнического университета, Пермь, e-mail: monyapb@yandex.ru

Ведерникова Ольга Степановна – магистрант Пермского национального исследовательского политехнического университета, Пермь, e-mail: ole444ka1995@mail.ru

Кротова Елена Львовна – кандидат физико-математических наук, доцент кафедры «Высшая математика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: lenkakrotova@yandex.ru

About the authors

Ryankov Pavel Evgenevich – Master Student Perm National Research Polytechnic University, Perm, e-mail: monyapb@yandex.ru

Vedernokova Olga Stepanovna – Master Student Perm National Research Polytechnic University, Perm, e-mail: vernikovaos@mail.ru

Krotova Elena Lvovna – Ph.D. in Physic-Mathematic Sciences, Associate Professor of the department "Higher mathematics" Perm National Research Polytechnic University, Perm, e-mail: lenkakrotova@yandex.ru

О РАЗРАБОТКЕ МОДЕЛИ НЕЙРОННОЙ СЕТИ ДЛЯ ВЫЯВЛЕНИЯ ЗЛОУМЫШЛЕННИКА В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПРЕДПРИЯТИЯ

А.С. Сорокин, А.С. Шабуров

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье описана разработка математической модели процесса обучения нейронной сети. Составлены характеристики пользователей, которые могут выявить нарушителя, и описаны действия по обучению нейронной сети. В результате была разработана модель искусственной нейронной сети для выявления потенциального злоумышленника внутри корпоративной системы для предприятия (организации).

Ключевые слова: искусственные нейронные сети, аппроксимация, потенциальный злоумышленник, оценка характеристик пользователей.

ABOUT THE DEVELOPMENT OF THE MODEL OF THE NEURAL NETWORK FOR THE IDENTIFICATION OF THE MALEFACTOR IN THE ENTERPRISE INFORMATION SYSTEM

A.S. Sorokin, A.S. Shaburov

Perm National Research Polytechnic University, Perm

In this article, a mathematical model of the learning process of a neural network was developed. The characteristics of users that can identify the malefactor is described, and the actions for training the neural network is described. As a result, a model of an artificial neural network was developed to identify a potential malefactor within the corporate system for the enterprise (organization).

Keywords: artificial neural networks, approximation, potential malefactor, evaluation of user characteristics.

В настоящее время существует много различных угроз информационной безопасности, появляются всё более изощренные атаки злоумышленников, а также создаются более эффективные методы несанкционированного доступа, характеризующиеся высокой сложностью обнаружения. Всё это является актуальной проблемой для защиты информации.

Рынок средств по информационной безопасности включает в себя большое разнообразие решений, однако подобрать эффективное средство борьбы с такими угрозами, – это трудная задача. Поэтому разработка новых способов и методов защиты информации приобретает всё большую актуальность.

В современном мире высока актуальность применения технологий искусственных нейронных сетей в области защиты информации посредством самообучаемости и быстрого обнаружения угроз.

Существует много разработанных моделей на основе искусственных нейронных сетей для обеспечения защиты информации. Такие модели могут быть использованы для фильтрации спама, для распознавания компьютерных атак, оценки защищенности объекта, мониторинга безопасности информационных систем, обнаружения вторжений, безопасного хранения информационных данных, защиты от ddos-атак, шифрования, создания хэш-функций, а также для выявления злоумышленника и последующих его действий [4].

Нейронную сеть в области информационной безопасности используют для решения задач аппроксимации, кластеризации, прогнозирования и классификации. Для выявления потенциального злоумышленника по его характеристикам подойдет нейросетевая аппроксимация [1].

Рассмотрим реализацию модели на основе НС, которая выявляет потенциальных злоумышленников среди пользователей в крупной организации, т.е. поиск внутренних нарушителей. Для этого нужно создать и обучить искусственную нейронную сеть, чтобы оценить параметры пользователей и их возможную угрозу для предприятия. Нейросеть будет обучаться с учителем, т.е. предполагается предъявление значений как входных, так и выходных сигналов.

Для создания модели искусственной нейронной сети, которая будет выявлять потенциального злоумышленника, необходимо выбрать данные пользователей для ввода в сеть. Если не провести предварительную работу над ними, то сеть не сможет найти зависимость между входными и выходными сигналами, что повлечёт за собой неверный результат [5].

В первую очередь необходимо определить размерность входного массива, она будет зависеть от параметров пользователя, которые нужно найти. Чтобы отыскать их, представим модель нарушителя.

Искать склонность к нарушениям у пользователей будем среди работчиков, обычных пользователей АС и обслуживающего персонала, такие как системный администратор, сотрудники обеспечения ИБ и т.д.

К входным данным хорошо подойдет степень влияния злоумышленника на критерии информационной безопасности, это конфиденциальность, целостность и доступность. Будет рассматриваться шанс пользователей нарушения этих критериев в процентной вероятности.

Канал передачи информации является важным фактором для защиты от злоумышленников. Технические каналы утечки информации есть в любом предприятии, которые нужно обеспечить от НСД. Поэтому будет использована вероятность утечки информации по акустическому, акустоэлектрическому, телефонному и оптическому каналам как входной параметр для НС.

Также пользователи могут подвергнуть организацию к созданию уязвимостей. Сотрудники из-за их оплошностей непреднамеренно могут нести угрозу и таким образом имеют возможность стать нарушителем. Этот параметр тоже будет учитываться нейронной сетью. Помимо этого выделим конкретную угрозу, которая будет приниматься к сведению НС, это вероятность заражения компьютера с помощью Интернета. В большой организации пользователи часто используют электронную почту, интернет-ресурсы для выполнения определённых задач, всё это способствует вероятности заражения АС.

Используем во входных данных степень наносимого ущерба предприятию. Подразделять его будем по размерам: общий ущерб, когда наносится вред объекту безопасности в целом, оказывая негативное воздействие на условия его деятельности; локальный ущерб, затрагивающий условия существования отдельных элементов объекта безопасности; частный ущерб, который наносит вред отдельным свойствам элементов объекта безопасности или отдельным направлениям его деятельности.

В Руководящем документе [3] в качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС. Другими словами, будем классифицировать потенциальных злоумышленников по уровню их возможностей обращения с АС и СВТ, разделенных на четыре уровня. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего [3]. Первый уровень определяет самые простые возможности пользователей с АС, такие как запуск задач, имеющих заранее подготовленные функции обработки. Во втором уровне имеется возможность создания и запуска собственных программ. Третий уровень подразумевает управление функционированием АС, т.е. воздействие на базовое ПО-системы. На четвертом уровне осуществляются проектирование, реализация и ремонт технических средств АС. Эти данные тоже будут обрабатываться НС.

Также для выявления потенциального злоумышленника включим такие параметры, как возраст пользователя, его материальное положение (доход в месяц), доступ к ГТ, опыт работы в организации, и наличие связей с конкурентами.

В итоге количество входных значений получилось 17. Всего таких данных будет 100, т.е. возьмем за основу 100 пользователей. Все категории используемых данных представлены в таблице.

Входные данные для искусственной нейронной сети

Параметры	Представление в ИНС
1. Возраст пользователя	Количество лет пользователю
2. Материальное положение	Доход пользователя в месяц
3. Допуск к ГТ	1 – особой важности; 2 – совершенно секретно; 3 – секретно; 4 – нет допуска к ГТ
4. Уровень возможностей в АС	1 – первый уровень; 2 – второй уровень; 3 – третий уровень; 4 – четвёртый уровень
5. Должность	1 – разработчик; 2 – обслуживающий персонал; 3 – обычный пользователь
6. Имеет связи с конкурентами	0 – нет, не имеет; 1 – да, имеются
7. Опыт работы в организации	Количество лет работы
8. Нарушение конфиденциальности	Вероятностная величина
9. Нарушение целостности	Вероятностная величина
10. Нарушение доступности	Вероятностная величина
11. Наносимый ущерб	1 – общий ущерб; 2 – локальный ущерб; 3 – частный ущерб
12. Заражение компьютера	Вероятностная величина
13. Утечка информации по акустическому каналу	Вероятностная величина
14. Утечка информации по акустоэлектрическому каналу	Вероятностная величина
15. Утечка информации по телефонному каналу	Вероятностная величина
16. Утечка информации по оптическому каналу	Вероятностная величина
17. Создание уязвимостей	Вероятностная величина

Выходные данные созданной нейронной сети будут представлять из себя процентную составляющую, того что пользователь является злоумышленником.

Следующим шагом является создание нейросети, которая научится оценивать потенциальных злоумышленников. Для разработки

берётся среда MatLab, так как она хорошо подходит для реализации моделей НС [6]. Сформируем двухслойную нейронную сеть прямого распространения, включающую 10 нейронов в скрытом слое и 1 нейрон в выходном слое (рис. 1). Если в дальнейшем сеть будет плохо обобщать данные, то тогда количество нейронов в скрытом слое стоит увеличить [2]. Введём параметры в созданную сеть таким образом, чтобы было 100 примеров по 17 значений.

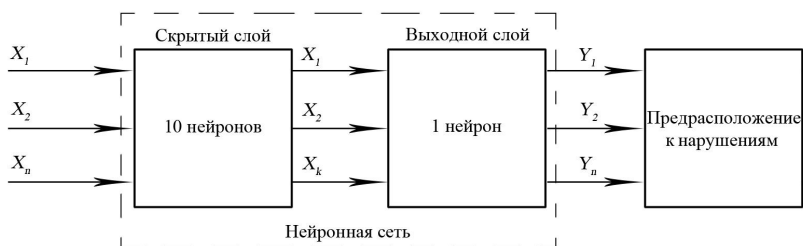


Рис. 1. Схема разработанной двухслойной нейронной сети для выявления потенциального злоумышленника

Перед обучением разделим параметры для тренировки, проверки и теста. Для тренировки будет использовано больше значений, так как сеть будет настраиваться в соответствии с полученной ошибкой при обучении. Данные для проверки используют для обобщения сети и для прекращения обучения, когда сеть перестанет улучшаться. Обучение будет продолжаться до тех пор, пока сеть не перестанет улучшаться на множестве проверок. Тестовый набор значений не влияет на обучение, и поэтому обеспечивает полную независимую оценку производительности сети, вовремя и после обучения.

Затем обучаем искусственную нейронную сеть, чтобы она нашла зависимость соответствия исходных и целевых показателей. Процесс обучения иллюстрируется графиком зависимости средней квадратичной ошибки от эпохи обучения – одна итерация в процессе обучения, которая предьявляет все примеры из обучающего множества и проверку качества обучения (рис. 2). Точкой указано, когда ошибка на проверочной (зелёной) линии перестает уменьшаться, затем обучение прекращается.

В результате получаем искусственную нейронную сеть, обученную на 100 тренировочных данных, которая способна находить процентную составляющую потенциальных злоумышленников среди пользователей по тем параметрам, которые были приведены выше.

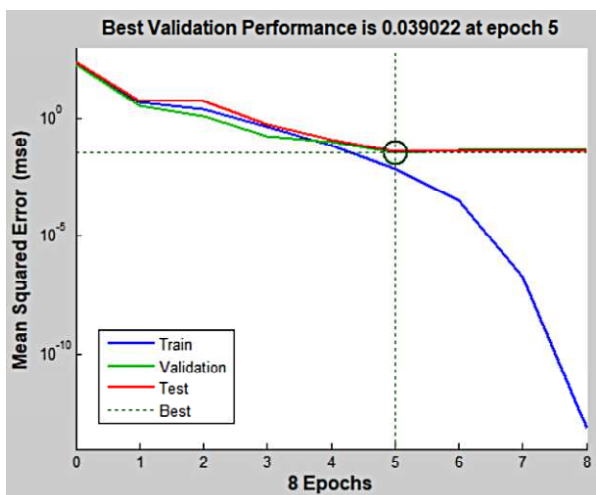


Рис. 2. График обучения нейронной сети

Таким образом, анализ критериев пользователей внутри организации позволил выявить наиболее яркие параметры, которые могут быть связаны с правонарушениями. Разработанная модель искусственных нейронных сетей для выявления потенциального злоумышленника внутри организации позволяет оценить склонность пользователей к преступлениям, что, в конечном счёте, способствует повышению уровня защищенности информации на предприятии.

Библиографический список

1. Бондарев В.Ю., Сорокин А.С., Кротова Е.Л. Искусственная нейронная сеть для выявления злоумышленника в автоматизированной рабочей системе // *Master's Journal / Журнал магистров*. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2016. – № 2. – С. 150–153.
2. Бондарев В.Ю., Сорокин А.С., Кротова Е.Л. Искусственная нейронная сеть как средство и метод статистической обработки данных // *Вестник УрФО. Безопасность в информационной сфере*. – 2016. – № 20. – С. 19–22.
3. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: руководящий документ (от 30 марта 1992). – М.: Гостехкомиссия РФ, 1992. – 5 с.

4. Марков Г.А. Глинская Е.В. Использование технологий нейронных сетей при решении задач информационной безопасности // Молодежный научно-технический вестник. – 2014. – № 3.

5. Сорокин А.С., Бондарев В.Ю., Кротова Е.Л. Искусственные нейронные сети. Подготовка входных и обработка выходных данных // Инновационные технологии: теория, инструменты, практика: материалы VIII Международ. интернет-конф. молод. уч., аспирант., студ. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2017 – С. 234–236.

6. Сорокин А.С., Бондарев В.Ю., Кротова Е.Л. Создание и обучение искусственной нейронной сети для статистического оценивания данных // Вестник УрФО. Безопасность в информационной сфере. – 2016. – № 20. – С. 29–32.

Сведения об авторах

Сорокин Андрей Станиславович – магистрант Пермского национального исследовательского политехнического университета, Пермь, e-mail: sly-kyper@yandex.ru

Шабуров Андрей Сергеевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: shans@at.pstu.ru

About the authors

Sorokin Andrey Stanislavovich – Master Student Perm National Research Polytechnic University, Perm, e-mail: sly-kyper@yandex.ru

Shaburov Andrey Sergeevich – Ph.D. in Technical Sciences, Associate Professor of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: shans@at.pstu.ru

MAC-УРОВЕНЬ В СЕТЯХ MANET

А.К. Стафеев, С.А. Тюрин

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассмотрен MAC-уровень сетей MANET.

Ключевые слова: MANET, MAC-уровень, DCF, EDCA, MCCA.

MAC LEVEL OF MANET NETWORKS

A.K. Stafeev, S.A. Tyurin

Perm National Research Polytechnic University, Perm

In this article the MAC layer of the MANET networks is considered.

Keywords: MANET, MAC layer, DCF, EDCA, MCCA.

Наиболее важным для эффективной работы радиосетей с коммутацией пакетов является канальный уровень, точнее, его MAC-подуровень из-за его концептуальной сложности и глобального сетевого влияния, так как нерациональная организация коллективного доступа к радиоканалу может значительно снизить скорость передачи пакетов по сети или даже совсем заблокировать ее работу вне зависимости от качества функционирования других уровней эталонной модели OSI.

Метод доступа DCF. В сетях Wi-Fi ad hoc (стандарт IEEE 802.11) базовым механизмом доступа к среде является режим распределенного управления DCF (Distributed Coordination Function – распределенный режим доступа), в его основе лежит метод множественного доступа с контролем несущей и избеганием коллизий CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Режим доступа DCF требует синхронизации станций. В спецификации 802.11 эта проблема решается достаточно элегантно – временные интервалы начинают отсчитываться от момента окончания передачи очередного кадра. Это не требует передачи каких-либо специальных синхронизирующих сигналов и не ограничивает размер пакета размером слота (рис. 1).

Станция, которая хочет передать кадр, предварительно прослушивает среду. Как только ею обнаруживается окончание передачи кадра, она начинает отсчитывать интервал времени, равный межкадровому интервалу (IFS). Если после окончания интервала IFS среда все

еще свободна, то начинается отсчет слотов фиксированной длительности. Кадр можно начать передавать только в начале одного из слотов при условии, что среда не занята. Станция выбирает для передачи слот на основании усеченного экспоненциального двоичного алгоритма отсрочки, аналогичного используемому в методе CSMA/CD. Номер слота выбирается как случайное целое число, равномерно распределенное в интервале $[0, CW]$, где CW означает Contention Window (конкурентное окно).

Условия, необходимые для начала передачи:

- 1) среда оставалась свободной в течение интервала IFS;
- 2) значение счетчика отсрочки равно нулю.

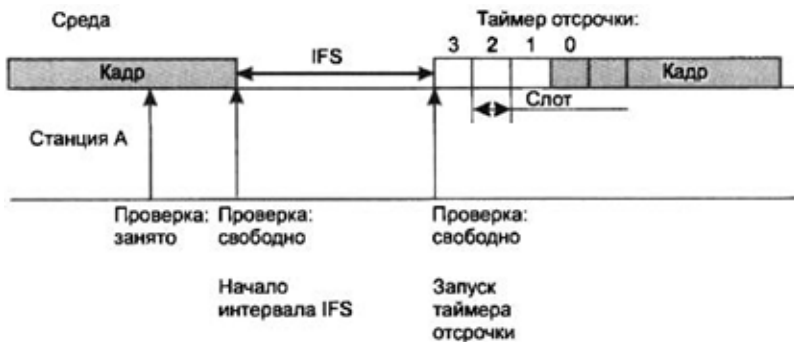


Рис. 1. Режим доступа DCF

Если же в начале какого-нибудь слота среда оказывается занятой, то уменьшение таймера не происходит, и таймер «замораживается». В этом случае станция начинает новый цикл доступа к среде, использует значение «замороженного» таймера в качестве номера слота и выполняет описанную процедуру проверки свободных слотов с вычитанием единиц, начиная с «замороженного» значения таймера отсрочки.

Размер слота зависит от способа кодирования сигнала; так, для метода FHSS размер слота равен 28 мкс, а для метода DSSS – 1 мкс. Размер слота выбирается таким образом, чтобы он превосходил время распространения сигнала между любыми двумя станциями сети плюс время, затрачиваемое станцией на распознавание ситуации занятости среды. В этом случае каждая станция сети сумеет правильно распознать начало передачи кадра при прослушивании слотов. Это,

в свою очередь, означает, что коллизия может случиться только в том случае, когда несколько станций выбирают один и тот же слот для передачи.

В этом случае кадры искажаются, и квитанции подтверждения приема от станций назначения не приходят. Не получив в течение определенного времени квитанцию, отправители фиксируют факт коллизии и пытаются передать свои кадры снова. При каждой повторной неудачной попытке передачи кадра интервал $[0, CW]$, из которого выбирается номер слота, удваивается. Начальное значение CW в соответствии со стандартом 802.11 должно выбираться в зависимости от типа физического уровня, используемого в беспроводной локальной сети.

Количество неудачных попыток передачи одного кадра ограничено, но стандарт 802.11 не дает точного значения этого верхнего предела. Когда верхний предел RL (Retry Limit – ограничение числа повторов) в N попыток достигнут, то кадр отбрасывается, а счетчик последовательных коллизий устанавливается в нуль. Этот счетчик также устанавливается в нуль, если кадр после некоторого количества неудачных попыток все же передается успешно [2].

В режиме доступа DFC могут применяться меры для устранения эффекта скрытого терминала (рис. 2). Для этого станция, которая хочет захватить среду и в соответствии с описанным алгоритмом, начинает передачу кадра в определенном слоте, вместо кадра данных сначала посылает станции назначения короткий служебный кадр RTS (Request To Send – запрос на передачу). На этот запрос станция назначения должна ответить служебным кадром CTS (Clear To Send – свободна для передачи), после чего станция-отправитель посылает кадр данных. Кадр CTS должен оповестить о захвате среды те станции, которые находятся вне зоны сигнала станции-отправителя, но в зоне досягаемости станции-получателя, т.е. являются скрытыми терминалами для станции-отправителя.

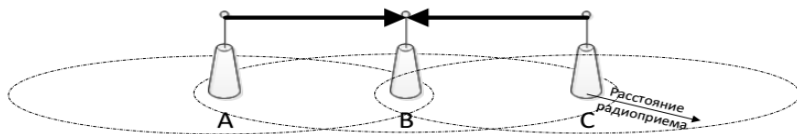


Рис. 2. Эффект скрытого терминала

Метод доступа к среде DCF имеет ограничения/недостатки:

1. При одновременном взаимодействии большого количества станций происходит множество коллизий, которые снижают общую доступную ширину канала (так же, как в Ethernet, который использует CSMA/CD).

2. Алгоритм не различает коллизию и повреждение пакета при передаче. Это приводит к существенному влиянию на общую производительность системы (многократное увеличение окна CW), в то время как фактически пакет может быть поврежден при передаче. Алгоритм DCF характеризуется также низкой пропускной способностью при больших трафиковых нагрузках.

3. Если станция получает доступ к эфиру, она может занимать его столько, сколько ей нужно. И если эта станция имеет низкую пропускную способность, то будет страдать пропускная способность всей сети.

4. Нет разделения трафика по приоритету, отсутствие гарантий QoS.

Методы доступа EDCA и МССА. Также необходимо рассмотреть более новый стандарт Wi-Fi Mesh (IEEE 802.11s), который решает некоторые из перечисленных ранее проблем. В стандарте определены два механизма: механизм конкурентного доступа – EDCA, который является базовым, и, опционально, механизм детерминированного доступа – МССА.

Алгоритм EDCA описан еще в стандарте IEEE 802.11e и, по существу, является расширением стандарта 802.11, включающим в себя возможность QoS (но его не обеспечивает), т.е. механизм управления трафиком согласно приоритетам, в соответствии с которыми высокоприоритетный трафик имеет больше шансов быть отправленным.

Детерминированный доступ (МССА) – это опциональный механизм, позволяющий станциям получать доступ к среде в заранее зарезервированные временные интервалы. При использовании МССА станции совместно координируют доступ к среде.

А именно станция, установившая резервирование, получает бесконкурентный доступ к среде в заранее зарезервированные временные интервалы, при этом все остальные станции, которые могут конкурировать с передачей данной станции, должны воздержаться от передачи. Применение механизма МССА снижает конкуренцию доступа к среде передачи, что позволяет существенно увеличить вероятность своевременной доставки данных и потенциально может быть

использовано для передачи трафика, чувствительного к задержкам. Использование МССА позволяет значительно повысить суммарную пропускную способность сети за счет более эффективного использования ресурсов канала и уменьшения вероятности коллизий. Согласно стандарту этот механизм не является обязательным для всех станций сети.

Создание МССА-резервирования инициируется узлом-источником, который также называется владельцем резервирования, а принимается или отклоняется узлом-адресатом данных. МССА-резервирование определяется тремя параметрами: периодичностью (МССFOP Periodicity), длительностью (МССAOP Duration) и начальным смещением (МССAOP Offset). МССAOP Periodicity указывает на то, сколько временных интервалов длительностью МССAOP Duration резервируются внутри DTIM-интервала (интервала между двумя последовательными DTIM-биконами), а величина МССAOP Offset определяет смещение первого интервала относительно DTIM-бикона (рис. 3). Величины МССAOP Offset и МССAOP Duration измеряются в интервалах длительностью 32 мкс. При установлении МССА-резервирования узел-источник выбирает параметры резервирования таким образом, чтобы резервируемые временные интервалы не пересекались с другими резервированиями, о которых ему уже известно.

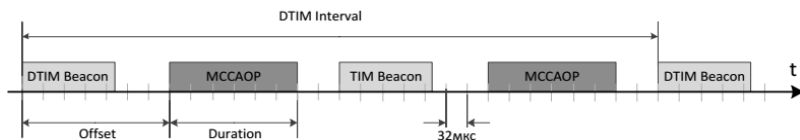


Рис. 3. МССА-резервирование с периодичностью 2

Также узел проверяет, что при добавлении вновь создаваемого резервирования не будут превышены величины MAFLimit и MaxTrackStates как у него самого, так и у его соседей. Величина MAFLimit определяет максимальную долю времени внутри DTIM-интервала, которая может быть использована под МССА-резервирования данным узлом и его соседями, и позволяет ограничивать объем ресурсов, используемых под МССА. А величина MaxTrackStates определяет максимальное число резервирований, которое устройство может хранить в своей памяти. Если все условия выполнены, то узел-источник отправляет узлу-адресату специальный

информационный элемент MCCAOP Setup Request, который содержит параметры планируемого резервирования и уникальный идентификатор резервирования. Если какое-то из условий не выполнено или не найдены свободные интервалы для резервирования, то узел отказывается от резервирования. Узел получает информационный элемент MCCAOP Setup Request, который содержит либо подтверждение установления резервирования, если все условия выполнены, либо отказ в установлении резервирования с указанием причины, либо альтернативные параметры резервирования. Если узел получает MCCAOP Setup Request с альтернативными параметрами, он может инициировать резервирование с полученными параметрами.

Для разрыва MCCA-резервирования владелец или получатель могут послать специальный информационный элемент MCCAOP Teardown. Также владелец резервирования закрывает резервирование, если в течение промежутка времени MCCAOP Timeout он не получал кадров подтверждения от адресата резервирования на кадры, переданные внутри интервалов резервирования. Аналогично адресат резервирования закрывает резервирование, если он в течение промежутка времени MCCAOP Timeout не получал кадров данных внутри интервалов резервирования.

Для того чтобы вновь устанавливаемые резервирования не перекрывались с уже существующими, узлы сети периодически в биконах (DTIM Beacon) или специальных служебных кадрах распространяют информационные элементы, содержащие информацию об уже существующих резервированиях (рекламируют резервирования).

Внутри интервалов резервирования (MCCAOP) для доступа к среде используется конкурентный метод доступа EDCA. При этом владелец резервирования для получения бесконкурентного доступа внутри MCCAOP использует специальные значения параметров EDCA (AIFS=PIFS, CWmin=0) для каждой из своих очередей. Если у владельца резервирования на момент начала MCCAOP не оказалось кадров данных в очереди, то он может завершить MCCAOP заранее и сообщить об этом соседним узлам с помощью служебного кадра CF-END.

Для того чтобы обеспечить владельцу резервирования бесконкурентный доступ к среде, соседи владельца и адресата резервирования воздерживаются от передачи внутри интервалов резервирования и возводят специальный таймер, называемый RAV, на все время резервирования. Также согласно стандарту узлы соседи владельца

и адресата резервирования не имеют право начинать передачу кадра с использованием EDCA, если эта передача пересекается с каким-либо интервалом резервирования соседнего узла [1].

Недостатки метода МССА:

1. Хотя метод МССА и позволяет бороться с эффектом скрытых станций, он удобен лишь при доставке потоковых данных постоянной интенсивности, например голосовых данных.

2. Метод МССА сложен в реализации, поэтому в стандарте он отмечен как опциональный, т.е. некоторые станции могут его не поддерживать. Если станция не поддерживает МССА, то она резервирования не устанавливает, а осуществляет доступ к среде на конкурентной основе. Эффективность МССА тем ниже, чем меньше станций сети его поддерживают.

Библиографический список

1. Красилов А.Н., Ляхов А.И. Использование МССА для предоставления QoS в сетях IEEE 802.11s // Материалы 34-й конф. молодых ученых и специалистов ИППИ РАН. – 2011. – С. 282–293.

2. Кулаков М.С. Анализ особенностей функционирования мобильных самоорганизующихся сетей MANET на уровне доступа к среде MAC // Т-Comm: Телекоммуникации и трансп. – 2014. – № 10. – С. 39–42.

Сведения об авторах

Стафеев Александр Константинович – магистрант Пермского национального исследовательского политехнического университета, Пермь, e-mail: stafa59@mail.ru

Тюрин Сергей Александрович – старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: tiurinsa@yandex.ru

About the authors

Stafeev Aleksandr Konstantinovich – Master Student Perm National Research Polytechnic University, Perm, e-mail: stafa59@mail.ru

Tyurin Sergey Aleksandrovich – Senior Lecturer of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: tiurinsa@yandex.ru

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ВЕЩЕЙ

С.П. Хиков, А.Н. Каменских

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье описана сущность интернет-вещей. Перечислены основные уязвимости и угрозы интернет-вещей. Рассмотрены проблемы информационной безопасности интернет-вещей и их причины. Предложены доступные способы защиты Интернета вещей.

Ключевые слова: интернет вещей, информационная безопасность, угроза безопасности.

PROBLEMS OF INFORMATION SECURITY INTERNET OF THINGS

S.P. Khikov, A.N. Kamenskih

Perm National Research Polytechnic University, Perm

This article describes the essence of the Internet of things. The main vulnerabilities and threats to the Internet of things are listed. The problems of information security of the Internet of things and their causes are considered. Available ways to protect the Internet of things are suggested.

Keywords: IoT, information security, security threat.

В настоящее время количество электроники, которая умеет выходить в Интернет (телефоны, компьютеры, телевизоры, холодильники и другие) все растет. Количество вещей, подключенных к Интернету, превысило количество людей на планете еще в 2008 г. и продолжает расти немалыми темпами [7]. Вся эта техника используется нами повседневно, помогает решать быденные задачи, и обеспечивает удобство и комфорт, может повысить качество жизни больных и пожилых людей. Но, приобретая ее, люди чаще всего не задумываются, что безопасность, у большинства таких устройств не находится на должном уровне.

Под термином Интернет вещей или Internet of Things, IoT подразумевается концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия как друг с другом, так и с внешней средой без участия человека. Они подразделяются на промышленный и потребительский.

В промышленном IoT основными разновидностями «вещей», которые надо подключать к сети, являются различные типы датчиков

(сенсоров) и приводов для сбора и обмена данными, с возможностью удаленного контроля и управления [9].

К потребительскому IoT относятся: носимые устройства, умный дом, умная одежда, Smart TV, IP-камеры, умные девайсы для животных, устройства для автомобилей.

Приобретая такие устройства, люди чаще всего не задумываются, что зачастую безопасность у них не находится на должном уровне. С одной стороны, удаленное управление системами позволяет с большим комфортом организовать свое жизненное пространство; а с другой – датчики и элементы управления системами жизнеобеспечения, оказавшись в руках злоумышленника, значительно увеличивают риски в области информационной безопасности [8].

Аналитики Gartner прогнозируют, что по итогам 2017 г. во всем мире к Интернету вещей будет подключено 8,4 млрд устройств. Результаты сканирования разработанной BullGuard программой IoT Scanner 310 тыс. пользовательских сетевых устройств показали, что 4,5 % (почти 14 тыс.) из них уязвимы и могут быть без труда взломаны. Аналитики BullGuard прогнозируют, что потенциально уязвимыми являются 378 млн устройств [1].

В таблице перечислены типичные уязвимости, обнаруженные в рамках исследования, проведенного компанией HPE [2].

Распространенные уязвимости устройств Интернета вещей

Уязвимость	Примеры
Незащищенный веб-интерфейс (мобильный, облачный)	Слабые пароли; ненадежные системы восстановления паролей; отсутствие механизма блокировки учетной записи; уязвимость для атак на основе межсайтовых скриптов, подделки запросов
Слабость средств аутентификации и проверки полномочий	Необоснованное повышение привилегий, отсутствие контроля доступа
Незащищенные сетевые сервисы	Уязвимость для атак на отказ в обслуживании, переполнение буфера, нечеткое тестирование; предоставление без необходимости доступа к сетевым портам и сервисам извне
Отсутствие шифрования данных и проверки целостности данных при передаче	Передача информации без шифрования
Отсутствие обеспечения приватности	Сбор данных о пользователе без необходимости; недостаточный контроль доступа к пользовательским данным; отсутствие механизмов анонимизации конфиденциальных данных

Уязвимость	Примеры
Недостаточные возможности настройки параметров безопасности	Отсутствие схемы разграничения привилегий; отсутствие разделения прав администратора и пользователей; допустимость слабых паролей; отсутствие журнала безопасности; отсутствие вариантов выбора механизмов шифрования данных; отсутствие предупреждений пользователя о событиях безопасности
Незащищенное программное или микропрограммное обеспечение	Отсутствие механизма защищенных обновлений; файлы обновлений не шифруются; файлы обновлений не проверяются перед загрузкой; незащищенный сервер обновлений
Недостаточная физическая защищенность	Наличие доступа к ПО через порты USB; наличие съемных носителей информации

Для устройств Интернета вещей характерны следующие угрозы:

- получение несанкционированного доступа;
- внедрение вредоносных программ;
- выявления паролей;
- перехват сетевого трафика;
- сканирование открытых портов;
- удаленный запуск приложений.

При успешной реализации таких угроз злоумышленники могут получить доступ к устройству для получения информации о пользователе, подсматривать через взломанные камеры, отслеживать перемещение устройств, создавать ботнеты с сотнями или тысячами уязвимых устройств, с помощью которых атакуют и взламывают серверы и веб-сайты, устраивать DDoS-атаки. На этом список возможных последствий не заканчивается, его можно продолжать и продолжать.

Одна из проблем устройств интернет-вещей – это недостаточное внимание обеспечению безопасности при проектировании и производстве. Ее следствием являются ошибки в программном коде, отсутствие обновлений для выпущенных продуктов. Причина этой проблемы – это то, что более половины продуктов IoT производится небольшими компаниями, существующими менее трех лет. Можно предположить, что лишь часть этих компаний в силах обеспечить нормальный уровень безопасности своих изделий [5]. Кроме того, цель производителей – это продать IoT-устройства. Результатом всего этого является то, что устройства IoT имеют очень слабую защиту или ее нет совсем, а рынок наполнен подобными уязвимыми устройствами [6]. Пока производители не уделяют должного внимания безопасности своей продукции, потребитель должен сам задуматься о защите своих данных.

Во-первых, стоит задуматься, стоит ли подключать устройство к Интернету. Может быть, эти функции не будут востребованы. Если не предполагается использовать его через сеть, то не следует подключать устройство к Интернету.

Во-вторых, будет безопаснее, если создать отдельную сеть для таких устройств, например, с помощью Wi-Fi маршрутизатора, тем самым обеспечив безопасность основной сети. В случае взлома этой сети ваш компьютер и мобильные устройства, подключенные к основной сети (которая является приоритетным интересом злоумышленников), будут в безопасности [4].

В-третьих, другим важным моментом являются смена пароля и обновление устройства. Большинство атак злоумышленников происходит путём перебора стандартных логинов и паролей производителей, поэтому при первой настройке устройства пароль, поставленный производителем, нужно изменить на уникальный. А регулярная проверка и установка обновлений позволят закрыть уязвимости, обнаруженные производителем.

Выполнение этих действий поможет уберечь устройства.

Другие проблемы связаны со спецификой таких устройств, это проблемы малых вычислительных ресурсов, что усложняет обеспечение безопасности большого числа устройств, как и отсутствие единых стандартов для их взаимодействия. Они в данный момент еще не решены.

Сможет ли Интернет вещей стать безопасным? Вероятно, да. Но лишь тогда, когда подавляющее большинство разработчиков начнет с большей ответственностью относиться к защите своих гаджетов [3]. Использование устройств интернет-вещей позволяет повысить эффективность в промышленной отрасли и улучшить качество жизни людей. Но при их использовании нужно быть осторожным.

Библиографический список

1. IoT-ботнет Reaper может задействовать для атак 378 млн уязвимых IoT-устройств [Электронный ресурс]. – URL: <https://iot.ru/bezopasnost/iot-botnet-reaper-mozhet-zadeystvovat-dlya-atak-378-mln-uyazvimykh-iot-ustroystv> (дата обращения: 09.11.2017).
2. Ботнеты и безопасность Интернета вещей [Электронный ресурс]. – URL: <https://www.osp.ru/os/2017/02/13052219/> (дата обращения: 15.11.2017).

3. Интернет вещей угрожает человечеству [Электронный ресурс]. – URL: <https://hyser.com.ua/tehnology/internet-veshhej-ugrozhaet-chelovechestvu-104393> (дата обращения: 09.11.2017).

4. Интернет вещи (iot) и их безопасность [Электронный ресурс]. – URL: <http://www.cleper.ru/articles/description.php?n=589> (дата обращения: 21.11.2017).

5. Как обезопасить Интернет вещей? [Электронный ресурс]. – URL: <https://rb.ru/story/IoT-security/> (дата обращения: 15.11.2017).

2. Новые угрозы и направления развития информационной безопасности в 2017 году [Электронный ресурс]. – URL: <http://1234g.ru/novosti/infobezопасnost-2017> (дата обращения: 15.11.2017).

3. Проблемы безопасности SmartTV [Электронный ресурс]. – URL: <https://cyberleninka.ru/article/n/problemy-bezопасnosti-smarttv> (дата обращения: 01.11.2017).

4. Проблемы информационной безопасности: интернет вещей [Электронный ресурс]. – URL: <https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezопасnosti-internet-veschey> (дата обращения: 01.11.2017).

5. Промышленный интернет вещей. Готовы ли сети? [Электронный ресурс]. – URL: <https://www.osp.ru/lan/2016/09/13050308> (дата обращения: 09.11.2017).

Сведения об авторах

Хиков Семен Павлович – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: Feg200@yandex.ru

Каменских Антон Николаевич – кандидат технических наук, старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: antoshkinoinfo@yandex.ru

About the authors

Khikov Semen Pavlovich – Student Perm National Research Polytechnic University, Perm, e-mail: Feg200@yandex.ru

Kamenskih Anton Nikolayevich – Ph.D. in Technical Sciences, Senior Lecturer of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: antoshkinoinfo@yandex.ru

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ ПРИ РАЗРАБОТКЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

В.А. Чалин, А.С. Шабуров

Пермский национальный исследовательский
политехнический университет, Пермь

В данной работе разработаны и проанализированы модель выявления, а также модель идентификации уязвимостей при разработке информационных систем персональных данных.

Ключевые слова: персональные данные, информационная система, уязвимость, угроза, пользователь, анализ, система защиты, методы.

DETECTION OF VULNERABILITY IN THE DEVELOPMENT OF INFORMATION SYSTEMS OF PERSONAL DATA

V.A. Chalin, A.S. Shaburov

Perm National Research Polytechnic University, Perm

In this paper, we developed and analyzed a detection model, as well as a vulnerability identification model for the development of information systems for personal data.

Keywords: Personal data, information system, vulnerability, user, analysis, system security, methods.

Введение. Информация, содержащая в себе данные о человеке или группе лиц, всегда имела высокую ценность. С развитием информационных технологий персональные данные превратились в самый дорогой товар. Информационные системы, обрабатывающие такие данные, должны иметь высокую степень защиты не только в период эксплуатации, но и на этапах их разработок.

Возможность реализации угрозы всегда напрямую зависит от действий злоумышленника по ее поиску. С другой стороны, работа специалиста в области защиты информации (ЗИ) имеет и другую цель – выявление уязвимостей и действия по их нейтрализации на ранних стадиях разработки информационной системы.

Целью данного исследования является анализ разработка эффективной модели выявления уязвимостей при разработки информационных систем персональных данных.

Согласно ГОСТ Р 56545-2015 «уязвимость» – это недостаток (слабость) программного (программно-технического) средства или

ИС в целом, который (которая) может быть использована для реализации угроз безопасности информации [1]. «Информационная система» – это совокупность содержащейся в базах данных (далее по тексту – БД) информации и обеспечивающих ее обработку информационных технологий и технических средств [1]. Известная уязвимость – это уязвимость, опубликованная в общедоступных источниках с описанием соответствующих мер защиты информации, исправлений недостатков и соответствующих обновлений [1]. Уязвимость нулевого дня – это уязвимость, которая становится известной до момента выпуска разработчиком компонента ИС соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений [1]. Впервые выявленная уязвимость – это уязвимость, не опубликованная в общедоступных источниках [1].

Прежде чем перейти к модели, необходимо пояснить, что ИС состоит из уровней [2]:

- уровень прикладного программного обеспечения (далее по тексту – ПО), отвечающий за взаимодействие с пользователем;
- уровень системы управления базами данных (далее по тексту – СУБД), отвечающий за хранение и обработку данных ИС;
- уровень операционной системы (далее по тексту – ОС), отвечающий за обслуживание СУБД и прикладного ПО;
- сетевой уровень, отвечающий за взаимодействие узлов ИС.

Основными источниками возникновения уязвимостей ИС являются [3, 6]:

- ошибки при разработке (проектировании) ИС (например, ошибки в ПО);
- ошибки при реализации ИС (ошибки администратора ИС) (например, неправильная настройка или конфигурация ПО, неэффективная концепция политики безопасности и т.п.);
- ошибки при использовании ИС (пользовательские ошибки) (например, слабые пароли, нарушение в политике безопасности и т.п.).

Для выявления уязвимостей используются специальные средства анализа защищенности сети (далее – САЗ):

- сетевые САЗ (СБ) (осуществляют удаленный анализ состояний контролируемых хостов на сетевом уровне);
- САЗ (СБ) уровня ОС (осуществляют локальный анализ состояний контролируемых хостов, порой требуется установка специального агента на контролируемых хостах).

– **Модель выявления уязвимостей** (рис. 1). Процесс выявления уязвимостей происходит следующим образом: контроль управления САЗ (далее – КУ САЗ) отправляет запрос на получение необходимых данных о состоянии информационной системы, получает ответ в виде так называемого цифрового слепка и делает анализ, выводом которого служат в данной ИС какие-либо потенциальные уязвимости. Все результаты сканирования находятся в БД уязвимостей.

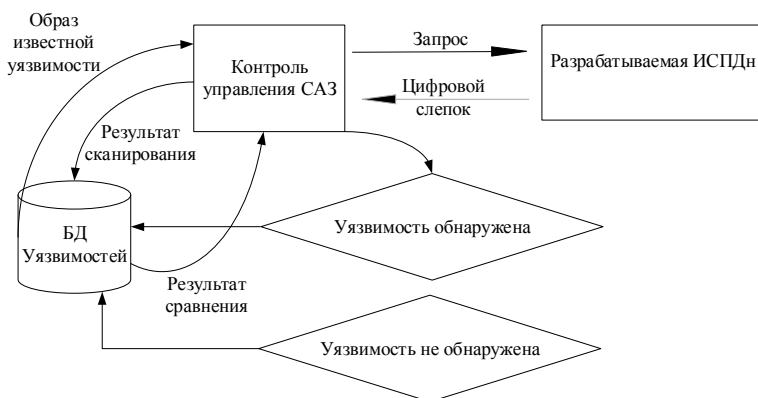


Рис. 1. Модель выявления уязвимостей ИСПДн

На основании сравнения образа из базы уязвимостей с обнаруженной уязвимостью формируется отчет о наличии уязвимостей.

Данная модель имеет два режима работы: режим сканирования (scan) и зондирования (probe), если в первом случае происходит пассивное выявление, то в режиме зондирования САЗ имитирует атаки на контролируруемую информационную систему.

Оба режима достаточно эффективны в своем конкретном случае, так как режим зондирования занимает больше времени на поиск, анализ и выявление уязвимостей, он больше подойдет для работы в уже эксплуатируемой информационной системе, а не как в нашем случае – на этапах разработки.

Сравнение и идентификация образов уязвимостей. Рассмотрим процесс сравнения подробнее, Процесс идентификации образа обнаруженной уязвимости ИС, который имеет специфические характеристики (элементы), осуществляется посредством процедуры его сравнения с образами известных уязвимостей и уязвимостей нулевого дня,

хранящихся в БД уязвимостей. Формализованное описание известных уязвимостей и уязвимостей нулевого дня оформляется в виде паспортов, которые содержат информацию о специфических характеристиках (элементах) конкретной уязвимости (рис. 2).

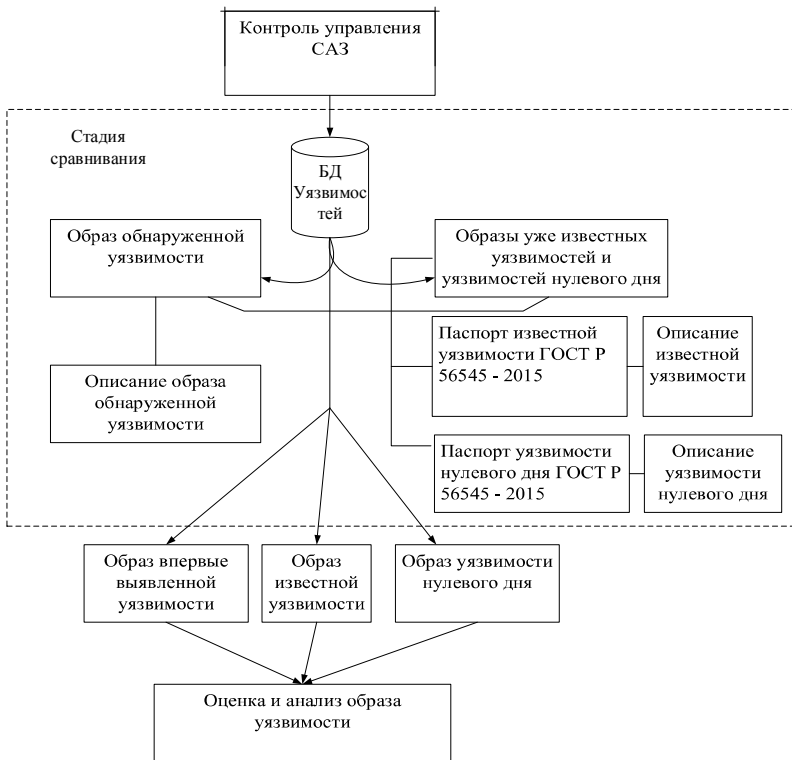


Рис. 2. Обобщенная модель идентификации и оценки образов уязвимостей ИС

Информационные системы персональных данных повсеместно используются различными организациями для обработки персональных данных сотрудников или клиентов. Разработка правильной, а главное, хорошо защищенной ИСПДН зачастую ложится на плечи системного администратора, что уже подразумевается наличием целого ряда уязвимостей. Стоит заметить, что работа оператора персональных данных контролируется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Заключение. Результатом исследовательской работы можно считать анализ существующих средств анализа защищенности ИС. Разработаны эффективные модели выявления уязвимостей, идентификации уязвимостей. Данное исследование позволит вывести работу сотрудника в области защиты информации на более высокий – качественный уровень.

Библиографический список

1. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. – М.: Стандартинформ, 2015.
2. Лукацкий А.В. Обнаружение атак. – СПб.: БВХ, 2001. – 624 с.
3. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. – М.: Стандартинформ, 2015.

Сведения об авторах

Чалин Владислав Александрович – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: chalin2008@yandex.ru

Шабуров Андрей Сергеевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: shans@at.pstu.ru

About the authors

Chalin Vladislav Alexandrovich – Student Perm National Research Polytechnic University, Perm, e-mail: sly-kyper@yandex.ru

Shaburov Andrey Sergeevich – Ph.D. in Technical Sciences, Associate Professor of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: chalin2008@yandex.ru

ПРИНЦИПЫ И ПРОБЛЕМЫ ЗАЩИТЫ РАСПРЕДЕЛЕННЫХ БАЗ ДАННЫХ

А.А. Чегодаев, А.Н. Каменских

Пермский национальный исследовательский
политехнический университет, Пермь

В данной работе рассказывается о проблемах защиты распределенных баз данных, в связи с несовершенством методик защиты, а также прилагаются некоторые способы повышения безопасности распределенных баз данных.

Ключевые слова: базы данных, распределенные базы данных, принципы и проблемы защиты, информационная безопасность.

PRINCIPLES AND PROBLEMS OF PROTECTION OF DISTRIBUTED DATABASES

A.A. Chegodaev, A.N. Kamensky

Perm National Research Polytechnic University, Perm

This paper describes the problems of protecting distributed databases, as well as some ways to improve the security of distributed databases.

Keywords: databases, distributed databases, principles and problems of protection, information security.

Введение. В общем случае под базой данных (БД) подразумевается совокупность сведений, объединенных по какому-то признаку.

Базы данных предназначены для хранения и обработки большого количества однородной информации, которая может представлять собой, например, сведения о сотрудниках университета, справочник лекарственных средств, результаты измерения температуры, давления и влажности в течение года, сведения о банковских вкладах, список счетов для оплаты телефонных переговоров и т. д.

Распределённая база данных – база данных, составные части которой размещаются в различных узлах компьютерной сети в соответствии с каким-либо критерием.

Система управления базами данных (СУБД) – это комплекс программных средств, предназначенный для создания, ведения и совместного использования БД многими пользователями.

С точки зрения конечного пользователя, распределенная база данных выглядит в точности так, как и обычная, нераспределенная.

Для сравнения распределенной и нераспределенной баз данных были взяты определенные критерии.

Физическое расположение. Как ясно из определения, распределенная база данных расположена в разных участках сети, в то время как нераспределенная база данных находится в одном узле сети.

Опорный узел. Опорным узлом является узел, без которого база данных не сможет работать. Эта проблема касается нераспределенных баз данных. У распределенных же баз данных, так как они располагаются в разных узлах сети, как правило, нет опорного узла.

Независимость от расположения. Другими словами, пользователь должен получать доступ к базе данных с любого узла. У обеих баз данных это условие выполняется.

Транзакции. Распределенная база данных поддерживает выполнение распределенных транзакций как единиц восстановления.

Программное обеспечение. Подразумевается программное обеспечение, через которое пользователь получает доступ к базе данных. В распределенной базе данных возможно использование разных программ для доступа.

Результат сравнения баз данных по вышеуказанным критериям представлен в таблице.

Результат сравнения баз данных по вышеуказанным критериям

Критерий	Нераспределенная база данных	Распределенная база данных
Физическое расположение	В одном узле сети	В нескольких узлах сети
Опорный узел	Есть	Нет
Независимость от расположения	Есть	Есть
Транзакция	Нераспределенная	Распределенная
Программное обеспечение	Одно	Как одна, так и несколько

В ходе работы обнаружили 3 основные угрозы, характерные для распределенных баз данных.

Человек посередине: очень актуально для распределенных баз данных, которые расположены в разных узлах сети. Для атаки типа человек посередине (Man-in-the-Middle) хакеру нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак этого типа часто используются sniffеры пакетов, транспортные протоколы и протоколы маршрутизации.

Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, а также для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа Man-in-the-Middle можно только с помощью криптографии. Если хакер перехватит данные зашифрованной сессии, у него на экране появится лишь бессмысленный набор символов. Следует иметь в виду, что если хакер получит информацию о криптографической сессии (например, ключ сессии), то это может сделать возможной атаку Man-in-the-Middle даже в зашифрованной среде.

Отказ в доступе (DoS) из-за невыполнения транзакции к одной из баз данных. Атаки DoS отличаются от других атак. Они не нацелены на осуществление доступа к вашей сети или на получение из нее какой-либо информации. Атака DoS делает вашу сеть недоступной для обычного ее использования из-за наступающего вследствие подобной агрессии превышения допустимых параметров функционирования сети, ее операционной системы или приложения.

В случае использования некоторых серверных приложений (таких как веб-сервер или FTP-сервер) атаки DoS могут приводить к тому, что все соединения, доступные для этих приложений, окажутся занятыми, и обслуживание обычных пользователей станет невозможным.

Большинство атак DoS удается осуществить из-за программных ошибок или брешей в системе безопасности и по причине общих слабостей системной архитектуры. Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов.

Угрозу атак типа DoS можно снижать тремя следующими способами:

- использование функции антиспуфинга – правильная конфигурация функций антиспуфинга на маршрутизаторах и межсетевых экранах предполагает включение, как минимум, фильтрации RFC 2827. В этом случае хакер уже не сможет замаскировать свою истинную личность и вряд ли решится провести атаку;
- реализация функции антиDoS – правильная конфигурация функций антиDoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто уменьшают число полукрытых каналов в любой момент времени;

- ограничение объема трафика (traffic rate limiting) – организация может попросить провайдера (ISP) ограничить объем трафика. Этот тип фильтрации позволяет уменьшить объем некритического трафика в вашей сети. Распространенное ограничение объемов трафика ICMP, который используется только для диагностических целей. А такие атаки, как (D)DoS, как раз часто используют ICMP.

Атаки на уровне приложений актуальны для распределённых баз данных тем, что в них могут использоваться разные программные обеспечения или одно, но разной версииности. Атаки на уровне приложений могут проводиться несколькими способами. Самый распространенный из них состоит в использовании хорошо известных слабостей серверного программного обеспечения (sendmail, НТТР, FTP). Используя эти слабости, хакеры могут получить доступ к компьютеру от имени пользователя, работающего с приложением (обычно это бывает не простой пользователь, а привилегированный администратор с правами системного доступа). Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам устранить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им обучаться.

Вот некоторые меры, которые можно предпринять, чтобы снизить уязвимость для атак подобного типа:

- просмотр лог-файлов операционных систем и сетевых лог-файлов и их анализ с помощью специальных аналитических приложений;
- использование самых свежих версий операционных систем и приложений и самых последних коррекционных модулей (патч);
- использование кроме системного администрирования систем распознавания атак (IDS).

Заключение. Большинство современных предприятий в случае возникновения потребности в защите распределенной базы данных, просматривая методики по защите, не учитывают все опасности ввиду отличия обычной базы данных от распределенной. В этой статье рассмотрены лишь наиболее часто встречающиеся угрозы, а также простые способы их избежания или уменьшения. Однако необходимо помнить, что защита информации может быть обеспечена только при разработке и внедрении комплекса программных, аппаратных и организационных мер для конкретного объекта информационной деятельности.

Библиографический список

1. Методы защиты сетевого трафика [Электронный ресурс]. – URL: http://www.rusnauka.com/18_APSN_2014/Informatica/4_173276.doc.htm (дата обращения: 20.09.2017).

2. Защита от хакеров корпоративных сетей / Дэвид М. Ахмад, Идо Дубравский, Хал Флинн [и др.]. – 2-е изд. – М.: Компания АйТи: ДМК-Пресс, 2002. – 358 с.

3. IPsec [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/IPsec> (дата обращения: 15.10.2017).

4. Защита информации в распределенных базах данных [Электронный ресурс]. – URL: <http://www.studmed.ru/docs/document24465/content> (дата обращения: 15.12.2017).

Сведения об авторах

Чегодаев Александр Алексеевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: redec22@gmail.com

Каменских Антон Николаевич – кандидат технических наук, старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: antoshkinoinfo@yandex.ru

About the authors

Chegodayev Alexander Alexeevich – Student Perm National Research Polytechnic University, Perm, e-mail: redec22@gmail.com

Kamenskih Anton Nikolayevich – Ph.D. in Technical Sciences, Senior Lecturer of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: antoshkinoinfo@yandex.ru

ИССЛЕДОВАНИЕ И МОДЕЛИРОВАНИЕ VPN-СЕТЕЙ, ПОСТРОЕННЫХ НА ОСНОВЕ ТЕХНОЛОГИИ MPLS

В.А. Якимова, В.И. Фрейман

Пермский национальный исследовательский
политехнический университет, Пермь

В данной статье рассмотрена актуальность применения технологии MPLS при подключении удаленных офисов компаний по VPN. Представлен обзор технологий организации VPN. Приведены модель для исследований и рекомендации по использованию технологий VPN.

Ключевые слова: MPLS, VPN 2 уровня, VPN 3 уровня, оверлейные технологии.

RESEARCH AND SIMULATION OF VPN NETWORKS BASED ON MPLS TECHNOLOGY

V.A. Yakimova, V.I. Freyman

Perm National Research Polytechnic University, Perm

This article considers the possibility of using MPLS technology for connecting remote offices of companies. The article is presented a review of VPN technology. The article gave us a model for research and recommendations for using of VPN technologies.

Keywords: MPLS, layer 2 VPN 2, layer 3 VPN, overlay technology.

Современные предприятия не могут эффективно функционировать без развитой ИТ-инфраструктуры. Современные технологии меняют бизнес компаний и предприятий – повсеместно появляются новые инновационные сервисы, расширяются способы обслуживания клиентов. ИТ-инфраструктура современных компаний должна быть способна поддержать все перемены, сопровождающиеся активным внедрением новых информационных технологий, таких как облачные решения и большие данные.

В связи с этим *актуальной* становится оценка эффективности применения оверлейных технологий, в частности VPN, позволяющих проложить туннель поверх сети, внутри которого возможна передача любого типа трафика. На сегодняшний день компании активно и повсеместно решают задачи, связанные с переходом от стандартной логики работы сети к новой логике.

Оверлейные технологии, используя дополнительные заголовки, которые присоединяются к исходному пакету, позволяют абстрагироваться от заголовков изначального пакета и обеспечить дальнейшую передачу по сети любого трафика [1]. Использование и применимость данных технологий нуждаются в дополнительном исследовании.

Целью работы является изучение и анализ VPN технологий, выбор программной среды для моделирования, разработка модели, проведение исследования различных технологий, а также формулирование выводов и рекомендаций.

В ходе работы были рассмотрены и проанализированы технологии VPN. Существуют две основных разновидности VPN технологий: VPN второго уровня модели OSI и VPN третьего уровня модели OSI.

Виртуализированные L2-магистраль потенциально имеют более высокие значения пропускной способности по сравнению технологиями L3 [2].

Технологии третьего уровня становятся больше ориентированными на обеспечение удаленного доступа пользователя к ресурсам ЦОД [3]. L3 обеспечивают необходимый уровень конфиденциальности, целостности и доступности информации в рамках распределенных сетей предприятий [4].

Технология MPLS может применяться для организации и L2, и L3 VPN. Если сеть оператора маршрутизирует клиентский трафик, то сеть уровня L3, если эмулирует соединения канального уровня (или функции коммутатора Ethernet), – L2 [5].

Следующим этапом работы был выбор среды для моделирования данных технологий. Были рассмотрены три эмулятора оборудования: Cisco VIRL, GNS3 и UNetLab. Сравнив функционал выбранных эмуляторов, их достоинства и недостатки, был выбран эмулятор сети GNS3. Следующим этапом работы была разработка модели сети. Была разработана сеть провайдера (рисунок), в задачу которого входит обеспечить связь L2 VPN или L3 VPN поверх сети MPLS между двумя офисами двух компаний в Перми и в Москве. В рамках модели были проанализированы сложность настройки оборудования, различные параметры сети, а также сценарии использования представленных выше оверлейных технологий.

Для построения сети ядра сети были выбраны маршрутизаторы Cisco c7200, в качестве клиентских маршрутизаторов Cisco c3745.

В качестве L2 VPN оператор связи предоставляет услугу псевдопровод VPWS (Virtual Private Wire Service) на основе технологии MPLS. Для сети L3 VPN на основе технологии MPLS в качестве локального протокола динамической маршрутизации используется OSPF. Данный протокол позволяет сообщить адрес Loopback-интерфейса всем заинтересованным сторонам.

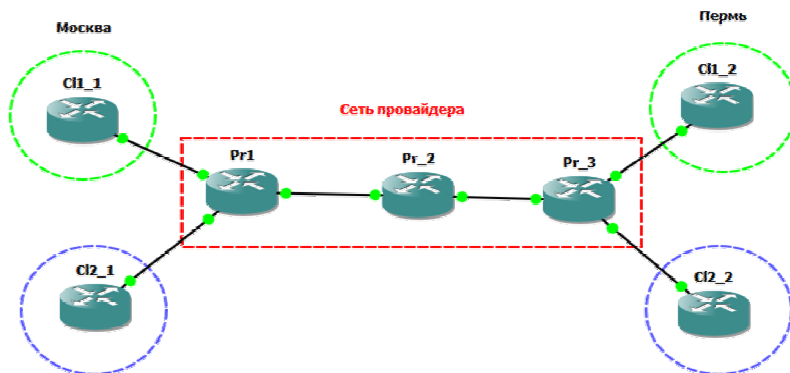


Рис. Модель сети в GNS3

Исследование и тестирование разработанной сети проводились в выбранном ранее симуляторе Dynamips с использованием графического интерфейса GNS 3.

Целью работы являются изучение прохождения пакетов по сети, а также проверка работоспособности сети, качества обслуживания пересылаемых клиентских данных от других клиентов сети. Для исследования была выбрана команда ping.

Для проверки канала в сеть отправлялись пакеты размером: 100, 600, 1515, 2000 байт.

Выполнили исследование участка сети 1–1 – 1–2. На первом этапе проверили филиал клиента 1–2 из главного офиса клиента в сети MPLS L3 VPN, используя пакеты разного размера. На втором этапе тестировали сеть MPLS L2 VPN.

Были рассмотрены MTU (maximum transmission unit) – максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации для технологий второго и третьего уровня.

Для сетей MPLS активно используются mini (baby) jumbo – это сверхдлинные Ethernet-кадры размером немного больше 1500 (не более 9000) байт.

Для тестирования использовалась команда ping. Пример тестового запроса представлен ниже.

Ping 192.168.0.2 size 100 repeat 100

Результаты тестирования занесены в табл. 1 и 2.

Таблица 1

Зависимость задержки от размера пакета для схемы MPLS L3 VPN

Размер пакета	Минимальное значение (мс)	Среднее значение (мс)	Максимальное значение (мс)
100	8	26	54
600	15	34	68
1515	–	–	–
2000	–	–	–

Таблица 2

Зависимость задержки от размера пакета для схемы MPLS L2 VPN

Размер пакета	Минимальное значение (мс)	Среднее значение (мс)	Максимальное значение (мс)
100	6	20	48
600	12	27	64
1515	34	52	100
2000	46	80	200

Для оборудования Cisco технологии MPLS L3 VPN размер mtu на интерфейсе 1508 байт, тогда как для технологии MPLS L2 VPN – 1530 байт.

Заключение. В ходе работы были рассмотрены технологии VPN второго и третьего уровня модели OSI, а также разработана модель сети провайдера, предоставляющего L2 VPN и L3 VPN клиентам. В качестве среды разработки использовался эмулятор Dynamips с графическим интерфейсом GNS 3.

Для проверки работоспособности сети, качества обслуживания пересылаемых клиентских данных была использована команда ping. Зависимость задержки от размера пакета для схемы MPLS L2 VPN и MPLS L3 VPN занесена в таблицы.

На основании проведенной работы можно сделать вывод, что в настоящее время многие компании выбирают L2 VPN, к преимуществам которой относится большая пропускная способность, как видно из таблиц. Еще одним преимуществом является поддержка кадров увеличенного размера. Как видно из результатов тестирования, пакеты размером 1515 и 2000 байт проходят по сети L2 VPN без потерь. Jumbo Frames увеличивают эффективность передачи данных за счет снижения накладных расходов (эффективность равна полезной нагрузке кадра, деленной на общий размер кадра).

Главным недостатком сетей L2 VPN является то, что она работает по принципу точка-точка на уровне L2, т.е. этой услугой можно объединить только две точки (офиса). Также предприятие, использующее данную услугу, само настраивает маршрутизацию трафика между своими узлами, поэтому данную технологию следует использовать предприятиям, имеющим штатных специалистов в ИТ-департаменте.

В сравнении с L2 важным достоинством L3 VPN является то, что задачу организации маршрутизации решает сервис-провайдер. Другим достоинством L3 VPN является поддержка функций QoS и инжиниринга трафика, что позволяет гарантировать требуемый уровень качества.

Главными недостатками сетей L3 VPN являются непрозрачность для услуг Ethernet, отсутствие поддержки кадров Ethernet увеличенного размера, а также более высокая стоимость по сравнению с сервисами Metro Ethernet. Как видно по результатам исследования, пакеты свыше 1508 байт не проходят по сети L3 VPN, а также зависимость времени задержки от размера пакета для схемы MPLS L3 VPN выше, чем для схемы MPLS L2 VPN.

Библиографический список

1 Барсков А. Сеть и виртуализация. Часть II [Электронный ресурс] // Журнал сетевых решений LAN. – 2013. – № 4. – URL: <http://www.osp.ru/lan/2013/04/13035152/> (дата обращения: 08.11.2017).

2 Богданов А.В., Станкова Е.Н., Мареев В.В. Виртуализация. Новые возможности известной технологии [Электронный ресурс] // Информационная система «Единое окно доступа к образовательным ресурсам». – 2008. – URL: <http://window.edu.ru/resource/802/58802> (дата обращения: 2.11.2017).

3 Колесов А. Наступает пора виртуализации [Электронный ресурс]. – 2007. – URL: <http://www.vmg.u.ru/articles/Nastupaet-pora-virtualizatsii> (дата обращения: 12.11.2013).

4 NeroHelp.info – Все самое актуальное из мира мультимедиа. Пустой квадрат и сила SDN: такая разная виртуализация [Электронный ресурс]. – URL: <http://nerohelp.info/5387-sdnvr.html> (дата обращения: 11.11.2017).

5 Барсков А. Виртуализируя WAN, или современная VPNология [Электронный ресурс] // Журнал сетевых решений LAN. – 2013. – № 6. – URL: <http://www.osp.ru/lan/2013/06/13036072> (дата обращения: 18.11.2017).

Сведения об авторах

Якимова Виктория Андреевна – магистрант Пермского национального исследовательского политехнического университета, Пермь, e-mail: melevik@mail.ru

Фрейман Владимир Исаакович – кандидат технических наук, профессор кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: vfrey@mail.ru

About the authors

Yakimova Viktoriya Andreevna – Master Student Perm National Research Polytechnic University, e-mail: melevik@mail.ru

Freyman Vladimir Isaakovich – Ph.D. in Technical Sciences, Professor of the department Automatics and telemechanics Perm National Research Polytechnic University, Perm, e-mail: vfrey@mail.ru

СОДЕРЖАНИЕ

Секция 1. НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ	3
Андреев Р.А., Андреева П.А., Кротов Л.Н. Применение технологии блокчейн для записи, доказательства и поощрения результатов интеллектуального труда	4
Бабенко Е.В., Понаморов П.К. Разработка функциональных моделей процессов тестирования знаний	11
Боброва И.А., Полевщиков И.С. Автоматизированная система сбора и обработки информации об успеваемости студентов	15
Гонин С.А., Полевщиков И.С. Аналитический обзор методов и средств тестирования Android-приложений	20
Горелова А.В., Кузьмин А.В. Анализ возможностей информационных систем для изучения анатомии человека	26
Ерискина Е.В., Курушин Д.С. Проверка модели предметной области, основанная на тесте с закрытыми вопросами	30
Журавлёв А.А. Разработка системы судейства спортивного соревнования	38
Калин М.В., Полевщиков И.С. Автоматизация процесса тестирования программного обеспечения на основе построения диаграмм причин-следствий	45
Никитиных Е.И. Разработка методики обработки 3D-моделей для создания 3D-персонажей на основе концепта	52
Харламов М.И., Гончаровский О.В. Навигация автономного мобильного робота с помощью системы позиционирования Marvelmind	56
Чащин А.А., Гончаровский О.В. SLAM-навигация автономного мобильного робота с камерой восприятия глубины цвета	61
Секция 2. АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ	65
Агибалов И.Г., Тупикин Д.А. Устройство для отображения информации с механической разверткой	66
Арефьева А.В., Тугов В.В. Разработка системы подготовки попутного нефтяного газа	70

Гатилова М.Н. Навигация и позиционирование	75
Горбачева О.М., Боровский А.С. Проблемы автоматизации систем очистки отработанного моторного и трансмиссионного масел	79
Докучаев А.В. Алгоритм прогнозирования поведения коррозии в нефтегазовом оборудовании	86
Ерёмин А.В., Чесноков М.В., Саитбатгалов Р.Р. Перспективы развития автоматического управления	92
Ждановский Е.О., Килин Г.А. Получение и предобработка экспериментальных данных для создания обучающей выборки для нейронной сети	96
Зиятдинов И.Р., Кавалеров Б.В. О возможностях коррекции неправильной настройки систем автоматического управления синхронным генератором газотурбинных электростанций в реальном времени	101
Исламов Р.Р., Александрова А.С., Шумихин А.Г. Исследование гармонического состава обучающей выборки нейросетевой модели динамического объекта	107
Крылова И.А., Кавалеров Б.В. Модель синхронного генератора в среде MatLab/Simulink с учетом насыщения магнитной цепи	114
Крюков В.В. Применение нечеткой логики в процессе управления редуцированием газа в магистральных трубопроводах	122
Наджафов А.Ф. Автоматизация операции по затяжке гайки подшипника вала несущего винта вертолетного редуктора ВР-8А	127
Петухов П.А., Додонов С.В., Толлок А.В. Применение метода функционально-воксельного моделирования к задачам поиска пути с помощью объектов сложной конфигурации	132
Работников М.А., Александрова А.С., Шумихин А.Г. Программная реализация алгоритма идентификации каналов управляемого объекта по экспериментальной комплексной частотной характеристике	139
Сазонов А.В., Азимов М.Б., Захаркина С.В., Власенко О.М. Система управления процессом дозирования на установке карусельного типа	146

Чудинов М.А. Реализация процесса сборки пакета OPENSCADA на основе модифицированных исходных текстов	152
Чудинов М.А. Модификация исходных текстов пакета OPENSCADA для решения задачи взаимодействия с микроконтроллером ARDUINO	158
Шаров Н.С., Тугов В.В. Разработка алгоритма управления напорной системой водоподачи с насосной станцией второго подъема	165
Секция 3. ИННОВАЦИОННЫЕ НАПРАВЛЕНИЯ В ЭНЕРГЕТИКЕ. ЭНЕРГОРЕСУРСΟΣБЕРЕЖЕНИЕ	171
Киселев С.Н., Столяров С.П. Деятельность инженера Р.А. Корейво по продвижению дизелизации российского речного флота в начале XX века	172
Мальцев И.А., Килин Г.А. Перспективы использования газотурбинных электростанций	179
Озерец Ю.В., Полюхович А.Д. Возобновляемые источники энергии и перспективы их использования	186
Русецкая М.И., Стасула Я.А. Блокчейн – новый уровень энергетики	193
Самосюк Н.А. Особенности формирования системы управления затратами на предприятиях энергетики Республики Беларусь	200
Секция 4. ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	207
Батуев К.А., Тур А.И., Кокоулин А.Н. Применение CRYPTOAPI для шифрования на языке С#	208
Белый И.А. Обзор программных средств защищенного хранения аутентификационных данных пользователей	215
Бурылов Д.А., Кокоулин А.Н. Методы и алгоритмы надежного удаления данных с физических носителей	221
Веселицкая П.Д., Кротова Е.Л. Применение технологии блокчейн в инфраструктуре открытых ключей	227
Губарев Е.А. Моделирование GRE OVER IPSEC VPN сети предприятия в среде CISCO PACKET TRACER	230
Гущарин Е.А., Оборин С.А., Фоминых Ю.С. Анализ генераторов шума для защиты информации по каналу ПЭМИ	235

Дробинина А.В., Безукладников И.И. Исследование нетрадиционных методов атакующих воздействий посредством скрытых каналов	242
Лесникова В.Г., Кокоулин А.Н. Исследование уязвимости операционных систем с использованием сканеров безопасности	248
Лихачева Ю.В. Оценка энергоэффективности протоколов LEACH и PEGASIS для беспроводных сенсорных сетей	256
Мазунина Е.С., Безукладников И.И. Защита сервисов от DDOS-атак на прикладном уровне	263
Миронова А.А., Безукладников И.И. О шумоподобных скрытых каналах	268
Пьянков П.Е., Ведерникова О.С., Кротова Е.Л. Сравнение стандартов шифрования	273
Сорокин А.С., Шабуров А.С. О разработке модели нейронной сети для выявления злоумышленника в информационной системе предприятия	280
Стафеев А.К., Тюрин С.А. MAC-уровень в сетях MANET ...	287
Хиков С.П., Каменских А.Н. Проблемы информационной безопасности интернет-вещей	294
Чалин В.А., Шабуров А.С. Выявление уязвимостей при разработке информационных систем персональных данных	299
Чегодаев А.А., Каменских А.Н. Принципы и проблемы защиты распределенных баз данных	304
Якимова В.А., Фрейман В.И. Исследование и моделирование VPN-сетей, построенных на основе технологии MPLS ...	309

Научное издание

**ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ: ТЕОРИЯ,
ИНСТРУМЕНТЫ, ПРАКТИКА**

Материалы IX Международной
интернет-конференции молодых ученых,
аспирантов, студентов
(20 ноября – 31 декабря 2017 г.)

Редактор и корректор *И.Н. Жеганина*

Подписано в печать 30.03.2018.
Формат 60×90/16. Усл. печ. л. 20,4.
Тираж 100 экз. Заказ 17/2018.

Издательство
Пермского национального исследовательского
политехнического университета.
Адрес: 614990, г. Пермь, Комсомольский пр., 29, к. 113.
Тел. (342) 219-80-33.