СИСТЕМНЫЙ АНАЛИЗ И ПРИКЛАДНАЯ ИНФОРМАТИКА
№ 2, 2016

SYSTEM ANALYSIS AND APPLIED INFORMATION SCIENCE
No 2, 2016

Международный Научно-технический журнал

Издается с декабря 2012 года

Учредитель

Белорусский национальный технический университет

Главный редактор

Федор Иванович Пантелеенко

Редакционная коллегия

В. Ф. Голиков (зам. главного редактора), В. А. Богуш, Т. В. Борботько, Р. Венерстен (Швеция), В. А. Ганэ, Н. Н. Гурский, Ю. М. Захарик, Э. Г. Лазаревич, А. А. Лобатый, В. А. Мищенко, А. Патрин (Польша), И. А. Сатиков, В. В. Старовойтов, П. П. Урбанович, А. Н. Чичко, В. Б. Байбурин (Россия), Е. И. Никифорович (Украина)

International Science and Technique Journal

Published since December, 2012

Founnder

Belarusian National Technical University

Editor-in-chief

Phyodor Panteleenko

Editorial board

V. Golikov (deputy editor-in-chief), V. Bogush, T. Borbotko, P. Venersten (Sweden), V. Ganeh, N. Gurskiy, J. Zaharik, E. Lazarevich, A. Lobaty, V. Mishchenko, A. Patrin (Poland), I. Satikov, V. Starovoytov, P. Urbanovich, A. Chichko, V. Bayburin (Russia), E. Nikiforovich (Ukraine)

Журнал включен в "Перечень научных изданий Республики Беларусь для опубликования результатов диссертационных исследований".

Журнал включен в международные каталоги и базы данных:

- Российский индекс научного цитирования (РИНЦ)
- Научная электронная библиотека eLIBRARY.RU
- Электронно-библиотечная система (ЭБС) издательства Лань
- DOAJ https://doaj.org/toc/2414-0481
- Google Scholar
- Киберленинка
- EBSCO
- BASE Search
- OpenAIRE
- WorldCat
- OpenDOAR
- ROAR

Содержание

Contents

Ответственный секретарь редакции
Лакин В. И.

Адрес редакции
ул. Франциска Скорины 25/3, Минск, 220114,
Республика Беларусь
Тел.+375 17 267-66-84
e-mail: CA_PI@bntu.by

Executive secretary of the editorial board
V. Lakin

Editorial board address
25/3 Franciska Skariny str., Minsk, 220114,
Republic of Belarus
Tel. +375 17 267-66-84
e-mail: CA_PI@bntu.by

Свидетельство о государственной регистрации средства массовой информации № 1540 от 08.06.2012, выданное Министерством информации Республики Беларусь

Подписано в печать 22.03.2016. Формат бумаги 60×84 1/8. Бумага офсетная.

Ризография. Усл. печ. л. 7,67. Уч.-изд. л. 3,00. Тираж 150 экз. Заказ 960.

Издатель и полиграфическое исполнение
Белорусский национальный технический университет.
ЛИ № 02330/0494349 от 16.03.2009.
Пр. Независимости, 65, г. Минск, 220013

УПРАВЛЕНИЕ ТЕХНИЧЕСКИМИ ОБЪЕКТАМИ

MANAGEMEMENT OF TECHNICAL OBJECTS

УДК 004.3:339.3

А. С.КИРИЕНКО

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ И МОНИТОРИНГА ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ ПРИ ПРОИЗВОДСТВЕ ПОЛИМЕРНО-БИТУМНЫХ ЛЕНТ НА ОСНОВЕ ПРИМЕНЕНИЯ SCADA СИСТЕМЫ

Представительство ОАО «Оргэнергогаз» в Республике Беларусь

В статье обосновывается целесообразность использования системы управления и мониторинга технологическими процессами производства, что позволит снизить затраты труда, а также повысить производительность за счет лучшей организации технологических процессов. основной задачей системы, является удаленный мониторинг, что дает возможность удаленно и оперативно давать оценку текущей ситуации на производстве, принимать обоснованные и своевременные управленческих решений.

Ключевые слова: *технологический процесс, удаленный мониторинг*

Введение

Битумно полимерная лента (далее лента) представляет собой рулонный материал, изготавливаемый путем одностороннего нанесения расплавленной битумно-полимерной мастики на полимерную (поливинилхлоридную, полиэтиленовую или иную подложку) ленту-основу.

В процессе производства ленты при нагревании мастики возможно выделение следующих вредных веществ: полициклических ароматических углеводородов, окиси углерода, диоксидов серы и азота, α-метилстирола. Данные вещества оказываю негативное воздействие на организм человека.

С целью сокращения необходимого количества персонала для обслуживания установки по производству ленты и сокращения времени его пребывания в производственном помещении, а также по экономическим соображениям, была модернизирована система мониторинга для устройства автоматической намотки ленты на бобины.

Ввиду сложности системы управления, постановка задачи сводится к выделению следующих промежуточных подзадач:

– сформировать основную концепцию системы мониторинга и разработать схему информационных потоков;

– произвести анализ рынка предложений программных и аппаратных средств, с последующим выбором их оптимальной конфигурации;

– выполнить модернизацию системы управления объектом мониторинга в части реализации возможности дистанционного управления;

– разработать пользовательский интерфейс системы мониторинга;

– выполнить пуско-наладочные работы.

Основная часть исследования

В настоящее время существует немалое количество линий по производству лент, однако принцип их работы практически идентичен.

Далее приведено описание производственного процесса и отдельных узлов производственной линии находящейся на заводе по производству полимерно-битумных лент ООО «Белпромизоляция».

Линия состоит из нескольких узлов, производственный цикл начинается с узла подготовки битумно-полимерной мастики. Здесь происходит подготовка битумной-полимерной мастики для последующего нанесения на ленту-основу, мастику варят с добавлением различных ингредиентов для достижения необходимых физико-механических показателей. Параллельно с подготовкой мастики в другом узле линии подготавливают ленту-основу.

Узел подготовки ленты-основы оснащен барабаном револьверного типа, который содержит три позиции для установки бобин ленты-основы. Перед началом производственного цикла в каждой позиции устанавливают и закрепляют бобину ленты-основы, далее лента-основа подается в узел нанесения на нее битумно-полимерной мастики с ближайшей к этому узлу бобины.

После того, как ближайшая бобина израсходована, барабан револьверного типа проворачивают таким образом, чтобы целая бобина закрепленная в другой позиции переместилась на место израсходованной. После чего производится замена израсходованной бобины на новую. Вышеописанные операции производятся для недопущения простоя производственной линии по причине отсутствия в ней ленты-основы в момент замены бобин последней.

Подготовленные материалы подаются в узел нанесения битумно-полимерной мастики на ленту-основу. В данном узле происходит нанесение битумно полимерной мастики на ленту-основу с последующим охлаждением и нанесением антиадгезивного материала.

Система охлаждения является жидкостной, имеет замкнутый контур и состоит из резервуаров для охлаждающей жидкости, барабана для охлаждения ленты, радиатора с вентилятором для охлаждения жидкости и технологических трубопроводов для ее перемещения.

Охлажденная лента с нанесенным на нее антиадгезионным материалом подается в автоматический узел намотки ленты на бобины.

Автоматический узел намотки ленты на бобины выполняет следующий ряд задач:

– обеспечивает подачу ленты и заготовок (трубок) в зону намотки (рабочую зону);

– закрепляет ленту на трубке;

– предотвращает самопроизвольное разматывание готовых бобин;

– регулирует скорость вращения бобины по мере изменения ее радиуса;

– обеспечивает постоянное натяжение ленты при ее намотке;

– обрезает ленту по достижении необходимого радиуса бобины;

– удаляет готовую бобину из рабочей зоны.

Система управления устройством автоматической намотки битумно-полимерных лент на бобины состоит из аппаратной и программной частей.

Аппаратная часть системы управления представляет собой совокупность программируемых логических устройств, исполнительных механизмов, датчиков, электромагнитных реле, сигнальных ламп и прочих элементов.

Программная часть системы управления представляет собой список инструкций в виде релейных диаграмм [1], а также перечень констант программирования для применяемых программируемых логических устройств управления.

Система управления разделена на несколько управляющих узлов, относящихся к одноименным узлам объекта управления соответственно.

Для управления узлами системы и обеспечения их согласованной работы используется программируемый логический контроллер [2]. (далее ПЛК) семейства MELSEC FX серии FX3U производства Mitsubishi [3, 4, 5].

Таким образом, ПЛК коммуникацирует с другими программируемыми контроллерами, а также с регулирующими системами и интерфейсами «человек-машина». Для этого предусмотрена возможность, во-первых, встраивать ПЛК в сети в качестве локальных станций и, во-вторых, применять его в качестве подчиненных устройств в открытых сетях (например, PROFIBUS/DP);

Структурная схема системы управления устройством автоматической намотки битумно-полимерных лент на бобины представлена на рис. 1.

Объект управления представляет собой установку состоящую из нескольких узлов:

– накопитель трубок

Рис. 1. Структурная схема системы управления устройством автоматической намотки битумно-полимерных лент на бобины

– узел подачи трубок
– намоточный узел
– узел фиксации ленты на бобине
– узел обрезки ленты

Схема информационных потоков

Информация «образуется» в датчиках, интегрированных непосредственно в объект управления и «перемещается» согласно схеме информационных потоков.

Схема информационных потоков приведена на рис. 2.

Процесс передачи информации можно разделить на несколько этапов:

– сигналы датчиков поступают в контроллер, где оцифровываются, представляются в виде регистров данных и передаются на АРМ оператора через шину Modbus RTU;

– предустановленная на АРМе оператора SCADA-система [6] получает регистры данных, формирует соответствующие теги и графический интерфейс пользователя, а также экспортирует полученные данные в хранилище (а в режиме управления импортирует из хранилища) данных на сервере в формате СУБД MS Access посредством Ethernet;

– SCADA-клиенты, установленные на АРМах начальника цеха и технолога импортируют данные из хранилища (а в режиме управления импортируют в хранилище) данных на сервере посредством Ethernet и формируют пользовательский интерфейс;

– данные из хранилища через DSL-маршрутизатор попадают в телефонную линию, далее в городскую АТС;

– с городской АТС данные поступают на базовую GSM-станцию и, оттуда, через GSM-канал (3G) попадают на смартфон с предустановленным мобильным SCADA-клиентом;

– мобильный SCADA-клиент на базе операционной системы Android принимает данные и формирует пользовательский интерфейс;

– управленческое воздействие с помощью мобильного SCADA-клиента возвращается в хранилище данных (изменяет значения в таблице на сервере), а из него на контроллер и объект управления, аналогичным образом в обратной последовательности.

Выполнение программы контроллера

Программируемый контроллер работает по заданной программе, которая, как правило, создается вне контроллера, а затем передается в контроллер и хранится в его памяти. Для программирования важно знать, как контроллер обрабатывает программу.

Программа состоит из череды отдельны команд, определяющих функционирование контроллера. Контроллер одну за другой отрабатывает управляющие команды в запрограммированной последовательности.

Выполнение всей программы постоянно повторяется, т. е. происходит ее циклическое выполнение. Время, необходимое для выпол-

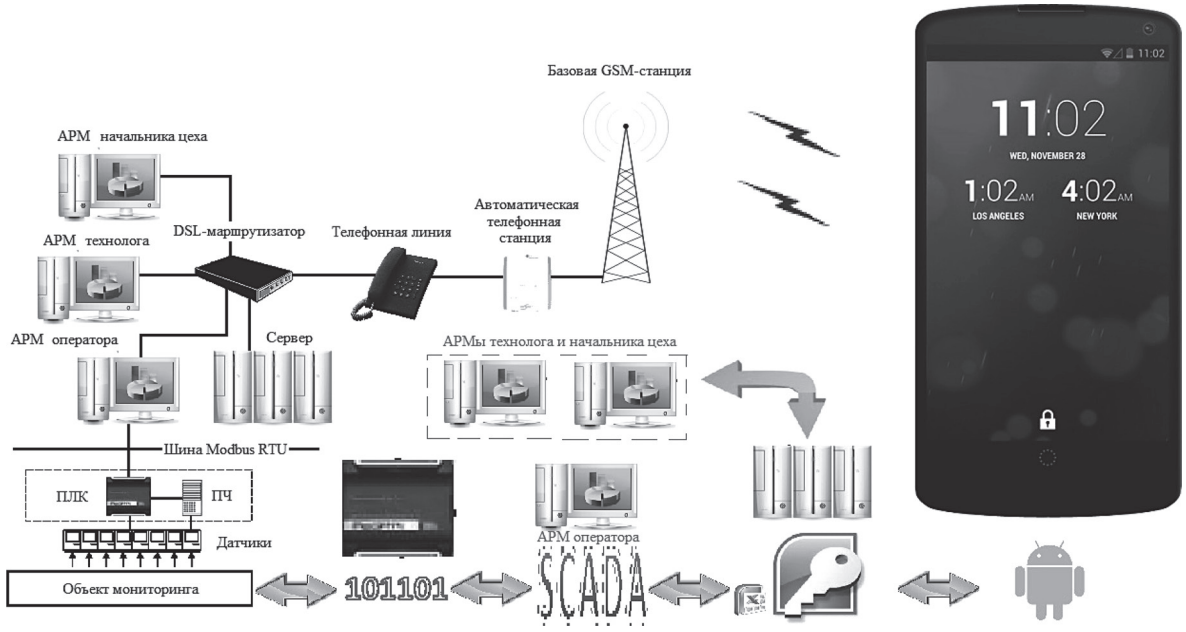


Рис. 2. Схема информационных потоков

нения программы, называется «временем цикла программы».

В начале программного цикла состояния входов опрашиваются и сохраняются в промежуточной памяти, т. е. создается так называемое отображение входов. При обработке программы контроллер обращается не непосредственно ко входам и выходам, а к их отображению.

Во время последующего прохождения программы контроллер обращается к состояниям входов, хранящимся в области отображения, поэтому изменения сигналов на входах распознаются лишь при следующем программном цикле.

Результаты логических операций, относящиеся к выходам, передаются в выходную буферную память (область отображения выходов). Лишь по окончании выполнения программы промежуточные результаты передаются на выходы. В выходной буферной памяти отображение выходов сохраняется до очередной перезаписи. После присвоения значений выходам программный цикл повторяется.

Разработка пользовательского интерфейса локальной Scada

Пользовательский интерфейс системы состоит из нескольких функциональных блоков, закрепленных за отдельными узлами объекта управления и отображающих их состояние.

Пример пользовательского интерфейса Scada-системы АРМов оператора, технолога и начальника цеха приведен на рис. 3.

Пользовательский интерфейс состоит из восьми блоков:

1 – индикатор состояния бобины и степени ее готовности, отображает процесс увеличения диаметра бобины в ходе намотки;

2 – индикатор стадии цикла, отображает стадию производственного цикла намотки одной бобины в процентном соотношении;

3 – индикатор наличия заготовок, отображает наличие и количество заготовок в накопителе в процентном соотношении от максимального;

4 – индикатор работы дополнительной вентиляционной системы, отображает состояние вентиляционной системы и предупреждает об ее отключении;

5 – кнопка включения и выключения дополнительной вентиляционной системы;

6 – индикатор длины ленты в бобине, отображает длину ленты в метрах на выпускаемых бобинах в текущий момент времени;

7 – регулятор длины ленты в бобине, позволяет изменять длину ленты в метрах на выпускаемых бобинах;

8 – индикатор бобин находящихся на складе с функцией ретроспективы, отображает количество изготовленных бобин за промежуток времени.

Разработка пользовательского интерфейса удаленной Scada

Пользовательский интерфейс мобильного Scada-клиента состоит из пяти окон, закрепленных за отдельными узлами объекта управления и отображающих их состояние.

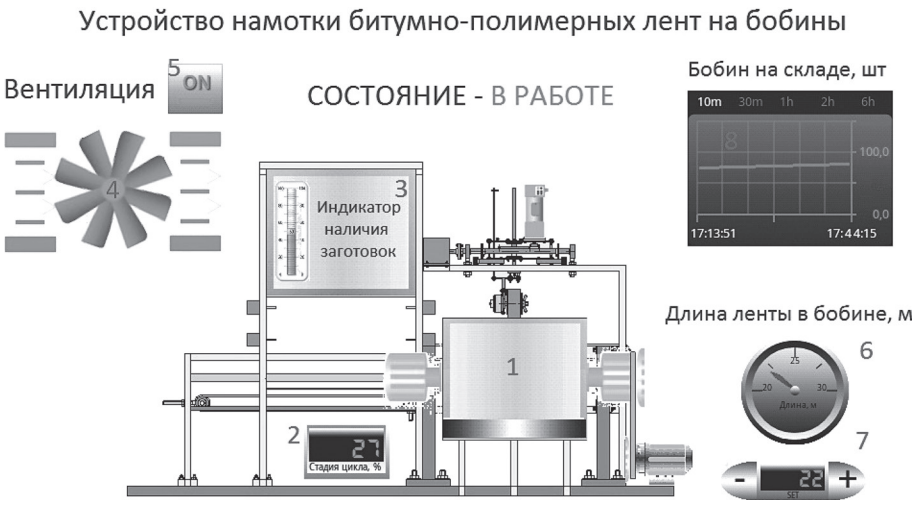


Рис. 3. Пример пользовательского интерфейса

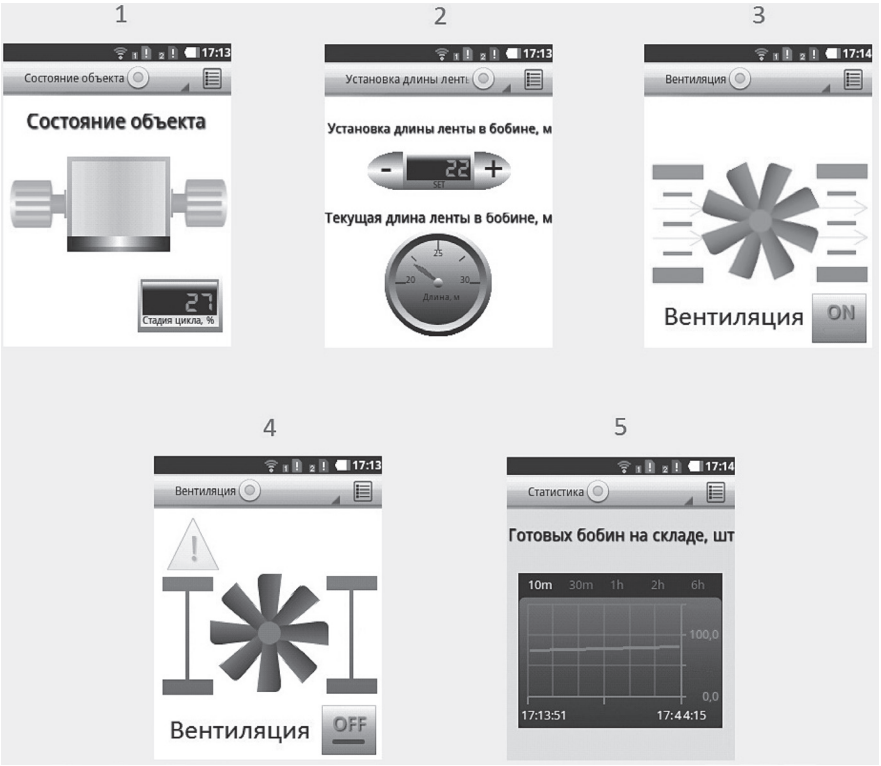


Рис. 4. Пример пользовательского интерфейса

Пример пользовательского интерфейса удаленной SCADA в виде скриншотов отдельных окон приведен на рис. 4.

Окна пользовательского интерфейса мобильного Scada-клиента отображают различную информацию о технологическом процессе и имеют некоторые органы управления.

Окно № 1 (поз. *1* на рис. 4) отображает:

– состояние бобины и степень ее готовности;

– стадию производственного цикла в процентном соотношении.

Окно № 2 (поз. *2* на рис. 4):

– отображает длину ленты в метрах на выпускаемых бобинах в текущий момент времени;

– позволяет изменять длину ленты в метрах на выпускаемых бобинах.

Окно № 3 (поз. *3*, *4* на рис. 4):

– отображает состояние дополнительной вентиляционной системы;

– предупреждает об отключении вентиляционной системы;

– позволяет включать и выключать дополнительную вентиляционную систему.

Окно № 5 (поз. 5 на рис. 4):

– отображает количество изготовленных бобин за промежуток времени;

– позволяет изменять временной диапазон предоставления данных о изготовленных бобинах.

Заключение

Внедрение данной системы позволит сократить время нахождения персонала в цеху по производству битумно-полимерных лент, что делает технологический процесс безвредным для организма человека.

Важнейшей заслугой системы является информационная обеспеченность, позволяющим оперативно и точно оценивать, анализировать текущую ситуацию, принимать обоснованные и своевременные управленческие решения. Также позволит руководителю предприятия находиться в своем офисе и из него удаленно наблюдать в режиме реального времени за работой всего производства и оборудования.

В целом данный проект повысит уровень качества, безопасности и информационной обеспеченности производства, позволит существенно увеличить производственные мощности линии в целом, уменьшить себестоимость готовой продукции и, в то же время, не потребует больших материальных затрат на его реализацию.

ЛИТЕРАТУРА

1. **Деменков Н. П.** Языки программирования промышленных контроллеров / Деменков Н. П. – под ред. К. А. Пупкова. – Москва: МГТУ им. Н.Э.Баумана, 2004. – 172 с.

2. **Петренко Ю. Н.** Программное управление технологическими комплексами в энергетике / Петренко Ю. Н., С. О. Новиков, А. А. Гончаров. – Минск: Вышэйшая школа, 2013. – 406 с.

3. Руководство Mitsubishi Electric: Программируемые логические контроллеры. Руководство по эксплуатации. Описание аппаратной части. 2-е изд. – 2008. – 256 с.

4. Руководство Mitsubishi Electric: Семейство FX. Программируемый логический контроллер. – 2009. – 88 с.

5. Руководство Mitsubishi Electric: Книга по автоматизации. Мир решений. – 2011/2012. – 188 с.

6. **Деменков Н. П.** SCADA-системы как инструмент проектирования АСУ ТП: учеб. пособие. – Москва: МГТУ им. Н.Э.Баумана, 2004. – 328 с.

References

1. **Demenkov N. P.** Programming languages of industrial controllers / Demenkov N. P. – under the editorship of K. A. Pupkov. – Moscow: MGTU of N.E. Bauman, 2004. – 172 pages.

2. **Petrenko Yu. N.** Program control by technological complexes in Power / Petrenko Yu. N., S. O. Novikov, A. A. Goncharov. – Minsk: Vysheyshy school, 2013. – 406 pages.

3. Management of Mitsubishi Electric: Programmable logical controllers. Operation manual. Description of the hardware. 2nd prod. – 2008. – 256 pages.

4. Management of Mitsubishi Electric: FX family. Programmable logical controller. – 2009. – 88 pages.

5. Management of Mitsubishi Electric: The book on automation. World of decisions. – 2011/2012. – 188 pages.

6. **Demenkov N.** Item SCADA system as instrument of design of industrial control system: studies. grant. – Moscow: MGTU of N.E. Bauman, 2004. – 328 pages.

Поступила	*После доработки*	*Принята к печати*
12.05.2016	*15.05.2016*	*20.05.2016*

UDC 004.3:339.3

Kirienko A. S.

AUTOMATED CONTROL SYSTEM AND MONITORING BY TECHNOLOGICAL PROCESSES BY PRODUCTION OF POLYMERIC AND BITUMINOUS TAPES ON THE BASIS OF APPLICATION OF SCADA OF SYSTEM

Expediency of use of a control system and monitoring of technological processes of production is proved in article that will allow to lower work expenses, and also to increase productivity due to the best production process.

The main objective of system, remote monitoring is that gives the chance far off and to quickly give an assessment to the current situation on production, to accept reasonable and timely administrative decisions.

Keywords: *technological process, remote monitoring*

Кириенко Александр Сергеевич, инженер 1-ой категории Представительства ООО «Оргэнергогаз» в Республике Беларусь. Специалист в области электрохимической защиты, неразрушающего контроля. В 2015 г. окончил Брянский государственный технический университет по специальности «Автоматизация технологических процессов и производств». С 2015 г. и по настоящее время обучаюсь в «Белорусский национально техническом университете» по специальности «Распределенная автоматизация на основе промышленных компьютерных сетей». E-mail: ac-kirienko@mail.ru.

Kiriyenko Alexander Sergeyevich, the engineer of the 1st category of Representative office of LLC Orgenergogaz in Republic of Belarus. The expert in the

field of electrochemical protection, nondestructive control. In 2015 I have graduated from Bryansk state technical university majoring in «Automation of technological processes and productions». Since 2015 and till present I am trained in «Belarusian national technical university» in the specialty «The distributed automation on the basis of industrial computer networks».

E-mail: ac-kirienko@mail.ru.

ОБРАБОТКА ИНФОРМАЦИИ И ПРИНЯТИЕ РЕШЕНИЙ

DATA PROCESSING AND DECISION-MAKING

УДК 541.48/.486

М. А. ЗИЛЬБЕРГЛЕЙТ

ОТБОР ИСХОДНЫХ ДАННЫХ ДЛЯ ФОРМИРОВАНИЯ МАССИВОВ БАЗЫ ДАННЫХ НА ПРИМЕРЕ МНОГОКОМПОНЕНТНОЙ СИСТЕМЫ NACL–KCL–MCL_2·H_2O

Государственное научное учреждение «Институт общей и неорганической химии» Национальной академии наук Беларуси

Использование данных из различных источников при формировании БД наталкивается на естественные трудности, характеризующихся частичной противоречивостью и несопоставимостью результатов, полученных разными исследователями в разное время. В работе предложен способ поиска данных типа unusual data (данные вызывающие сомнения) при формировании баз данных из нескольких источников. В качестве критерия для поиска таких данных предложено использовать метод распознавания образов – решающее правило. При использовании двух и более решающих правил, рассматривающие различные аспекты данных, образуются пересечения, в которых присутствуют объекты, которые невозможно правильно классифицировать при помощи таких решающих правил. В качестве примера поиска данных типа unusual data показано применение этого метода при анализе данных по гетерогенному равновесию в системе NaCl–KCl–MgCl·H2O, опубликованных в 12 различных источниках за разные периоды времени. В частности предложены три критерия отбора для семи разных составов твердой фазы, трех составов, различающихся количеством компонентов в нем – т. е. одно, двух и трех компонентов, а также для составов, в которых входят и не входят кристаллогидраты. В результате получены наборы решающих правил, которые с вероятностью 92–98% правильно классифицируют отобранные объекты. Часть неправильно классифицированных объектов характерны для всех трех критериев отбора. Эти объекты предложено отмечать в БД, как данные вызывающие сомнения. Получено решающее правило, позволяющее с вероятностью 98% прогнозировать наличие или отсутствие кристаллогидрата в твердой фазе в зависимости от состава насыщенного раствора NaCl, KCl, MCl2·H2O.

Ключевые слова: *отбор исходных данных, данные вызывающие сомнения, unusual data, распознавание образов, линейные и нелинейные классификаторы, решающее правило, пересечение множеств, многокомпонентная гетерогенная химическая система.*

Введение. Предшествующий период накопления химических знаний можно очевидно охарактеризовать как период, связанный с хаотичным сбором экспериментального материала. Результатом деятельности явилось создание многочисленных химических справочников, в которых были собраны десятки, если не сотни экспериментальных данных, относящихся к одной и той же изучаемой проблеме. Эти данные собирались различными исследовательскими коллективами, различными авторами и иногда с использованием различных методов проведения эксперимента и анализа. Попытка свести эти данные воедино зачастую наталкиваются на проблемы, связанные с противоречивостью и несопоставимостью некоторых экспериментальных значений. Ручной отбор и анализ такого материала представляется крайне трудоемкой и непосильной задачей. Подход к такого рода исследованиям в плане анализа пропущенных данных развит в работах [1–4]. В тоже время работы, посвященные очистке данных, чаще всего ограничиваются исследованием на уровне непосредственного эксперимента путем применения стандартных статистических критериев для удаления выбросов.

В данном исследовании приведен подход поиска сомнительных данных из разных источников уже после того как они были собраны и опубликованы в справочных изданиях. Под термином сомнительные данные в данном случае предполагается поиск данных, которые в зарубежной статистической литературе носят название unusual data, т. е. данные вызывающие вопросы.

В качестве исходного метода исследования выдвинута концепция использования одного из методов распознавания образов – формирование решающего правила для поиска unusual data. В данном сообщении нет смысла останавливаться на основных идеях распознавания образов и получения решающего правила, так как они подробно изложены в соответствующей литературе [5–7]. Отметим лишь, что решающее правило представляет собой функцию, значение которой или ее знак позволяет отнести объект к тому или иному классу. Известно, что если решающее правило не дает полного распознавания, то существуют записи, которые не распознаются по такому правилу. Если использовать два и более решающего правила, классифицирующие совокупность объектов по различным признакам, то возможно обнаружить пересечение записей, которые не соответствуют двум и более классификациям. В последнем случае предлагается обозначать их как unusual data и помечать соответствующим образом. Иными словами существуют данные, которые не могут быть распознаны различными решающими правилами, что дает возможность предполагать о наличие в таких данных дефектов.

Экспериментальный материал для анализа

В качестве исходного материала нами выбраны данные по гетерогенному рав-новесию в системе NaCl–KCl–MgCl–H_2O. Выбор такой системы обусловлен тем, что на технологические процессы галургического разделения солей данного состава в зависимости их растворимости и соотношения компонентов, а также температуры до сих пор являются предметом изучения. Источник информации – «Справочник экспериментальных данных по растворимости многокомпонентных водно-солевых систем», т. 2, Четырехкомпонентные и более сложные системы, составители А. Б. Здановский, Е. И. Ляховская, Р. Э. Шлеймович, Государственное издательство научно-технической литературы, Ленинград, 1964 г. В данном издании использовались данные E. Kayser, Kali, № 17, 7–8, 38, 1923; Н. С. Курнаков, Н. А. Осокорева, Калий, № 2, 27, 1932, Труды ГИПХ, вып. 16, 42–45, 1932, Соликамские карналиты, 61–67, 1935; Е. А. Ахумов, М. П. Головков, ЖОХ, т. 5, вып. 4, 507, 1935; Н. И. Хайдуков, Э. Г. Линецкая, Калий, № 8, 33, 1935; Н. С. Курнаков, А. И. Заславский, Е. И. Лукьянова, ГИПХ, 1936. F. Frowein, E. von Muehlendahtl, Z. anorg. Chem., v. 39, 1492–1493б 1926; G. Leimbach, Kali, № 1, 12–13, 1926; J. D Ans, A. Bertsch, A. № 9, 153–154, 1915; H/ Keitel, Mitt, KFA, v. 32, 112–117, 1922; W. Feit, K. Przibylla, Kali, № 18, 394, 1909; № 14, 300, 1910; Michels Przibylla, Die Kalirohsalze, Ihre Gewinnung und Verarbeitung, Leipzig, 106, 1916; H. Precht, B/Wittjen, Ber., v. 14, 1673, 1881; Serowy, Kali, № 17, 347–348, 1923, а также единичные дополнительные данные ряда авторов за 1898–1913 годы, приведенные на 743 стр. данного справочника. Количество отобранных записей составило 231. *Запись базы данных* – это строка таблицы, содержащая набор значений свойств.

Авторы справочника в предисловии к изданию упоминают, что они на основании полученных данных создают сводную вероятностную таблицу, однако способ сведения данных так и не указан.

Фрагмент таблицы из упомянутого выше справочника приведен на рис. 1.

Температурные интервалы выбранных записей находились в пределах 0–105 ^oC. Качественный состав твердой фазы характеризовался следующим образом: NaCl+KCl, NaCl+KCl+$KCl{\cdot}MgCl_2{\cdot}6H_2O$, NaCl+$KCl{\cdot}MgCl_2 6H_2O$+$MgCl_2{\cdot}6H_2O$, NaCl+$KCl{\cdot}MgCl_2{\cdot}6H_2O$, KCl+$KCl{\cdot}MgCl_2{\cdot}6H_2O$, NaCl, KCl.

Для разделения использовались линейные и нелинейные дискриминаторы, которые давали наилучшее в данных условиях разделение.

Обсуждение полученных результатов

Таким образом, для классификации использовались три вида решающего правила: для 7 разных составов твердой фазы, трех составов, различающихся количеством компонентов в нем – т. е. 1, 2 и 3 компонента, а также для составов, в которых входят и не входят кристаллогидраты.

В табл. 1–3 приведены результаты классификации для предложенных выше решающих правил.

Очевидно, что даже самый трудный способ классификации (7 различных составов твердой фазы) дал вполне удовлетворительные результаты – суммарный итог разделения составил около 91%, при этом наихудшие результа-

736

$NaCl—KCl—MgCl_2—H_2O$

Н. С. Курнаков, Н. А. Осокорева, Калий, № 2, 27 (1932) [25 и 100°]; Труды ГИПХ, вып. 16, 42—45 (1932); Соликамские карналлиты, стр. 61—64, 1935

t, °C	Жидкая фаза: вес. % NaCl	вес. % KCl	вес. % $MgCl_2$	г/100 г солей NaCl	г/100 г солей KCl	г/100 г солей $MgCl_2$	M/1000 M H_2O 2NaCl	M/1000 M H_2O 2KCl	M/1000 M H_2O $MgCl_2$	индексы 2NaCl	индексы 2KCl	индексы H_2O	d	Твердая фаза
10	12,57	6,59	9,50	43,86	22,99	33,14	27,15	11,16	25,19	42,76	17,57	1575	1,235	$NaCl + KCl$
	5,42	4,43	18,59	19,06	15,57	65,37	11,67	7,48	49,10	17,10	10,96	1465	1,245	" "
	1,92	2,67	25,43	6,41	8,92	84,67	4,22	4,60	68,41	5,46	5,96	1295	1,270	$NaCl + KCl + KCl \cdot MgCl_2 \cdot 6H_2O$
	1,09	0,57	29,66	3,48	1,82	94,70	2,45	1,05	81,69	2,88	1,23	1174	1,289	$NaCl + KCl \cdot MgCl_2 \cdot 6H_2O$
	0,68	2,63	26,08	2,31	8,95	88,74	1,48	4,50	69,86	1,95	5,93	1319	1,265	$KCl + KCl \cdot MgCl_2 \cdot 6H_2O$
	0,27	0,07	34,78	0,80	0,20	99,00	0,67	0,13	101,41	0,66	0,13	978	1,334	$NaCl + KCl \cdot MgCl_2 \cdot 6H_2O + MgCl_2 \cdot 6H_2O$
20	13,85	8,33	7,60	46,51	27,97	25,52	30,39	14,33	20,47	46,62	21,98	1534	1,235	$NaCl + KCl$
	1,88	3,23	25,44	6,15	10,57	83,28	4,17	5,62	69,29	5,27	7,11	1265	1,275	$NaCl + KCl + KCl \cdot MgCl_2 \cdot 6H_2O$
	1,42	1,29	28,30	4,58	4,16	91,26	3,17	2,26	77,59	3,82	2,72	1205	1,283	$NaCl + KCl \cdot MgCl_2 \cdot 6H_2O$
	0,35	0,08	35,22	0,98	0,24	98,80	0,84	0,16	103,54	0,80	0,15	957	1,337	$NaCl + KCl \cdot MgCl_2 \cdot 6H_2O + MgCl_2 \cdot 6H_2O$
25	6,87	6,39	15,87	23,58	21,94	54,48	14,97	10,89	42,76	21,81	15,87	1457	1,244	$NaCl + KCl$

Рис. 1. Снимок таблицы экспериментальных данных из [8]

Таблица 1. **Результаты классификации солей для 7 разных составов твердой фазы**

Исходные группы	Размер групп	Полученные группы						
		1	2	3	4	5	6	7
1	116	108 (93,10%)	8 (6,90%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	0 (,00%)	0 (0,00%)
2	44	0 (0,00%)	40 (90,91%)	0 (0,00%)	1 (2,27%)	3 (6,82%)	0 (0,00%)	0 (0,00%)
3	24	0 (0,00%)	1 (4,17%)	23 (95,83%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	0 (0,00%)
4	6	0 (0,00%)	0 (0,00%)	1 (16,67%)	4 (66,67%)	1 (16,67%)	0 (0,00%)	0 (0,00%)
5	5	0 (0,00%)	1 (20,00%)	0 (0,00%)	0 (0,00%)	4 (80,00%)	0 (0,00%)	0 (0,00%)
6	17	2 (11,76%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	15 (88,24%)	0 (0,00%)
7	19	2 (10,53%)	0 (0,00%)	0 (0,00%)	0 (0,00%)	1 (5,26%)	0 (0,00%)	16 (84,21%)

Таблица 2. **Результаты классификации солей для разных составов твердой фазы, различающихся количеством компонентов в нем**

Исходные группы	Размер групп	Полученные группы		
		1	2	3
1	36	30 (83,33%)	6 (16,67%)	0 (0,00%)
2	127	0 (0,00%)	115 (90,55%)	12 (9,45%)
3	68	0 (0,00%)	1 (1,47%)	67 (98,53%)

Таблица 3. **Результаты классификации солей для разных составов твердой фазы, различающихся наличием или отсутствием кристаллогидратов**

Исходные группы	Размер групп	Полученные группы	
		1	2
1	79	79 (100,00%)	0 (0,00%)
2	152	4 (2,63%)	148 (97,37%)

ты были получены для групп четыре и пять. Это и неудивительно, так как их количество среди всей выборки составило примерно 2,3–3%. Можно было бы выбросить эти результаты, т. к. они были найдены только у одного автора. Однако учитывая, что их опубликовал классик науки о физико-химическом анализе водно-солевых систем – академик Н. С. Курнаков, они были оставлены.

Ниже представлены все номера всех записей, качество классификации которых оказалось неудовлетворительным для варианта раз-

деления семи солей в твердой фазе: 10, 17, 64, 65, 82, 83, 84, 101, 102, 120, 121, 127, 129, 137, 137, 144, 171, 173, 175, 185, 187, 188, 201, 208, 209, 223, 225.

Суммарный результат классификации составил 92%, среди которых оказались неудовлетворительными следующие записи: 3, 84, 121, 126, 127, 129, 177, 185, 189, 193, 194, 198, 208, 209, 218. Очевидно, что уже имеется пересечение с предыдущей таблицей, состоящее из записей: 84, 121, 127, 129, 185. Следовательно, эти записи уже два раза не смогли войти в результаты удачной классификации.

В этом случае (табл. 3) результат классификации равен 98%, а в качестве неудовлетворительных были выделены следующие записи – 64, 65, 83, 84, 102, 120, 201. Как и в предыдущем случае существуют результаты, которые дважды или трижды повторяются как неудачные, например, 64, 65, 83, 84, 126, 129, 185, 193, 194, 198, 102, 120, 201. Следовательно, наборы этих записей следует пометить в базе данных как вызывающие вопросы.

Кроме того предлагаемый нами способ оценки данных в данном конкретном сообщении позволит ответить также и на ряд практических вопросов, связанных с определением качественного состава твердой фазы, находящимся в равновесии с насыщенным раствором при разных температурах. Например, для последней, наиболее удачной классификации в качестве примера приведено решающее правило, которое имеет вид:

$$F_1 = -135{,}761 - 0{,}565196 \cdot Col\_1 + 8{,}70281 \cdot Col\_2 + 7{,}66225 \cdot Col\_3 + 8{,}69064 \cdot Col\_4,$$

$$F_2 = -105{,}677 - 0{,}490061 \cdot Col\_1 + 7{,}9137 \cdot Col\_2 + 7{,}01466 \cdot Col\_3 + 7{,}53163 \cdot Col\_4,$$

где *Col_1* – температура раствора, °С; *Col_2* – NaCl, %мас; *Col_3* – KCl, %мас; *Col_4* – $MgCl_2$, %мас.

Подставив в уравнение соответствующие значения концентраций равновесного состава, с вероятностью 98% можно прогнозировать наличие кристаллогидрата в составе твердой фазы. Прочие решающие правила позволяют с меньшей вероятностью (91–92%) дать прогноз о качественном составе твердой фазы.

Заключение

В представленной работе рассмотрена возможность поиска сомнительных данных в справочниках при объединении их БД. В качестве метода исследования предлагается использовать один из алгоритмов распознавания образов – разработка решающего правила. На наш взгляд такой подход оказался полезен для выявления данных типа unusual data в многокомпонентной гетерогенной системе NaCl–KCl–$MCl_2 \cdot H_2O$, собранной из 12 различных источников.

Получено решающее правило, позволяющее с вероятностью 98% прогнозировать наличие или отсутствие кристаллогидрата в твердой фазе в зависимости от состава насыщенного раствора NaCl, KCl, $MCl_2 \cdot H_2O$.

Литература

1. **Россиев, А. А.** Моделирование данных при помощи кривых для восстановления пробелов в таблицах / А. А. Рос–сиев // Методы нейроинформатики: сборник научных трудов / Красноярский гос. тех. унив.; под ред. А. Н. Горбаня. – Красноярск, 1998. – С. 6–22.

2. **Зильберглейт, М. А.** Восстановление пропущенных данных при изучении свойств совмещенных эластомеров и пластиков / М. А. Зильберглейт, Р. М. Долинская // Материалы. Технологии. Инструменты. – 2011. –Т. 16. – № 1. – С. 111–114.

3. **Загоруйко, Н. Г.** Алгоритмы обнаружения эмпирических закономерностей/ Н. Г. Загоруйко, В. Н. Ёлкина. – Новосибирск.: Наука, 1985. – 110 с.

4. **Горелик, А. Л.** Методы распознавания / А. Л. *Горелик, В*. А. С*крипкин.* – М.: Высшая школа, 1984. – 262 с.

5. **Вапник, В. Н.** Теория распознавания образов / В. Н. *Вапник*, *А*. Я. *Червоненкис*. – М.: Наука, 1974. – 416 с.

6. **Фомин, Я. А.** Распознавание образов: теория и применения / Я. А. Фомин. – М.: ФАЗИС, 2012. – 429 с.

7. **Фомин, Я. А.** Статистическая теория распознавания образов / Я. А. *Фомин, Г. Р. Тарловски*. – М.: Радио и связь, 1986. – 624 с.

8. **Здановский, А. Б.** Справочник экспериментальных данных по растворимости многокомпонентных водно-солевых систем /А. Б. Здановский, Е. Е. Ляховская, Р. Э. Шлеймович. – М.: Государственное научно-техническое издательство химической литературы, 1954. – 1270 с.

References

1. **Rossiev, A. A.** Simulation data using recovery curves for gaps in the tables / A. A. Rossiev // The neuroinformatics methods: collection of scientific papers / Krasnoyarsk State. Technical. Univer.; – Krasnojarsk, 1998. – P. 6–22.

2. **Zil'berglejt, M. A.** Recovery of missing data in the study of the properties of elastomers and plastics, combined / M. A. Zil'berglejt, R. M. Dolinskaja // Materials. Technologies. Instruments. – 2011. – V.. 16. – № 1. – P. 111–114.

3. **Zagorujko, N. G.** Detection algorithms empirical regularities / N. G. Zagorujko, V. N. Jolkina. – Novosibirsk.: Nauka, 1985. – 110 p.

4. **Gorelik, A. L.** Detection Methods / A. L. Gorelik, V. A. Skripkin. – M.: Vysshaja shkola, 1984. – 262 p.

5. **Vapnik, V. N.** The theory of pattern recognition / V. N. Vapnik, A. Ja. Chervonenkis. – M.: Nauka, 1974. – 416 p.

6. **Fomin, Ja. A.** Pattern Recognition: Theory and application / Ja. A. Fomin. – M.: FAZIS, 2012. – 429 p.

7. **Fomin, Ja. A.** Statistical theory of pattern recognition / Ja. A. Fomin, G. R. Tarlovski. – M.: Radio i svjaz', 1986. – 624 p.

8. **Zdanovsky, A. B.** /Reference book of experimental data on solubility of multicomponent water-salt systems – M.: State scientific and technical publishing house of chemical literature, 1954. – 1270 p.

Поступила	*После доработки*	*Принята к печати*
25.03.2016	*15.04.2016*	*10.05.2016*

M. A. Zilbergleit

SELECTION OF BASIC INFORMATION FOR FORMATION OF THE DB BY WAY OF EXAMPLE OF MULTICOMPONENT SYSTEM NACL–KCL–MGCL2·H2O

In article is offered the way of a search of the facts like unusual data (these raising doubts) by forming databases from several sources. As criterion for search of such data it is offered to use a method of pattern recognition – decision rule. By using two and more decision rules there are crossings at which objects which can't be classified correctly by means of such decisive rules are formed. As an example of a search of the data like unusual data application of this method is shown in the analysis of the data of heterogeneous balance in NaCl–KCl–MgCl H_2O system published in 12 various sources for the different periods of time. Accuracy of classification has made 92–98%.

Keywords: *selection of the source data, the data is questionable, unusual data, pattern recognition, linear and non-linear classifiers, decision rule, set intersection of multicomponent heterogeneous chemical system.*

Зильберглейт М. А. – доктор химических наук, заведующий лабораторией Института общей и неорганической химии НАНБ. Закончил Белорусский государственный технологический университет по специальности химическая технология переработки нефти и газа. Работал в ИФОХ НАНБ, Главгазе БССР, БГТУ. Подготовил 9 кандидатов наук в области химии, полиграфии и информационных технологий. Более 100 публикаций, патентов, учебных пособий. Специализация – оптимизация и управление химико-технологическими процессами. E-mail: mazi@list. ru.

УДК 004.9:681.3

В. Г. МИХАЙЛОВ

О ПОДХОДАХ К СОЗДАНИЮ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ PDM-ERP

ООО «Мидивисана», г. Минск

Рассмотрены проблемы, сложившиеся в области создания систем PDM и их интеграции с ERP. Проведен анализ причин низкой эффективности существующих PDM: недостаточность первичной информации заносимой в модуль PDM, структур БД, занесения обозначений в одно поле, применение ссылочного характера ведения состава, что приводит к снижению его функциональности и создает проблемы с интеграцией с ERP. Показано, что для предприятий с полным циклом необходима единая интегрированная информационная система, созданная на единых базах данных, использующая в качестве первичного документа карточку ДСЕ, а не сам файл (3D-модели, чертежа, документа). Для нее необходима иная в отличии от существующих универсальная структура баз данных, в которую можно занести любую информацию. Предложена реализация новой системы CDRP, объединяющую по функционалу PDM-ERP и обеспечивающую основные потребности предприятия.

Ключевые слова: *PDM, ERP, интегрированная информационная система предприятия, база данных.*

Ведение

В настоящее время процесс проектирования, подготовки и управления производством на всех предприятиях ведется в электронном виде. Результатом электронного проектирования изделий, являются файлы моделей, конструкторской документации (КД), созданные в различных 2D, 3D пакетах [1]–[7], размещенные в разных каталогах. Для работы с сборкой в 3D пакете эти файлы должны быть собраны в рабочий каталог либо создан конфигурационный файл их размещения, после чего осуществляется загрузка сборки. Это возлагается на **PDM** (Product Data Management/управление данными об изделии) и является его основной функцией. Необходимость в PDM обуславливается потребностью управления операциями с моделями, ведения электронного архива конструкторской и технологической документации (КД и ТД), размещением их в базах данных (БД), правами доступа, контролированием и координацией процесса совместного проектирования, осуществлением их поиска, исключением дублирования разработки ранее созданных компонентов, обеспечения проведения изменений, выдачи КД в производство. Любое серийное изделие на 60–70% состоит из уже ранее созданных. Система PDM является первичным звеном необходимой информации всех служб предприятия и организации производства, осуществления документооборота КД и ТД в электронном виде.

Полученные данные от PDM по составу используются при планировании, управлении производством расчетов выпуска деталей, количества материалов для них, потребности в оборудовании, оснастки, трудовых кадров и тому подобному. Это относится к функции **ERP** (управлении ресурсами) и другим системам. Системы PDM и ERP тесно между собой связаны (рис. 1) [1] и по логике должны быть построены на единых основных базах данных.

Однако, как показала практика развитие PDM и интеграция их с ERP пошло по иному пути, вызвавшему множество проблем, что снизило эффективность PDM и часто не оправдывает возлагаемых надежд на их использование [4], [5], [8]–[11].

Анализ проблем

Рассмотрим проблемы и недостатки PDM, препятствующие созданию интегрированной информационной системы предприятий (ИИСП) и подходы в создании новой подсистемы CDRP

Рис. 1. Интегрированная информационная система РКК «Энергия»

(Cross Designing Resourse Planning/сквозного проектирования–планирования ресурсов), объединяющей основные функции PDM и ERP.

Согласно первоначального НАТОвского определения еще 80 гг. PDM должен был вести всю информацию об изделии на всех его стадиях. Однако развитие PDM (Teamcenter, Windchill, mySAP-PLM, IPS и др. [1]–[3], [6], [7]) пошло по пути минимизации ведения проектной информации. Функционал PDM был нацелен на узкий круг задач: внесение первичной ограниченной информации об изделии, ее составе, электронное согласование документов, управлении правами доступа и контроль процесса проектирования. Несмотря на интересные решения PDM Windchill [2] по использованию интернет-технологий при работе с удаленными пользователями с визуализацией сжатой графики многие важные функции обеспечения внутренних потребностей проектных служб, широкого поиска (в первую очередь аналогов), информационной поддержки проектирования и ТПП у большинства PDM все же развиты слабо либо решаются другими средствами [3]. Причиной этому является непонимание полной картины информационного обеспечения, требующегося сейчас предприятиям с полным циклом – проектирование-производство-утилизация и узкое видение реализации PDM со стороны разработчиков. Необходимо учитывать, что в руках конструктора находится вся первичная информация об деталь-сборочной единице (ДСЕ), материалах, комплектующих, производителе и т. п. И для внесения всей этой разнообразной информации необходима соответствующая структура баз данных, которую нельзя решить путем простого увеличения числа полей. Различие в подходах ведения информации заключается в том, что при использовании PDM вначале в 3D (2D) пакете создается файл КД с реквизитами, затем на основе его формируется карточка файла. А в ERP по БД вначале определяется обозначение ДСЕ и создается его карточка, к которой затем прикрепляется файл КД. Эти карточки имеют различный объем и состав информации. В большинстве случаев в PDM из-за того, что обозначение файла КД заносится в одно поле и невозможно провести сортировку по его частям практически нереально получить обозначение КД, приходится пользоваться ERP системой либо амбарной книгой архива.

На большинстве PDM, как правило, заносятся только обозначение, наименование, разработал, дату и состав (путем ссылки на файлы КД). Фактически PDM ведет только справочник файлов моделей и состав файлов сборок и информации о них, что не всегда соответствует информации о ДСЕ в ERP. В PDM можно только посмотреть состав, переходя по де-

Рис. 2. Упрощенная структура БД большинства PDM

реву изделия, сложно найти аналоги. В виду ограниченности информации и функционала существующие PDM часто не оправдывают возлагаемых надежд на их использование. Из-за этого и нежелания вносить информацию проистекает отрицательное отношение конструкторов и технологов к PDM, отмечаемое на форумах САПР. Несмотря на это без PDM все же нельзя обойтись, особенно для 3D пакетов.

В ERP содержится более полная информация о детали, сборке, а состав включает помимо всех деталей также документацию, материалы и др. Упрощенно структура БД PDM по ведению основной информации приведена на рис. 2.

Отметим, что в существующих PDM имеется и другие таблицы, но они относятся к вспомогательным функциям, а основной информации явно недостаточно. Можно конечно внести информацию об материалах, комплектующих, их изготовителе, прикрепив файл сканированной информации или ссылку из интернета либо хранить информацию в реквизитах самого файла. Ряд PDM допускает возможность небольшое увеличение числа полей. Но это не то, что требуется. Нужна структурированная система данных, БД, их справочников, рассчитанных на занесение любой информации.

Анализ существующих пакетов PDM позволяет выделить их следующие недостатки:

– структура БД PDM, ее информация, бизнес-логика построения отличается от ERP. Большинство пакетов PDM не связаны непосредственно с ERP (АСУ) системами и не имеют общих баз данных. Из-за чего информацию приходится конвертировать, при которой возможны ошибки. Для конвертации необходимо разрабатывать программы-конверторы либо заказывать и покупать их. Стоимость их разработки соизмерима с PDM;

– не предусмотрено дополнительное кодирование ДСЕ (нет поддерживающих справочников) и выдача им обозначений (не позволяет запись в одно поле);

– нет возможности проведения сортировок формируемых перечней ДСЕ из-за занесения обозначения в одно поле и ведения состава путем ссылок на ДСЕ;

– большинство PDM имеет слабую систему поиска – в основном по обозначению, наименованию, разработчику, дате. Этого недостаточно для больших БД предприятий (>150–200 тыс. ДСЕ). Например, чтобы найти ДСЕ, не имея его точного обозначения путем просмотра неотсортированной выборки 7 тыс. записей по ребрам и косынкам, требуется 17 мин;

– в PDM не реализована функция определения применяемости ДСЕ в конечных изделиях, что затрудняет проведение изменений;

– нет возможности сформирования перечня и массива непосредственного состава файлов моделей, чертежей по определенным критериям, например, для передачи КД, их файлов заказчику либо только в конкретном виде файлов и тому подобному;

– невозможно получение слепка состояния всего изделия на определенный период. Из-за чего в дальнейшем потребуется вручную разбираться в спецификациях (например, при обеспечении запчастями);

– PDM не содержат технологической информации: о маршрутах, нормативах материалов и др. Из-за чего возникают проблемы с комплектацией и рассылкой документации и ее обновлением в производстве (выпуск изделий по старой документации) и ошибки в планировании и сбои в производстве;

– нет выделения исполнения ДСЕ при заказах изделий с определенным исполнением и информации о наличии изделий на складах;

– нет связи изменений и извещений;

– нет возможности выделения изделий серийного и экспериментального (единичного) производства и соответствующего распределения работ по ним;

– частое изменение версий графических пакетов влечет необходимость изменений в пакетах PDM и вызывает потребность в их поддержке, ее покупке и значительно удорожает

затраты на PDM. Один раз купив определенную PDM, сложно от нее уйти;

– не возможно изменить систему и ее структуру. Приходится довольствоваться тем, что есть;

– поскольку разработчики большинства PDM считают, что многие функции должна выполнять ERP (АСУ) требуется параллельное использования программы АСУ, в которой повторно необходимо заново набирать обозначение ДСЕ, осуществлять его поиск и затем выполнять требуемую функцию.

О реализации CDRP

Все перечисленные выше недостатки обусловили необходимость создания новой системы, объединяющей функции PDM, ERP и устраняющей описанные недостатки. Данную система предлагается назвать CDRP (Cross Designing–Resourse Planing/Сквозное проектирование–управление ресурсами).

В ней применен метод непосредственного занесения обозначения с разделением на части как в справочник ДСЕ так и в состав. Благодаря этому можно производить требуемые сортировки по составу, их частям, легко выделять головные сборки, узлы, которые оказываются в верхней части таблицы просмотра. Использована система внесения изменений близкая к бумажному варианту с сохранением аннулированных и внесением новых записей с соответствующими кодами действия, содержащая ссылки на извещение. Это позволяет лучше отслеживать ее историю. Изменения готовятся самим конструктором в БД и проводятся (актуализируются) другой службой после утверждения бумажных документов (извещения) за счет специального механизма изменения кода действия изделия.

Основные БД CDRP включают в себя: справочник деталей (с большим число полей, в т. ч. кодируемых); изменений, решений; оригинальных обозначений и основных сведений о ДСЕ и предприятиях их выпускающих; конструкторский состав (72 поля); конструктивные параметры (10 полей), где записывается различная кодированная информация, включая графические и текстовые файлы КД, расчетов, презентаций, информация по материалу, штампу чертежа и т. п.; конструктивно-технологические признаки, позволяющие закодировать детали по этим признакам и вести по ним поиск; параметрику деталей (основные характеризующие параметры изделий, габаритные, весовые параметры и т. п.); ссылочные документы (взамен, аннулированные, НТД, примененные материалы и др.); конструкторский состав чертежей (для возможности работы с составными (ссылочными) чертежами и документами); извещения, включая графические файлы их содержаний; маршрутов от цехов до рабочего места; материальные нормативы; архивные сведения и согласование документов.

Каждая из этих БД включает дополнительные БД и реляционно с ними связанные справочники поддержки. Упрощенная структура БД PDM CDRP приведена на рис. 3.

Рис. 3. Структура БД PDM CDRP

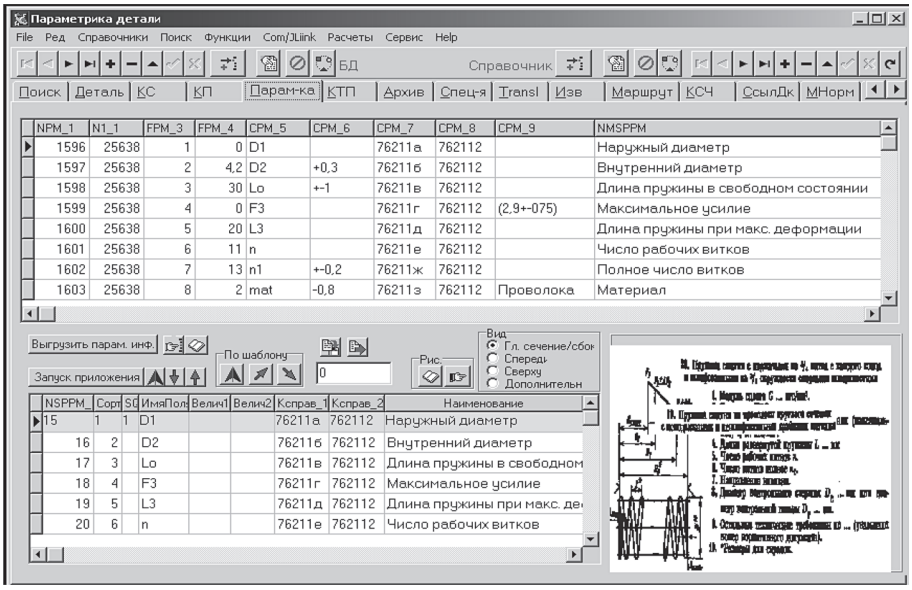


Рис. 4. Пример реализации поисковой БД по пружинам

В CDRP первичным документом является карточка ДСЕ с разделенным обозначением на 5 полей. Она содержит 28 полей, включая наименование на английском. Имеется функция перевода наименование на английский язык для формирования каталогов запчастей. Карточка ДСЕ связана с таблицами дополнительной информации, ссылочными документами, изменений, извещений, решений, параметрами, согласованием и далее с их файлами.

Благодаря чему можно вести любую информации и делать необходимые выборки, что невозможно в большинстве PDM. А сочетании с другими модулями (планирования производства, складского учета и перемещений) можно решать практически все основные задачи проектирования и производства.

В CDRP широко применяется метод кодирования информации (особенно в БД конструктивные параметры, конструктивно-технологические признаки), позволяющий занести любую информацию в универсальные поля, за счет некоторой избыточности полей в строке (рис. 4).

И одна и та же таблица может использоваться для занесения иной информации. Благодаря такой структуре данных CDRP имеет мощную поисковую систему, охватывающую не только справочник ДСЕ, конструкторский состав, но и другие базы данных и позволяющий гарантированно найти требуемое ДСЕ. Использование аналогов уже созданных компонентов, наработок и решений позволяет получить выигрыш в сроках проектирования и ТПП. Именно для этого и нужна мощная поисковая система.

Предусмотрен контроль выполнения работ через выявление незаполненных сборок, фиксация электронного утверждения КД с идентификацией файлов КД по контрольному числу. Разработчик после утверждения не может их изменить. Имеются функции формирования перечней сданной в электронный архив документации.

CDRP создана в среде Windows 7/10 с помощью C++Builder+ODAC на СУБД ORACLE 10–12 g. Программа выполняет широкий круг задач отделов главного конструктора и технолога: позволяет хранить и получать различную информацию о конструкторских документах, изделиях, материалах, их жизненном цикле, снабжать конструктора необходимой информацией, вести широкий поиск по различным направлениям, выполнять расчет подготовки производства и потребности материалов, формировать спецификации, включая заказные, каталоги запчастей, отслеживать конструктивные решения, отклонения, вести договора, выполнение планов, управлять работой графических и текстовых пакетов.

Программное средство интегрировано с системами автоматизированного проектирования. Creo, AutoCAD, офисными средствами Word, Excel, просмотровщиками и другими средствами, поддерживающими COM, Java-технологии.

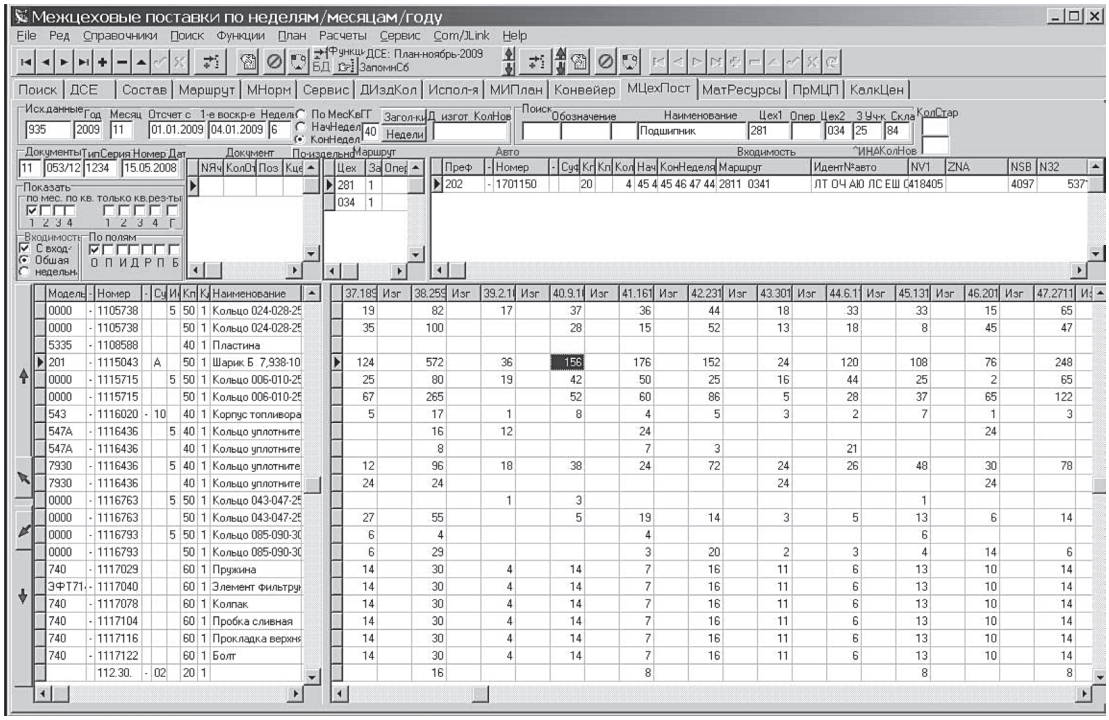


Рис. 5. Пример реализации межцеховых поставок с учетом сроков

Помимо модуля PDM в CDRP имеются модули MPL (планирования производства) и MDP (управления движения продукции/складского учета) с общими БД ДСЕ и составов.

Модуль MPL предназначен для служб ПДБ, УВК, маркетинга занимающихся планированием выпуска продукции. Он обеспечивает формирование планов понедельно, помесячно, квартально и по году с учетом сроков и цикла изготовления и поиздельно и варианта исполнения (рис. 5).

Информация по планированию формируется путем задания спецификации месячного, квартального, годового плана с учетом признаков серийной продукции и ОКР, а также изделий под заказ. Имеется возможность производить раздельное разузлование по БД конструкторского и технологического составов с учетом исполнений изделий и подключения маршрутов по аналогам ДСЕ. Их результаты с учетом распределения по изделиям, входимости и маршрутов посредством процедур ORACLE включаются в месячный план (понедельно). На основе помесячных планов формируется итоговый квартальный, годовой план по ДСЕ (без входимости и указания изделий).

Модуль движения продукции предназначен для служб УВК, УМТС, ПДБ цехов. Связан с PDM-ERP модулями через общие БД. Базируется на подходе внесения информации в БД о движении МЦ через товарно-транспортные накладные, приходные ордера, требования, лимитные карты, приемо-сдаточные накладные и др., выставлении счетов и осуществлении их проводок, получении остатков на складах и использовании этой информации при планировании производства.

Модуль MDP связан с заводским справочником ДСЕ-материалов и справочником организаций, позволяющими осуществлять быстрый поиск и занесение необходимой информации в документы. Для унификации нумерации документов используется дополнительное поле серия документа.

В результате такого подхода, примененного в CDRP, получаем очень удобную универсальную систему PDM-ERP, обеспечивающую основные потребности предприятия.

Заключение

1. Как показала практика применения существующих PDM они выполняют только ограниченную часть функций (загрузку и управление файлами моделей, ведения электронного архива, организационно-распорядительные функции). Однако этого сейчас недостаточно и часто не оправдывает возлагаемых надежд на их использование.

2. Причинами низкой эффективности являются недостаточность первичной информации заносимой в PDM, использование в качестве первичного элемента файла КД, отсутствие возможности подключения реляционных БД, занесения обозначений в одно поле, применение ссылочного характера ведения состава, что не позволяют проводить выборки с требуемыми сортировками и усложняют поиск файлов КД, а также отсутствие технологической информации: о маршрутах, нормативах материалов, рассылки документации и ее обновлением в производстве (выпуск изделий по старой документации) из-за чего возникают ошибки в планировании и сбои в производстве.

3. Большинство пакетов PDM не интегрированы непосредственно с ERP (АСУ) системами и не имеют общих баз данных. Из-за чего информацию приходится конвертировать. Для этого необходимо разрабатывать программы конверторы либо заказывать и покупать их, что увеличивает затраты. Возможны ошибки при конвертации.

4. Для предприятий необходима единая интегрированная информационная система, созданная на единых базах данных, использующая в качестве первичного документа карточку ДСЕ, а файл модели является вторичным. Требуется иная в отличии существующих универсальная структура баз данных, в которую путем привязки дополнительных реляционных БД (их строк) к записи основной БД, а также за счет кодирования и некоторой избыточности можно было бы занести любую информацию.

5. Предложена реализация новой системы CDRP, не имеющей описанных недостатков и объединяющую по функционалу PDM-ERP и обеспечивающая основные потребности предприятия.

Литература

1. Актуальность применения PDM решений системы TeamCenter в ракетно-космической промышленности [Электронный ресурс]. – 2010. – Режим доступа: http://lab18.ipu.ru/projects/conf2009/2/10..htm. – Дата доступа: 25.10.2015.

2. PTC Windchill PDM Essentials [Электронный ресурс]. – 2015. – Режим доступа: http://www.ptc.com/product-lifecycle-management/windchill/pdm-essentials. – Дата доступа: 25.08.2015.

3 Рекламные материалы фирмы Интермех [Электронный ресурс] – 2016. – Режим доступа: http://www.ips.intermech.ru – Дата доступа: 20.04.2016.

4. Михайлов, В. Г. Анализ и сравнение существующих PDM [Электронный ресурс]. – Режим доступа: http://www.belerp.com/modules.php?name=Pages&pa=showpage&pid= 76 – Дата доступа: 13.02.2007.

5. Михайлов, В. Г. Какой должна быть PDM-система [Электронный ресурс]. – Режим доступа: http://www.belerp.com/modules.php?name=Pages&pa=showpage&pid= 56 – Дата доступа: 25.07.2006.

6. 1С: Предприятие 8. PDM Управление инженерными данными [Электронный ресурс]. – Режим доступа: http://solutions.1c.ru/catalog/pdm/features – Дата доступа: 25.07.2014.

7. Описание «Omega Production» [Электронный ресурс]. – 2010. – Режим доступа: http://www.omegasoftware.ru/about_system/system_description/ – Дата доступа: 24.03.2016.

8. Ostroukh A. V. Integration of PDM and ERP systems within a unified information space of an enterprise // Ostroukh A. V., Gusenitsa D. O., Golubkova V. B., Yurchik P. F. IOSR Journal of Computer Engineering (IOSR-JCE). 2014. Vol. 16. Issue 02. V6. pp. 31–33. DOI: 10.9790/0661-16263133. ANED: 11.0661/iosr-jce-E016263133.

9. Yongjun Feng, Integration Model Based on the Integration of «CAD/CAPP/PLM/ERP» Framework Research // Chemical engineering transactions, Vol. 46, 2015, p. 6, DOI: 10.3303/CET1546186

10. Pierre Breuls, Integrating PDM with ERP [the Electronic resource]. –http://www.docmanage.com/magazine/backissues/8-5/BAAN.htm – Access Date: 25.04.2016.

11. Jiu Sun Research and Application of PDM and CAD Integration Technology // Jiu Sun and Yuemiao Wang / [the Electronic resource]. – Access mode: www.atlantis-press.com/php/download_paper.php?id... – Access Date: 25.04.2016.

References

1. An urgency of application PDM of decisions of system TeamCenter in the space-rocket industry [the Electronic resource]. – 2010. – the Access mode:
http:// lab18.ipu.ru/projects/conf2009/2/10..htm. – Access Date: 10/25/2015.

2. PTC Windchill PDM Essentials [an electronic resource]. – 2015. – Access mode: http://www.ptc.com/product-lifecycle-management/windchill/pdm-essentials. – Access Date: 8/25/2015.

3. Firm Intermech advertizing materials [the Electronic resource] – 2016. – Access mode: http://www.ips.intermech.ru – access Date: 4/20/2016.

4. Mikhailov, V. G. Analiz and comparing existing PDM [the Electronic resource]. – Access mode: http://www.belerp.com/modules.php?name=Pages&pa=showpage&pid=76 – Access Date: 2/13/2007.

5. Mikhailov, V. G. Whats should be PDM-system [the Electronic resource]. – Access Mode: http://www.belerp.com/modules.php?name=Pages&pa=showpage&pid=56 – Access Date: 7/25/2006.

6. 1C: the enterprise 8. PDM Control of the engineering data [the Electronic resource]. – Access mode: http://solutions.1c.ru/catalog/pdm/features – Access Date: 7/25/2014.

7. The description «Omega Production» [the Electronic resource]. – 2016. – Access mode: http://www.omegasoftware.ru/about_system/system_description – Access Date: 3/24/2016.

8. Ostroukh, A. V. Integration of PDM and ERP systems within a unified information space of an enterprise // A. V Ostroukh, D. O. Gusenitsa, V. B. Golubkova, P. F. Yurchik / IOSR Journal of Computer Engineering (IOSR-JCE). 2014. Vol. 16. Issue 02. V. 6. pp. 31–33. DOI: 10.9790/0661-16263133. ANED: 11.0661/iosr-jce-E016263133.

9. Yongjun Feng, Integration Model Based on the Integration of «CAD/CAPP/PLM/ERP» Framework Research // Chemical engineering transactions, Vol. 46, 2015, p. 6, DOI: 10.3303/CET1546186.

10. Pierre Breuls Integrating PDM with ERP [the Electronic resource]. – http://www.docmanage.com/magazine/backissues/8–5/BAAN.htm – Access Date: 25.04.2016.

11. Jiu Sun Research and Application of PDM and CAD Integration Technology // Jiu Sun and Yuemiao Wang / [the Electronic resource]. – Access mode: www.atlantis-press.com/php/download_paper.php?id... – Access Date: 25.04.2016.

Поступила	*После доработки*	*Принята к печати*
15.04.2016	*30.04.2016*	*10.05.2016*

Vladimir Mikhailov

ABOUT APPROACHES OF CREATION OF INTEGRATED INFORMATION SYSTEM PDM-ERP

The problems which has added in the field of creation of systems PDM and their integration with ERP is considered. The analysis of the reasons of low efficiency existing PDM is carried out: insufficiency of the primary information brought in PDM unit, structures of a DB, entering of designations in one field, application of referential character of guiding of composition that leads to lowering of its functionality and creates problems with integration with ERP.

It is shown that the uniform integrated information system created on uniform databases is necessary for the enterprises with a full stroke, using as the primary document card part-bom-unit, instead of a file. For it other is necessary in difference from databases existing the general-purpose structure in which it is possible to bring any information.

Implementation of the new system CDRP, uniting on functional PDM-ERP and providing enterprise basic needs is offered.

Keywords: *PDM, ERP, the integrated enterprise information system, a database.*

Владимир Георгиевич Михайлов, канд. техн. наук 05.05.03, ведущий инженер ООО «Мидивисана», г. Минск.

Специалист в области разработки систем CALS/PLM (PDM, ERP), автомобилестроения, моделирования динамических систем в пакетах MATLAB\SIMULIK, оценки напряженно-деформированного состояния в пакете ANSYS, испытаниям подвесок, рам ТС, пневматики, гидравлики, тензометрирования,

Tel.: + 375-(029)785–09–16. E-mail: sapr7@mail. ru.

Mikhailov Vladimir, PhD (Cand. Tech. Sci., from 1982) in Applied and mechanical Engineering.

He was a Senior Research and Engineer-designer at Minsk Automobile plant, from 1972 to 1984, Leading Research, Chief of Research laboratory in CenterSystem, Minsk (design and development ERP) from 1984 to 1991, and was leading Engineer-designer at Minsk Wheel plant from 1994 to 2010, now a leading engineer of Open Stock Company «Midivisana», Republic Belarus, Minsk. His research interests include design and development of Software PDM, ERP, application Oracle on C++, PL/SQL, Java, modeling dynamic systems, vibration.

The expert in the field of system engineering CALS/PLM (PDM, ERP), motor industry, modeling of dynamic systems in packets MATLAB\SIMULIK (S-Function Builder), estimations of the intense-deformed state in packet ANSYS, tests of suspension, frames of the vechicle, a pneumatics, hydraulics.

Tel.: + 375-(029)785–09–16. E-mail: sapr7@mail. ru.

УДК 004.021

Ю. Д. ИВАНОВ, И. Н. НИКОЛОВ, Б. В. ЛОЗКА

ДЕКОДИРОВАНИЕ СТРУКТУРНО ЛОГИЧЕСКИХ КОДОВ

Одесский национальный политехнический университет, Одесса, Украина

В работе приводится описание основных положений структурно-логического кодирования, а также особенности кодов СЛК. Приводятся основные положения обобщенного алгоритма декодирования СЛК, в основе которого лежит метод совершенной матричной расстановки (СМР) вершин n-мерного куба для адекватного представления и преобразования булевых функций, который базируется на методе порождающих последовательностей переменных построения максимальных покрытий вершин куба. Структурно-логические коды (СЛК) используют природную логическую избыточность инфимумных дизъюнктивных нормальных форм (ИДНФ) булевых функций, которые являются основой построения кодов СЛК, для исправления ошибок, которые возникают при передаче данных в реальных дискретных каналах, по каналам с независимыми ошибками. Основной задачей является определение базисных соотношений между реализованными кодами СЛК логической избыточности и граничными значениями кратности независимых ошибок, которые исправляются. Принципиальным отличием кодов СЛК от всех известных корректирующих кодов является то, что избыточность, необходимая для исправления ошибок преобразования дискретной информации, не вводится в кодовую последовательность, а задается естественным образом, при построении кодовых комбинаций СЛК.

Ключевые слова: *структурно-логические коды, булевы функции, обобщенный метод декодирования, совершенная матричная расстановка, единый кодирующий формат.*

Введение

При структурно-логическом кодировании (СЛК) каждая конъюнкция инфимумной дизъюнктивной нормальной формы (ИДНФ) булевой функции (БФ), представляющей дискретные данные, разворачивается в кодовую комбинацию единого кодирующего формата (ЕКФ) куба E^n [1, 2, 3].

Корректирующие свойства СЛК обусловлены естественной логической избыточностью переменных развертывания куба E^n в порождающей последовательности

$$x_i^1 x_j^2 x_i^1 x_k^3 x_i^1 x_j^2 x_i^1 \ldots x_z^n \ldots x_i^1 x_j^2 x_i^1 x_k^3 x_i^1 x_j^2 x_i^1 \qquad (1)$$

где n – мерность куба,

$$z \neq \ldots \neq k \neq j \neq i \neq 0,1,\ldots, n-1.$$

В последовательности (1) верхние индексы переменных обозначают уровни развертывания ребер (куб E^1), граней (куб E^2), кубов E^3 и т. д., а каждая из переменных участвует в организации кубов E^n несколько раз, что и обеспечивает требуемую логическую избыточность для коррекции ошибок в кодовой комбинации (ЕКФ) СЛК.

В результате структурно-логического кодирования строится последовательность вершин кубов E^n, представляющих собой кодовые комбинации ЕКФ, число их комбинаций заданной БФ определяется числом конъюнкций ее ИДНФ.

Полученная последовательность вершин кубов ЕКФ трансформируется в канале преобразования, и отдельные разряды двоичных чисел искажаются в результате воздействия канальных ошибок.

При декодировании комбинаций ЕКФ реализуется логическая избыточность переменных развертывания куба E^n, и ошибки в кодовой комбинации исправляются.

Задача состоит в том, чтобы разработать алгоритм декодирования, при котором все вершины кода ЕКФ, комбинация СЛК, были полностью восстановлены за счет предельно полного использования избыточности переменных развертывания куба E^n, выполненного с учетом положений алгоритма декодирования [3, 6], что обеспечит простую и корректную процедуру преобразования канальной последовательности вершин куба ЕКФ при приеме.

Основная часть

Из канала преобразования принимается комбинация СЛК, то есть куб E^n ЕКФ. Порядок следования принимаемых вершин куба ЕКФ определяется порождающей последовательностью переменных развертывания куба E^n (1). Каждая принимаемая вершина представляет собой n-разрядное двоичное число, где n – мерность куба E^n.

Первая принятая n-разрядная вершина E_1^0 образует со второй принятой вершиной E_2^0 по переменной развертывания первого уровня x_i^1 ребро, то есть куб E_1^1. Первое принятое ребро куб x_j^2 по переменной развертывания второго уровня x_j^2 образует со вторым принятым кубом E_2^1 грань, то есть куб E_1^2. Куб E_2^1, полученный путем объединения также по переменной развертывания первого уровня E_3^0, образован из третьей и четвертой принятых вершин E_3^0 и E_4^0. Прием вершин E_5^0, E_6^0, E_7^0 и E_8^0 приведет к образованию куба E_1^3. В общем случае, последовательность принятых из канала преобразования вершин кубов ЕКФ в виде n-разрядных двоичных кодов, обозначим как 1, 2, 3, 4, …, и представим согласно совершенной матричной расстановке (СМР) [4] матрицей вершин куба ЕКФ (рис. 1). В примере приведена СМР из 8-ми подматриц кубов E^2 ЕКФ с вершинами:

1, 2, 3, 4 – 5, 6, 7, 8 – 9, 10, 11, 12 – 13, 14, 15, 16 – 17, 18, 19, 20 – 21, 22, 23, 24 – 25, 26, 27, 28 – 29, 30, 31, 32.

Каждый из кубов E^2, E^3, E^4, E^5, ЕКФ может быть использован для анализа принятых кодовых комбинаций кода СЛК. СМР куба E^5 ЕКФ может служить основой реализации кубов большей мерности E^6, E^7, E^8 и т. д. ЕКФ кода СЛК при использовании соответствующих переменных развертывания порождающей последовательности (1).

Число логических связей каждой из переменных развертывания E^5 составляет [3]

$$L(x_i) = L(x_j) = L(x_k) = L(x_s) =$$

$$= L(x_v) = 2^{n-1} = 16,$$

где $n = 5$ мерность куба E^5.

Для кубов ЕКФ E^2, E^3, E^4 число логических связей будет соответственно 2, 4, 8.

Логические связи определяют участие каждой переменной развертывания куба соответ-

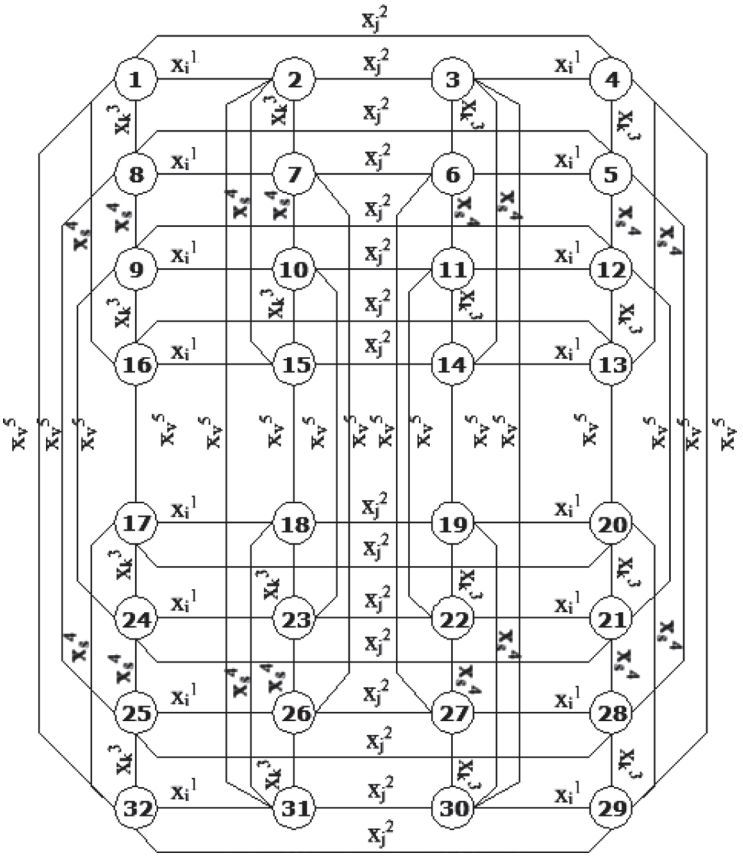


Рис. 1. Совершенная матричная расстановка куба E^5.

ствующей мерности при организации этого куба $L(x)$ раз.

Согласно [5] порядковые номера переменных E_1^3 1-го уровня развертывания порождающей последовательности (1) будет 1, 3, 5, 7 для куба E_1^3 СМР куба E^5. Соответственно для кубов E_2^3, E_3^3 и E_4^3 порядковые номера переменных будут 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31. Порядковые номера переменных развертывания совпадают с номерами вершин, участвующих в преобразовании по этим переменным. Таким образом, пары вершин, участвующие в преобразовании по переменной E_1^1 1-го уровня развертывания для куба E^5 ЕКФ будут следующими:

1–2, 3–4, 5–6, 7–8, 9–10, 11–12, 13–14,
15–16, 17–18, 19–20, 21–22, 23–24, (2)
25–26, 27–28, 29–30, 31–32;

При развертывании куба E_1^1 (вершины 1–2) и куба E_2^1 (вершины 3–4) в куб x_j^2 по переменной 2-го уровня x_j^2 все последовательно объединенные вершины $1-2-3-4$ должны быть геометрическими соседями и отличаться друг от друга на 1 двоичную единицу, в том числе и вершины 1–4. Поэтому пары вершин, участвующие в преобразовании по переменной 2-го уровня развертывания для куба E^5 ЕКФ x_j^2 будут следующими:

1–4, 2–3, 5–8, 6–7, 9–12, 10–11, 13–16,
14–15, 17–20, 18–19, 21–24, 22–23, (3)
25–28, 26–27, 29–32, 30–31;

Аналогично находим пары вершин, участвующие в преобразовании по переменной 3-го уровня развертывания для куба E^5 ЕКФ x_k^3:

1–8, 2–7, 3–6, 4–5, 9–16, 10–15, 11–14,
12–13, 17–24, 18–23, 19–22, 20–21, (4)
25–32, 26–31, 27–30, 28–29;

Пары вершин, которые участвуют в преобразовании по переменной 4-го уровня развертывания для куба E^5 ЕКФ x_s^4 будут такими:

1–16, 8–9, 2–15, 7–10, 3–14, 6–11, 4–13,
5–12, 17–32, 24–25, 18–31, 23–26, (5)
19–30, 22–27, 20–29, 21–28;

Пары вершин, преобразуемые по переменной x_v^5 куба E^5 составим таким образом:

1–32, 8–25, 9–24, 16–17, 2–31, 7–26,
10–23, 15–18, 3–30, 6–27, 11–22, (6)
14–19, 4–29, 5–28, 12–21, 13–20;

Принимаемый из канала преобразования куб E^n мерности n = 2, 3, 4, 5, …, т. е. куб E^2, E^3, E^4, E^5, …, записывается в матрицу СМР декодирования (рис. 1). Для куба E_3^2 входом в матрицу является вершина 4, для куба E_5^2 – вершина 8, для куба E^4 – вершина 16, для куба E^5 – вершина 32.

В пределах записанного куба E^n определяются пары вершин, преобразуемых по переменной развертывания 1-го уровня x_i^1, по переменной 2-го уровня и т. д., то есть определяются все пары вершин, преобразуемые по переменным развертывания, определяющими записанный куб заданной мерности. Так, например, для куба E^2 по переменной развертывания x_j^2 будут преобразованы вершины 1–2, 3–4 (2), а по переменной развертывания x_j^2 (второй уровень развертывания куба E^2) будут преобразованы вершины 1–4, 2–3 (3). Для куба E^2 пары вершин по переменным x_k^3, x_s^4, x_v^5, отсутствуют.

Истинное значение переменных развертывания x_i^1, x_j^2 может быть определено путем суммирования указанных пар вершин 1–2, 3–4 и 1–4, 2–3 по mod 2. Полное восстановление всех вершин 1, 2, 3, 4 при определенных переменных x_i^1, x_j^2 возможно, если хотя бы одна из вершин принята без ошибок. В общем случае, при искажении в грани (куб E^2) не более одной вершины, все вершины грани полностью восстанавливаются, поскольку все переменные развертывания могут быть найдены однозначно.

При декодировании куб E^2 ЕКФ определяется как минимальный интервал декодирования (МИД), для которого принципиальным является понятие надежной вершины.

Надежная вершина E_k^0 позволяет определить в пределах принятых кубов в ЕКФ, конкретные переменные развертывания, по которым восстанавливаются все вершины, кодовой комбинации кода СЛК. Восстановление вершин куба ЕКФ осуществляется согласно порождающей последовательности (1). Надежной является та вершина E_k^0, для которой справедливо соотношение

$$E_k^0 \oplus E_{k+1}^0 = E_k^0 \oplus E_{k-1}^0 = 1 \qquad (7)$$

Во всех других случаях, вершина E_k^0 считается вероятно ненадежной:

$$\begin{cases} E_k^0 \oplus E_{k+1}^0 = 1 \\ E_k^0 \oplus E_{k-1}^0 \neq 1 \end{cases} \qquad (8)$$

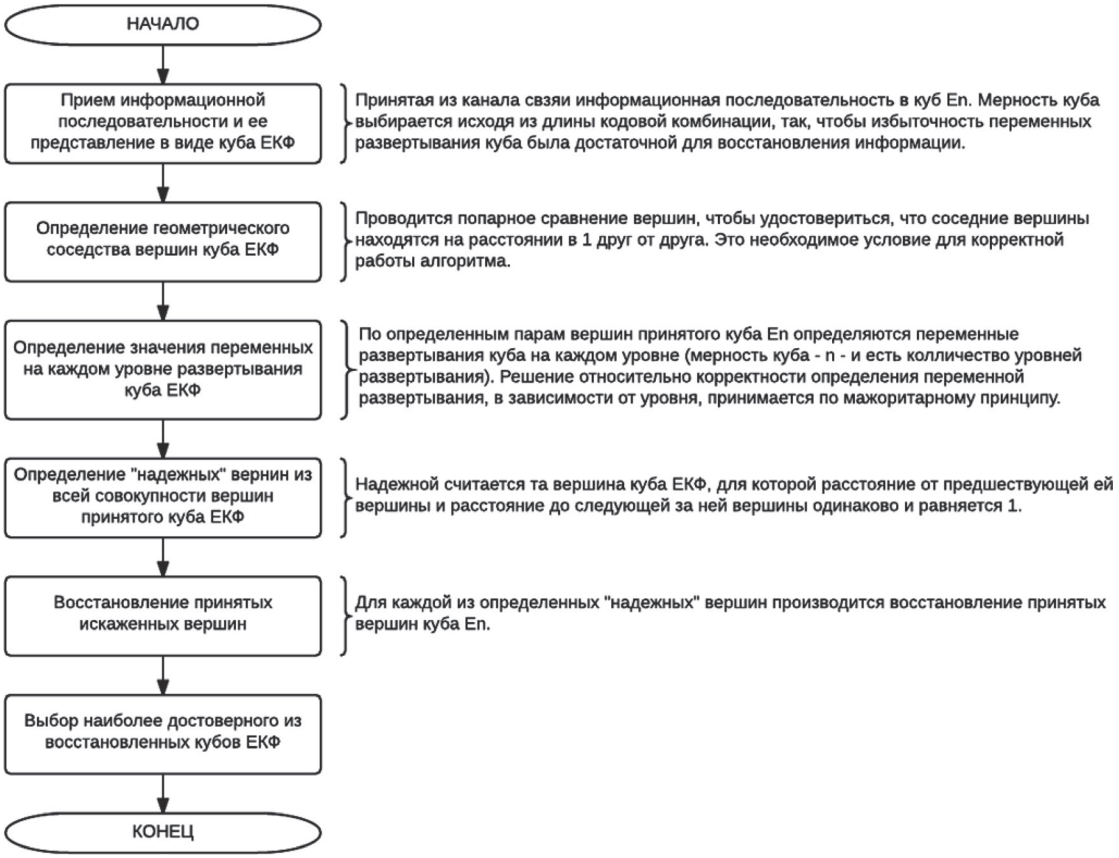


Рис. 2. Блок-схема обобщенного алгоритма декодирования кода СЛК

и

$$\begin{cases} E_k^0 \oplus E_{k+1}^0 \neq 1 \\ E_k^0 \oplus E_{k-1}^0 = 1 \end{cases} \quad (9)$$

Для каждой последовательной пары принимаемых вершин E_k^0, E_{k+1}^0 определяется переменная $x_{(0,1,\ldots,n-1)}$ геометрического соседства этих вершин. При наличии ошибок в вершинах E_{k*}^0 или $E_{(k+1)*}^0$ разница может быть определена по нескольким переменным.

Если разница между вершинами определена только по одной переменной x_i, то формально эти вершины определены без ошибок

$$E_k^0 \underset{\ldots}{\overset{x_i}{}} E_{k+1}^0 \quad (11)$$

Далее приводится этапы алгоритма декодирования СЛК.

Принятая из канала связи кодовая комбинация записывается в приемную матрицу куба E^n. Элементы этой матрицы есть вершины куба E^n и представляют собой n-разрядное двоичное число, где n-мерность куба. Т. е. на входе мы принимаем непрерывную двоичную кодовую комбинацию и разбиваем ее на n-разрядные последовательности.

Проводится последовательное попарное сравнение вершин куба E^n, для определения их геометрического соседства – необходимое условие корректной работы алгоритма.

Из всего множества вершин куба E^n необходимо определить «надежные» вершины, по которым проводиться восстановление искаженных вершин. Вершина считается надежной, если предыдущая и последующая вершины являются ее геометрическими соседями.

По парам вершин куба E^n определяются переменные на каждом n уровне. Если переменных несколько, выбор одной принимается по принципу большинства.

Далее производится восстановление искаженных вершин куба E^n по каждой из определенных надежных вершин, получая разные вариации куба E^n. Из восстановленных кубов выбирается наиболее достоверный.

Блок-схема обобщенного алгоритма кодов СЛК представлена на рис. 2.

Выводы

В работе разработаны и обоснованы основные положения обобщенного алгоритма

декодирования кодовых комбинаций СЛК, кубов ЕКФ E^n, обеспечивающего максимально полную реализацию корректирующих свойств кода СЛК при использовании всех логических связей переменных развертывания куба E^n.

Приведенный алгоритм декодирования искаженной канальной последовательности вершин куба ЕКФ достаточно просто может быть реализован программно.

Разработанный обобщенный алгоритм декодирования кодов СЛК обеспечивает надежную работу декодера как в канале с независимыми, так и пакетированными ошибками, за счет обобщенного подхода при проведении процедуры декодирования.

Литература

1. **Ленков, С. В.** Метод представления дискретной информации на основе инфимумных дизъюнктивних нормальных форм булевых функций / С. В. Лєнков, К. Ф. Боряк, Ю. Д. Иванов, О. С. Селюков. – Сборник научных работ Военного Института Киевского национального университета им. Т. Шевченка, 2008 – С. 90–97.

2. **Иванов Ю. Д.** Метод синтеза инфимумных дизъюнктивных нормальных форм логических функций / Ю. Д. Иванов. – Труды Одесского Политехнического университета, 2006 – С. 178–183.

3. **Иванов Ю. Д.** Метод структурно-логического кодирования инфимумных дизъюнктивних нормальных форм булевых функций в базисе куба E^n / Ю. Д. Иванов, И. В. Пампуха, О. С. Захарова, Г. Б. Жиров. – Сборник научных работ Военного института Киевского национального университета им. Т. Шевченка, 2008 – С. 46–49.

4. **Иванов Ю. Д.** Метод построения совершенной матричной расстановки как основы синтеза дизъюнктивних нормальных форм булевых функций / Ю. Д. Иванов. – Сборник научных работ Военного института Киевского национального университета им. Т. Шевченка, 2008. – С. 58–62.

5. **Иванов Ю. Д.** Основные положения декодирования структурно-логических кодов / Ю. Д. Іванов, І. В. Пампуха, О. С. Захарова, В. В. Якимов. – Сборник научных работ Военного института Киевского национального университета им. Т. Шевченка, 2007 – С. 110–116.

6. **Иванов Ю. Д.** Обобщенный метод структурно-логического декодирования инфимумных форм подачи булевых функций / Ю. Д. Иванов, И. В. Пампуха, В. О. Осипа, М. М. Охрамович. – Сборник научных работ Военного института Киевского национального университета им. Т. Шевченка, 2006 – С. 48–53.

References

1. **Lenkov, S. V.** Submission method of discrete information based on the infimum disjunctive normal forms of boolean functions / S. V. Lenkov, K. F. Borjak, Ju. D. Ivanov, O. S. Seljukov. – Sbornik nauchnyh rabot Voennogo Instituta Kievskogo nacional'nogo universiteta im. T. Shevchenka, 2008 – P. 90–97.

2. **Ivanov Ju. D.** The synthesis method of infimum disjunctive normal forms of logic functions / Ju. D. Ivanov. – Trudy Odesskogo Politehnicheskogo universiteta, 2006 – P. 178–183.

3. **Ivanov Ju. D.** Structural logic coding method of infimum disjunctive normal forms of boolean functions in the basis of the cube E^n / Ju. D. Ivanov, I. V. Pampuha, O. S. Zaharova, G. B. Zhirov. – Sbornik nauchnyh rabot Voennogo instituta Kievskogo nacional'nogo universiteta im. T. Shevchenka, 2008 – P. 46–49.

4. **Ivanov Ju. D.** The method of constructing the perfect matrix arrangement as the basis for the synthesis of disjunctive normal forms of Boolean functions / Ju. D. Ivanov.- Sbornik nauchnyh rabot Voennogo instituta Kievskogo nacional'nogo universiteta im. T. Shevchenka, 2008. – P. 58–62.

5. **Ivanov Ju. D.** The main provisions of the structural and decoding logic code/ Ju. D. Ivanov, I. V. Pampuha, O. S. Zaharova, V. V. Jakimov. – Sbornik nauchnyh rabot Voennogo instituta Kievskogo nacional'nogo universiteta im. T. Shevchenka, 2007 – P. 110–116.

6. **Ivanov Ju. D.** The generalized method of structural and logical decoding infimum forms submission of boolean functions / Ju. D. Ivanov, I. V. Pampuha, V. O. Osipa, M. M. Ohramovich. – Sbornik nauchnyh rabot Voennogo instituta Kievskogo nacional'nogo universiteta im. T. Shevchenka, 2006 – P. 48–53.

Поступила	*После доработки*	*Принята к печати*
15.04.2016	30.04.2016	10.05.2016

Y. Ivanov, I. Nikolov, B. Lozka

DECODING OF STRUCTURALLY AND LOGICAL CODES

The article deals with the description of the main points of the structural and logical coding and the features of SLC codes. There are shown the basic points of the generalized algorithm of decoding SLC, which is based on the method of perfect matrix arrangement (PMA) of the n-dimensional cube vertices for adequate representation and transformation of boolean functions, which is based on the method of generating sequences of variables for building the maximum coverage of the cube vertices. The structural and logical codes (SLC) use natural logic redundancy of the infimum disjunctive normal forms (IDNF) of boolean functions, which make the basis for building the SLC codes and correcting the errors, that occur during data trans-

fer in real discrete channels, on the channels with independent errors. The main task is to define the basic relations between the implemented SLC codes of the logical redundancy and boundary values of multiplicity of independent errors which are corrected. The principal difference between the SLC codes and the well-known correcting codes is that the redundancy, that is needed to correct the errors in converting the discrete information, is not introduced into an additional code sequence but is defined in a natural way, during the construction of codewords of SLC.

Keywords: *structural and logical codes, infimum disjunctive normal form, boolean functions, generalized method of decoding, perfect matrix arrangement, a common encoding format.*

Иванов Юрий Дмитриевич окончил Киевский институт инженеров гражданской авиации в 1965 году по специальности радиоинженер. Кандидат технических наук по специальности «Компьютерные системы».

Преподаватель Института информационной безопасности, радиоэлектроники и телекоммуникаций Одесского национального политехнического университета, доцент кафедры информационных технологий проектирования в электронике и телекоммуникациях.

Научные интересы включают в себя вопросы помехоустойчивого кодирования нетрадиционной логики, цифровая фильтрация, каналы преобразования дискретных данных теория алгоритмов.

Николов Илья Николаевич родился в 1993 году. Получил степень магистра в 2016 году в Одесском национальном политехническом университете, Украина.

Научные интересы: технологиями веб-проектирования, алгоритмы повышения помехоустойчивости и надежности систем передачи информации, каналы преобразования дискретных данных.

Работает разработчиком программного обеспечения.

Лозка Богдан Владимирович родился в 1992 году. Получил степень специалиста (с отличием) по специальности «Информационные технологии проектирования» в 2014 году в Одесском национальном политехническом университете, Украина.

С 2015 года является аспирантом по специальности «Компьютерные системы и компоненты», работает программистом.

Научные интересы включают в себя методы имитационного моделирования информационных систем, теория алгоритмов, дискретная обработка информационных данных.

E-mail: massabo34@gmail. com

УДК 65.011.56: 62-82

А. В. ПУЗАНОВ

ИСПОЛЬЗОВАНИЕ AUTODESK SIMULATION MULTIPHYSICS ДЛЯ ИССЛЕДОВАНИЯ ПОЛЕЙ ТЕМПЕРАТУР, НАПРЯЖЕНИЙ И ДЕФОРМАЦИЙ В КОНСТРУКЦИИ ШЕСТЕРЕННОГО НАСОСА

ОАО «Специальное конструкторское бюро приборостроения и автоматики»

Шестеренные насосы наиболее распространенный тип гидромашин. Они используются в различных отраслях: в нефтегазовой и перерабатывающей промышленности, в станкостроении, в мобильной военной, дорожно-строительной и сельскохозяйственной технике. Необходимость обеспечения работоспособности гидромашин для мобильной техники в широком климатическом диапазоне требует повышения точности методик расчета при проектировании их элементов. В статье приведены результаты моделирования полей температур и вызванных ими напряжений и деформаций. Полученные результаты позволили обосновать конструктивные и технологические решения, обеспечивающие повышение работоспособности гидромашин при критических значениях температур окружающей среды.

Ключевые слова: *гидромашины, шестеренные насосы, моделирование, поля температур.*

Введение

Среди устройств генерации гидравлической энергии насосы и гидромоторы шестеренного типа занимают лидирующие позиции, что обусловлено простотой, высокой надежностью и ремонтопригодностью их конструкции. Однако данный тип гидромашин имеет и ряд известных проблем: резкое снижение надежности работы при эксплуатации на морозе; заклинивание при высоких температурах [1, 2].

Принимая во внимание, что обычно данный тип насосов используется в мобильной технике в различных климатических зонах, в том числе для прогрева гидросистемы до температуры штатной работы гидрооборудования, обеспечивающей оптимальное значение вязкости рабочей жидкости, анализ воздействия перепада температур на работоспособность гидромашин шестеренного типа при их проектировании, становится актуальной научно-технической задачей.

Наиболее популярным решением обозначенных проблем является увеличение зазоров между сопряженными деталями. Однако, это решение приводит к увеличению перетечек рабочей жидкости из напорной во всасывающую магистраль, а, следовательно, к снижению гидравлического КПД [3]. Таким образом, для обеспечения заданной в техническом задании (ТЗ) мощности гидромашины необходимо увеличение либо скорости вращения приводного вала, либо габаритов качающего узла. Кроме того, наличие перетечек рабочей жидкости ограничивает максимальное давление, достижимое насосом (или крутящего момента – для мотора). Поскольку обычно механический привод вращения осуществляется непосредственно от двигателя внутреннего сгорания, а относительная скорость вращения ограничена материалом пар трения, то решение проблемы форсирования мощности сводится к увеличению габаритов гидромашины.

С уменьшением зазоров возрастает вероятность заклинивания подвижных частей при повышении температуры вследствие линейного расширения используемых разнородных материалов [4], а также из-за снижения вязкости и несущей способности рабочей жидкости (силы реакции гидростатического подшипника).

Поиск оптимальных значений зазоров, внесение и расположение специальных конструктивных элементов для снятия температурных деформаций возможно либо проведением натурной доработки, либо посредством использования средств компьютерного моделирования. Для решения обозначенных выше про-

блем необходим анализ полей скоростей и давления рабочей жидкости, тепловых деформаций деталей, их кинематики и контактной прочности. Решение этих задач в связанной постановке возможно посредством использования современного программного обеспечения для проведения мультидисциплинарного (мультифизичного) анализа. На сегодняшний день на рынке программного обеспечения представлены несколько комплексов, имеющих различные области применения, спектр решаемых задач и ценовой диапазон [5–7]:

• ANSYS – универсальный программный комплекс конечно-элементного (КЭ) анализа линейных и нелинейных, стационарных и нестационарных пространственных задач механики деформируемого твердого тела и механики конструкций, задач механики жидкости и газа, теплопередачи и теплообмена, электродинамики, акустики, многодисциплинарного связанного анализа и оптимизации на основе всех выше приведенных типов анализа.

• DS. Simulia (ABAQUS) – программный комплекс для прочностного конечно-элементного анализа сложных линейных и нелинейных инженерных задач.

• ADINA – программный комплекс для междисциплинарного анализа конструкций и гидродинамики (линейный и высоконелинейный анализ конструкций; тепловой анализ; гидродинамика; взаимодействие потоков с конструкциями).

• MSC.MARC – мировой стандарт КЭ-систем для нелинейного конечно-элементного анализа больших реальных задач. Программный комплекс многодисциплинарного анализа: статический и динамический анализ, механика разрушений, автоматический контакт, комплексный тепловой и теплопрочностной анализ и связанные задачи жидкости и конструкции.

• Autodesk Simulation Multiphysics (Algor) – основная разработка Autodesk в области анализа цифрового прототипа изделия. Поддерживает прямой импорт геометрии и ассоциативный обмен данными из Autodesk Inventor. Включает типы расчетов: статические напряжения и линейная динамика; статическая и динамическая прочность; комбинированный прочностной и кинематический анализ; моделирование динамики многомассовых систем с поддержкой крупномасштабного движения и больших деформаций с учетом их контактного взаимодействия; электростатика; вычислительная гидродинамика; теплоперенос и теплопередача, моделирование комплексных физических процессов.

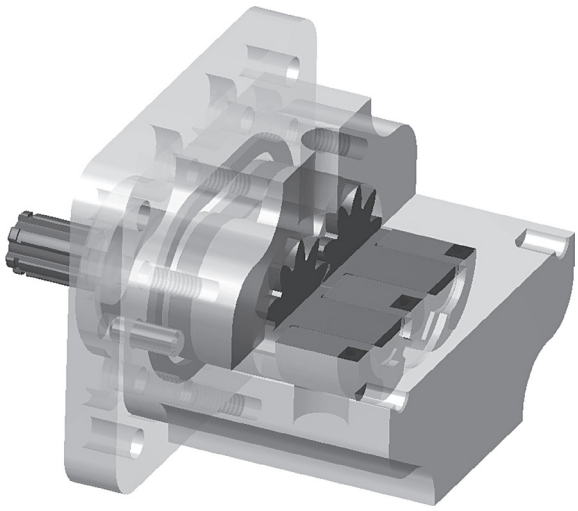


Рис. 1. Модель гидромашины шестеренного типа

Принимая во внимание факт базового средства разработки геометрии модели в конструкторских подразделениях – Autodesk Inventor, для анализа устойчивости конструкций шестеренных насосов (НШ) к воздействию температуры (согласно требованиям ГОСТ 30630.2.1-2013) нами был использован Autodesk Simulation Multiphysics, который с 2015 года поставляется в виде двух отдельных программных комплексов: Autodesk Simulation Mechanical и Autodesk Simulation CFD.

Для исследования воздействия изменения температуры на функциональность гидромашины, гидродинамики потока жидкости и деформации механических элементов, образующих ее проточную часть, нами разработана комплексная модель функционирования НШ, учитывающая взаимовлияние силовых факторов различной физической природы.

Геометрическая модель шестеренного насоса (рис. 1) разработана в программном комплексе Autodesk Inventor и представляет собой параметрическую 3D-модель гидромашины, выполненной из типовых конструкторско-технологических элементов, обеспечивающих технологичность их изготовления [8].

На первом этапе проводим гидродинамический анализ и анализ тепломассообмена потока рабочей жидкости внутри насоса в программном комплексе Autodesk Simulation CFD.

Для заполнения внутреннего объема насоса жидкостью необходимо выполнить ее геометрическое описание. Для генерации этого объема существуют 3 варианта: 1) посредством выполнения процедуры «производный компонент» непосредственно в Autodesk Inventor; 2) посредством соответствующих функций в Autodesk Simulation CFD (используя три метода – по удобству и предпочтениям пользователя); 3) посредством функции VoidFill в Autodesk Inventor Fusion (входит в состав Autodesk Simulation).

Для обеспечения принципа ассоциативности нами был реализован иной способ: создана ассоциативная 3D-копия корпусных деталей (совпадающая с внешним контуром насоса). При трансляции всей сборки в Autodesk Simulation CFD, программа сама дробит эту геометрию на внутренние замкнутые объемы. Нам остается определить для них свойства рабочей жидкости. Таким образом, при внесении изменений в конструктивное исполнение деталей, внутренний объем жидкости перестраивается автоматически.

Для исследуемой модели приняты следующие допущения: установившаяся температура внешней среды, отсутствие ее изменения при контакте деталей, однородность рабочей жидкости.

В качестве рабочей жидкости использовалось масло по стандарту SAE: VG68 (20W). Свойства жидкости зависят от температуры и давления. Модель течения – турбулентный поток (хотя поток перетечек ламинарный, а функции турбулентности необходимы для оценки диссипации потока).

Модель анализировалась в двух вариантах:

1. зафиксированы все подвижные детали (имитация заторможенного гидромотора);

2. подвижные детали приводятся в движение согласно кинематической схемы работы гидромашины в режиме насоса.

Для первого варианта исследуются гидромеханические и температурные воздействия рабочей жидкости на механические элементы гидромашины, проводится анализ перетечек и определение объемного КПД гидромашины. Для второго варианта изучается пульсация подачи и давления насоса для снижения волновых процессов в гидроприводе.

В данной работе отражены результаты исследований первого варианта, поскольку влияние пульсации давления при изменении температуры внешней среды незначительно, а при заклинивании механизма исследование пульсаций бессмысленно.

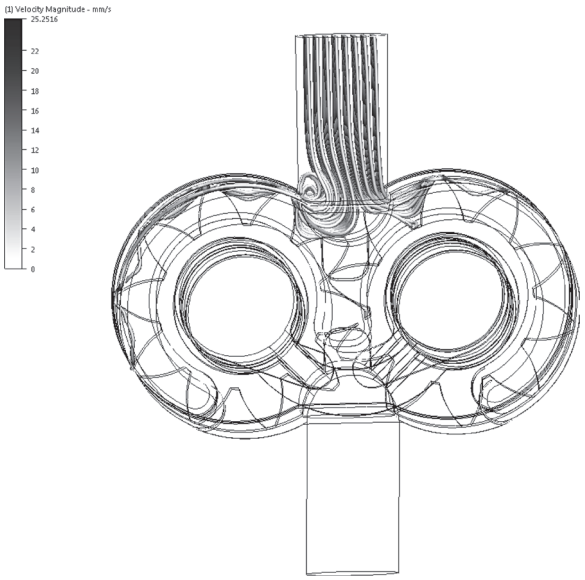


Рис. 2. Линии тока перетечек рабочей жидкости

Линии тока перетечек рабочей жидкости при T = +60 °C представлены на рис. 2. Используя полученные на этом этапе результаты, проводим работы по повышению объемного КПД при изменении температуры посредством локализации и минимизации перетечек рабочей жидкости внутри корпуса шестеренного насоса.

Из рисунка видно, что основной расход перетечек происходит по радиальным зазорам между ведущей и ведомой шестернями. Объемный расход утечек при T = +60 °C составил q = 444 мм^3/с, при T = –50 °C составил q = 103 мм^3/с,

При снижении перетечек за счет уменьшении зазоров необходимо принимать во внимание, что в процессе эвольвентного зубчатого зацепления происходит изменение объема, ограниченного сопряженными зубьями. При нулевых зазорах наблюдается заклинивание передачи, вызванное превышением предела сжатия замкнутой жидкости.

Работа НШ при отрицательных температурах ограничена мощностью, увеличившейся из-за повышения вязкости жидкости [2]. Допустимая вязкость обычно определяется всасывающей способностью или «прокачиваемостью» гидромашины. При снижении температуры происходит защемление опор валов в подшипниках, что увеличивает трение и снижает меха-

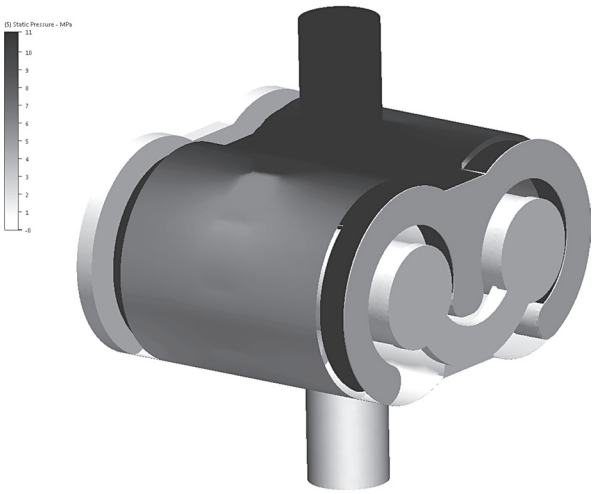


Рис. 3. Поле распределения давления рабочей жидкости по внутреннему объему насоса

нический КПД. При повышении температуры происходит заклинивание торцевых поверхностей ведущей и ведомой шестерен, что приводит к снижению механического КПД, но увеличение радиального зазора в подшипниках и в рабочей зоне насоса приводит к росту перетечек жидкости и снижает гидравлический КПД.

На рис. 3 представлено поле давления рабочей жидкости – результат моделирования гидромеханического воздействия рабочей жидкости на механические элементы гидромашины (для наглядности все твердотельные элементы скрыты).

Определение значений деформации и контактных напряжений при изменении температуры исследуем посредством Autodesk Simulation Mechanical. В качестве исходных данных использовалась та же геометрия гидромашины, а также результаты предыдущего анализа: поле распределения давления и температуры рабочей жидкости по поверхностям деталей механической системы (рис. 4).

При разбиении на конечные элементы в данных программных продуктах точное совпадение (положение и размер) КЭ необязательно.

Стоит отметить, что существует возможность импорта результатов CFD анализа в программные продукты сторонних разработчиков (Abaqus, Ansys, Cosmos, Nastran, FeMap, I-DEAS), но необходимо соблюдать совпадение конечно-элементной сети, что не всегда возможно.

Результаты моделирования напряженно-деформированного состояния ходовой части гидромашины анализируем с точки зрения обе-

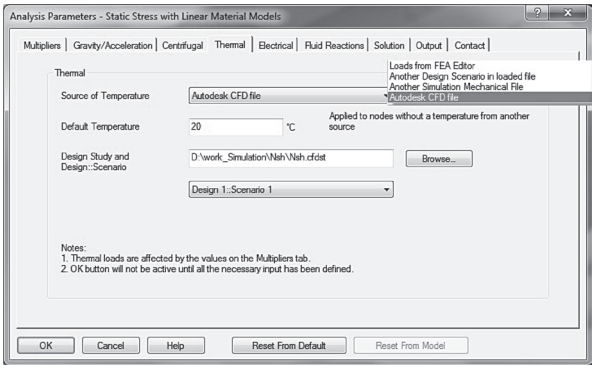


Рис. 4. Настройка использования в качестве нагрузки для анализа напряженно-деформированного состояния изделия результатов CFD анализа

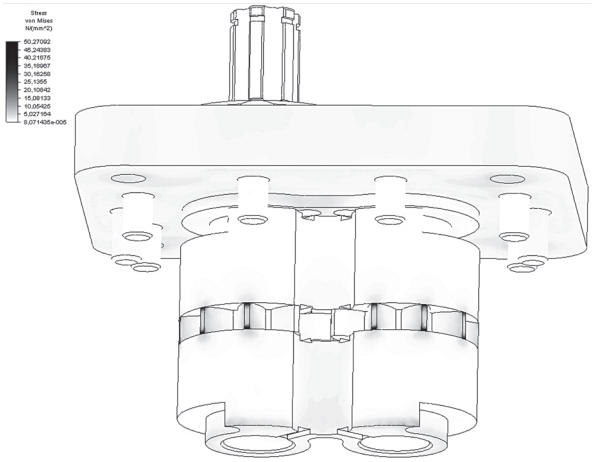


Рис. 5. Напряжения в конструкции шестеренного насоса при температуре +60 °С

спечения коэффициента запаса по критерию прочности каждого элемента конструкции гидромашины в пределах от 2 до 2,5. Для этого используются результаты, подобные представленным на рис. 5. Обеспечение коэффициентов запаса по критерию прочности в указанном диапазоне реализуется конструктором посредством подбора материалов с соответствующими свойствами или изменением геометрии деталей.

В результате анализа полученных результатов были локализованы места контактных напряжений в зоне сопряжения наружного диаметра шестерен с торцевой поверхностью подшипникового узла (которые составили 145 МПа при +60 °С и 276 МПа при –50 °С). В процессе конструктивной доработки контактные напряжения удалось снизить до уровня допустимых значений (соответственно 50 МПа при +60 °С и 89 МПа при –50 °С) – подбором материалов с близкими значениями коэффициентов линейного расширения, а также за счет увеличения

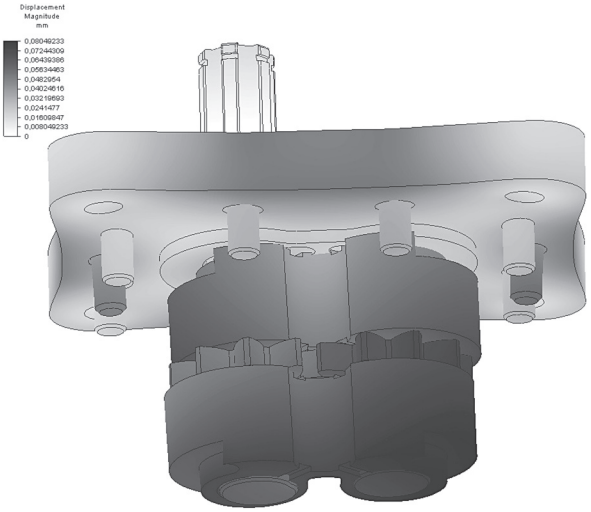


Рис. 6. Деформация насосного агрегата при температуре –50 °С

зазоров между сопряженными элементами подшипниковых узлов, принимая во внимание ограничение по перетечкам рабочей жидкости внутри корпуса насоса (определяемым по технологии, описанной выше).

Для снижения перетечек рабочей жидкости проектировщику необходимо обеспечить жесткость геометрии деталей, поскольку при изменении эквидистантности их сопряженных поверхностей будет нарушена сила гидромеханического взаимодействия в зазорах, что приведет к продавливанию пограничного слоя жидкости, переходу с режима вязкого трения на сухое, локальному контакту и росту температуры и, как следствие, к лавинообразному развитию износа [9].

Полученные в результате исследования модели результаты деформированного состояния конструкции шестеренной гидромашины (рис. 6), подверженной воздействию высоких и низких температур, позволили проектировщику внести ряд изменений: добавить ребра жесткости и термокомпенсирующие отверстия и пазы, подобрать толщину корпусных и подшипниковых элементов для снижения негативного влияния этих деформаций.

Заключение

В результате использования мультидисциплинарного программного обеспечения нами разработана комплексная модель гидро-термоупругости гидромашины шестеренного типа. Модель позволяет проводить исследования термо- и гидромеханических процессов и их влияния на эксплуатационные характеристики гидромашин и гидроприводов; проводить моделирование стойкости гидромашин к механическим и климатическим воздействиям; проводить анализ возможных вариантов конструктивных доработок.

Анализ температурных деформаций позволил внести ряд конструкторских доработок, реализация которых предопределила снижение контактных напряжений и повышение жесткости конструкции гидромашины шестеренного типа. Результаты исследований позволили получить обоснование конструктивных решений, назначить допуска на изготовление, а также сократить технологическое время приработки, выработку рекомендаций по использованию шестеренных гидромашин для обеспечения комфортных условий ее работы при изменении температуры окружающей среды.

Анализ контактных напряжений при различных значениях температуры и рабочего давления гидромашины позволил нам выработать регламент работы насосного агрегата при граничных значениях температуры, а также предложить алгоритм нагружения насоса при запуске на морозе для снижения контактного износа и увеличения ресурса.

Литература

1. **Башта, Т. М.** Гидравлика, гидравлические машины и гидравлические приводы. 2-е изд. перер. (Учебник для машиностроительных ВУЗов). / Т. М. Башта, С. М. Руднев, Б. Б. Некрасов – М. Машиностроение. 1982. 423 с.

2. **Юдин, Е. М.** Шестеренные насосы. Основные параметры и их расчет. – М.: Машиностроение. 1964. 237 с.

3. **Уплотнения** и уплотнительная техника. Справочник. Под общ. ред. А. И. Голубевой и Л. А. Кондакова. – М.: Машиностроение. 1986. 464 с.

4. **Исаченко, В. П.** Теплопередача: учебник для вузов / В. П. Исаченко, В. А. Осипова, А. С. Сукомел. – М.: Энергоиздат, 1981. – 416 с.

5. **Компьютерный** инжиниринг: учеб. пособие / А. И. Боровков [и др.]. – СПб.: Изд-во Политехн. ун-та, 2012. – 93 с.

6. **Современные** программные средства конечно-элементного анализа [Электронный ресурс]. – Режим доступа: http://www.stroitmeh.ru/lect79.htm, свободный.

7. **Пузанов, А. В.** Инженерный анализ в Autodesk Simulation Multiphysics. – М: ДМК Пресс, 2013. 912с.

8. **Пузанов, А. В.** Принцип постпроизводственного проектирования гидроприводов /А. В. Пузанов // Системный анализ и прикладная информатика – 2015 № 3. С. 36-41.

9. **Пузанов, А. В.** Моделирование контактных взаимодействий деталей ходовой части аксиально-поршневых гидромашин средствами MSC. AFEA (часть I) /А. В. Пузанов // CAD/CAM/CAE Observer. – 2008. № 5. – С. 85–87.

References

1. **Bashta, T. M.** Gidravlika, gidravlicheskie mashiny i gidravlicheskie privody. 2-e izd. perer. (Uchebnik dlja mashinostroitel'nyh VUZov). / T. M. Bashta, S. M. Rudnev, B. B. Nekrasov M. Mashinostroenie. 1982. 423 s.

2. **Judin, E. M.** Shesterennye nasosy. Osnovnye parametry i ih raschet. – M.: Mashinostroenie. 1964. 237 s.

3. **Uplotnenija** i uplotnitel'naja tehnika. Spravochnik. Pod obshh. red. A. I. Golubevoj i L. A. Kondakova. – M.: Mashinostroenie. 1986. 464 s.

4. **Isachenko, V. P.** Teploperedacha: uchebnik dlja vuzov / V. P. Isachenko, V. A. Osipova, A. S. Sukomel. – M.: Jenergoizdat, 1981. – 416 s.

5. **Komp'juternyj** inzhiniring: ucheb. posobie / A. I. Borovkov [i dr.]. SPb.: Izd-vo Politehn. un-ta, 2012. 93 s.

6. **Sovremennye** programmnye sredstva konechno-jelementnogo analiza [Jelektronnyj resurs]. – Rezhim dostupa: http://www.stroitmeh.ru/lect79.htm, svobodnyj.

7. **Puzanov, A. V.** Inzhenernyj analiz v Autodesk Simulation Multiphysics. – M: DMK Press, 2013. 912s.

8. **Puzanov, A. V.** Princip postproizvodstvennogo proektirovanija gidroprivodov /A. V. Puzanov // Sistemnyj analiz i prikladnaja informatika – 2015 № 3. S. 36 41.

9. **Puzanov, A. V.** Modelirovanie kontaktnykh vzaimodeistvii detalei hodovoi chasti aksialno-porshnevykh gidromashin sredstvami MSC. AFEA (part I) /A. V. Puzanov // CAD/CAM/CAE Observer. – 2008. № 5. – S. 85–87.

Поступила	*После доработки*	*Принята к печати*
25.03.2016	15.04.2016	10.05.2016

PUZANOV A. V.

USE OF AUTODESK SIMULATION MULTIPHYSICS FOR RESEARCH OF TEMPERATURE FIELDS, STRESS AND DEFOMATION IN THE CONSTRUCTION OF GEAR PUMP

JSC «Special Design Bureau of Instrument Making and Automation»

Gear pumps are the most common type of hydraulic machines. They are used in various industries: oil and gas processing industry, in machine tools, mobile military, road-building and agricultural machinery. The need to ensure efficiency of hydraulic mobile applications in a wide climatic range requires increasing the accuracy of the calculation methods for the design of their elements. The results of temperature field modeling and caused them stress and strain. The results obtained allowed to justify the design and technological solutions, providing an increase of hydraulic performance at critical ambient temperatures.

Keywords: *temperature field modeling, stress and strain, hydraulic performance.*

Автор

Пузанов Андрей Викторович, к. т. н., помощник Генерального директора по науке
ОАО «Специальное конструкторское бюро приборостроения и автоматики».
601919, Россия, Владимирская обл., г. Ковров, ул. Крупской, 55.
Телефон рабочий: (49232) 9-37-84
E-mail: avp@oao-skbpa.ru

УДК 681.327.12.001.362

М. М. ЛУКАШЕВИЧ, [1] *В. В. СТАРОВОЙТОВ.*[2]

МЕТОДИКА ПОДСЧЕТА ЧИСЛА ЯДЕР КЛЕТОК НА МЕДИЦИНСКИХ ГИСТОЛОГИЧЕСКИХ ИЗОБРАЖЕНИЯХ

[1]*Белорусский государственный университет информатики и радиоэлектроники*
[2]*Объединенный институт проблем информатики Национальной академии наук Беларуси*

В статье исследуется методика автоматического подсчета числа ядер клеток на гистологических изображениях. Эта операция широко применяется при диагностике различных заболеваний и морфологическом анализе клеток. В связи с этим, процедура автоматического подсчета числа ядер клеток является ключевым этапом в системах микроскопического анализа медицинских изображений гистологических препаратов. Основной целью работы была разработка эффективной схемы автоматического подсчета ядер клеток на основе современных методов обработки изображений: направленной фильтрации, адаптивной бинаризации изображений и математической морфологии. В отличие от известных исследований, представленный подход не предусматривает сегментацию ядер клеток на изображении, а лишь предполагает их обнаружение и подсчет их количества. Это позволяет избежать сложных алгоритмических вычислений и обеспечивает хорошую точность подсчета ядер клеток.

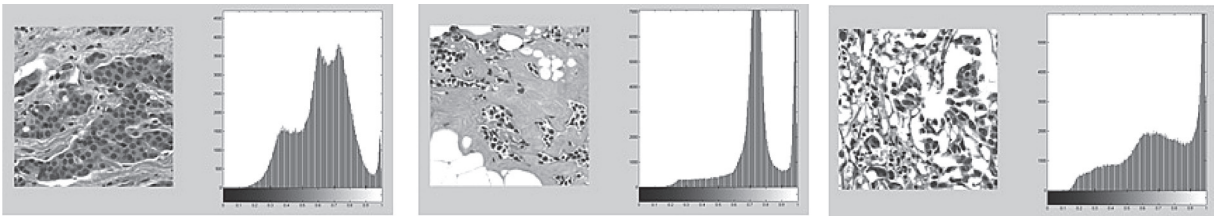
В работе описан ряд экспериментов, выполненных для оценки эффективности предложенной методики с использованием доступной в интернете тестовый базы медицинских гистологических изображений. Определены критичные параметры алгоритмов, настраиваемые на каждом этапе анализа изображений. Для каждого параметра определен интервал тестируемых значений, а затем реализована процедура выбора не только оптимальных значений каждого параметра, но их из взаимная комбинация, на основе общепринятых количественных оценок точности (Precision) и полноты (Recall). Полученные результаты сравнивались с последними достижениями в данной области и показали приемлемый уровень точности предложенной методики. Прототип программного обеспечения, разработанного в рамках проведенного исследования, можно рассматривать как автоматический инструмент для анализа ядер клеток. Разработанный подход может быть адаптирован к различным задачам анализа ядер клеток различных органов.

Ключевые слова: *изображения гистологических препаратов, обработка и анализ цифровых изображений, бинаризация*

Введение

Разработка автоматизированных систем обработки медицинских изображений является наиболее важным и быстро развивающимся направлением в области микроскопических исследований гистологических препаратов. Компьютерный анализ микроскопических изображений клеток широко применяется в ряде прикладных областей, включая диагностику заболеваний и морфологический анализ клеток, что особенно важно в медико-биологических исследованиях и биоинформатике. Подход, основанный на микроскопических исследованиях, играет важную роль при решении следующих задач: обнаружение злокачественных и раковых клеток, определение естественных морфологических изменений клеток, исследование характеристик клеток в динамике (например, во время процедуры терапии). В связи с этим, процедура автоматического подсчета числа ядер клеток является ключевым блоком в системах микроскопического анализа медицинских изображений гистологических препаратов. С 1970-х годов ведутся активные работы по разработке методов и алгоритмов для решения данной проблемы [1, 2], а обнаружение клеточных структур и подсчет числа ядер клеток являются общими задачами для многих исследований.

Одним из наиболее простых, быстрых и очевидных методов подсчета ядер клеток является пороговая сегментация изображений, что по-



а *б* *в* *г* *д* *е*

Рис. 1. Примеры гистологических изображений *а*, *в*, *д* и их гистограммы яркости соответственно *б*, *г*, *е*

зволяет разделить объекты интереса и фон. Другой подход заключается в использовании различных детекторов краев (LoG фильтр, фильтры Лапласа и т. д.). Тем не менее, обнаружение и сегментации ядер клеток является сложной задачей в силу того, что клетки имеют неоднородную структуру и высокую вариабельность. Еще одной особенностью гистологического изображения является неоднородная подсветка регистрируемого препарата, что также накладывает ограничения на использование традиционных подходов.

В последние годы было предложено большое число методов и алгоритмов сегментации, разделения и классификации ядер клеток при проведении процедуры гистологического анализа. Более сложные решения состоят из нескольких этапов анализа изображений и включают в себя использование нескольких независимых алгоритмов. Эти решения основаны на традиционных алгоритмах анализа и обработки изображений, таких как метод активных контуров, метод морфологического водораздела, морфологические операции, алгоритм *k*-средних, метод опорных векторов и т. д. [3–12]. В последних работах для повышения эффективности исследователи предлагают комбинировать различные подходы. Обзор методов и алгоритмов, используемых для решения задач обнаружения, сегментации и классификации клеток медицинских изображениях можно найти в работах [1, 2]. В данной работе решалась задача автоматического подсчета ядер клеток на гистологических изображениях независимо от их размера.

В зависимости от качества подготовленного для исследования препарата и оптического оборудования, микроскопические изображения могут быть как полутоновыми, так и цветными. Большое число различных объектов на гистологических изображениях является серьезным недостатком, влияющим на процедуру анализа изображений данного класса. Анализ клеточных структур является трудной задачей из-за сложности природных объектов (зашумленность, неоднородный фон, вариабельность характеристик объекта). Большинство ядер клеток являются частью гистологических структур со сложными и нерегулярными визуальными признаками [13]. Примеры медицинских гистологических изображений и их гистограммы яркости представлены на рис. 1. Форма гистограмм доказывает тот факт, что задачу автоматического обнаружения и сегментации ядер клеток сложно решить с помощью только лишь пороговых методов.

2. Методы и данные

2.1. Данные. Исследуемые гистологические препараты окрашивались гематоксилином и эозином (один из самых распространённых методов окрашивания в гистологии), после чего были получены цифровые изображения (H&E изображения), вошедшие в общедоступную базу медицинских гистологических изображений [14, 15]. Гистологические срезы были оцифрованы с помощью сканера Zeiss Mirax Scan, оснащенного Zeiss Plan-Apochromat 20x (числовая апертура = 0,8) и AVT Marlin F-146C Firewire 1/2’’ CCD камерой, размер пикселя 4,65×4,65 мкм. Комбинация 20x увеличения и 1x C-Mount адаптера позволили получить разрешение изображения 0,23×0,23 мкм. Все слайды были отсканированы в 20x увеличении и при полном разрешении. Полученные изображения были преобразованы в файлы изображений JPEG с 85% качеством JPEG. Размер изображения – 600×600 пикселей. Тестовая база состоит из 36 цветных изображений, которые содержат 7931 ядер клеток. В базе изображений присутствуют снимки различных органов (молочной железы, почек, слизистой оболочки желудка, соединительной ткани, тонкой кишки и т. д.). Координаты центров ядер клеток были отмечены тремя экспертами-патологоанатомами и представлены в виде 36 xml-фай-

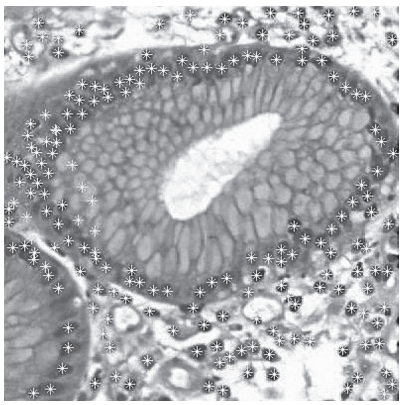
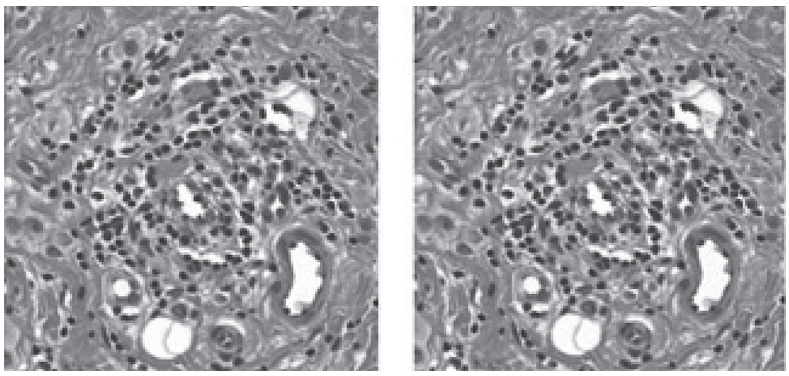


Рис. 2. Пример H&E изображения с отмеченными центрами ядер клеток



а *б*

Рис. 3. *а* – исходное изображение, *б* – изображение после уменьшения числа цветов в цветовом пространстве RGB

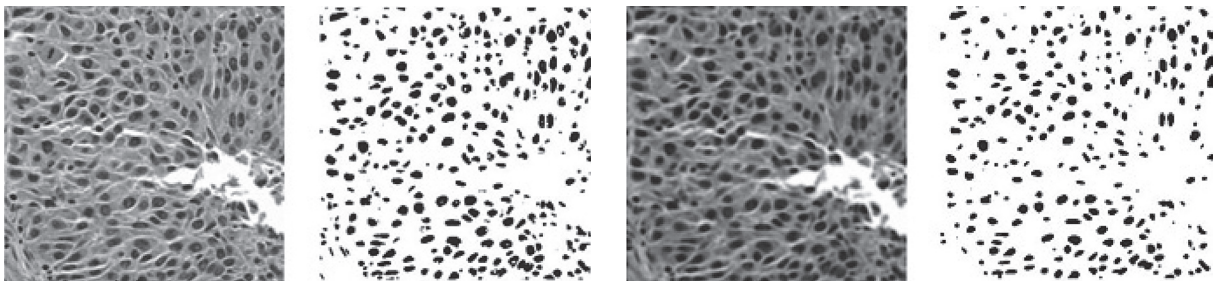
лов (для каждого гистологического изображения соответственно), рис. 2.

2.2. Основная идея. Предложенная методика подсчета числа ядер клеток на гистологических изображениях состоит из следующих этапов: 1. уменьшение числа цветов в цветовом пространстве RGB; 2. изменение контраста изображения; 3. применение направленной фильтрации [17]; 4. пороговая сегментация; 5. морфологической обработки.

Этап предварительной обработки включает в себя несколько этапов. Исходные изображения из тестовой базы содержат ограниченное число основных цветов (розовый, фиолетовый и оттенки синего). Предлагается уменьшить количество цветов в исходной палитре изображения с использованием алгоритма квантования цвета методом минимизации дисперсии [18]. Результаты реализации данного алгоритма практически не заметны, но играют решающее значение на последующих этапах анализа, рис. 3.

На следующем этапе происходит увеличение контрастности изображений путем растяжения значений интенсивностей динамического диапазона. Далее предлагается использовать направленный фильтр, который обрабатывает изображение, руководствуясь дополнительной информацией о каждом пикселе. При удачном выборе дополнительной информации направленный фильтр превосходит по качеству билатеральную фильтрацию. Бинаризация реализуется с помощью алгоритма Sauvola [19], который анализирует обрабатываемую картинку и адаптивно вычисляет индивидуальный порог бинаризации для каждого пикселя. Найденный порог используется для бинаризации значения текущего пикселя [19–21], рис. 4.

Затем применяются операции математической морфологии – открытие и закрытие с использованием структурного элемента небольшого размера. Операция закрытия «закрывает» небольшие внутренние «дырки» в изображении, и убирает углубления по краям области. Открытие позволяет избавиться от небольших кусочков изображения, выходящих за границу области. После этого определяется число областей на изображении, соответствующих ядрам клеток.

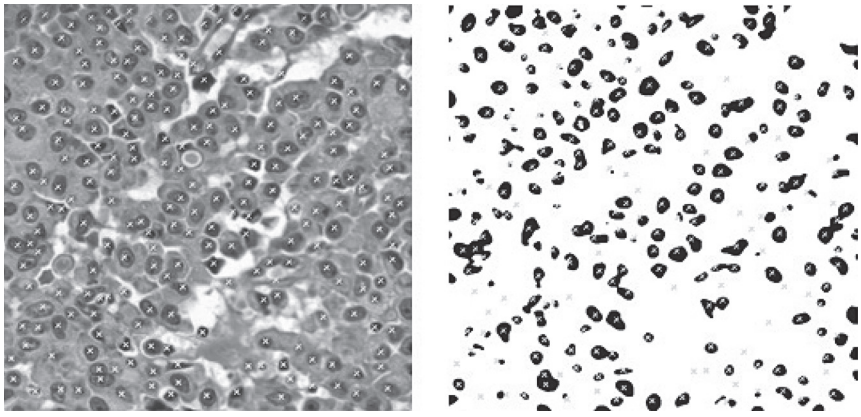


а *б* *в* *г*

Рис. 4. Улучшение результатов бинаризации с помощью направленного фильтра: *а* – полутоновое изображение без применения направленного фильтра, *б* – результат пороговой бинаризации; *в* – полутоновое изображение с применением направленного фильтра; *г* – результат пороговой бинаризации

Таблица 1. **Выбор оптимальным значений параметров алгоритмов, реализуемых на отдельных этапах предложенной методики**

Этап обработки	Параметр	Тестируемые диапазоны значений параметров	Значение параметров, дающее максимальные значения точности и полноты
квантование цвета методом минимизации дисперсии	количество цветов в цветовом пространстве	3, 4, 5, 7, 9	4
направленная фильтрация	размер маски степень размытия	3×3, 4×4, 5×5, 7×7 0,3, 0,4, 0,5, 0,55, 0,6, 0,7	3×3 0,55
Бинаризация методом Sauvola	размер анализируемой области при бинаризации порог	5×5, 7×7, 15×15, 30×30, 45×45, 55×55, 65×65, 75×75, 85×85, 95×95, 105×105, 115×115, 125×125, 135×135, 145×145 0,2, 0,25, 0,3, 0,35, 0,4, 0,45, 0,5, 0,7, 0,9	75×75 0,3
Морфологическая фильтрация (замыкание и отмыкание)	радиус структурного элемента форма структурного элемента	1, 2, 3, 4, 5 диск	3 диск



а *б*

Рис. 5. Пример определения ядер клеток

2.3. Результаты экспериментов и оценка эффективности предложенной методики.

Предложенная методика реализована в системе Matlab. Был проведен ряд экспериментов по оценке ее эффективности с использованием описанной выше тестовый базы изображений. Определены критичные параметры алгоритмов, настраиваемые на каждом этапе анализа изображений. Для каждого параметра был установлен интервал тестируемых значений, а затем реализована процедура выбора не только оптимальных значений каждого параметра, но их из взаимная комбинация, на основе оценки значений точности (*Precision*) и полноты (*Recall*), табл. 1.

Пример результата определения ядер клеток приведен на рис. 5.

Эффективность подсчета ядер клеток оценивалась с использованием следующих значений: *TP* – истинно-положительное решение; *FP* – ложноположительное решение; *FN* – ложноотрицательное решение. На основе данных параметров вычислялись точность (*Precision*) и полнота (*Recall*), которые являются метриками, используемыми при оценке большей части алгоритмов извлечения информации:

$$Precision = \frac{TP}{TP + FP}, \quad (1)$$

$$Recall = \frac{TP}{TP + FN}. \quad (2)$$

F-мера представляет собой *гармоническое среднее* между точностью и полнотой. Она стремится к нулю, если точность или полнота стремится к нулю:

$$F = 2\frac{Precision \cdot Recall}{Precision + Recall} \quad (3)$$

Полученные результаты сравнивались с последними достижениями в данной области на указанной тестовой базе [7, 9–10], табл. 2.

Таблица 2. **Сравнение эффективности предложенной методики с последним достижениями в исследуемой предметной области**

	Предложенная методика	Wiennert	Al-Kofahi
Точность	0,8363±0,0120	0,908±0,04	0,707±0,13
Полнота	0,9570±0,0016	0,859±0,04	0,916±0,04
F-мера	0,8926	0,8828	0,7980

3. Обсуждение результатов

Табл. 2 показывает эффективность предложенной методики на описанной тестовой базе изображений. Разработанный подход может быть адаптирован к различным задачам подсчета ядер клеток. Его главное преимущество – это автоматический подход к подсчету ядер клеток. В процессе анализа на этапах фильтрации и морфологической обработки были «потеряны» ядра с небольшой площади. Однако это позволило получить более достоверные результаты для других ядер клеток, что связано с улучшением результатов бинаризации, когда исчезают области, не являющиеся ядрами. Дальнейшие исследования будут направлены на повышение эффективности этапа сегментации и расширение набора тестовых баз изображений.

Заключение

Предложена методика автоматического обнаружения ядер клеток и подсчета их числа на основе направленной фильтрации, алгоритма бинаризации Sauvola и морфологических операций. В отличие от известных алгоритмов данных подход не предусматривает сегментацию ядер клеток, а только предполагает обнаружение и оценку их количество. Это позволяет избежать сложных алгоритмических вычислений и обеспечивает хорошую точность подсчета ядер клеток. Прототип программного обеспечения, разработанного в рамках проведенного исследования, можно рассматривать как автоматический инструмент для анализа ядер клеток. Работа частично выполнена в рамках гранта фонда фундаментальных исследований № Ф15ЛИТ-031.

Литература

1. **Methods** For Nuclei Detection, Segmentation, and Classification in Digital Histopathology: A Review – Current Status and Future Potential / Irshad, H. [et. al] // IEEE Reviews in Biomedical Engineering, 2014. – Vol. 7. – P. 97–114.

2. **Recent** Advances in Morphological Cell Image Analysis / Chen S. [et. al] // Computational and Mathematical Methods in Medicine, 2012. – 10 p.

3. **Jung C., Kim C.** Impact of the Accuracy of Automatic Segmentation of Cell Nuclei Clusters on Classification of Cell Nuclei Clusters on Classification of Thyroid Follicular Lesions / C. Jung, C. Kim // Cytometry. Part A, 2014. – P. 709–719.

4. **Multi**-resolution Approach for Combining Visual Information using Nuclei Segmentation and Classification in Histopathological Images / Saharma, H. [et. al] // Proceedings of the 10th International Conference on Computer Vision, Theory and Applications, 2015. – P. 37–46.

5. **Alilou, M.** Segmentation of cell nuclei in heterogeneous microscopy images: A resalable templates approach / M. Alilou, V. Kovalev, V. Taimouri // Computerized Medical Imaging and Graphics, 2013. – Vol. 37. – P. 488–499.

6. **Kowal, M.** Nuclei Segmentation for Computer-Aded Diagmosis of Breast Cancer / M. Kowal, P. Filipczuk // Int. Journal Appl. Math. Comput. Science, 2014. – Vol. 24. – No. 1. – P. 19–31.

7. **Detection** and segmentation of cell nuclei in virtual microscopy images: a minimums-model approach / Wienert, S. [et al] // National Scientific Reports, 2012. – 2:503.

8. **White** Blood Cell Segmentation by Color-Space-Based K-Means Clustering / Zang, C. [et. al] // Sensors, 2014. Vol. – 14. – P. 16128–16147.

9. **Region**-based progressive localization of cell nuclei in microscopic images with data adaptive modeling / Y. Song [et. al] // BMC Bioinformatics. – 2013. Vol. 14. № 1. – P. 173–180.

10. **Coelho, L. P.** Nuclear segmentation in microscope cell images: a hand-segmented dataset and comparison of algorithms / L. P. Coelho, A. Shariff, R. F., Murphy // Proc. of the IEEE International Symposium Biomedical Imaging, 2009. – P. 518–521.

11. **Wavelet**-Based Multiscale Texture Segmentation: Application to Stromal Compartment Characterization on Virtual Slides / N. Signolle [et. al] // Signal Processing, 2010. – Vol. 90. – № 8. – P. 2412–2422.

12. **Segmentation** of cytological image using color and mathematical morphology / O. Lezoray [et. al] // Acta Stereologica, 1999. – 18. – P. 1–14.

13. **An** Image Analysis-Based Approach for Automated Counting of Cancer Cell Nuclei / Loukas, C. G. [et. al] // Cytomettry. Part A, 2003. – P. 30–42.

14. **Improved** automatic detection and segmentation of cell nuclei in histopathology images / Al-Kofahi, Y. [et. al] // IEEE Trans. on Biomedical Engineering, 2010. – Vol. 57. – № 4. – P. 841–852.

15. **Cell**-based quantification of molecular biomarkers in histopathology specimens / Al-Kofahi, Y. [et. al] // Histopathology, 2011. – 59(1) – P. 40–54.

16. Image Smoothing via L_0 Gradient Minimization / L. Xu [et. al] // ACM Transactions on Graphics. – December 2011. – Vol. 30. – No. 6. – article 174.

17. He K., Sun J., Tang X. Guided image filtering // Pattern Analysis and Machine Intelligence, IEEE Transactions on. – 2013. – Т. 35. – №. 6. – С. 1397–1409.

18. Wan S. J., Prusinkiewicz P., Wong S. K. M. Variance-based color image quantization for frame buffer display // Color Research & Application. – 1990. – Т. 15. – №. 1. – С. 52–58.

19. Sauvola, J. Adaptive document image binarization / J. Sauvola, M. Pietikainen // Pattern Recognition, 2000. – Vol. 33. – P. 225–236.

20. Shafait, F. Efficient implementation of local adaptive thresholding techniques using integral images / Shafait, F., Keysers, D. and Breuel, T. M. // Document Recognition and Retrieval XV. – 2008.

21. Stathis, P. An Evaluation Technique for Binarization Algorithms / Stathis, P., Kavallieratou E., Papamarkos N. // Journal of Universal Computer Science, 2008. – Vol. 14. – No. 18. – P. 3011–3030.

Поступила	*После доработки*	*Принята к печати*
15.04.2016	*30.04.2016*	*10.05.2016*

M. M. Lukashevich, V. V. Starovoitov

AN APPROACH TO CELL NUCLEI COUNTING IN HISTOLOGICAL IMAGE ANALYSIS

In the paper a method of automatical counting the number of cell nuclei in histological images is studied. This operation is commonly used in the diagnostics of various diseases and morphological analysis of cells. In this connection, the procedure of automatical count the number of cell nuclei is a key step in the systems of medical imaging microscopic analysis of histological preparations. The main aim of our work was to develop an efficient scheme of automatic counting cell nuclei based on advanced image processing methods: directional filtering, adaptive image binarization and mathematical morphology. Unlike prior research, the presented approach does not provide segmentation of cell nuclei in the image, but only requires to detect them and count their number. This avoids complex algorithmic calculations and provides good accuracy of counting cell nuclei.

The paper describes a series of experiments conducted to assess the effectiveness of the proposed method using the available online database of medical test histological images. Critical parameters defined algorithms, configurable at each stage of image analysis. For each parameter we have defined value ranges, and then realized a selection of optimal values for every parameter and a mutual combination of them. It is based on generally accepted quantitative measures of precision and recall. The results were compared with the state-of-art investigations in this field and demonstrated an acceptable level of accuracy of the proposed method. The software prototype developed during the study can be regarded as an automatic tool for analysis of cell nuclei. The presented approach can be adapted to various problems of analysis of cell nuclei of various organs.

Лукашевич Марина Михайловна, кандидат технических наук. Доцент кафедры ЭВМ учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Беларусь. Сфера научный интересов: обработка изображений, распознавание образов, системы технического зрения.

Старовойтов Валерий Васильевич, доктор технических наук, профессор. Главный научный сотрудник ОИПИ НАН Беларуси. Лауреат премии Ленинского комсомола БССР и Государственной премии Республики Беларусь. С 2000г. преподает по совместительству в разных университетах курсы, связанные с обработкой и анализом цифровых изображений. Сфера научный интересов: обработка и анализ цифровых изображений, полученных в разных участках электромагнитного спектра. Опубликовал более 150 работ в научных журналах и трудах конференций, 3 монографии. Индекс Хирша по данным Академии Google равен 12. Подготовил 6 кандидатов наук.

E-mail: valerys@newman.bas-net.by

ЗАЩИТА ИНФОРМАЦИИ

INFORMATION SECURITY

УДК 004.056.55

А. В. СИДОРЕНКО, И. В. ШАКИНКО, Ю. В. СИДОРЕНКО

АЛГОРИТМ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ДВУМЕРНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ

Белорусский государственный университет

Предложен новый алгоритм шифрования изображений на основе динамического хаоса. При этом для шифрования используется модифицированная процедура перестановки элементов. Процедура же изменения значений элементов производится с учетом проведенной перестановки. Модифицированная процедура перестановки включает в себя следующие этапы: (1) формирование таблицы перестановки, (2) перестановку блоков изображения, (3) перестановку внутри областей изображения. Процедура «перестановка блоков – перестановка элементов внутри областей» проводится определенное количество раз ***q****. В данной работе использовалось значение* ***q*** *= 3. При проведении второй процедуры изменения значений к элементам изображения добавляется псевдослучайная последовательность* ***G****, для формирования которой предлагается следующий алгоритм. Он заключается в: (1) формировании распределения элементов гаммы* ***G*** *по значениям яркостей; (2) инициализации элементов гаммы* ***G****; (3) перестановке элементов гаммы* ***G****. Модифицированная процедура перестановки, как показали расчеты, позволяет уменьшить количество вычислений новых позиций элементов с использованием хаотических отображений в* ***a*** *раз. В данной работе использовались значения* ***a****, равные 16 и 64. Для осуществления предлагаемой процедуры изменения значений элементов требуется формирование* ***d*** *псевдослучайных значений из интервала [0, 1) с равномерным законом распределения. При этом для большинства практических задач достаточным является значение* ***d*** *= 256. Проведено тестирование предлагаемого алгоритма, которое заключается в следующем. Вычислены значения коэффициентов корреляции между исходным и зашифрованным изображениями, между соседними элементами (пикселями) зашифрованного изображения в вертикальном, горизонтальном, диагональном направлениях. Проведена оценка ключевой чувствительности алгоритма шифрования. Также определяются: нормированное среднее изменение интенсивности (UACI) и отношение количества различающихся бит к общему количеству бит изображения. Результаты тестирования предлагаемого алгоритма свидетельствуют о его работоспособности и возможности применения в задачах защиты информации в виде изображений.*

Ключевые слова: *динамический хаос, хаотическое отображение, шифрование, изображение, информационная безопасность.*

Введение

На современном этапе развития телекоммуникационных технологий изображения широко используются при работе различных веб-приложений. При этом для большинства приложений остро стоит вопрос защиты передаваемой информации. С учетом того, что размер изображений достаточно большой, а некоторым приложениям необходимо работать в режиме реального времени, процесс шифрования должен осуществляться достаточно быстро. Традиционные алгоритмы шифрования, например, такие как AES и DES, разрабатывались без учета этих требований и не являются подходящими для данных целей [1]. Поэтому возникает необходимость в создании новых алгоритмов шифрования.

Алгоритмы шифрования изображений на основе динамического хаоса

Новым подходом, используемым при шифровании изображений, является применение явления динамического хаоса. В частности, в схемах на основе данного явления используются две независимые процедуры [2]: перестановки и изменения значений элементов (пикселей) изображения. Проведение процедуры перестановки, во-первых, позволяет снизить корреляцию между значениями соседних элементов изображения, а во-вторых, делает визуальную

информацию изображения более устойчивой к потере фрагментов зашифрованного изображения из-за ошибок в канале связи [3]. Перестановка элементов должна осуществляться способом, похожим на случайный, и быть обратимой [4]. Данным условиям удовлетворяют двумерные хаотические отображения. Однако поскольку данная процедура не меняет сами значения элементов, то гистограмма распределения элементов по яркостям сохраняется и содержит информацию об исходном изображении. Возникает необходимость в проведении процедуры изменения значений элементов изображения.

Для снижения вычислительных затрат на осуществление процесса шифрования в данной работе используется модифицированная процедура перестановки элементов и процедура изменения значений элементов с учетом перестановки.

Модифицированная процедура перестановки элементов изображения

Модифицированная процедура перестановки включает в себя следующие этапы: 1) формирование таблицы T; 2) перестановку блоков изображения; 3) перестановку элементов внутри областей изображения.

На первом этапе формируется таблица T, содержащая m строк и n столбцов. При этом значением каждого элемента таблицы T является упорядоченная пара чисел, равных индексам соответствующего элемента:

$$t_{ij} = (i, j), \qquad (1)$$

где t_{ij} – ij-ый элемент таблицы T, $i = 1 \ldots m$, $j = 1 \ldots n$.

После этого к элементам таблицы T применяется процедура перестановки w раз с использованием выбранных хаотических отображений. При этом значения параметров данных хаотических отображений выступают в роли ключа шифрования. При выборе m и n меньших, чем размеры исходного изображения m_u и n_u, количество элементов в таблице в a раз меньше, чем в исходном изображении. Таким образом, при проведении перестановки требуется в a раз меньше вычислений с использованием хаотических отображений для определения новых позиций элементов. На втором этапе изображение разбивается на равные прямоугольные блоки. При этом размеры блоков выбираются таким образом, чтобы количество блоков по горизонтали было равно m, а по вертикали – n. Выбор именно таких размеров блоков позволяет использовать сформированную на предыдущем этапе таблицу T при проведении процедуры перестановки. На следующем этапе осуществляется перестановка сформированных блоков. Проведение данного этапа позволяет равномерно распределить по всему изображению его элементы. Однако взаимное положение элементов внутри каждого блока сохраняется. Для изменения взаимного положения элементов внутри блоков на изображении выделяются области размером m на n элементов. После этого осуществляется перестановка элементов внутри данных областей. Пара процедур «перестановка блоков – перестановка элементов внутри областей» проводится некоторое количество раз q. В данной работе использовалось значение $q = 3$.

Процедура изменения значений элементов изображения

Поскольку перестановка элементов изображения не изменяет значения самих элементов, то гистограмма распределения элементов по яркостям не изменяется после проведение перестановки и содержит информацию об исходном изображении. Таким образом, возникает необходимость в проведении дополнительной процедуры изменения значений элементов. Для уменьшения вычислительных затрат на осуществление процесса шифрования в данной работе предлагается схема процедуры изменения значений элементов на основе перестановки.

При проведении предлагаемой процедуры к элементам изображения добавляется псевдослучайная последовательность (гамма). При использовании гаммы для расшифровки символа исходного сообщения требуется знание только соответствующего символа зашифрованного сообщения и соответствующего элемента гаммы. Таким образом, если зашифрованное сообщение передается по каналу связи с помехами, то количество неверно расшифрованных символов исходного сообщения равно количеству символов зашифрованного сообщения, значения которых были изменены в рас-

сматриваемом канале связи вследствие помех. Следует отметить, что при использовании блочных алгоритмов шифрования с использованием некоторых режимов шифрования, изменение значения одного символа зашифрованного сообщения может привести к неверному расшифрованию половины символов исходного сообщения.

Для формирования псевдослучайной последовательности $\{g_i\}_{i=1}^{N} = G$ предлагается выполнение следующих этапов: 1) формирование распределе ния элементов гаммы по значениям яркостей; 2) инициализация элементов гаммы G; 3) перестановка элементов гаммы G.

На первом этапе вычисляются значения элементов последовательности $\{z_k\}_{k=1}^{d}$, где z_k имеет смысл количества элементов гаммы G со значением, равным b_k, $k = 1\ldots d$, d – количество возможных значений элементов изображения.

При формировании i-го значения элемента последовательности $\{z_k\}_{k=1}^{d}$ возможно использование биномиального распределения с математическим ожиданием ν_i и дисперсией μ_i равными:

$$\nu_i = N_i p_i , \tag{2}$$

$$\mu_i = N_i p_i (1 - p_i) , \tag{3}$$

где

$$N_i = \begin{cases} N, & i = 1 \\ N_{i-1} - z_{i-1}, & i > 1 \end{cases}, \tag{4}$$

$$p_i = 1(d - i + 1) , \tag{5}$$

N – количество элементов гаммы G, $i = 1\ldots d$.

Для моделирования случайной величины с биномиальным законом распределения существует ряд подходов [5]. При выполнении условий

$$Np(1 - p) > 5 , \tag{6}$$

для $p \in [0.1,0.9]$, и

$$Np(1 - p) > 25 , \tag{7}$$

для любого p, биноминальное распределение может быть аппроксимировано нормальным распределением. При этом для вычисления значений элементов последовательности $g_i = b_k$ потребуется формирование d псевдослучайных значений из интервала [0, 1) с равномерным законом распределения. Стоит отметить, что на практике значение d обычно равно 256, а условия (6) и (7) выполняются для изображений с количеством элементов большим, чем $N = 90 \cdot 90 = 8100$.

На следующем шаге каждому элементу гаммы G присваивается значение

$$g_i = b_k , \tag{8}$$

где индексы i и k связаны соотношением

$$\sum_{j=1}^{k-1} z_j < i \le \sum_{j=1}^{k-1} z_j + z_k , \tag{9}$$

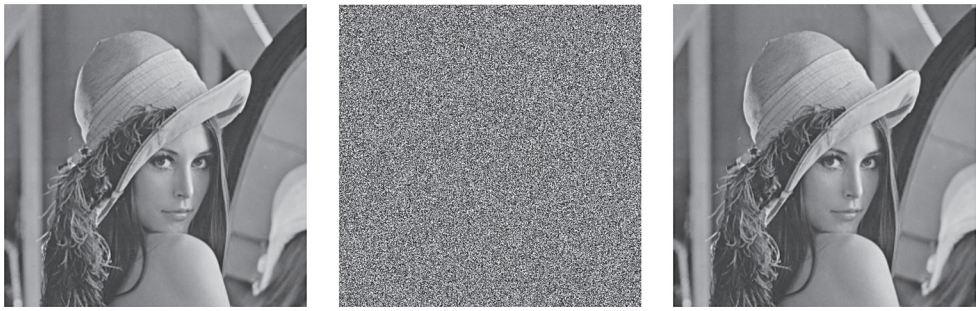
где $i = 1\ldots N$, $k = 1\ldots d$.

После этого проводится перестановка элементов последовательности G с использованием таблицы T, сформированной при проведении процедуры перестановки элементов изображения.

Предлагаемый алгоритм шифрования

Предлагаемый алгоритм шифрования сводится к следующей последовательности действий: 1) формирование таблицы перестановки T; 2) инициализация элементов гаммы G; 3) применение к элементам изображения I выбранное количество раз q пары процедур «перестановка блоков – перестановка элементов внутри областей» с использованием таблицы T; 4) добавление к изображению I_T, полученному на шаге (3), посредством операции «сложение по модулю 2» элементов гаммы G; 5) применение к элементам изображения I_G, полученного на шаге (4), выбранное количество раз q пары процедур «перестановка блоков – перестановка элементов внутри областей» с использованием таблицы T.

Для расшифровки полученного изображения требуется выполнение операций: 1) формирование таблицы перестановки T_{Inv}, обратной T; 2) инициализация элементов гаммы G; 3) применение к элементам зашифрованного изображения I_C выбранное количество раз q пары процедур «перестановка блоков – перестановка элементов внутри областей» с использованием таблицы T_{Inv}; 4) добавление к полученному изображению I_G, полученному на шаге (3), посредством операции «сложение по модулю 2» элементов гаммы G; 5) применение к элементам изображения I_T, полученного на шаге (4), выбранное количество раз q пары процедур «перестановка блоков – перестановка эле-



а *б* *в*

Результаты применения предлагаемого алгоритма шифрования к тестовому изображению «Lena.bmp»: *а* – исходное, *б* – зашифрованное и *в* – расшифрованное изображения

Таблица 1. **Значения коэффициентов корреляции**

Изображение	Алгоритм	$R_c \cdot 10^3$	$R_h \cdot 10^3$	$R_v \cdot 10^3$	$R_d \cdot 10^3$
«Lena.bmp»	предлагаемый	2,04	1,82	–3,97	9,20
	AES	–1,91	–7,80	9,23	2,34
«Baboon.bmp»	предлагаемый	–1,27	6,74	2,00	–2,83
	AES	2,55	7,86	4,81	–1,59
«Peppers.bmp»	предлагаемый	0,88	–5,99	2,26	–6,67
	AES	3,65	3,97	–10,00	1,81

ментов внутри областей» с использованием таблицы T_{Inv}.

Результаты и их обсуждение

Приводятся результаты применения предлагаемого алгоритма шифрования к изображениям «Lena.bmp», «Peppers.bmp» (512×512 пикселей) и «Baboon.bmp» (300×300 пикселей). Для формирования таблицы перестановки T использовались хаотические отображения «Кот Арнольда» и отображение Чирикова. Размеры таблицы T выбирались равными 64×64 и 75×75 для изображений с размерами 512×512 и 300×300, соответственно. Количество пар процедур «перестановка блоков – перестановка элементов внутри областей» q было выбрано равным 3. Результаты применения предлагаемого алгоритма шифрования к тестовому изображению «Lena.bmp» представлены на рисунке.

Визуально исходное и зашифрованное изображения существенно различаются, у зашифрованного изображения отсутствует структурированность. В качестве количественного параметра, характеризующего, насколько схожи изображения, использовался коэффициент корреляции R_c между элементами исходного и зашифрованного изображений. Также для зашифрованного изображения были вычислены значения коэффициентов корреляции между соседними элементами в горизонтальном R_h, вертикальном R_v и диагональном R_d направлениях (табл. 1). Для оценки равномерности распределения элементов изображения по значениям яркости использовалась дисперсия D гистограммы данного распределения.

Для сравнения приводятся результаты, полученные при использовании известного алгоритма AES. Как следует из приведенных данных, значения коэффициентов корреляции и дисперсии D, полученные при использовании предлагаемого алгоритма и алгоритма AES, схожи по величине.

Одним из параметров, характеризующих стойкость алгоритма шифрования, является чувствительность к изменениям секретного ключа. Для оценки данного параметра для двух зашифрованных изображений, полученных при использовании одного и того же исходного изображения и ключей шифрования, различающихся одним битом, были вычислены: количество пикселей, изменивших значение (Number of Pixel Changing Rate, NPCR); нормированное среднее изменение интенсивности (Unified Average Change Intensity, UACI); а также отношение количества различающихся бит к общему количеству бит изображения, выраженное в про-

Таблица 2. **Значения дисперсии гистограммы распределения элементов изображения по яркостям и значения параметров для оценки чувствительности алгоритма к изменениям ключа**

Изображение	Алгоритм	$D \cdot 10^{-3}$	A, %	UACI	NPCR·10^2
«Lena.bmp»	предлагаемый	1,19	49,98	0,335	99,60
	AES	1,10	50,03	0,335	99,62
«Baboon.bmp»	предлагаемый	0,29	50,01	0,336	99,60
	AES	0,34	49,98	0,334	99,57
«Peppers.bmp»	предлагаемый	0,93	49,98	0,335	99,61
	AES	1,16	49,99	0,335	99,61

центах (A) (табл. 2). Из полученных значений следует, что предлагаемый алгоритм проявляет чувствительность к изменениям ключа шифрования, сравнимую с чувствительностью алгоритма AES.

Заключение

Предложен новый алгоритм шифрования изображений на основе динамического хаоса. Отличительной особенностью данного алгоритма является уменьшение количества вычислений с использованием хаотических отображений. Модифицированная процедура перестановки позволяет уменьшить необходимое количество вычислений новых позиций элементов с использованием хаотических отображений в a раз. В данной работе использовалось значения a, равные 16 и 64. Для осуществления предлагаемой процедуры изменения значений элементов требуется формирование d псевдослучайных значений из интервала [0,1) с равномерным законом распределения. При этом для большинства практических задач $d = 256$.

Результаты тестирования предлагаемого алгоритма свидетельствуют о его работоспособности и возможности применения в реальных задачах защиты изображений в каналах передачи информации.

Литература

1. **Cheng, P.** A fast image encryption algorithm based on chaotic map and lookup table / P. Cheng [et al.] // Nonlinear Dynamics. – 2015. – Vol. 79, Issue 3. – P. 2121–2131.

2. **Hanchinamani, G.** Image encryption based on 2-D Zaslavskii chaotic map and pseudo Hadmard transform / G. Hanchinamani, L. Kulakami // Int. J. of Hybrid Information Technology. – 2014. – Vol. 7, Issue 4. – P. 185–200.

3. **Gschwandtner, M.** Transmission error and compression robustness of 2D chaotic map image encryption schemes / M. Gschwandtner, A. Uhl, P. Wild // EURASIP J. on Information Security [Electronic resource]. – 2007. – Mode of access: http:// jis. eurasipjournals. com/content/2007/1/048179. – Date of access: 08.04.2015.

4. **Wong, K.** Image encryption using chaotic maps / K. Wong // Intelligent computing based on chaos / L. Kocarev [et al.]. – Berlin, 2009. – Ch. 16. – P. 333–354.

5. **Харин Ю. С.** Математические и компьютерные основы статистического анализа данных и моделирования: учеб. пособие / Ю. С. Харин, В. И. Малюгин, М. С. Абрамович. – Минск: БГУ, 2008. – 455 с.

References

1. **Cheng, P.** A fast image encryption algorithm based on chaotic map and lookup table / P. Cheng [et al.] // Nonlinear Dynamics. – 2015. – Vol. 79, Issue 3. – P. 2121–2131.

2. **Hanchinamani, G.** Image encryption based on 2-D Zaslavskii chaotic map and pseudo Hadmard transform / G. Hanchinamani, L. Kulakami // Int. J. of Hybrid Information Technology. – 2014. – Vol. 7, Issue 4. – P. 185–200.

3. **Gschwandtner, M.** Transmission error and compression robustness of 2D chaotic map image encryption schemes / M. Gschwandtner, A. Uhl, P. Wild // EURASIP J. on Information Security [Electronic resource]. – 2007. – Mode of access: http://jis.eurasipjournals.com/content/2007/1/048179. – Date of access: 08.04.2015.

4. **Wong, K.** Image encryption using chaotic maps / K. Wong // Intelligent computing based on chaos / L. Kocarev [et al.]. – Berlin, 2009. – Ch. 16. – P. 333–354.

5. **Kharin Yu. S.** Mathematical and computer basics of statistical data analysis and modeling: textbook / Yu. S. Kharin, V. I. Malugin, M. S. Abramovich. – Minsk: BSU, 2008. – 455 p.

Поступила *25.03.2016* | *После доработки* *15.04.2016* | *Принята к печати* *10.05.2016*

Sidorenko A. V., Shakinko I. V., Sidorenko Yu. V.

IMAGE ENCRYPTION ALGORITHM USING TWO-DIMENSIONAL CHAOTIC MAPS

Belarusian State University

A new image encryption algorithm based on dynamic chaos is proposed. The encryption is performed using the modified element permutation procedure. The element value changing procedure is carried with regard to the performed permutation. The modified permutation procedure includes the following steps: (1) permutation table creation; (2) permutation of image blocks, (3) element permutation in the image regions. The procedure «block permutations – permutation in the image regions» is performed ***q*** *times – for this study* ***q*** *= 3. The second element value changing procedure is realized with the use of the pseudorandom sequence* ***G*** *that is added to the image elements. The following algorithm is proposed for the formation of this pseudorandom sequence: (1) the formation of the sequence* ***G*** *element distribution by brightness; (2) sequence* ***G*** *element initialization; (3) permutation of the sequence* ***G*** *elements. It is shown that, owing to the modified permutation procedure, the amount of calculations for new positions of the elements using chaotic maps is reduced by a factor of* ***a*** *– in this study* ***a*** *is equal to 16 and 64. The implementation of the proposed element value changing procedure necessitates the formation of* ***d*** *pseudorandom values from the interval [0, 1) with a uniform distribution. Actually, for the majority of practical cases* ***d*** *= 256 is applicable. The proposed algorithm has been tested as follows. The correlation coefficients have been computed for the original and encrypted images, and also for the adjacent elements in the vertical, horizontal, diagonal directions. The algorithm key sensitivity has been evaluated. Besides, the values of the unified average change intensity (UACI) and the ratios of differing bits to the total number of bits have been determined. As demonstrated by the testing results, the proposed algorithm is highly operable and may be successfully used to solve the tasks of information security.*

Keywords: *dynamic chaos, chaotic map, encryption, image, information security.*

Авторы

Сидоренко Алевтина Васильевна. Профессор кафедры физики и аэрокосмических технологий БГУ.

Научные интересы: защита информации в телекоммуникационных системах, теоретическая информатика, радиофизика, биофизика. E-mail: sidorenkoa@yandex.ru.

Шакинко Иван Владимирович. Аспирант кафедры телекоммуникаций и информационных технологий БГУ.

Научные интересы: защита информации в телекоммуникационных системах, динамический хаос и его применение.

Сидоренко Юлия Владимировна. Доцент кафедры физики полупроводников и наноэлектроники БГУ, к. ф.-м. наук.

Научные интересы: защита информации, физика полупроводников.

УДК 003.26.09

В. Ф. ГОЛИКОВ, В. Л. ПИВОВАРОВ

ПОВЫШЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА, СФОРМИРОВАННОГО В УСЛОВИЯХ УТЕЧКИ ИНФОРМАЦИИ О ЗНАЧЕНИИ НЕКОТОРОЙ ЕГО ЧАСТИ

Белорусский национальный технический университет

В статье рассматривается возможность повышения конфиденциальности криптографического ключа, сформированного в условиях утечки информации о значениях некоторой части ключа. Такая ситуация может сложиться при формировании общего криптографического ключа симметричной криптосистемы при использовании квантового канала, прослушиваемого криптоаналитиком, или другими методами, не использующими односторонние функции. Предлагается способ преобразования со случайными секретными параметрами сформированной ключевой последовательности, с помощью которого можно увеличить энтропию последней. Суть разработанной процедуры заключается в том, что абоненты A и B секретно от криптоаналитика, но согласовано между собой, выбирают некоторые биты в сформированной ключевой последовательности, (в дальнейшем называемые «помеченными»), а затем производят заранее объявленное преобразование этой последовательности, используя при этом информацию о помеченных битах.

Так как количество и порядковые номера помеченных битов неизвестны криптоаналитику, то и расположение известных ему ранее битов, изменяется случайным образом и становиться неопределенным. Принципиальным моментом этого способа является получение помеченных битов, номера которых известны только A и B, не используя для этого защищенный канал связи. Описывается один из возможных методов получения помеченных битов, основанный на случайном и независимым инвертировании сформированной ключевой последовательности абонентами A и B с последующим анализом четностей пар битов. Оценивается эффективность метода.

Ключевые слова: *криптографический ключ, утечка информации, секретное преобразование, повышение неопределенности.*

Введение

В современных технологиях защиты информации криптографические методы играют большую роль. Перспективным направлением в криптографии является использование квантовых эффектов. Так в задаче формирования общего криптографического ключа симметричной криптосистемы используют квантовый канал для передачи ключевой информации в виде одиночных фотонов. Одним из главных недостатков квантового способа формирования ключа является наличие возможности у криптоаналитика, подключившегося к квантовому каналу, узнать часть ключевой информации, в предельном случае до 25% [1]. В связи с этим широко известные классические протоколы [2, 3] запрещают использовать сеансы формирования ключа, если обнаружен факт «прослушивания» канала. Такое ограничение существенно сужает область применения классических протоколов, сводя ее к тривиальной ситуации – безопасный ключ может быть сформирован только при отсутствии «прослушивающего» криптоаналитика. Подобные утечки информации возникают и при других методах формирования общего криптографического ключа с использованием открытого канала связи [4, 5].

В статье рассматривается возможность повышения конфиденциальности криптографического ключа, сформированного в условиях утечки информации о значениях некоторой части ключа.

Постановка задачи

Пусть субъекты *A* и *B,* используя, например, квантовый канал передачи информации,

сформировали общую бинарную последовательность $X_{AB} = \{0, 1\}^{2n}$, где $2n$ – длина последовательности в битах (четное число). Криптоаналитику E, прослушавшему квантовый канал, известно d битов $(0 \le d << n)$. A и B знают об этом, но им неизвестно, количество и какие биты ключа известны E. Требуется сформировать криптографический ключ K_{AB} длиной n, $n \le 2n$, неопределенность которого, если ее измерять энтропией, равнялась бы $H_K \ge 2n - d$.

Решение

Предлагается способ преобразования со случайными секретными параметрами исходной ключевой последовательности X_{AB} в K_{AB}, с помощью которого можно увеличить энтропию последнего. Суть разработанной процедуры заключается в том, что A и B секретно от E, но согласовано между собой, выбирают некоторые биты случайным образом в последовательности X_{AB}, (в дальнейшем будем их называть «помеченными»). Затем производят заранее объявленное преобразование последовательности X_{AB}, используя при этом информацию о помеченных битах.

Так как количество и порядковые номера помеченных битов неизвестны E, то и расположение известных ему ранее d битов, изменяется случайным образом и становиться неопределенным. Принципиальным моментом этого способа является получение помеченных битов, номера которых известны только A и B, не используя для этого защищенный канал связи.

Рассмотрим основные этапы предлагаемого способа.

1. A и B случайным образом независимо и секретно друг от друга, а также от E, инвертируют $2r$ битов в своих последовательностях X_{AB}, $r \le n$.

2. A и B разбивают полученные после инвертирования последовательности X_A и X_B на фрагменты по два бита в каждом и вычисляют четности каждой пары:

$$C_i^A = a_j \oplus a_{j+1},\ C_i^B = b_j \oplus b_{j+1},$$

где $C_i^A = \{0,1\}$, $C_i^B = \{0,1\}$ – четности i-той пары соответственно X_A, X_B; a_j, b_j – биты i-той пары соответственно в X_A, X_B; i – номер пары, $i = \overline{1,n}$; j – номер бита в i-той паре, $j = 2i - 1$, $j = \overline{1,2n}$. При этом $a_j = b_j$, если оба бита не инвертированы или оба бита инвертированы; $a_j = 1 - b_j$, если один из битов инвертирован.

3. A и B сообщают друг другу по открытому каналу связи четности своих последовательностей C_i^A, C_i^B.

4. A и B производят сравнение четностей своей последовательности с четностями последовательности партнера, т. е. C_i^A сравнивается с C_i^B для каждого i. В результате такого сравнения каждый субъект определяет номера пар, для которых выполняется: $C_i^A \ne C_i^B$ или $C_i^A \ne C_i^B$.

Равенство четностей возникает в результате следующих событий:

1. В i-тых парах A и B все четыре бита не инвертированы, либо инвертированы:

$$(a_j, a_{j+1}), (b_j, b_{j+1}) \text{ или } (\overline{a_j}, \overline{a_{j+1}}), (\overline{b_j}, \overline{b_{j+1}}).$$

2. В каждой i-той паре A и B инвертировано по одному биту безразлично какому:

$$(\overline{a_j}, a_{j+1}), (\overline{b_j}, b_{j+1}) \text{ или } (\overline{a_j}, a_{j+1}), (b_j, \overline{b_{j+1}}), \ldots$$

Неравенство четностей возникает в результате следующих событий:

В i-той паре одной из последовательностей инвертирован только один бит, безразлично какой, а в i-той паре другой последовательности инвертировано оба бита или ни одного:

$$(\overline{a_j}, a_{j+1}), (\overline{b_j}, \overline{b_{j+1}})$$

или

$$(\overline{a_j}, a_{j+1}), (b_j, b_{j+1}), \ldots$$

3. A и B из всех пар выбирают пары, для которых $C_i^A = C_i^B$, а из них те пары, в которых инвертировано только по одному биту, рассуждая следующим образом «… я знаю, что в моей паре инвертирован только один бит, а четность этой пары совпадает с четностью пары партнера, значит и в его паре инвертирован только один бит…». Рассуждая аналогично, второй субъект тоже выбирает эти же пары. Криптоаналитик не знает какие биты были инвертированы в X_A и X_B, поэтому не может распознать выбранные A и B пары, несмотря на то, что четности пар ему известны. Пары, относящиеся к группе *1* и *2*, для криптоаналитика неразличимы по их четностям. Выбранные пары в дальнейшем будем называть помеченными.

4. A и B проводят некоторое заранее оговоренное преобразование (известное E) своих последовательностей X_A и X_B, (например, пере-

становки), используя при этом значения битов из помеченных пар, их порядковые номера j, количество помеченных пар. В результате такого преобразования порядковые номера битов исходной последовательности X_{AB} изменяются. Так как количество и порядковые номера помеченных бит случайны, то конечная последовательность случайным образом отличается от исходной, а знания криптоаналитика E о d битах исходной последовательности из детерминированной информации превращаются в вероятностную.

5. A и B производят обратное инвертирование своих последовательностей.

Исследование эффективности

Самостоятельный интерес представляют анализ криптостойкости конечного ключа, ее зависимость от возможных стратегий криптоаналитика, от выбора параметров n, r и значения d. Криптоаналитику E известно: d, n, r, а также C_i^A, C_i^B. Оценим его возможности по нахождению помеченных пар.

Знание четностей пар C_i^A, C_i^B, во-первых, позволяет E выбрать пары, которые потенциально могут оказаться помеченными. К таким относятся пары, для которых $C_i^A = C_i^B$. Поэтому желательно, чтобы количество таких пар было максимально возможным, чтобы затруднить в дальнейшем их перебор. Определим отчего зависит вероятность образования таких пар. Если из последовательностей X_A и X_B взять наугад по одной паре, то вероятность того что в каждой из них инвертирован один бит, равна

$$P_{A,B}(1,1) = P_A(1)P_B(1),$$

где $P_A(1)$, $P_B(1)$ – вероятность того что инвертирован один бит в паре из X_A, X_B соответственно. Очевидно, что $P_A(1) = P_B(1)$, поэтому ограничимся нахождением $P_A(1)$. Искомая вероятность равна

$$P_A(1) = P\left(a_j, \overline{a_{j+1}}\right) + P\left(\overline{a_j}, a_{j+1}\right) = 2\frac{r}{n}\left(1 - \frac{r}{n}\right).$$

Аналогично

$$P_B(1) = 2\frac{r}{n}\left(1 - \frac{r}{n}\right).$$

Следовательно,

$$P_{A,B}(1,1) = 4\frac{r^2}{n^2}\left(1 - \frac{r}{n}\right)^2 \qquad (1)$$

Выражение (1) имеет максимум, равный 1/2, при $r = 0{,}5n$. Таким образом, максимально возможное число помеченных пар равно половине общего числа пар.

Кроме того, выбор условия $r = 0{,}5n$ имеет дополнительное положительное влияние на неопределенность X_{AB}. Знание значения четности каждой пары криптоаналитиком, позволяет ему выдвигать гипотезы относительно значений битов в этих парах. Например, если $C_i^A = 0$, то вероятность того, что в X_{AB} биты этой пары одинаковы равна

$$P = P\left(a_j = a_{j+1}\right) + P\left(\overline{a_j} = \overline{a_{j+1}}\right) = \left(1 - \frac{r}{n}\right)^2 + \frac{r^2}{n^2}.$$

При $r = 0{,}5n$ вероятность $P = 1/2$, что делает гипотезу о равенстве битов в паре и гипотезу о противоположности этих битов равновероятными. Таким образом, при $r = 0{,}5n$ знание C_i^A и C_i^B не может быть использовано E.

Будем оценивать криптостойкость ключа по отношению полному перебору его значений.

Поскольку после проделанного случайного преобразования X_{AB} в K_{AB}, криптоаналитик E не знает местоположение известных ему ранее битов, то для него объем полного перебора K_{AB} равен $M_k = 2^{2n}$. Однако, зная алгоритм преобразования с точностью до количества помеченных битов и их номеров, E может использовать свои знания о d битах исходного ключа X_{AB}, используя для этого следующую стратегию.

E последовательно выдвигает гипотезы о количестве помеченных битов и проверяет их учитывая пары, которые не могут быть помеченными, осуществляя полный перебор значений оставшихся бит, исключая из него d известных ему битов.

Например, пусть $2n = 12$,

$$X_{AB} = a_1 a_2\, a_3 a_4\, a_5 a_6\, a_7 a_8 a_9 a_{10} a_{11} a_{12}.$$

A и B инвертируют в X_{AB} по 6 битов $(2r = 6)$:

$$X_A = a_1 a_2 \overline{a_3} a_4 \overline{a_5} a_6\, a_7 \overline{a_8}\, \overline{a_9}\, \overline{a_{10}} a_{11} a_{12},$$

$$X_B = \overline{a_1}\,\overline{a_2}\, a_3 \overline{a_4}\, a_5 a_6 \overline{a_7} a_8 \overline{a_9} a_{10} \overline{a_{11}} a_{12}.$$

Сравнивая четности пар с одинаковыми порядковыми номерами получим:

$$C_1^A = C_1^B,\ C_2^A = C_2^B,\ C_3^A \neq C_3^B,$$

$$C_6^A \neq C_6^B,\ C_6^A \neq C_6^B,\ C_6^A \neq C_6^B.$$

Для A и B помеченными парами являются пары с номерами: 2, 4. В качестве преобразования используем изъятие помеченных пар и размещение первого бита пары на первой позиции, второго на последней. Получим:

$$X_A = a_7 \overline{a_3} a_1 a_2 \overline{a_5} a_6 \overline{a_9}\,\overline{a_{10}} a_{11} a_{12} a_4 \overline{a_8},$$

$$X_B = \overline{a_7}\, a_3 a_1 \overline{a_2}\, a_5 a_6 \overline{a_9} a_{10} \overline{a_{11}} a_{12} \overline{a_4} a_8.$$

После обратного инвертирования A и B имеют одинаковый ключ

$$K_{AB} = a_7\, a_3 a_1 a_2\, a_5 a_6 a_9 a_{10} a_{11} a_{12} a_4 a_8.$$

Пусть E знает три бита $d = 3$, т. е. для него X_{AB} представляется как

$$X_E = x_1 a_2 x_3 x_4 x_5 a_6 x_7 x_8 x_9 a_{10} x_{11} x_{12},$$

где $x_1, x_3, x_4, x_5, x_7, x_8 x_9 x_{10} x_{12}$ – неизвестные для E биты.

Криптоаналитик E знает, что пары с номерами 3, 5, 6 не могут быть помеченными.

E выдвигает гипотезу H_0: в X_{AB} помечено 0 пар. Этой гипотезе соответствует последовательность K_{AB}, равная:

$$x_1 a_2 x_3 x_4 x_5 a_6 x_7 x_8 x_9 a_{10} x_{11} x_{12}.$$

E выдвигает гипотезу H_1: в X_{AB} помечена 1 пара: Этой гипотезе соответствуют последовательности K_{AB}, равные:

$$x_1 x_3 x_4 x_5 a_6 x_7 x_8 x_9 a_{10} x_{11} x_{12} a_2;$$

$$x_3 x_1 a_2 x_5 a_6 x_7 x_8 x_9 a_{10} x_{11} x_{12} x_4,$$

$$x_7 x_1 a_2 x_3 x_4 x_5 a_6 x_9 a_{10} x_{11} x_{12} x_8.$$

E выдвигает гипотезу H_2: в X_{AB} помечено 2 пары. Этой гипотезе соответствуют последовательности K_{AB}, равные:

$$x_9 x_1 x_3 x_4 x_5 a_6 x_7 x_8 x_{11} x_{12} a_2 a_{10};$$

$$x_9 x_1 x_3 x_4 x_5 a_6 x_7 x_8 x_{11} x_{12} a_2 a_{10};$$

$$x_9 x_3 x_1 a_2 x_5 a_6 x_7 x_8 x_{11} x_{12} x_4 a_{10}.$$

E выдвигает гипотезу H_3: в X_{AB} помечено 3 пары. Этой гипотезе соответствуют последовательности K_{AB}, равные:

$$x_9 x_4 x_1 x_3 a_6 x_7 x_8 x_{11} x_{12} a_2 x_5 a_{10}.$$

Таким образом, перебор неизвестных значений элементов ключа при трех гипотезах равен соответственно: C_1^3, C_1^3, C_2^3, C_3^3. С учетом неизвестных E бит $x_1, x_3, x_4, x_5, x_7, x_8, x_9, x_{10}, x_{11}$ полный перебор значений K_{AB} будет равен $M = (C_0^3 + C_1^3 + C_2^3 + C_3^3)2^9 = 2^{12}$.

Суммарный объем перебора для E при данной стратегии оказался таким же, что и перебор всех значений X_E без использования своих априорных знаний $M = M_K$, где $M_K = 2^{12}$. Однако, надо иметь ввиду, что, во-первых, вероятности перечисленных гипотез различны, т. е. в конечном итоге эффективность рассматриваемой стратегии будет зависеть от вероятностных характеристик количества помечаемых бит. В связи с этим целесообразно исследовать статистические свойства числа помечаемых пар. Найдем распределение вероятностей числа помечаемых пар.

Согласно приведенному выше алгоритму в последовательностях X_A и X_B помечается пара, в которой оказался один инвертированный бит. Обозначим число таких пар через S. Очевидно, что S зависит от количества пар в последовательностях X_A и X_B, содержащих один инвертированный бит. Обозначим число таких пар через R_A и R_B. Таким образом имеем систему случайных величин (S, R_A, R_B). Обозначим распределение вероятностей этой системы как $P(S = s, R_A = r_A, R_B = r_B)$. Так как S зависит от R_A и R_B, то справедливо:

$$P(s, r_A, r_B) = P(s|r_A, r_B)\, B(r_A, r_B),$$

где $P(s|r_A, r_B)$ – условная вероятность. Так как R_A и R_B независимые случайные величины, то получим:

$$P(s, r_A, r_B) = P(s|r_A, r_B)\, P(r_A)\, P(r_B). \qquad (2)$$

Вероятность числа помеченных пар получим интегрированием (1) по r_A и r_B

$$P(s) = \sum_{r_A = f(s)} \sum_{r_B = f(s, r_A)} P(s|r_A, r_B) P(r_A) P(r_B), \quad (3)$$

где $f(s)$, $f(s, r_A)$ – области интегрирования, учитывающие связи между переменными r_A, r_B, s. Найдем составляющие (3). Начнем с определения $P(r_A)\, P(r_B)$.

Процесс образования r_A и r_B идентичен, поэтому для упрощения обозначений рассмотрим его исходя из следующей постановки задачи. Имеется бинарная случайная последовательность длиной $2n$, в ней случайным образом инвертировано $2r$ битов. В результате этого образовалось: R_0 пар без инвертированных бит (a_j, a_{j+1}); R_1 пар с одним инвертированным битом, причем из них R_{01} пар содержат в паре биты, расположенные в порядке (a_j, $1 - a_{j+1}$), R_{10} пар содержат в паре биты, расположенные в порядке ($1 - a_j$, a_{j+1}), R_2 пар с двумя инвертированными битами ($1 - a_j$, $1 - a_{j+1}$).

Система случайных величин (R_0, R_{01}, R_{10}, R_2) имеет полиномиальное распределение $P(R_0 = r_0, R_{01} = r_{01}, R_{10} = r_{10}, R_2 = r_2)$ с коэффициентами

$$\frac{n!}{r_0!r_{01}!r_{10}!r_2!}. \quad (4)$$

Учитывая связи между рассматриваемыми величинами можно записать следующие соотношения:

$$\begin{cases} r_{01} + r_{10} = r_1 \\ r_0 + r_1 + r_2 = n \\ r_1 + 2r_2 = r \end{cases} \quad (5)$$

Тогда (4), можно записать как

$$\frac{n!}{\left(n - r - \frac{r_1}{2}\right)!\,(r_1 - r_{10})!\,r_{10}!\left(r - \frac{r_1}{2}\right)!}. \quad (6)$$

Знание этих коэффициентов позволит найти распределение вероятностей случайной величины R_1 (а это R_A или R_B), как отношения количества значений бинарной последовательности $M(r_1)$ при которых $R_1 = r_1$

$$M(r_1) = \sum_{r_{10}=0}^{r_1} \frac{n!}{\left(n - r - \frac{r_1}{2}\right)!\,(r_1 - r_{10})!\,r_{10}!\left(r - \frac{r_1}{2}\right)!} \quad (7)$$

к общему количеству возможных значений бинарной последовательности M

$$M = \sum_{r_1=0}^{2r} \sum_{r_{10}=0}^{r_1} \frac{n!}{\left(n - r - \frac{r_1}{2}\right)!\,(r_1 - r_{10})!\,r_{10}!\left(r - \frac{r_1}{2}\right)!}. \quad (8)$$

Следует иметь в виду, что r_1 может принимать только четные значения, поскольку общее число инвертированных бит $2r$ четное число. Максимально возможное значение r_1 равно $2r$.

Можно показать, что величина M равна $\binom{2N}{2r}$. Тогда искомая вероятность равна

$$P(R_1 = r_1) = \frac{M(r_1)}{\binom{2N}{2r}}.$$

Таким образом, окончательно имеем

$$P(r_A) = P(r_B) = \frac{M(r_1)}{\binom{2n}{2r}}. \quad (9)$$

Вероятность $B(s|r_A, r_B)$ – это вероятность того, что, если в последовательностях X_A и X_B соответственно образовалось R_A и R_B пар с одним инвертированным битом, то число таких совпадающих пар будет S. Вычислим эту вероятность по аналогии с [6]. Если в последовательности X_A содержится r_A пар типа r_1, то число возможных комбинаций, в которых из r_B пар типа R_1 s пар совпадает с аналогичными парами из R_A, равно $\binom{r_A}{s}\binom{n - r_A}{r_B - s}$. Так как сама последовательности X_A может принимать $\binom{n}{r_A}$ значений, то общее число значений X_A и X_B в которых совпадает s пар типа R_1 равно $M(s) = \binom{r_A}{s}\binom{n - r_A}{r_B - s}\binom{n}{r_A}$. Общее же число всевозможных комбинаций равно $M = \binom{n}{r_A}\binom{n}{r_B}$, тогда искомая вероятность равна

$$P(s|r_A, r_B) = \frac{\binom{r_A}{s}\binom{n - r_A}{r_B - s}}{\binom{n}{r_B}}. \quad (10)$$

Имея все составляющие (1), окончательно можно записать

$$P(s) = \sum_{r_A = f(s)} \sum_{r_B = f(s, r_A)} \frac{\binom{r_A}{s}\binom{n - r_A}{r_B - s}}{\binom{n}{r_B}} \times$$

$$\times \left\{ \frac{\sum_{r_{10}=0}^{r_A} \frac{n!}{\left(n - r - \frac{r_A}{2}\right)!\,(r_A - r_{10})!\,r_{10}!\left(r - \frac{r_A}{2}\right)!}}{\binom{2n}{2r}} \times \right.$$

$$\left. \times \frac{\sum_{r_{10}=0}^{r_B} \frac{n!}{\left(n - r - \frac{r_B}{2}\right)!\,(r_B - r_{10})!\,r_{10}!\left(r - \frac{r_B}{2}\right)!}}{\binom{2n}{2r}} \right\}. \quad (11)$$

Суммирование в (11) должно вестись с учетом того, что величины r_A и r_B принимают только четные значения 0, 2, 4, …, $2r$, а также условия: $\min(r_A, r_B) \geq s \geq \max(0, r_A + r_B - n)$. По-

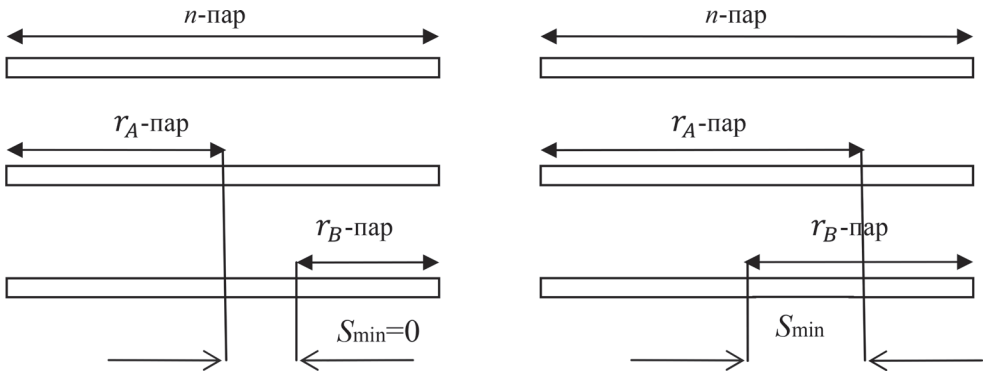
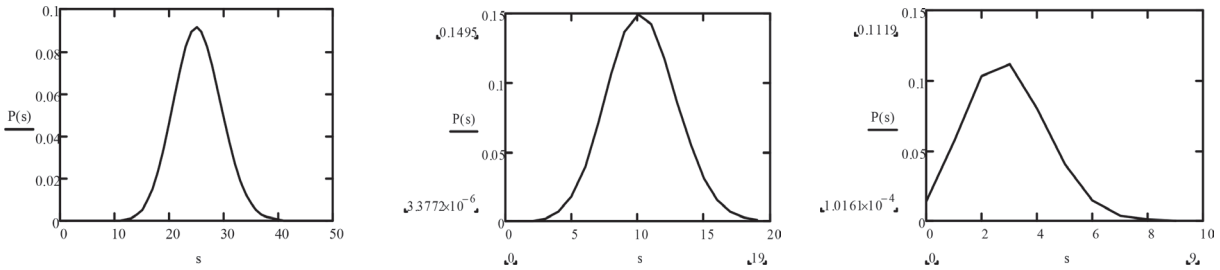


Рис. 1. Границы величины S



а *б* *в*

Рис. 2. Распределение вероятностей для $n = 100$ при $r = 50$, $r = 20$, $r = 10$

следнее условие вытекает из того, что с одной стороны число совпадающих пар не может быть больше, чем минимальное число пар типа r_1 в одной из последовательностей, а с другой, если суммарное значение числа совпадающих пар обеих последовательностей превосходит общее число пар, то минимальное значение s не может быть меньше, чем величина превышения (рис. 1). Распределение вероятностей (11) изображено на рис. 2 для $n = 100$ при $r = 50$, $r = 20$, $r = 10$ соответственно. Из рисунков видно, что число битов, их порядковые номера, помечаемые сторонами A и B секретно от E, зависят от числа инвертированных битов r и колеблются в достаточно широком диапазоне, что затрудняет криптоанализ сформированного ключа методом полного перебора. Так, например, если криптоаналитик попытается перебрать все возможные варианты с помеченными парами при $n = 100$ и $r = 50$, ограничив возможный диапазон значений S наиболее вероятным [20, 30], то количество вариантов составит примерно 10^{25}.

Заключение

Предложенный способ повышения конфиденциальности криптографического ключа, сформированного в условиях утечки информации о значениях некоторой его части позволяет существенно затруднить попытку вычисления его значения полным перебором, если речь идет о ключе блочного алгоритма шифрования, и не допустить расшифрования части зашифрованного сообщения, если утечка произошла в системе поточного шифрования. Открытым остается вопрос о выборе вида преобразования, использующего помеченные пары битов.

Литература

1. **Bennet, C. H. Brassard, G.** Quantum cryptography: quantum key distribution and coin tossing/ Int. conf. on computers systems ans signal processing. – Bangalore, 1984. P. 175–179.

2. **Брассар Ж.** Современная криптология. – М.: Полимед, 1999. – 178с.

3. **Боумейстер, Д.** Физика квантовой информации. / Д. Боумейстер, А. Экерт, А. Цайлингер. – М.: Постмаркет, 2002. – 276с.

4. **Способ** распределения криптографического ключа между абонентами: пат. 17856 Респ. Беларусь: МПК 04L 9/08 (2006.01) / В. Ф. Голиков; дата публ.: 19.07.2011.

5. **Голиков, В. Ф.** Оценка потерь конфиденциальности при неклассических способах формирования криптографического ключа / В. Ф. Голиков, Ф. Абдольванд // Информатика.– 2011. –№ 2 (30). – С. 104–110.

6. **Беляев, Ю. К.** Вероятностные методы выборочного контроля. – М.: изд. Наука,1975.– 407с.

References

1. **Bennet, C. H. Brassard, G.** Quantum cryptography: quantum key distribution and coin tossing/ Int. conf. on computers systems ans signal processing. – Bangalore, 1984. P. 175–179.
2. **Brassar, J.** Modern cryptology. – M.: Polymed, 1999. – 178 p.
3. **Baumeister, D.** The physics of quantum information. / D. Baumester, A. Ekert, A. Tsailinger. –M:. Postmarket, 2002. – 276 p.
4. **Method** of cryptographic key distribution between subscribers: pat. 17856 Rep. Belarus: IPC 04L 9/08 (2006.01) / V. F. Golikov; date publ.: 19.07.2011.
5. **Golikov, V. F.** Estimation of loss of confidentiality of non-classical methods of forming a cryptographic key / V. F. Golikov, F. Abdolvand // Informatika. – 2011. – № 2 (30). – P. 104–110.
6. **Belyaev, Y. K.** Probabilistic methods of sampling. – M.: Science, 1975. – 407 p.

Поступила	*После доработки*	*Принята к печати*
03.05.2016	*15.05.2016*	*20.05.2016*

Holikau U. F., Pivovarov V. L.

CRYPTOGRAPHIC KEY IMPROVED PRIVACY UNDER THE CONDITIONS OF SOME OF CRYPTOGRAPHIC KEY VALUE DATA LEAK

Belarusian National Technical University

The article outlines the possibility of increasing the privacy of cryptographic key generated in the conditions of data leakage of some of its values. Such a situation can occur in the formation of a common cryptographic key of a symmetric cryptosystem employing a quantum channel, listened by a cryptanalyst, or other methods that do not make use of one-way functions. A method with the conversion parameters to increase the entropy of a generated secret random key sequences suggested. The essence of the procedure developed is that the subscribers A and B (secretly to a cryptanalyst), but in agreement with each other, choose some of the bits in the generated key sequence (further referred to as «tagged») and produce a pre-announced conversion of this sequence, using the data about the tagged bits.

Since the amount and serial numbers of tagged bits are unknown to a cryptanalyst, the layout of the bits known to a cryptanalyst before randomly changes and becomes uncertain. The fundamental point of this method is to obtain tagged bits, the positions of which are known only to subscribers A and B without using the secure communication channel. One of the possible methods of obtaining tagged bits based on a random and independent inversion of a generated key sequence by the subscribers A and B and followed by the analysis of parities pairs of bits is analyzed. The efficiency of the method is evaluated.

Keywords: *cryptographic key, dataleak, secret conversion, increased uncertainty.*

Голиков Владимир Федорович

Доктор технических наук, профессор. Заведующий кафедрой «Информационные технологии в управлении» Белорусского национального технического университета. Сфера научных интересов: защита информации, криптография.

E-mail: vgolikov@bntu.by

Пивоваров Вадим Леонидович

В 2012 окончил Белорусский Государственный Университет по специальности «Информатика». Аспирант Белорусского национального технического университета, специалист по программированию на языке C#. Соавтор трех научных работ по тематике информационной безопасности. Участник XX Научно-практической конференции «Комплексная защита информации».

E-mail: vadim.pif@gmail.com

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

INFORMATION TECHNOLOGIES IN EDUCATION

УДК 004.942

Ю. Б. ПОПОВА, А. И. БУРАКОВСКИЙ

ПРЕДСТАВЛЕНИЕ ЗНАНИЙ В ОБУЧАЮЩИХ СИСТЕМАХ НА ОСНОВЕ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ

Белорусский национальный технический университет

Использование информационных технологий и, в частности, информационных обучающих систем увеличивает возможности как преподавателя, так и обучаемого, в достижении своих целей в образовательном процессе, учитывая индивидуальные характеристики каждого и предоставляя возможности непрерывного образования. Несмотря на большое количество исследований в этой области и очевидные преимущества таких систем, их использование пока ограничено. Одной из главных причин здесь является использование точных количественных методов в такой сложно-структурированной и нечеткой области как учебный процесс. При проектировании информационных обучающих систем разработчики сталкиваются с проблемой моделирования знаний, которые условно могут быть разделены на две категории: предметные и персональные. Предметные знания определяются программой обучения и представляют знания эксперта (преподавателя) о составе и структуре учебного предмета. Персональные знания позволяют определить степень изученного материала обучаемым. Эти знания динамичные, изменяются в процессе обучения и предназначены для адаптации информационных обучающих систем к конкретному обучаемому. В настоящее время существует большое количество моделей представления знаний, среди которых наиболее используемыми являются логические, продукционные, сетевые, фреймовые и математические. Главными преимуществам математической модели является точность, работа с абстракциями, передача информации логически однообразным способом. Математическая модель представления знаний на основе теории нечетких множеств позволяет, в отличие от остальных, учесть семантическую неопределенность оценивания экспертом (преподавателем) степень подготовки обучаемого.

Ключевые слова: *знания, информационные обучающие системы, математическая модель, нечеткие множества.*

Введение. В настоящее время система образования активно развивается за счет внедрения информационных технологий, которые позволяют повысить доступность образования и его качество. Новые технологии предоставляют преподавателю и студенту более широкие (по сравнению с традиционным обучением) возможности в преподавании и изучении дисциплин. Ин формационные обучающие системы (ИОС), реализуя комплекс программно-технических и учебно-методических средств, позволяют автоматизировать процесс обучения, а также выстроить для каждого обучающегося персональную траекторию изучения материала, независимо от того, где территориально находится обучающий [1].

Базой для проектирования ИОС являются работы Брусиловского П. Л., Савельева А. Я., D. Callear [2–5] и многих других. Однако, несмотря на большое количество исследований, существует ряд причин, по которым использование ИОС в учебных заведениях ограничено. Среди главных причин можно выделить следующие:

- ИОС покрывают лишь некоторое количество действий из всего учебного процесса;
- ИОС обладают низкой степенью адаптации к индивидуальным способностям обучаемых.

Указанные выше причины, как правило, вызваны использованием точных количественных методов в такой сложно-структурированной и нечеткой области, как учебный процесс. Использование точных методов не позволяет учесть лингвистическую неопределенность, неточность категорий логики, а также субъективизм эксперта, что в свою очередь накладывает ограничения на качественное отображение знаний преподавателя в ИОС. В связи с этим можно утверждать, что задача разработки средств представления знаний в ИОС, учитывающей их семантическую неоднознач-

ность, является актуальной для достижения цели реализации адаптивной обучающей системы, способной самостоятельно определять текущий уровень знаний студента и адаптировать маршрут обучения в зависимости от этого параметра.

1. Знания в информационных обучающих системах. Понятие «знание» по своей сути является очень обширным и многозначным. Например, в работе [6] к *знаниям* относят информацию о логике решения задач, а к *данным* – информацию, которая должна быть проанализирована в соответствии с этой логикой. Также в [6] выделены специфические признаки, отличающие знания от данных:

- внутренняя интерпретируемость, означающая, что в знаниях находится информация, раскрывающая смысл элементов знаний;
- структурированность знаний, заключающаяся в возможности декомпозиции сложных объектов на более простые и установлении соответствующих связей между ними;
- связность знаний, отражающая причинно-следственные и временные отношения между фактами, процессами и явлениями;
- активность знаний, содержащая планы действий и управляющие процедуры.

В свою очередь знания можно разделить на два вида: формализованные (явные) и неформализованные (неявные). Формализованные знания могут быть представлены в виде строгих, конкретных и четких умозаключений (формул, моделей, законов). Их можно записать, запомнить, передать устно. Также формализованному знанию можно научиться самостоятельно, следуя четким правилам. Например, для вычисления дискриминанта квадратного уравнения нужны знания формулы дискриминанта, т. е. запомнив формулу дискриминанта и применив ее в реальной жизни, можно утверждать о знании дискриминанта квадратного уравнения.

Понятие неформализованных (неявных) знаний было впервые предложено Марком Полани в [7]. Эти знания появляются только как результат тренировок под руководством инструктора и являются результатом обучения или личного опыта. Любые, сколь угодно ясно сформулированные правила сами по себе не помогут этому научиться [8].

До недавнего момента считалось, что информационные обучающие системы не приспособлены определять уровень неформализованных знаний. Развитие компьютерных систем, широкие исследования в области моделей представления знаний, разработка и внедрение ИОС показали, что определение уровня неформализованных знаний представляет собой достаточно сложную задачу и является одним из сдерживающих факторов широкого применения ИОС в учебном процессе.

2. Модели представления знаний в обучающих системах. В ИОС в качестве источника знаний используются базы знаний. Однако в очень многих ИОС база знаний представляет собой простой набор теоретического материала, формул, графиков и т. д. Примеров баз знаний с позиции термина «база знаний» искусственного интеллекта практически нет. Связано это, прежде всего, с нерешенностью вопроса представления знаний. Суть проблемы заключается в том, что необходимо создать и описать некую модель хранения знаний, с которой могли бы взаимодействовать остальные компоненты ИОС наподобие человеческого интеллекта. Механизм взаимодействия компонентов ИОС с базой знаний строится на основании выбранной модели представления знаний. Таким образом, можно утверждать, что выбор модели представления знаний является ключевым фактором при построении информационных обучающих систем.

На данный момент существует огромное количество моделей, позволяющих представлять знания в ИОС. Все они имеют свои достоинства и недостатки. Выбор модели представления знаний зачастую зависит от предметной области. Условно все модели можно разделить на следующие группы [6]: логические, продукционные, сетевые, фреймовые, математические.

В основе *логической модели* лежит тот факт, что вся информация, которая требуется для решения прикладной задачи, рассматривается как совокупность фактов и утверждений, представленных формулами в некоторой логике [6]. Достоинством логических моделей является то, что модель базируется на классическом аппарате математической логики, методы которой хорошо изучены и обоснованы. Также имеются достаточно эффективные процедуры вывода, база знаний предназначена для хранения большого количества аксиом, из которых по правилам вывода можно получать другие

знания. Основной недостаток: логики, адекватно отражающей человеческое мышление, еще не создано [9].

Продукционные модели являются наиболее часто используемыми в представлении знаний. Они основаны на правилах, которые представляют знание как предложение «Если условие истина, то действие». Достоинствами продукционных моделей являются наглядность и высокая модульность (отдельные логические правила могут быть добавлены в базу знаний, изменены или удалены независимо от других) [9]. Модульный принцип разработки систем позволяет автоматизировать их проектирование, обеспечить легкость внесения дополнений и изменений, реализовать простоту логического вывода. Однако продукционная модель обладает одним существенным недостатком: в случае, когда таких продукций накапливается большое количество (больше нескольких сотен), то они могут противоречить друг другу.

Сетевые модели основаны на семантической сети, и их формально можно задать в виде $H = < I, C_1, C_2, \ldots, C_n, G >$, где I – множество информационных единиц, $C_1, C_2, \ldots, C_n$ – множество типов связей между информационными единицами, G – связи из заданного набора типов связей, входящих в I [6]. В работе [9] приводятся следующие достоинства и недостатки сетевой модели.

Достоинства:

- описание объектов и событий производится на уровне очень близком к естественному языку;
- обеспечивается возможность соединения различных фрагментов сети;
- отношения между понятиями и событиями образуют небольшое, хорошо организованное множество;
- для каждой операции над данными или знаниями можно выделить некоторый участок сети, который охватывает необходимые в данном запросе характеристики;
- обеспечивается наглядность системы знаний, представленной графически;
- близость структуры сети, представляющей знания, семантической структуре фраз на естественном языке;
- соответствие сети современным представлениям об организации долговременной памяти человека.

Недостатки:

- сетевая модель не дает ясного представления о структуре предметной области, поэтому формирование и модификация такой модели затруднительны;
- сетевые модели представляют собой пассивные структуры, для обработки которых необходим специальный аппарат формального вывода и планирования.

Основным отличием фреймовой модели от всех остальных является то, что в ней жестко фиксируется структура информационных единиц, называемых протофреймом. В общем виде она выглядит следующим образом:

(Имя фрейма:
Имя слота 1 (значение слота 1)
Имя слота 2 (значение слота 2)
.....
Имя слота К (значение слота К)).

При конкретизации фрейма ему и слотам присваиваются конкретные имена и происходит заполнение слотов. Таким образом, из протофреймов получаются фреймы- экземпляры. Переход от исходного протофрейма к фрейму-экземпляру может быть многошаговым за счет постепенного уточнения значений слотов [10]. Авторы работ [9, 11] выделяют следующие достоинства фреймовой модели:

- способность отображать концептуальную основу организации памяти человека;
- универсальность, так как позволяют отобразить все многообразие знаний.

Также в работе [11] приводятся такие достоинства как:

- естественность и наглядность представления, модульность;
- поддержку возможности использования значений слотов по умолчанию.

Из недостатков модели можно выделить следующие [12]:

- высокая сложность фреймовой системы;
- разрозненные части информации, объединенные во фреймы, не могут быть выстроены в последовательность высказываний. Иначе говоря, языки описания знаний во фреймовой модели не являются языками, родственными естественным, а ближе к изобразительным средствам.

Методы построения *математических моделей* часто основаны хотя и на неточной, но в целом объективной информации об объекте

[11]. Однако возможны ситуации, когда при построении моделей решающее значение имеют сведения, полученные от эксперта, обычно качественного характера. Они отражают содержательные особенности изучаемого объекта и формулируются на естественном языке. Описание объекта в таком случае носит нечеткий характер. При использовании для отображения знаний теории нечетких множеств булева алгебра распространена на действительные числа. В булевой алгебре 1 представляет истину, а 0 – ложь. То же имеет место и в нечеткой логике, но кроме того используются также все дроби между 0 и 1, чтобы указать на частичную истинность [13–15]. Так запись «μ(высокий (X)) = 0,75» говорит о том, что предположение «X – высокий» в некотором смысле на три четверти истинно, а на одну четверть ложно.

Главными преимуществами математической модели являются точность, работа с абстракциями и передача информации логически однообразным способом.

Точность таких моделей можно проверить, проведя необходимые наблюдения или поставив эксперимент. Также важным плюсом является тот факт, что логика математики позволяет извлекать только те элементы, которые важны для дедуктивной логики рассуждения, исключая все посторонние значения. Недостатком же является сложность математического аппарата. Возникают трудности перевода языка математики на язык реальной жизни.

Зачастую в структуре знаний классы объектов являются нечеткими понятиями. Также лица, излагающие эти знания, могут делать выводы, содержащие элементы неуверенности, либо основанные на опыте. Подобные ситуации заставляют искать новые подходы к описанию знаний и их оцениванию. Одним из новых подходов является переходот знаний в классическом понимании к знаниям нечетким. Нечеткие знания можно описать через следующие лингвистические переменные:

Θ = Отношение принадлежности = {Принадлежит, Скорее всего принадлежит, Вероятно принадлежит, ..., Вероятно не принадлежит, Скорее всего не принадлежит, Не принадлежит};

Δ = Отношение следования = {Следует, Скорее всего следует, Вероятно следует, ..., Вероятно не следует, Скорее всего не следует, Не следует};

AND/OR = Отношение связи = {И/ИЛИ, Скорее всего И/ИЛИ, Вероятно И/ИЛИ, ...}.

Предполагается, что эти переменные имеют разную степень значения в зависимости от силы принадлежности к тому или иному свойству.

Тогда под нечетким знанием можно понимать следующее.

Если

$$\left(a_1\Theta_1X_1\Psi_1a_2\Theta_2X_2\Psi_2\ldots a_n\Theta_nX_n\Psi_n\ldots\right)$$
$$\Delta a_{n+1}\Theta_{n+1}X_{n+1}\Psi_{n+1},$$

где a_i, X_i – значения лингвистических переменных, Θ_i – значение переменной принадлежности из Θ, Ψ_1 – значение переменной связи из AND/OR, Δ – терм-значение переменной следования из **Δ**. Поскольку нечеткое знание определяется через лингвистические переменные, то и операции нечеткого логического вывода можно количественно определить на базе операций с соответствующими функциями принадлежности.

В обучающих системах знания условно можно разделить на две категории:

- предметные – знания эксперта (преподавателя) о составе и структуре учебного предмета, которые определяются программой обучения;
- персональные – знания о степени изученности предмета в рамках изучаемого курса обучаемым. Эти знания динамичные, изменяются в процессе обучения и предназначены для адаптации ИОС к конкретному обучающему.

3. Математическая модель на основе нечетких множеств. В основе *математической модели* предметных знаний на основе теории нечетких множеств лежит нечеткий ориентированный граф $\tilde{G} = (E, S, \mu_{\tilde{G}}(e), \mu_{\tilde{G}}(s))$ (рис. 1).

Вершины графа – это множество E концептов (предметных элементов). Дуги графа отображают отношения $S \subset E \times E$, которые характеризуют структуры предметных знаний. Вершины и дуги содержат функции принадлежности нечетких множеств, которые являются представлением эксперта (преподавателя) о предмете. Функции принадлежности задаются экспертом самостоятельно.

Математическая модель персональных знаний на основе теории нечетких множеств имеет явные преимущества в представлении неформализованных знаний по отношению

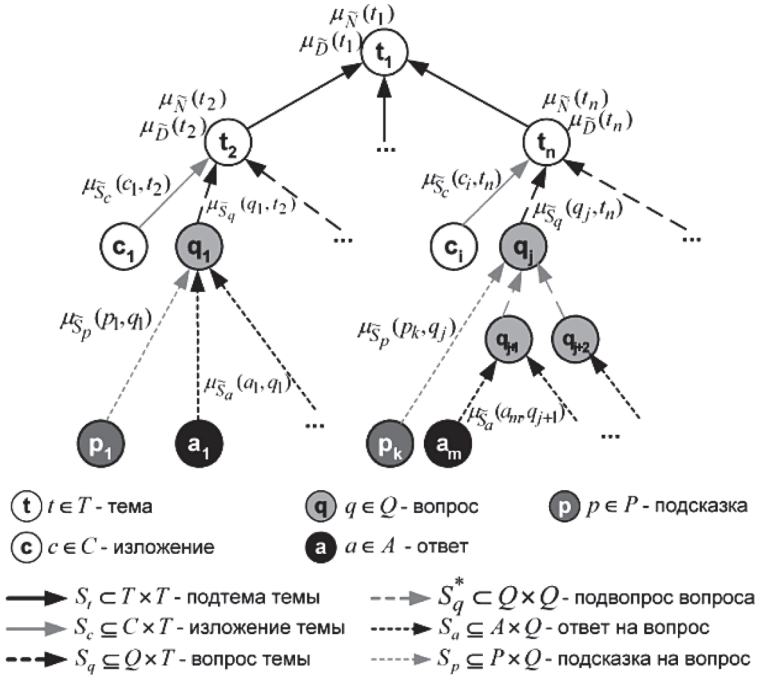


Рис. 1. Математическая модель предметных знаний [16]

к другим. В ее основе лежит нечеткий ориентированный граф $\widetilde{G}' = (E', S', \mu_{\widetilde{G}'}(e'), \mu_{\widetilde{G}'}(s'))$ (рис. 2).

Вершины графа G' показывают состав уже изученных предметных знаний – подмножество $E' \subset E$; дуги графа G' являются отражением уже изученных предметных знаний. Дуги графа инициализируются значениями функций принадлежности, которые определяются как результат построения нечетких подмножеств множества *E*, и обуславливают друг друга как:

$$A' \sim \underset{\tilde{S}_a \circ S_q^*}{\overset{av}{\rightarrow}} \tilde{A}P' \sim \underset{\tilde{s}_p}{\overset{gr}{\rightarrow}} \tilde{P}; \tilde{Q} = \tilde{A} \setminus \tilde{P}; Q' \sim \underset{S_q \circ S_t}{\overset{av}{\rightarrow}} \tilde{P},$$

где $\widetilde{A} \subset Q'$ – нечеткое множество, характеризующее степень знания вопроса; $\tilde{P} \subset Q'$ – нечеткое множество, характеризующее степень незнания вопроса; $\tilde{Q} \subset Q'$ – нечеткое множество, отражающее оценку уровня владения вопросом учащимся; $\tilde{T} \subset T'$ – нечеткое множество, отражающее оценку степени освоения учащимся материала темы; $\overset{av}{\sim\!\!\rightarrow}$ обозначение операции индуцирования в average-форме; $\overset{gr}{\sim\!\!\rightarrow}$ – обозначение операции индуцирования в форме граничного объединения.

Такое определение функций принадлежности вышеперечисленных нечетких множеств повышает степень полноты и достоверности оценки подготовки обучаемого благодаря учету всех факторов, влияющих на ответ учащегося, и, что самое важное, степени их влияния [16].

Построение персональных знаний необходимо для определения степени изучения предметных знаний и нахождения в соответствии с установленной степенью достижения целей подмножества тем $T'' \subseteq T$, которые необходимо изучить обучаемому для получения целостного образа знаний по предметной области:

$$T'' = \begin{cases} N, \ N \neq 0, \\ D \bigcup \overline{T'}, \ N \neq 0 \end{cases}$$

где $N = \text{supp}(\tilde{N} \setminus \tilde{T}), D = \text{supp}(\tilde{D} \setminus \tilde{T})$.

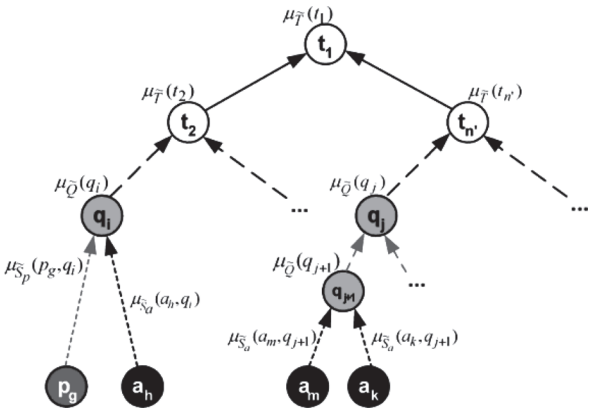


Рис. 2. Математическая модель персональных знаний [16]

Результатом установления состава множества $T^{"}$ является адаптация системы навигации процесса обучения. Необходимость индивидуализированного подхода к обучению требует также и адаптации содержания учебного курса [16].

Такое модельное представление позволяет, в отличие от известных способов, учесть семантическую неопределенность оценивания экспертом (преподавателем) степени подготовки обучаемого и адаптировать систему навигации электронного учебного курса адекватно качественной и лингвистически неточной характеристике уровня знаний обучаемого. Применение теории нечетких множеств и отношений при формировании персональных знаний позволяет значительно повысить степень полноты и достоверности оценки степени подготовки учащегося благодаря учету различных факторов, влияющих на ответ учащегося при компьютерном контроле знаний, и, что самое важное, степени их влияния [8].

Заключение**.** Знания не имеют четкой границы, вследствие чего оценивать их четко достаточно сложно. В ЭВМ знания могут быть представлены только как система данных с интерпретатором. Поэтому необходима модель, которая бы позволила четко представить нечеткие величины (знания) в обучающих системах и свести погрешности в факте освоения знаний к минимуму. Результаты исследований показали, что для этого подходит математическая модель на основе теории нечетких множеств. Построение модели предметных знаний и модели текущих знаний студента на основе нечеткого ориентированного графа позволит определять в автоматическом режиме уровень усвоения того или иного методического материала. Использование оверлейного наложения одной модели на другую, а также применение операций произведения и свертки над характеристическими функциями нечеткого множества позволит адаптировать маршрут обучения к каждому студенту индивидуально. В настоящее время ведется разработка обучающей системы, в которой знания будут представлены математической моделью на основе теории нечетких множеств.

Литература

1. **Бураковский А. И., Попова Ю. Б.** Математические модели пользователей в адаптивных обучающих системах: Информационные технологии в образовании, науке и производстве: Материалы МНТИК. Режим доступа: [http://www.bntu.by/news/67-conference-mido/1545–2014–11–22–12–18–35.html].

2. **Брусиловский, П. Л.** Адаптивные и интеллектуальные технологии в сетевом обучении / П. Л. Брусиловский // Новости искусственного интеллекта. – 2002. – № 5. – С. 25–31.

3. **Брусиловский, П. Л.** Интеллектуальные обучающие системы / П. Л. Брусиловский // Информатика. Информационные технологии. Средства и системы. – 1990. – № 2. – С. 3–22.

4. **Савельев, А. Я.** Автоматизированная обучающая система КОНТАКТ на базе ЕС ЭВМ: версия КОНТАКТ/ОС. Вып. 2 / Под ред. Ницецкого Л. В. – Рига: РПИ, 1979. —67 с.

5. **Garret, B.** The value of intelligent multimedia simulation for teaching clinical decision-marking skills. / B. Garret, D. Callear // Nurse Educ Today. – 2001. – № 21. – P. 382–390.

6. **Спицын, В. Г.** Представление знаний в информационных системах: учебное пособие. / В. Г. Спицын, Ю. Р. Цой. – Томск: Изд-во Томского политехнического университета, 2008. – С. 8.

7. **Полани, М.** Личностное знание / М. Полани. – М.: Прогресс, 1985. – 103 с.

8. **Попов, Э. В.** Искусственный интеллект: Кн. 1. Системы общения и экспертные системы. / Справочник под ред. Э. В. Попова. – М.: Радио и связь, 1990. – 464 с.

9. **Клыков, М. С.** Основы управления: учебное пособие / М. С. Клыков, Н. П. Григорьев, Т. И. Балалаева. – Хабаровск: Издательство ДВГУПС, 2007 – С. 2.

10. **Берштейн, Л. С.** Функционально-структурное исследование ситуационно-фреймовой сети эксплуатационной системы с нечеткой логикой / Л. С. Берштейн [и др.] // Изв. АН. Сер. Техническая кибернетика. – 1994. – № 2. – С. 120–124.

11. **Головчинер, М. Н.** Введение в системы знаний. Курс лекций / М. Н. Головчинер. – Томск, 2011. – С. 20.

12. **Коробова, И. Л.** Методы представления знаний / И. Л. Коробова. – Тамбов, Издательство ТГТУ, 2003. – С. 10–13.

13. **Борисов, А. Н.** Обработка нечеткой информации в системах принятия решений. / А. Н. Борисов [и др.]. – М.: Радио и связь, 1989. – 304 с.

14. **Карелин, В. П.** Модели и методы представления знаний и выработки решений в интеллектуальных информационных системах с нечеткой логикой / В. П. Карелин // Вестник Таганрогского института управления и экономики. – 2014. – № 1(19) – С. 75–83.

15. **Белоус, В. А.** Современные модели представления знаний в обучающих системах / В. А. Белоус, Е. С. Кудинов, М. Э. Желнин. // Ученые записки. Электронный научный журнал Курского государственного университета. – 2010. – № 1. – С. 9–14.

16. **Денисова, И. Ю.** Математические модели представления знаний эксперта в информационной обучающей системе дистанционного обучения / И. Ю. Денисова, М. В. Баканова // Известия Пензенского государственного педагогического университета. ПГУ. – 2011. – С. 360–361.

References

1. **Burakovskij A. I., Popova Y. B.** Mathematical models of users in adaptive learning systems: Informacionnye tehnologii v obrazovanii, nauke i proizvodstve: Materialy MNTIK. Rezhim dostupa: [http://www.bntu.by/news/67-conference-mido/1545–2014–11–22–12–18–35.html].

2. **Brusilovskij, P. L.** Adaptive and intelligent technologies in network learning / P. L. Brusilovskij// Novosti iskusstvennogo intellekta. – 2002. – № 5. – P. 25–31.

3. **Brusilovskij, P. L.** Intelligent tutoring systems / P. L. Brusilovskij // Informatika. Informacionnye tehnologii. Sredstva i sistemy. – 1990. – № 2. – P. 3–22.

4. **Savel'ev, A. Ja.** Automated Training System CONTACT based on ES computers: version KONTAKT/OS. Vyp.2/ Pod red. Niceckogo L. V. – Riga: RPI, 1979. – 67 p.

5. **Garret, B.** The value of intelligent multimedia simulation for teaching clinical decision-marking skills / B. Garret, D. Callear// Nurse Educ Today. – 2001. – № 21. – P. 382–390.

6. **Spicyn, V. G.** Knowledge representation in information systems. / V. G. Spicyn, Ju. R. Coj. – Tomsk: Izd-vo Tomskogo politehnicheskogo universiteta, 2008 – P. 8.

7. **Polani, M.** Personal knowledge / M. Polani // M.: Progress, 1985. – 103 p.

8. **Popov, Je. V.** Iskusstvennyj intellekt: Kn. 1. The communication systems and expert systems. / Spravochnik pod red. Je. V. Popova. – M.: Radio i svjaz', 1990. – 464 p.

9. **Klykov, M. S.** Fundamentals of Management: uchebnoe posobie / M. S. Klykov, N. P. Grigor'ev, T. I. Balalaeva. – Habarovsk: Izdatel'stvo DVGUPS, 2007. – P. 2.

10. **Bershtejn, L. S.** Functional-structural research of situational framing network operating system with fuzzy logic / L. S. Bershtejn [i dr.] // Izv. AN. Ser. Tehnicheskaja kibernetika. – 1994. – № 2. – P. 120–124.

11. **Golovchiner, M. N.** Introduction to knowledge system. Kurs lekcij / M. N. Golovchiner. – Tomsk, 2011. – P. 20.

12. **Korobova, I. L.** Methods of knowledge representation / I. L. Korobova. – Tambov, Izdatel'stvo TGTU, 2003. – P. 10–13.

13. **Borisov, A. N.** Processing fuzzy information in decision-making systems / A. N. Borisov [i dr.] – M.: Radio i svjaz', 1989. – P. 304.

14. **Karelin, V. P.** Models and methods of knowledge representation and decision-making in intelligent information systems with fuzzy logic / V. P. Karelin // Vestnik Taganrogskogo instituta upravlenija i jekonomiki. – 2014. – № 1(19). – P. 75–83.

15. **Belous, V. A.** Modern knowledge representation models in training systems / V. A. Belous, E. S. Kudinov, M. Je. Zhelnin // Uchenye zapiski. Jelektronnyj nauchnyj zhurnal Kurskogo gosudarstvennogo universiteta. – 2010. – № 1. – P. 9–14.

16. **Denisova, I. Ju.** Mathematical models of expert knowledge representation in e-learning system / I. Ju. Denisova, M. V. Bakanova // Izvestija Penzenskogo gosudarstvennogo pedagogicheskogo universiteta. PGU. – 2011. – P. 360–361.

Поступила	*После доработки*	*Принята к печати*
10.05.2016	*15.05.2016*	*20.05.2016*

Y. B. Popova, A. I. Burakovski

REPRESENTATION OF KNOWLEDGE IN LEARNING SYSTEMS BASED ON THE THEORY OF FUZZY SETS

Belarusian National Technical University

Using of information technologies and e-learning systems increases opportunities of teachers and learners in reaching their studying process goals. It takes into account the individual characteristics of each and provides opportunities for e-learning. But e-learning systems using is limited despite of many researchers and the obvious advantages of such systems. One of the main reasons of such limitation is the usage of precise quantitative techniques in a hard-structured and fuzzy area as a learning process. In designing of information learning systems developers are faced with the problem of modeling knowledge which can be divided into two categories conventionally: personal and subject. Subject knowledge is defined education program and represents expert knowledge (the teacher) about the composition and structure of the subject. Personal knowledge can determine the level of the material studied by learner. This kind of knowledge is dynamic, changing in the educational process and designed to adapt e-learning systems to the particular learner. There are a large number of knowledge representation models. Commonly used models are logical, productional, network, frame-based and mathematical models. The main advantage of the mathematical model is the accuracy, abstraction processing, communication logically uniform way. Mathematical model of knowledge representation based on the theory of fuzzy sets take into consideration the semantic ambiguity expert assessment (teacher) degree of preparation to learner.

Keywords: *knowledge, e-learning, mathematical model, fuzzy sets.*

Yuliya B. Popova, PhD, Associate Professor at the Software Department of the Belarusian National Technical University. Her research interests include methods and algoritms of optimization in technical systems, engineering of adaptive learning systems and learning management systems (LMS), modeling of student knowledge, software testing and quality assurance.

E-mail: julia_popova@mail.ru

Alexander Burakovski received the graduate degree in software engineering from the Belarusian National Technical University in 2012 and the Master's degree in system analysis and control of information processing in 2013. He is currently working on PhD degree program. His current research interests include modeling of student knowledge based on fuzzy sets and fuzzy logic.

Работа выполняется в рамках научно-исследовательской работы ГБ 11–254 «Математическое и программное обеспечение систем обработки информации в образовании и автоматизированных систем управления техническими объектами».

УДК 004.42

В. А. МАТЮШЕНКО, В. Ю. ФИЛОН, Н. И. БЕЛОДЕД

ИНФОРМАЦИОННАЯ СИСТЕМА АВТОМАТИЗАЦИИ ПОДГОТОВКИ ДОКУМЕНТОВ УЧЕБНОГО ПРОЦЕССА

Академия управления при Президенте Республики Беларусь

Информационные технологии стремительно покоряют мир, проникая во все сферы человеческой деятельности. Образование не стало исключением. Важным направлением информатизации образования является развитие систем университетского менеджмента. Современные информационные системы улучшают и облегчают управление всеми видами деятельности учреждения. Целью предлагаемой работы является разработка системы, позволяющей автоматизировать процесс формирования отчетных документов. В статье описывается проблема подготовки документов учебного процесса. Было принято решение о проектировании и создании информационной системы в среде Microsoft Access. В качестве результата показаны 4 типа отчетов, полученные при использовании разрабатываемой системы. Применение данной системы уже сейчас позволяет автоматизировать процесс и сократить трудозатраты на подготовку отчетных документов. Все отчеты реализуются в программном продукте Microsoft Excel и могут быть использованы для дальнейшего анализа и обработки.

Ключевые слова: *информационная система, автоматизация, база данных, фактическая нагрузка профессорско-преподавательского состава, документы учебного процесса.*

Введение

XXI-й век – век доминирования информации и информационных технологий. Они стремительно покоряют мир, проникая во все сферы человеческой деятельности, что привело современное общество к общеисторическому процессу, называемому информатизацией. Этот процесс заключается в свободном доступе любого гражданина к информации, проникновении информационных технологий в научные, производственные, общественные сферы, высоком уровне информационного обслуживания.

Поэтому одним из приоритетных направлений государственной политики Республики Беларусь стало формирование информационного общества. 26 марта 2016 года была утверждена государственная программа развития цифровой экономики и информационного общества на 2016–2020 годы.

Создание информационного общества требует информатизации деятельности всех отраслей экономики и социальной сферы. Одной из сфер, где новые информационные технологии оказались наиболее эффективными и востребованными, стала сфера образования и науки, результаты которой относятся к числу наиболее значимых и приоритетных в современной системе общечеловеческих ценностей. Ведь именно от того, в какой степени и как будут решены проблемы информатизации образования, будет зависеть уровень подготовки специалистов всех отраслей народного хозяйства, именно это определяет развитие нашего государства в ближайшем будущем.

Актуальность темы определяется стремительным ростом использования информационных технологий в системе высшего образования.

Использованию информационных технологий в учреждении образования способствуют:

• внешние факторы, связанные с повсеместной информатизацией общества и необходимостью соответствующей подготовки специалистов;

• внутренние факторы, связанные с распространением современной компьютерной техники и программного обеспечения, принятием государственных и межгосударственных программ информатизации образования, появлением необходимого опыта информатизации у преподавателей.

Система университетского менеджмента

Важным направлением информатизации образования является развитие систем университетского менеджмента. Проблема актуальна в глобальном масштабе: и на постсоветском пространстве, и в странах Европейского Союза. Это, в частности, связано с постоянной модернизацией национальных систем образования, развитием Болонского процесса, со сложностью предметной области и отсутствием достаточно полных и адекватных ее описаний.

В настоящее время в образовательные учреждения внедряются программные комплексы, призванные помочь в организации административной деятельности. Академия управления при Президенте Республики Беларусь (далее – Академия управления) не является исключением. В данном учреждении образования внедрены такие программные продукты, как «1С Бухгалтерия 7.7», программный комплекс «Канцлер», электронный библиотечный каталог, система электронного документооборота «SMBisness», IBM Notes (Lotus Notes), АСУ «Спрут» и другие.

Вышеперечисленные программные продукты позволяют автоматизировать некоторые процессы управления учреждением образования, но качественное и оперативное управление всеми видами деятельности учреждения возможно только с применением интегрированной информационной системы (ИИС).

В Академии управления, являющейся ведущим высшим учебным заведением в Республике Беларусь по подготовке, переподготовке и повышению квалификации руководящих кадров, была создала такая система.

ИИС содержит множество комплексов приложений: для управления организацией и учебным процессом – а также информационные системы, с которыми в перспективе предполагается интеграция ИИС Академии управления. На рис. 1 представлена обобщенная схема ИИС управления обобщенными приложениями Академии управления.

В комплексе управления учебным процессом особое место занимает ИИС «Учебная работа» или же ИИС (ВУЗ). Одной из важнейших составных частей ИИС (ВУЗ) является информационная система управления учебным процессом на уровне кафедры.

Интегрированная информационная система образовалась путем постепенной автоматизации подразделений Академии управления. На кафедре управления информационными ресурсами была создана информационная система, которая автоматизирует деятельность кафедры. ИС «Кафедра» предоставляет доступ к подсистемам, отвечающим за оперативную

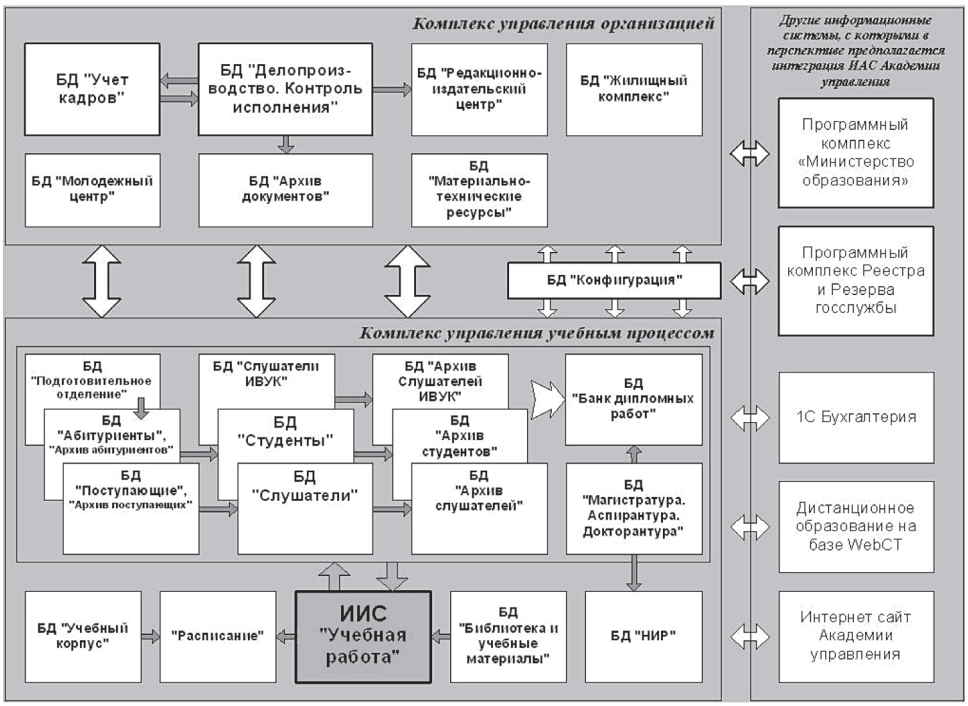


Рис. 1. ИИС Академии управления

информацию, расписание, учебный план, планирование и учет выполнения нагрузки, заседание кафедры. Данная система успешно внедрена в работу кафедры, но ее совершенствование продолжается.

Проблема подготовки отчетных документов

Основной метод подведения итогов учебной деятельности за отчетный период (месяц, семестр, учебный год) в большинстве высших учебных заведений и в Академии управления, в частности, включает формирование отчетов распределения плановой и фактической учебной нагрузки профессорско-преподавательского состава. Для этого профессорско-преподавательский состав заполняет свои индивидуальные планы, которые передаются методистку. Методист, в свою очередь, переносит данные с индивидуальных планов в электронную таблицу среды MS Excel. С помощью вычислений происходит сравнение фактически выполненной учебной нагрузки с плановой и формируются необходимые отчеты.

«Ручной» анализ значительных объемов исходных данных, высокая трудоемкость при обработке информации, большие затраты внимания на выполнение рутинных операций, – все это, в следствии, приводит к низкой оперативности, снижению качества выполняемой работы, возникновению ошибок, а также к некорректно заполненным документам.

В связи с этим, для дальнейшей модернизации ИС было предложено автоматизировать процесс подготовки итоговой документации.

Автоматизация данного процесса позволит:

- исключить многократное переписывание одних и тех же данных;
- сократить время анализа данных;
- устранить допустимость ошибок;
- быстро вносить какие-либо изменения [1].

На данный момент существует множество программных продуктов, решающих эту задачу. Но приобретение, установка и дальнейшее сопровождение таких решений доступно далеко не каждому учебному заведению. Поэтому на кафедре управления информационными ресурсами была разработана и создана информационная система автоматизации подготовки документов учебного процесса.

Информационная система автоматизации подготовки отчетных документов

В качестве системы управления базами данных (далее – СУБД) и средств разработки автоматизированной системы был выбран Microsoft Access.

Microsoft Access является СУБД реляционного типа, в которой присутствуют все инструменты, средства и возможности, характерные для современных систем управления базами данных. [2].

Для решения новых функциональных задач была создана база данных V09_Нагрузка. Она содержит 42 таблицы, 20 из которых связанных с ИИС (ВУЗ), 27 запросов, 12 модулей, 1 макрос, 3 отчета и 2 формы.

Главная страница информационной системы представлена в виде пользовательской формы с возможностью выбора необходимой подсистемы и настройки других параметров. Интерфейс главной пользовательской формы представлен на рис. 2.

Рис. 2. Главная пользовательская форма

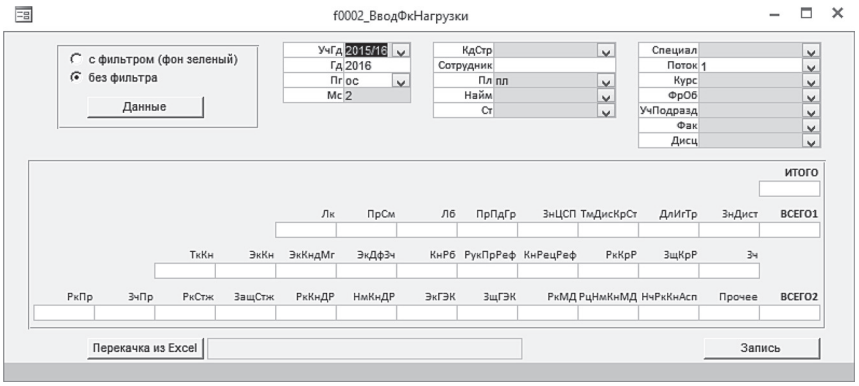


Рис. 3. Форма ввода данных

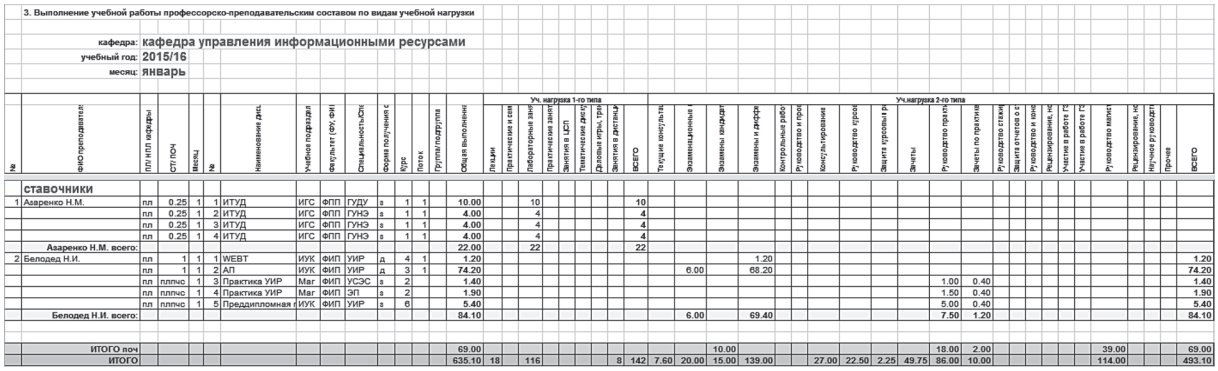


Рис. 4. Выполнение учебной нагрузки профессорско-преподавательским составом по дисциплинам

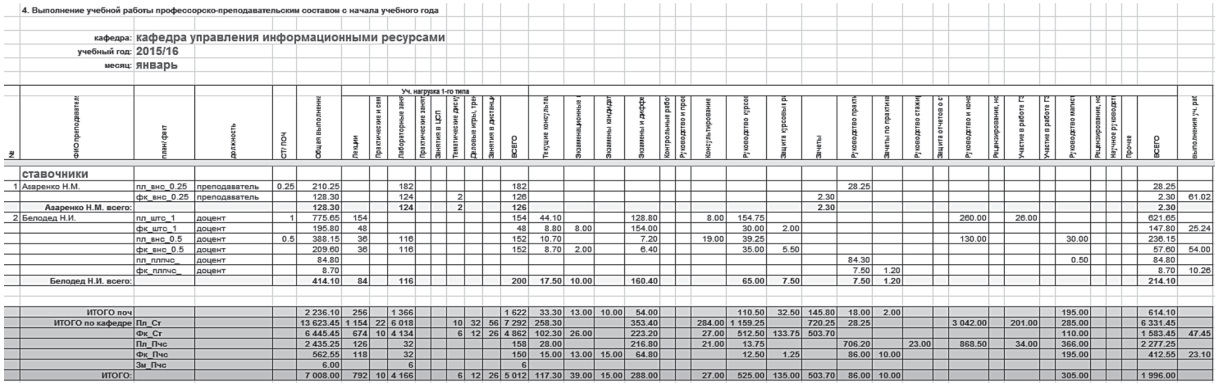


Рис. 5. Промежуточные итоги выполнения нагрузки профессорско-преподавательским составом по видам занятий с начала учебного года

База данных редактируется методистом, преподавателем и администратором информационной системы. Для учета учебной нагрузки пользователю необходимо редактировать данные о фактической нагрузке. Данный процесс может быть выполнен непосредственно в СУБД с использованием формы, либо в среде MS Excel с дальнейшим импортом файла в систему («Перекачка из Excel»). На рис. 3 представлена форма ввода данных.

После ввода данных программа завершает подготовку отчетных документов сообщением: «Расчет нагрузки произведен». На данном этапе реализовано формирование четырех видов выходных документов: выполнение учебной работы профессорско-преподавательским составом, работы по учебным подразделениям, а также по видам учебной нагрузки и с начала учебного года. Ниже представлен пример сформированных отчетов по кафедре «Управление информационными ресурсами» за январь 2016 года (рис. 4–7).

Заключение

На кафедре управления информационными ресурсами Академии управления при Прези-

2. Выполнение учебной работы профессорско-преподавательским составом по учебным подразделениям

кафедра: кафедра управления информационными ресурсами
учебный год: 2015/16
месяц: январь

№	Ф.И.О.преподавателя	Учебная нагрузка (годовая)			Выполнено за месяц															
					всего			по учебным подразделениям												
								ИГС			ИУК						ОДиА			
		пл. ставка	почас.		пл. ставка	почас.		пл. ставка	почас.		пл. ставка	в т.ч. магист.	почас.				пл. ставка	почас.		
			пл	зам		пл	зам		пл	зам			пл	зам	в т.ч. магист. пл	в т.ч. магист. зам		пл	зам
	ставочники																			
1	Авраменко Н.М.	210.25			22.00			22.00												
2	Белодед Н.И.	775.65	84.80		75.40	8.70					75.40		8.70		3.30					
	всего ставочники	9 754.60	1 176.25		474.30	91.80		98.45			375.85	104.40	91.80		21.60					
	всего почасовики		1 269.80			69.00							69.00		52.80					
	всего по кафедре	9 754.60	2 446.05		474.30	160.80		98.45			375.85	104.40	160.80		74.40					
	ИТОГО	12 200.65			635.10			98.45			536.65									

Рис. 6. Выполнение учебной нагрузки профессорско-преподавательским составом по подразделениям и с учетом плановой нагрузки

1. Выполнение учебной работы профессорско-преподавательским составом

кафедра: кафедра управления информационными ресурсами
учебный год: 2015/16
месяц: январь

Учебное подразделение	Факультет	Штатные (часы-пл. ставка)			Почасовики (часы-почас)						ВСЕГО	ИТОГО
					планируемая почас. (пл)			непланируемая почас. (зам)				
		дневная форма пол. обр.	заочная форма пол. обр.	всего	дневная форма пол. обр.	заочная форма пол. обр.	всего	дневная форма пол. обр.	заочная форма пол. обр.	всего	(шт. и поч.)	с начала уч. года
ИГС	ФПП		98.45	98.45							98.45	936.05
всего по ИГС			**98.45**	**98.45**							**98.45**	**936.05**
ИУК	ФИП	161.70	107.40	269.10	25.80	135.00	160.80				429.90	6 146.90
ИУК	ФУ		106.75	106.75							106.75	918.15
Маг. в том числе	ФИП	8.00	96.40	104.40	15.00	59.40	74.40				178.80	656.90
всего по ИУК		**161.70**	**214.15**	**375.85**	**25.80**	**135.00**	**160.80**				**536.65**	**7 065.05**
ИТОГО по кафедре		**161.70**	**312.60**	**474.30**	**25.80**	**135.00**	**160.80**				**635.10**	**8 001.10**

Рис. 7. Выполнение учебной нагрузки профессорско-преподавательским составом по учебным подразделениям

дренте Республики Беларусь была спроектирована и разработана информационная система автоматизации подготовки отчетных документов. Данная система решает следующие задачи:

- надежное хранение данных о запланированной нагрузке преподавателей;
- ввод и хранение данных о фактически выполненной нагрузке;
- предоставление необходимой информации в виде отчетов;
- сравнение выполненной учебной нагрузки преподавателей, кафедр и института с запланированной;
- составление индивидуальной нагрузки преподавателей.
- взаимодействие с другими информационными ресурсами информационной системы кафедры;
- снижение трудозатрат на подготовку документов.

Представленная система может эксплуатироваться независимо от других подсистем комплекса. Все отчеты реализуются в Microsoft Excel и могут быть использованы для дальнейшего анализа и обработки.

Литература

1. **Матюшенко В. А, Белодед Н. И.** Информационная система автоматизации подготовки документов учебного процесса // Управление информационными ресурсами: материалы XII Междунар. науч.-практ. конф. (Минск, 11 декабря 2015 г.). – Мн.: Акад. упр. при Президенте Респ. Беларусь, 2015. – С. 129–130.

2. **Гандерлой, Майк.** Автоматизация Microsoft Access с помощью VBA: [пер. с англ.] / Майк Гандерлой, Сьюзан Сейлз Харкинз. – Москва: Вильямс, 2006. – С. 315–316.

References

1. **Matjushenko V. A, Beloded N. I.** Information system of automation of preparation educational process documents // Information Resources Management: abstracts of the 12th International Scientific and Practical Conference (Minsk, December, 11, 2015). – Minsk, the Academy of Public Administration under the Aegis of the President of the Republic of Belarus, 2015. – Pp. 129–130.

2. **Mike Gunderloy.** Automating Microsoft Access with VBA [Translation from English]. Moscow: Williams, 2006. – Pp. 315–316.

Поступила *10.05.2016*

После доработки *15.05.2016*

Принята к печати *20.05.2016*

Matyushenko V. A., Filon V. U., Beloded N. I.

INFORMATION SYSTEM OF AUTOMATION OF PREPARATION EDUCATIONAL PROCESS DOCUMENTS

The Academy of Public Administration under the Aegis of the President of the Republic of Belarus

Information technology is rapidly conquering the world, permeating all spheres of human activity. Education is not an exception. An important direction of information of education is the development of university management systems. Modern information systems improve and facilitate the management of all types of activities of the institution. The purpose of this paper is development of system, which allows automating process of formation of accounting documents. The article describes the problem of preparation of the educational process documents. Decided to project and create the information system in Microsoft Access environment. The result is four types of reports obtained by using the developed system. The use of this system now allows you to automate the process and reduce the effort required to prepare accounting documents. All reports was implement in Microsoft Excel software product and can be used for further analysis and processing.

Keywords: *information system, automation, database, the actual load of the teaching staff, educational process documents.*

Матюшенко Валентина Александровна

Студентка 5 курса специальности «Управление информационными ресурсами» Академии управления при Президенте Республики Беларусь.

Matyushenko Valentina, a 5th year student of Information Resources Management of the Academy of Public Administration under the Aegis of the President of the Republic of Belarus.

E-mail: valentinkamaybe@gmail.com

Филон Виктория Юрьевна

Студентка 4 курса специальности «Управление информационными ресурсами» Академии управления при Президенте Республики Беларусь.

Filon Victoria, a 4th year student of Information Resources Management of the Academy of Public Administration under the Aegis of the President of the Republic of Belarus.

E-mail: psih_vikyska@mail.ru

Белодед Николай Иванович

Доцент кафедры управления информационными ресурсами Академии управления при Президенте Республики Беларусь, кандидат технических наук, доцент.

Сфера научных интересов: интегрированные информационные системы управления, инновации в образовании.

Beloded Nikolay, Associate Professor of Information Resources Management Department of the Academy of Public Administration under the Aegis of the President of the Republic of Belarus, PhD in. His scientific interests focus on integrated information management systems and innovations in education.

E-mail: nbeloded@gmail.com

РИНЦ, SCIENCE INDEX

Адрес входа: http://elibrary.ru/project_risc.asp

Российский индекс научного цитирования (РИНЦ) – это национальная информационно-аналитическая система, аккумулирующая более 2 миллионов публикаций российских авторов, а также информацию о цитировании этих публикаций из более 3000 российских журналов. Она предназначена не только для оперативного обеспечения научных исследований актуальной справочно-библиографической информацией, но является также и мощным инструментом, позволяющим осуществлять оценку результативности и эффективности деятельности научно-исследовательских организаций, ученых, уровень научных журналов и т. д.

Регистрация авторов

Регистрация пользователя в Научной электронной библиотеке является необходимым условием для получения доступа к полным текстам публикаций, размещенных на платформе eLIBRARY.RU, независимо от того, находятся ли они в открытом доступе или распространяются по подписке. Зарегистрированные пользователи также получают возможность создавать персональные подборки журналов, статей, сохранять историю поисковых запросов, настраивать панель навигатора и т.д.

Для работы с авторским профилем в системе SCIENCE INDEX также необходимо вначале зарегистрироваться, но уже в качестве автора. Регистрация автора в SCIENCE INDEX объединена с регистрацией пользователя на портале Научной электронной библиотеки eLIBRARY.RU. Для регистрации в SCIENCE INDEX нужно просто заполнить несколько дополнительных полей.

Google Академия

Homepage

Publisher: Belarusian National Technical University
Society/Institution: Belarusian National Technical University
Country of publisher: Belarus
Platform/Host/Aggregator: Elpub.ru
Date added to DOAJ: 12 Feb 2016
LCC Subject Category: Technology: Technology (General): Industrial engineering. Management engineering: Information technology
Publisher's keywords: complicated technical systems, system analysis, data processing, information technologies, information security
Language of fulltext: Russian, English
Full-text formats available: PDF

PUBLICATION CHARGES

Article Processing Charges (APCs): No.
Submission Charges: No.
Waiver policy for charges? No.

EDITORIAL INFORMATION

Double blind peer review
Editorial Board
Aims and scope
Instructions for authors
Time From Submission to Publication: 8 weeks

More