Научно-технический журнал

Информационные системы и технологии

№ 2 (64) март-апрель 2011

Издается с 2002 года. Выходит 6 раз в год

Учредитель – Федеральное государственное образовательное учреждение высшего профессионального образования «Государственный университет — учебно-научно-производственный комплекс»

Сдано в набор 15.02.2011 г.
Подписано в печать 25.02.2010 г.
Формат 70x108 1/16.
Усл. печ. л. 7,5. Тираж 300 экз.
Заказ №_____
Отпечатано с готового оригинал-макета на полиграфической базе ОрелГТУ
302030, г. Орел, ул. Московская, 65

Подписной индекс 15998
по объединенному каталогу
«Пресса России»

Журнал входит в **Перечень ведущих рецензируемых научных журналов и изданий**, определенных ВАК для публикации трудов на соискание ученых степеней кандидатов и докторов наук.

Рубрики номера

Адрес учредителя журнала

302020, г. Орел, Наугорское шоссе, 29
(4862) 42-00-24; www.ostu.ru;
E-mail: admin@ostu.ru

Адрес редакции

302020, г. Орел, Наугорское шоссе, 40
(4862) 43-40-39; www.ostu.ru; E-mail: isit@ostu.ru

Зарег. в Федеральной службе по надзору в сфере связи и массовых коммуникаций.
Св-во о регистрации средства массовой информации ПИ № ФС77-35333 от 17.02.2009 г.

Scientific and technical journal

Information Systems and Technologies

№ 2 (64) March - April 2011

The journal is published since 2002, leaves six times a year

The founder –State University-Education-Science-Production Complex

It is handed over in a set of 15.02.2011,
25.02.2011 are sent for the press
Format 70x108 1/16.
Press conditions L. 7,5. Circulation 300 copies
The order №_____
It is printed from a ready dummy on polygraphic base of OrelSTU
302030, Orel, street Moscow, 65

Index on the catalogue of the «Pressa Rossii» 15998

Journal is included into the list of the Higher Examination Board for publishing the results of thesises for competition the academic degrees.

In this number

The edition

Konstantinova G.A.
Motina A.I.
Mitin A.A.

The address of the founder of magazine

302020, Orel, Highway Naugorskoye, 29
(4862) 42-00-24; www.ostu.ru;
E-mail: admin@ostu.ru

The address of the edition

302020, Orel, Highway Naugorskoye, 40
(4862) 43-40-39; www.ostu.ru;
E-mail: isit@ostu.ru

Journal is registered in Federal Departament for Mass Communication.
The certificate of registration
ПИ № ФС77-35333 from 17.02.2009.

СОДЕРЖАНИЕ

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И КОМПЬЮТЕРНЫЕ СЕТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

CONTENT

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ

УДК 004.045; 004.51

О.В. АМЕЛИНА

ОБЪЕКТНО-ОРИЕНТИРОВАННАЯ РЕАЛИЗАЦИЯ ЯЗЫКА ОПИСАНИЯ ПРОЦЕССОВ ДИАЛОГА ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Статья посвящена объектно-ориентированной реализации языка описания процессов диалога для информационных систем средствами языка Object Pascal, которая строится исходя из формальной семантики языка взаимодействующих последовательных процессов и метода чисто функциональной реализации.

Ключевые слова: *объектно-ориентированное программирование; интерфейс пользователя; процессы диалога; язык описания процессов диалога; информационные системы.*

Большие возможности, предоставляемые современными средами программирования, такими, как Borland Delphi или Microsoft Visual Studio, оказываются недостаточными для создания приложений, имеющих развитый графический интерфейс пользователя (ГПИ). Набор визуальных компонент и событийная модель управления не помогут, например, в случае, когда несколько параллельно работающих обработчиков событий, совместно изменяя общее состояние диалога, могут повести себя непредсказуемым образом. Для разрешения подобного рода проблем в работе [1] предлагается описать диалог на формальном языке параллельных процессов, например, на CSP [2], а затем транслировать это описание в структуры обработчиков событий и конструкции языка программирования.

В указанной работе [1] предложен язык описания процессов диалога, разработаны его синтаксис, семантика и метод реализации средствами функционального языка Haskell. Учитывая, что объектно-ориентированные технологии разработки информационных систем являются одними из наиболее распространенных и эффективных, в данной статье предлагается реализация языка процессов диалога средствами объектно-ориентированного языка Object Pascal. Синтаксис и семантика языка процессов диалога будут заимствованы из работы [1].

Процесс – это математическая абстракция взаимодействия системы и ее окружения. Будем употреблять термин «процесс» для обозначения поведения объектов диалога, так как оно может быть описано в терминах ограниченного набора событий, выбранного в качестве его алфавита. В описании языка используются следующие синтаксические элементы:

```
d ∈ ProcDef
p ∈ Proc
op ∈ Op
np ∈ ProcName
ne ∈ EventName
e ∈ Event
exp ∈ Exp
x ∈ Var
v ∈ Value
```

,

где ProcDef – определения процессов; Proc – выражения, определяющие процесс; Op – операции композиции процессов; ProcName – множество возможных имён процессов; EventName – множество возможных имён событий; Event – множество событий; Exp – свободные от побочного эффекта выражения языка Object Pascal; Var – переменные; Value – значения.

Далее определим структуру объектов языка в форме контекстно-свободных грамматик и параллельно будем транслировать это описание в конструкции Object Pascal.

События – это объекты, служащие для синхронизации процессов. Если событие отражает синхронизацию процесса с окружением, то есть с пользователем, то в момент его совершения происходит ввод данных от пользователя к функциональному ядру или вывод на экран данных, хранящихся в функциональном ядре. Если синхронизируются два процесса, то событие одновременно включает в себя передачу данных между процессами. В нашей реализации будем использовать три вида событий:

```
e ::= ne | ne!exp | ne?x
```

Обозначение события может быть одновременно и обозначением канала, по которому передаются данные. Таким образом, ne!exp означает передачу значения exp по каналу ne (событие вывода), а ne?x означает получение значения переменной x по каналу ne (событие ввода).

В соответствии с этими определениями разработаем структуру классов, их иерархия представлена на рисунке 1.

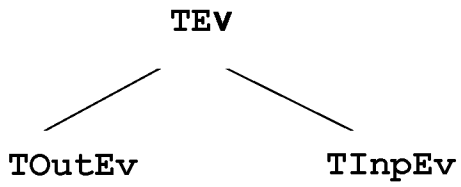


Рисунок 1 – Иерархия классов событий

События класса TEv имеют в состоянии только имя (EvName - для хранения достаточно строки из 8 символов – Type STR8 = string[8]) и служат для синхронизации процессов диалога.

```
TEv = class
    public
      evName:Str8;
   end;
```

События классов TInpEv и TOutEv вместе с именем события имеют имя канала chName. В интерфейсе пользователя события класса TInpEv используются для получения данных от устройств ввода, поэтому они содержат данные о визуальном представлении события (Тип TevVis определяется пользователем). События класса TOutEv используются для передачи данных от пользовательского интерфейса к функциональному ядру. Эти данные имеют форму параметров. Тип Tparam — абстрактный класс с методом parToStr, форматирующим параметр в строку. В классе TParCoord форматируется координата; в классе TParPnt – форматируется точка (две координаты).

```
TInpEv = class(TEv)
```

```
 public
   chName: Str8;
   evVis: TevVis;
end;

TOutEv=class(TEv)
 Public
   evName:Str8;
   chName: Str8;
   chVal: TParam;
   constructor Create(ev: Str8; v:TParam);
end;
```

Реализация процессов диалога строится на основе следующих определений абстрактного синтаксиса:

d ::= np (x_1, … x_k) = p

p ::= Exit | e→p | e_1→p_1 [] e_2→p_2 … [] e_n→p_n | p Op p_1

| case exp of v_1→p_1 ; v_2→p_2 … ; v_m→p_m

op ::= [e_0, e_1,…, e_k] | Δ | [> | >> .

Определение процесса d ставит в соответствие его имени np со списком формальных параметров (x_1, … x_k) выражение p, определяющее процесс. Процесс может быть:

I) префиксом, вида e→p;

II) альтернативой – e_1→p_1 [] e_2→p_2 … [] e_n→p_n

III) композицией процессов p Op p_1, помеченной операциями:

1)[e_0, e_1,… e_k] – параллельное выполнение с синхронизацией по событиям e_0, e_1,… e_k;

2) Δ – прерывание;

3) [>- отключение;

4) >> – последовательное выполнение.

IV) процессом, зависящим от окружения локальных переменных, определяется в виде: case exp of v_1→p_1 ; v_2→p_2 … ; v_m→p_m . Он ведёт себя в зависимости от вычисленного значения выражения exp.

Коротко поясним семантику операторов языка процессов. Правило для оператора префикса можно сформулировать так: процесс P после участия в событии e ведет себя как P.

Для оператора выбора справедливо следующее. Если процесс P может синхронизироваться по событию e и далее вести себя как процесс P', то процесс P [] Q тоже может синхронизироваться по событию e и далее вести себя как P' или процесс Q может синхронизироваться по событию e и далее вести себя как Q'.

Оператор параллельной композиции вида P[e_0, e_1,…, e_k]Q позволяет построить систему из двух процессов P и Q, работающих независимо друг от друга, если происходят события, не входящие во множество {e_0, e_1,… e_k}. Но когда такое событие произойдет, параллельные события должны синхронизироваться. В этом случае, если один процесс готов обработать это событие, а другой нет, то первый должен заблокироваться до тех пор, пока второй не достигнет точки синхронизации.

Оператор прерывания в выражении P Δ Q позволяет описать композицию из двух процессов, в которой первый процесс P, нормально развиваясь, в любой момент времени может быть прерван вторым процессом Q. Прерывание происходит тогда, когда в окружении появляется возможность наступления события, в котором может

участвовать процесс `Q`. За этим событием второй процесс начинает определять поведение композиции в целом, а первый станет активным только по завершении второго.

Оператор отключения в выражении `P [> Q` позволяет описывать поведение процесса `P`, который может быть отключён процессом `Q`.

Правило для оператора последовательной композиции утверждает, что если процесс `P` по событию `e` преобразуется в процесс `P'`, то последовательная композиция процессов `P >> Q` по этому событию преобразуется в `P' >> Q`. Если же в последовательной композиции первый процесс завершил работу, то композиция ведет себя как второй процесс.

В соответствии с данными определениями на Object Pascal процесс можно представить следующим образом:

```
TProc = class
 private
   rho:TList;
 public
  procedure menue; virtual;abstract;
  function isInmenue(ev:str8):boolean;virtual;abstract;
  function next (ev: TOutEvent):TProc;virtual;abstract;
end;
```

`TProc` – это абстрактный класс, потомками которого будут являться классы, реализующие перечисленные выше виды процессов. Описание методов приведем позднее, так как реализованы они будут в классах-потомках.

Каждый процесс класса `TProc` имеет окружение связей переменных `rho` типа TList, который является списком связей переменных с их окружением. Связь реализуется объектом класса `TAssoc`:

```
TAssoc = class
 public
   key:string;
   val: TParam;
   constructor Create(k: Str8; v: TParam);
   function show:Str80;
end;
```

Данный класс имеет поле `key` типа `string` для хранения имен переменных и поле `val` типа `TParam` для хранения значения. Эти же значения используются и при передаче параметров функциональному ядру.

В соответствии с абстрактным синтаксисом языка процессов диалога иерархия классов процессов представлена на рисунке 2.

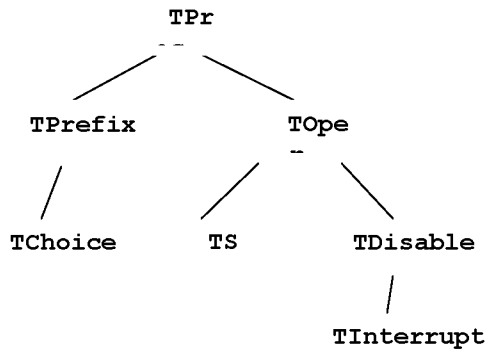


Рисунок 2 – Иерархия классов процессов

Далее приведем реализацию иерархии классов на Object Pascal.

```
TPrefix=class(TProc)
  private
    evName:Str8;
    chName:Str8;
    after:TProc;
    stTr: StateTrans;
  public
    constructor Create(ev: Str8; ch: Str8; st: StateTrans;
p,pa:TProc);
    procedure menue; override;
    function isInmenue(ev:str8):boolean;override;
    function next (ev: TOutEvent):TProc;override;
  end;

  TChoice=class(TProc)
   private
    alter:TProc;
   public
    constructor Create(ev: Str8; ch: Str8; st: StateTrans;
p,pa:TProc);
    procedure menue; override;
    function isInmenue(ev:str8):boolean;override;
    function next (ev: TOutEvent):TProc;override;
  end;
```

Для реализации композиции процессов введем базовый класс, экземпляр которого будет хранить левый и правый операнды композиции процессов.

```
  TOper=class(TProc)
   private
    left,right:TProc;
   public
    constructor Create(l,r:TProc);
  end;
```

Далее описаны классы, реализующие операции последовательного выполнения, отключения и прерывания.

```
  TSeq= class(TOper)
   public
    procedure menue; override;
    function isInmenue(ev:str8):boolean;override;
    function next (ev: TOutEvent):TProc;override;
  end;
  TDisable=class(TSeq)
   public
    procedure menue; override;
    function isInmenue(ev:str8):boolean;override;
    function next (ev: TOutEvent):TProc;override;
  end;
  TInterrupt=class(TDisable)
   public
    function next (ev: TOutEvent):TProc;override;
  end;
```

Каждый процесс класса `TProc` имеет методы: `menue` – возвращает меню процесса; `isInMenue` – проверяет, может ли событие участвовать в данном процессе; `next` – для заданного события возвращает следующий за ним процесс.

Метод `menue` рекурсией по структуре объекта-процесса строит список

событий. В случае, если процесс – префикс, то меню – список, содержащий EvName; если процесс – альтернатива, то меню – список с головой EvName и хвостом – меню альтернативного процесса alter. Если процесс принадлежит классу TOper, то его меню – конкатенация (сцепление списков) меню его операндов.

Аналогично реализуется метод isInmenue.

```
function TPrefix.isInMenue(ev:Str8):Boolean;
begin
  isInMenue:=evName = ev;
end;

function TChoice.isInMenue(ev:Str8):Boolean;
begin
  isInMenue:=evName = ev or alter.isInMenue(ev);
end;

function TSeq.isInMenue(ev:Str8):Boolean;
begin
  isInMenue:=right.isInMenue(ev);
end;

function TDisable.isInMenue(ev:Str8):Boolean;
begin
  isInMenue:= left.isInMenue(ev) or right.isInMenue(ev);
end;

function TInterrupt.isInMenue(ev:Str8):Boolean;
begin
  isInMenue:= left.isInMenue(ev) or right.isInMenue(ev);
end;
```

Поведение процессов реализуется методом next. Для класса TPrefix этот метод, получив событие **ev**, сравнивает его со своим **evName**, в случае равенства происходит следующее:

1) в окружение rho добавляется связь имя канала – значение канала:

```
rho.add(TAssoc.Create(chName, ev.chVal))
```

2) процесс-продолжение получает новое окружение:

```
after.rho:=rho
```

3) результат метода next – процесс-продолжение.

Если равенства не обнаружено – результат – nil (пустой процесс – Bleep).

Для класса TChoice метод next работает следующим образом. Если для заданного события применим метод как и для класса TPrefix, то он применяется, иначе работает метод next процесса alter.

Для класса TSeq событие **ev** обрабатывается процессом left и формируется следующий процесс p:

```
p := left.next(ev).
```

Если этот процесс имеет абстрактный класс TProc (это соответствует процессу Exit), значит, процесс left завершил свою работу и следующим процессом будет right; иначе следующий процесс – последовательная композиция процессов p и right.

Для класса TDisable делается попытка обработать событие **ev** процессом right с целью проверить возможность отключения процесса:

```
q:= right.next(ev).
```

Если полученный следующий процесс равен `nil`, то должен работать левый процесс с возможностью его отключения правым процессом:

```
if q = nil then next := TDisable.Create(left.next(ev),right)
else next := q {если же он не nil, то он и работает}.
```

Для класса `TInterrupt`, как и для класса `TDisable`, делается попытка выполнения правого процесса. Если это возможно (т.е. следующий процесс `q` не `nil`), тогда следующий процесс – последовательность `q` и `self` :

```
next:= TSeq.Create(q,self),
```

иначе `next:= TInterrupt.Create(left.next(ev),right)`.

В заключение отметим, что предлагаемый метод реализации языка процессов диалога позволяет разработать алгоритм управления логикой диалога, а также инструментарий для проектирования поведения пользовательского интерфейса.

СПИСОК ЛИТЕРАТУРЫ

1. Гордиенко А.П. Процессы диалога // Известия ОрёлГТУ. Серия «Информационные системы и технологии».– 2005.– № 2(8). – С. 50-61.
2. Хоар Ч. Взаимодействующие последовательные процессы.– М.: Мир, 1989.

Амелина Ольга Викторовна
ФГОУ ВПО «Госуниверситет – УНПК», г. Орел
Кандидат экономических наук, доцент кафедры «Информационные системы»
Тел.: 8 909 229 88 00
E-mail: shu-shu-oa@yandex.ru

O.V. AMELINA

OBJECT-ORIENTED REALIZATION OF LANGUAGE OF DESCRIPTION PROCESSES OF DIALOGUE FOR THE INFORMATIVE SYSTEMS

The paper is devoted to an object-oriented implementation of the dialog process defintion language for the information systems using Object Pascal. It is built on the formal semantics of interacting sequential processes and on a purely functional implementation of the language.

Keywords: *Object-oriented programming, user interface, processes of dialogue, language for describing the processes of dialogue, information systems.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Gordienko A.P. Processy' dialoga // Izvestiya OryolGTU. Seriya «Informacionny'e sistemy' i texnologii», 2005. – №2 (8). – S.50-61.
2. Xoar Ch. Vzaimodejstvuyushhie posledovatel'ny'e processy'. – M.: Mir, 1989.

УДК 004.051

О.А. БИСТЕРФЕЛЬД

МЕТОДИКА АВТОМАТИЗИРОВАННОГО ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ПРОГРАММ И ПРОГРАММНЫХ КОМПЛЕКСОВ

Для автоматизированного оценивания эффективности программных средств при их проектировании и в процессе эксплуатации предлагается применять программу расчета показателя эффективности программ и программных комплексов. В программе используется критерий, учитывающий минимизируемые и максимизируемые показатели характеристик оцениваемых программных средств с заданными весовыми коэффициентами, обладающий линейной чувствительностью к значениям показателей характеристик.

Программа содержит базу данных, запросы к базе данных, экранные формы для доступа к базе данных и отчеты с обработанными данными базы данных. База данных обеспечивает хранение данных по программам и комплексам (их вариантам), а также значения показателей их характеристик. Постоянно пополняемая по ходу выполнения проекта коллекция данных может быть использована при управлении качеством проектных работ и контроле целостности комплексов в процессе эксплуатации.

Ключевые слова: *программное обеспечение; качество; эффективность; характеристики; оценивание.*

ВВЕДЕНИЕ

Президент России Дмитрий Медведев в своем послании Федеральному Собранию выделил пять основных приоритетных направлений по модернизации экономики и технологическому развитию, являющихся ключевыми для выхода России на новый технологический уровень. Одним из таких направлений стало широкое использование информационных технологий, без которых сегодня невозможно заниматься стратегическим планированием [1].

Тенденции развития информационно-коммуникационных технологий, диктуемые потребностями общества в информационном обеспечении всех сторон человеческой деятельности, влекут за собой непрерывный рост сложности программ и баз данных. Масштабы таких функционально законченных прикладных программных комплексов достигают сотен тысяч и миллионов строк текста, а объемы баз данных – от сотен мегабайт до десятков гигабайт и выше. Трудоемкость создания таких комплексов и баз данных измеряется сотнями и тысячами человеко-лет, а длительность жизненного цикла может составлять десяток и более лет [2].

Динамика общественных процессов требует значительного ускорения разработки прикладных программ и баз данных, снижения трудоемкости и обеспечения возможности их совершенствования в процессе эксплуатации, наращивания или изменения функций при изменении требований к ним со стороны пользователей. В этих условиях является актуальной задача автоматизации таких процессов, как:

- сравнение эффективности различных вариантов реализации программных средств при их проектировании;
- отслеживание эффективности программных средств в процессе их эксплуатации.

Автором разработана программа расчета показателя эффективности программ и программных комплексов [3]. Функциональное назначение программы –

автоматизированный расчет показателя эффективности для различных вариантов реализации программных средств, анализ эффективности программных средств в процессе их эксплуатации.

ХАРАКТЕРИСТИКИ КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ГОСТ Р ИСО/МЭК 9126-93 определяет шесть характеристик, которые с минимальным дублированием описывают качество программного обеспечения. Данные характеристики образуют основу для дальнейшего уточнения и описания качества программного обеспечения [4].

Функциональные возможности (Functionality)

Набор атрибутов, относящихся к сути набора функций и их конкретным свойствам. Функциями являются те, которые реализуют установленные или предполагаемые потребности.

Надежность (Reliability)

Набор атрибутов, относящихся к способности программного обеспечения сохранять свой уровень качества функционирования при установленных условиях за установленный период времени.

Практичность (Usability)

Набор атрибутов, относящихся к объему работ, требуемых для использования и индивидуальной оценки такого использования определенным или предполагаемым кругом пользователей.

Эффективность (Efficiency)

Набор атрибутов, относящихся к соотношению между уровнем качества функционирования программного обеспечения и объемом используемых ресурсов при установленных условиях.

Сопровождаемость (Maintainability)

Набор атрибутов, относящихся к объему работ, требуемых для проведения конкретных изменений (модификаций).

Мобильность (Portability)

Набор атрибутов, относящихся к способности программного обеспечения быть перенесенным из одного окружения в другое.

Существуют только несколько общепринятых метрик для вышеперечисленных характеристик. Организации и группы по стандартизации могут устанавливать свои собственные модели процесса оценивания и методы формирования и проверки метрик, связанных с этими характеристиками, для охвата различных областей применения и стадий жизненного цикла [4].

ОСНОВНЫЕ ЭТАПЫ ПРОЦЕССА ОЦЕНИВАНИЯ КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Процесс состоит из трех стадий: установление (определение) требований к качеству, подготовка к оцениванию и процедура оценивания. Данный процесс может применяться в любой подходящей фазе жизненного цикла для каждого компонента программной продукции [4].

В практике применения рассматриваемой методики процесс оценивания использовался на разных стадиях жизненного цикла программ неоднократно: при

проектировании (для выбора рациональных проектных решений), при сертификации программ (для обоснования выбора варианта реализации), к набору показателей в этих двух случаях добавлялись и экономические, например, трудоемкости проектирования и трудозатраты на эксплуатацию вариантов реализации. При эксплуатации цель оценки – контроль целостности систем (своевременное обнаружение деградации показателей, например, из-за чрезмерного заполнения баз данных и т.д.)

Установление требований к качеству

Целью начальной стадии является установление требований в терминах характеристик качества и возможных комплексных показателях (подхарактеристик). Требования выражают потребности внешнего окружения для рассматриваемой программной продукции и должны быть определены уже в начале разработки.

Так как программная продукция разделяется на основные компоненты, требования для продукции в целом могут отличаться от требований для отдельных компонентов [4]. Сам набор требований может изменяться на разных стадиях жизненного цикла продукции и отражать изменение целей оценивания.

Подготовка к оцениванию

Целью второй стадии является подготовка основы для оценивания. На этой стадии осуществляются выбор метрик (показателей качества), определение уровней ранжирования, определение критерия оценки.

Способ, которым определялись характеристики качества, не допускает их непосредственного измерения. Существует потребность в установлении метрик (показателей), которые соотносятся с характеристиками программной продукции. Каждый количественный признак и каждое количественно оцениваемое взаимодействие программного обеспечения с его окружением, которые соотносятся с характеристикой, могут быть приняты в качестве метрики (показателя).

Метрики могут по-разному зависеть от окружения и фаз разработки процесса, в которых они используются. Метрики, используемые в процессе разработки, должны быть соотнесены с соответствующими метриками пользователя, потому что метрики из представления пользователя являются решающими.

Количественные признаки могут быть измерены, используя метрики качества. Результат, т.е. измеренное значение, отображается в масштабе. Данное значение не показывает уровень удовлетворения требований. Для этой цели шкалы должны быть разделены на диапазоны, соответствующие различным степеням удовлетворения требований.

Для определения качества продукции результаты оценивания различных характеристик должны быть подытожены. Оценщик должен подготовить для этого процедуры [4]. Предлагается использовать для расчета обобщенного показателя описанную ниже программу [3].

Процедура оценивания

Последняя стадия включает измерение, ранжирование и оценку. Результатом является заключение о качестве программной продукции. С учетом других факторов, таких, как время и стоимость, принимается решение руководством по приемке или отбраковке, по выпуску или невыпуску программной продукции [4] (при проектировании и сертификации), по мерам восстановления целостности продукции (при эксплуатации).

ИНТЕГРАЛЬНАЯ ОЦЕНКА КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Известен целый ряд критериев синтеза оптимальных модульных систем обработки данных [5], основанных на минимизации различных характеристик (показатели характеристик Pmni, например, время обслуживания заданного множества запросов пользователей системы, суммарное времени загрузки системы и обслуживания запросов и т.д.). Для систематической интегральной оценки качества проектирования программ, программных комплексов и системы в целом необходим учет дополнительных характеристик, которые должны быть максимизированы (показатели характеристик Pmxj). В программе [3] используется обобщенный показатель K, учитывающий и минимизируемые (Pmni), и максимизируемые (Pmxj) показатели характеристик с весовыми коэффициентами kpi и kpj:

$$K = C_{\Sigma} \prod_i P_{mni}^{-k_{pi}} \prod_j P_{mxj}^{k_{pj}} \quad . \tag{1}$$

Постоянная C_{Σ} в выражении (1) может быть использована для масштабирования значений показателей для удобства графического представления результатов при оценке вариантов технических решений программ, установлении, оценке и контроле уровня целостности системы в целом и компонентов системы. Весовые коэффициенты, как правило, выбираются экспертной группой, учитывается и конкретная цель оценивания.

Критерий обладает линейной чувствительностью к значениям показателей характеристик, при которой относительные изменения любого показателя приводят к таким же изменениям K (с учетом весовых коэффициентов):

$$\frac{\Delta K}{K} = -\sum_i k_{pi} \frac{\Delta P_{mni}}{P_{mni}} + \sum_j k_{pj} \frac{\Delta P_{mxj}}{P_{mxj}} \quad .$$

ПРОГРАММА РАСЧЕТА ПОКАЗАТЕЛЯ ЭФФЕКТИВНОСТИ ПРОГРАММ И ПРОГРАММНЫХ КОМПЛЕКСОВ

Программа расчета показателя эффективности программ и программных комплексов содержит базу данных, запросы к базе данных, экранные формы для доступа к базе данных и отчеты с обработанными данными базы данных. база данных обеспечивает хранение данных по системе в целом, по компонентам системы (программы и программные комплексы), а также значения показателей их характеристик.

Информационная модель программы представлена на рисунке 1.

После ввода показателей автоматизированно определяются значения критерия и могут быть выведены отчеты со сравнительными оценками программ. Формы представления результатов расчета, как готовые разделы документов, различны: табличный отчет (рис. 2, а), табличный отчет с диаграммой (рис. 2, б), диаграмма (рис. 2, в).

Постоянно пополняемая по ходу выполнения проекта коллекция данных обеспечивает оценки вариантов технических решений программ и может быть использована при управлении качеством работ и контроле соответствия создаваемой системы требованиям ТЗ, а также при контроле целостности системы (компонентов) в процессе эксплуатации.

Незаменима методика, с точки зрения сокращения трудозатрат и сроков разработки соответствующих разделов документации, необходимой для сертификации программных продуктов в условиях, когда для сложных

специализированных систем сертифицируются десятки и сотни программ с достаточно однотипными требованиями.

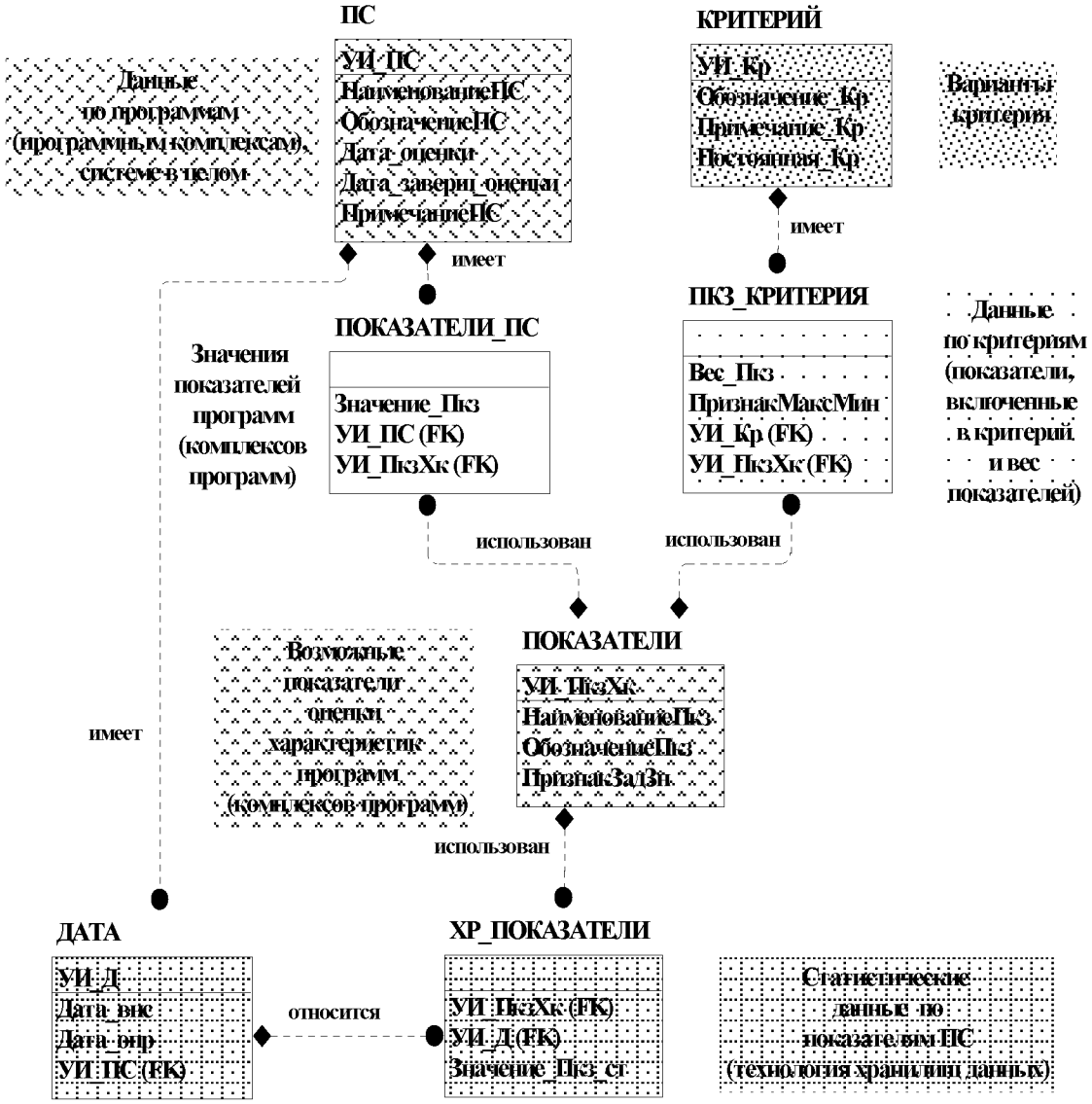


Рисунок 1 – Информационная модель программы расчета показателя эффективности программ и программных комплексов

Сравнение программных средств (по критерию К)

Показатели	Максимизируемые										Минимизируемые				Критерий
	Тнар	Рнад/Тзад	Рполн/Тзад	Ракт	Рбум/Тзб	Рмаш/Тзм	Ркорр/Тзкр	Ркомф/Тзкф	Рвозд/Тзад	Рисд	Трр	Тэксп+Тэксп	Твос	Тполн	
Весовые коэффициенты / ПС	1	1	1	1	1	1	1	1	1	1	1	1	2	1	(постоянная С = 1Е-18)
Комплекс "Информация по продукции"	3218	0,9	0,9	0,9	0,97	0,97	0,95	0,999	0,95	0,99	19,4	1	1	1000	5,7783
		10	10		10	10	10	10	10			10			
Комплекс "Информация по продукции" Вариант 2	3618	0,95	0,9	0,9	0,97	0,97	0,95	0,999	0,95	0,99	17,4	2	2	1000	1,8598
		10	10		10	10	10	10	10			10			

а)

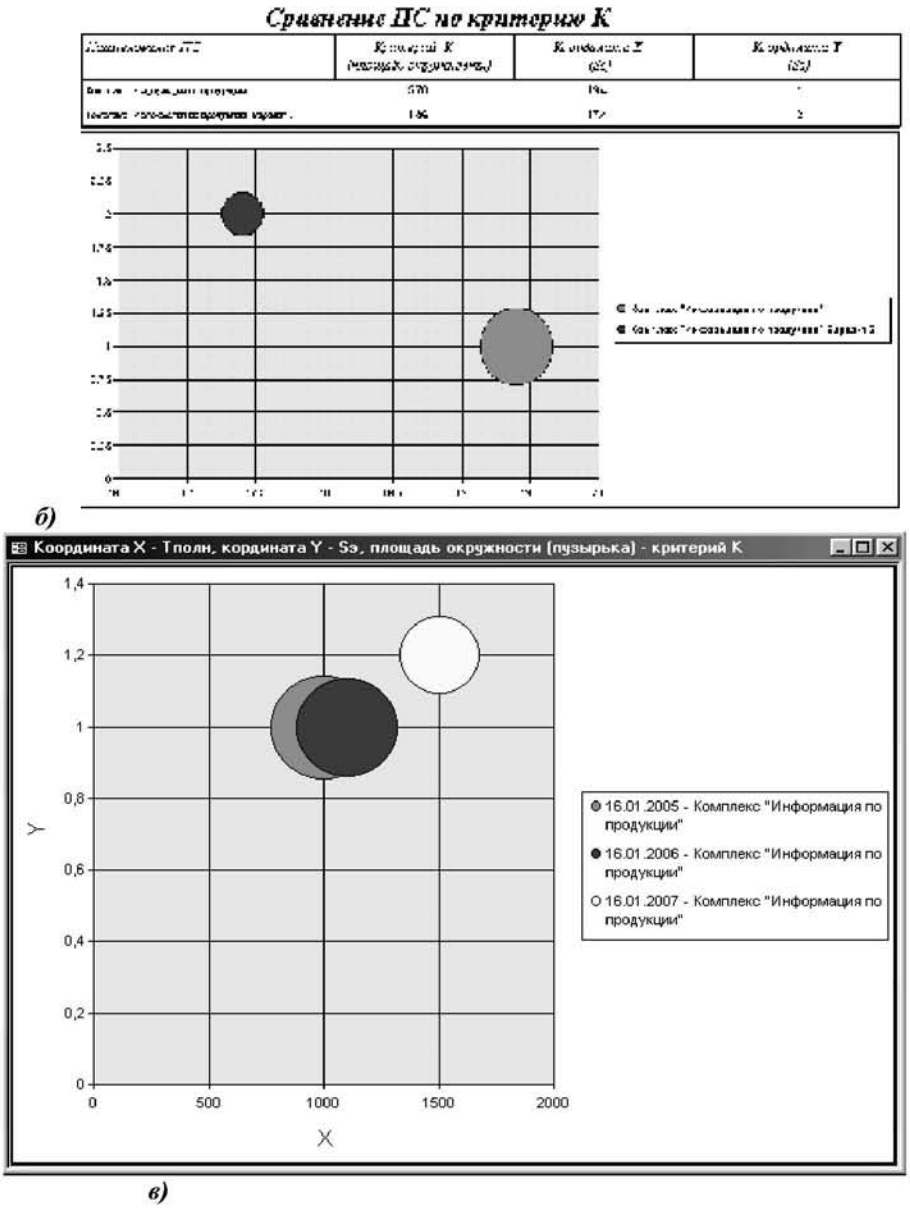


Рисунок 2 – Формируемые программой отчеты и формы с диаграммами

СПИСОК ЛИТЕРАТУРЫ

1. Послание Президента РФ Д.А. Медведева Федеральному Собранию от 12 ноября 2009 года.
2. Боэм Б.У. Инженерное проектирование программного обеспечения: пер. с англ.; под ред. А.А. Красилова. – М.: Радио и связь, 1985. – 512 с.
3. Программа расчета критерия эффективности программ и программных комплексов: свидетельство об отраслевой регистрации разработки №8232 / О.А. Бистерфельд, Н.Ю. Хлебников. – № 50200700938; заявл. 26.04.2007; опубл. 3.05.2007. – Инновации в науке и образовании. – № 4(27). – 1 с.
4. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции, характеристики качества и руководства по их применению.
5. Мамиконов А.Г., Кульба В.В. Синтез оптимальных модульных систем обработки данных. – М.: Наука, 1986. – 276 с.

Бистерфельд Ольга Александровна
Рязанский государственный университет имени С.А. Есенина, г. Рязань
Кандидат технических наук, доцент кафедры информатики и вычислительной техники
Тел.: (4912) 21-55-43
E-mail: bist19@yandex.ru

O. A. BISTERFELD

METHOD OF AUTOMATICALLY EVALUATION OF THE EFFICIENCY OF SOFTWARE

For automated performance evaluation of software tools in their design and operation are encouraged to use a calculation program of the efficiency of computer programs and software packages. The program uses a criterion that takes into account and minimized, and maximized indicators characteristics evaluated the software with predetermined weighting factors. Criterion has a linear sensitivity to the values of indices of characteristics. The program contains a database, query to the database, on-screen forms to access the database and reports to the processed data of the database. The database provides storage for programs and complexes (their options), as well as the values of their characteristics. Constantly replenished in the course of the project data collection can be used in the management of quality design work and integrity monitoring systems in operation.

Keywords: software; quality; efficiency; performance; evaluation.In the paper description of the software intended for registration and complex processing of the diagnostic information at realization of an electric method of diagnosing of the bearing is presented.

Keywords: *automation process of measurement; USB 2.0; mikrokontaktirovanie; NIT.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Poslanie Prezidenta RF D.A. Medvedeva Federal'nomu Sobraniyu ot 12 noyabrya 2009 goda.
2. Boe`m B.U. Inzhenernoe proektirovanie programmnogo obespecheniya: per. s angl.; pod red. A.A. Krasilova. – M.: Radio i svyaz', 1985. – 512 s.
3. Programma raschyota kriteriya e`ffektivnosti programm i programmny`x kompleksov: svidetel'stvo ob otraslevoj registracii razrabotki № 8232 / O.A. Bisterfel'd, N.U. Xlebnikov. – № 50200700938; zayavl. 26.04.2007; opubl. 3.05.2007. – Innovacii v nauke i obrazovanii. – № 4(27). – 1 s.
4. GOST R ISO/ME'K 9126-93. Informacionnaya texnologiya. Ocenka programmnoj produkcii, xarakteristiki kachestva i rukovodstva po ix primeneniyu.
5. Mamikonov A.G., Kul'ba V.V. Sintez optimal'ny'x modul'ny'x sistem obrabotki danny'x. – M.: Nauka, 1986. – 276 s.

УДК 004.932.4

В.Т. ЕРЕМЕНКО, А.В. ТЮТЯКИН, А.А. КОНДРАШИН

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ОБРАБОТКИ ИЗОБРАЖЕНИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ДИАГНОСТИКИ

Данная статья посвящена решению ряда задач в рамках обработки изображений в системах технической и медицинской диагностики. В статье обоснована применимость известных способов и алгоритмов обработки изображений для улучшения и реставрации графической информации в системах диагностики. Определены элементы профилей автоматизированной обработки изображений, методы и алгоритмы. Представлены базовые принципы выбора данных профилей.

Ключевые слова: *диагностика; обработка изображений; профиль; выбор профилей обработки изображений.*

ВВЕДЕНИЕ

Большинство задач технической и медицинской диагностики сводится к анализу черно-белых полутоновых изображений, получаемых методами рентгенографии, ультразвуковой локации, магнитно-резонансного сканирования (МРС) и т.п. [1, 6, 9]. В большинстве практических случаев качество изображений, получаемых посредством диагностической аппаратуры, не позволяет принимать корректные решения на основе их анализа. Это требует предварительной обработки этих изображений с целью улучшения их качества, а в ряде случаев и реставрации (восстановления) их отдельных фрагментов.

Большинство способов и алгоритмов улучшения и реставрации изображений ориентировано на мультимедийные приложения, допускающие потери информации в процессе обработки, при условии, что они незаметны или малозаметны для человеческого глаза. С другой стороны, основными требованием к методам и алгоритмам улучшения и реставрации диагностических изображений является недопустимость потерь важной для диагностики информации, содержащейся в изображениях. Другой важной отличительной особенностью их обработки в системах диагностики является большое разнообразие диагностических изображений и, как следствие, необходимость выбора профилей обработки, т.е. типов, параметров, характеристик и опциональных возможностей ее алгоритмов, в зависимости от характеристик конкретного изображения.

БАЗОВЫЕ ПРИНЦИПЫ ВЫБОРА ПРОФИЛЕЙ ОБРАБОТКИ ДИАГНОСТИЧЕСКИХ ИЗОБРАЖЕНИЙ

Наиболее простым подходом к решению данной задачи является ее возложение на разработчика программных средств обработки изображения, который в руководстве по их применению должен указать рекомендуемые профили обработки для каждого из распространенных типов изображений. Однако при этом практически невозможно разработать рекомендации, позволяющие выбрать адекватные профили для каждого из изображений, встречающихся на практике.

Потенциально большую гибкость выбора указанных профилей обеспечивает возложение данной задачи на пользователя, который, в зависимости от характера подвергаемого обработке изображения и на основании собственных опыта и интуиции, а также (опционально) рекомендаций разработчика программного обеспечения самостоятельно выбирает профили обработки. Однако, как правило, пользователь не является специалистом в области обработки изображений. Поэтому

велика вероятность того, что выбранные им профили не будут оптимальны.

Исходя из вышесказанного, представляется рациональным автоматизированный выбор профилей обработки на основании параметров и характеристик обрабатываемого изображения. Наиболее информативными из них, очевидно, являются следующие:

- форма и минимальные размеры информативных элементов изображения;
- минимальные расстояния между указанными элементами;
- уровень шумов изображения и их характер (преобладание белого шума, фликкер-шума или их сочетание).

Первые две из указанных характеристик обычно известны пользователю диагностической системы и задаются им. Третью рационально определять автоматически, методами пространственного корреляционного анализа.

На основании вышеперечисленных характеристик изображения, в свою очередь, выбираются собственно профили обработки. Наиболее простым и алгоритмически надежным, очевидно, является табличный метод их выбора по базе профилей. Он представляет собой электронную таблицу, устанавливающую соответствие между каждым из различимых (с точки зрения выбора профилей) сочетаний характеристик изображения и профилями обработки, наиболее приемлемыми при данном сочетании. Возможны и другие методы выбора, например, основанные на алгоритмах нечеткой логики [2].

Ограниченный объем данной статьи не позволяет рассмотреть в ней практические аспекты задания и определения вышеперечисленных характеристик изображения, а также вопросы формирования базы профилей и методики их выбора по указанной базе. Авторы планируют посвятить данной тематике ряд отдельных статей.

Необходимо, чтобы файл изображения после обработки включал в себя также информацию о примененных профилях обработки. Необходимо сохранить также и необработанное изображение с целью возможности сопоставления с обработанным при анализе и/или изменении профилей (при необходимости).

АНАЛИЗ ПРИМЕНИМОСТИ ИЗВЕСТНЫХ СПОСОБОВ, ПРИЕМОВ И АЛГОРИТМОВ ОБРАБОТКИ ИЗОБРАЖЕНИЙ В СИСТЕМАХ ДИАГНОСТИКИ

Повышение качества изображений достигается двумя видами обработки изображений: исправлением (реставрацией) и улучшением [1, 2]. Под реставрацией обычно понимается процедура восстановления или оценивания элементов изображения с целью коррекции искажений и наилучшей аппроксимации идеального неискаженного изображения. Улучшение изображений, в свою очередь, состоит в преобразовании их в вид, более приемлемый для восприятия наблюдателем или для компьютерной обработки [1, 7, 8].

При обработке диагностических изображений практический интерес представляет второй из вышеназванных видов обработки [3], имеющий своей целью не приближение воспроизводимого (обрабатываемого) изображения к некоторому идеализированному оригиналу, а лишь улучшение его восприятия.

Способы и приемы улучшения изображений можно разделить на следующие основные группы [2]:

- видоизменение гистограмм, состоящее в преобразовании распределения яркостей (например, осветлении) всего изображения или его отдельных участков, с

целью улучшения его восприятия;

- фильтрация изображений с целью подавления их паразитных составляющих (в первую очередь – шумов) и выделения информативных компонент;

- сочетание вышеперечисленных способов и приемов.

Перечень и основные характеристики распространенных способов улучшения изображений, а также степени их применимости в системах технической и медицинской диагностики представлены в нижеприведенной таблице 1 [1, 2, 4]. Там же представлены основные элементы их профилей. Расшифровка аббревиатур, использованных в таблице 1, приведена в примечаниях к ней.

При этом ни один из данных способов не позволяет самостоятельно решить все задачи обработки диагностических изображений [1, 3, 5]. Их решение, как правило, обеспечивается посредством комбинации указанных способов.

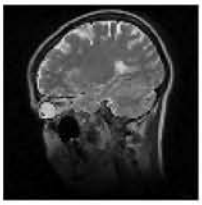
Таблица 1 – Основные характеристики распространенных способов улучшения изображений

Способ	Эффекты	Применимость в системах диагностики	Элементы профиля
1	2	3	4
Идеальный ФНЧ	Сглаживание, подавление шума	Нет	Частота среза, профиль БПФ
ФНЧ Баттерворта		В ряде частных случаев	Порядок фильтра, частота среза, профиль БПФ
ФНЧ Гаусса		Да	Частота среза, профиль БПФ
Идеальный ФВЧ	Выделение и/или подчеркивание границ	Нет	Частота среза, профиль БПФ
ФВЧ Баттерворта		В ряде частных случаев	Порядок фильтра, профиль БПФ, частота среза
ФВЧ Гаусса		Да	Частота среза, профиль БПФ
Повышение резкости с использованием лапласиан	Выделение и/или подчеркивание границ	Да	Выбор дискретной формулировки Производной
Медианная фильтрация	Подавление шума	Да	Размер маски, коэффициенты маски
Сглаживающий фильтр	Подавление шума	В ряде частных случаев	Размер маски, коэффициенты маски
Эквализация гистограммы	Выделение деталей, нормализация	Да	Нет

Продолжение таблицы 1.

1	2	3	4
Приведение гистограммы	Выделение информативных элементов	Да	Вид гистограммы
Локальное улучшение (эквализация)	Выделение мелких деталей в неравномерном изображении	Да	Размер окна
Локальное улучшение (приведение)	Выделение информативных деталей	Да	Вид гистограммы, размер окна
Усреднение изображений	Подавление шума	В ряде частных случаев	Длина серии
Пороговое подавление шума	Подавление шума	В ряде частных случаев	Размер окна
Пороговый метод	Выделение объектов	В ряде частных случаев	Порог преобразования
Примечания: ФНЧ, ФВЧ – соответственно фильтры нижних и верхних частот; БПФ – быстрое преобразование Фурье			

Таблица 2 – Результаты фильтрации тестовых изображений

Изображение, размерность в пикселях	Тип фильтра, размерность матрицы	σ	$K_Ш$
1	2	3	4
Рентгеновский снимок, 1907x1636 	ФНЧП, 3x3	0,96 %	
	ФНЧТ, 3x3	0,88 %	
	ФНЧГ, 3x3	0,78 %	
	ФНЧП, 5x5	1,30 %	
	ФНЧТ, 5x5	1,11 %	
	ФНЧГ, 5x5	0,96 %	
	Медианный, 3x3	0,88 %	
	Медианный, 5x5	1,18 %	
Результат МРС, 512x512 	ФНЧП, 3x3	1,41 %	
	ФНЧТ, 3x3	1,24 %	
	ФНЧГ, 3x3	1,04 %	
	ФНЧП, 5x5	2,63 %	
	ФНЧТ, 5x5	2,11 %	
	ФНЧГ, 5x5	1,52 %	
	Медианный, 3x3	0,96 %	
	Медианный, 5x5	2,04 %	

Продолжение таблицы 2.

1	2	3	4
Результат УЗИ, 640x480 	ФНЧП, 3x3	4,47 %	
	ФНЧТ, 3x3	4,02 %	
	ФНЧГ, 3x3	3,46 %	
	ФНЧП, 5x5	6,47 %	
	ФНЧТ, 5x5	5,48 %	
	ФНЧГ, 5x5	4.37 %	
	Медианный, 3x3	4,17 %	
	Медианный, 5x5	7,37 %	
Фликкер-шум, 512x512	ФНЧП, 3x3		1,11
	ФНЧТ, 3x3		1,10
	ФНЧГ, 3x3		1,09
	ФНЧП, 5x5		1,16
	ФНЧТ, 5x5		1,14
	ФНЧГ, 5x5		1,11
	Медианный, 3x3		1,11
	Медианный, 5x5		1,17
Белый шум, 512x512	ФНЧП, 3x3		1,38
	ФНЧТ, 3x3		1,33
	ФНЧГ, 3x3		1,31
	ФНЧП, 5x5		1,41
	ФНЧТ, 5x5		1,38
	ФНЧГ, 5x5		1,33
	Медианный, 3x3		1,41
	Медианный, 5x5		1,43

Примечания:

ФНЧП, ФНЧТ и ФНЧГ – фильтры нижних частот с прямоугольной, треугольной и Гауссовой весовой функцией соответственно;

$K_{Ш}$ – коэффициент подавления шума, рассчитанный как отношение его среднеквадратических значений до и после фильтрации;

σ – нормированное среднеквадратическое отклонение изображения после фильтрации от исходного, рассчитанное по выражению:

$$\sigma = \frac{100\%}{I_{\max}} \times \sqrt{\frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [K(i,j) - I(i,j)]^2}$$

где m и n – размер изображения в пикселях по горизонтали и по вертикали;

$I(i,j)$ и $K(i,j)$ – интенсивность пикселя с координатами (i,j) соответственно до и после фильтрации;

$I_{\max}$ – максимально возможная интенсивность пикселя, равная $2^N - 1$, где N – разрядность отсчетов интенсивностей пикселей.

Естественно предположить, что ни один из возможных профилей указанных способов улучшения изображений не является оптимальным (т.е. обеспечивающим наиболее приемлемое сочетание информативных и неинформативных составляющих после обработки) для всех диагностических изображений, которые могут встретиться на практике. Это иллюстрирует таблица 2, в которой в качестве примеров

представлены основные количественные характеристики результатов фильтрации (коэффициенты подавления шумов и относительные среднеквадратические отклонения различных типов диагностических изображений от ориг-налов после фильтрации) при различных профилях алгоритмов фильтрации. Из таблицы 2 нетрудно заметить, что указанные количественные характеристики существенно зависят от профиля алгоритма фильтрации, а также от конкретного изображения. То же характерно и для других групп алгоритмов обработки. Следовательно, необходим выбор профилей обработки каждого изображения в зависимости от его параметров и характеристик.

Исходя из изложенных ранее базовых принципов выбора профилей обработки диагностических изображений, его целесообразно осуществлять автоматически, в соответствии со следующей последовательностью процедур:

1) задание пользователем формы и минимальных размеров информативных элементов изображения, а также минимальных расстояний между ними;

2) автоматическое оценивание уровня и характера шумов изображения;

3) автоматический выбор профилей обработки изображения, например, по базе профилей;

4) формирование файлов результата, содержащих исходное и полученное после обработки изображения, а также информацию о примененном профиле обработки.

ЗАКЛЮЧЕНИЕ

Таким образом, предлагаемый подход к обработке диагностических изображений позволяет эффективно решить проблему выбора профилей обработки. Основными преимуществами данного подхода по сравнению с существующими являются:

- выбор профилей, обеспечивающих наиболее приемлемое сочетание степеней подавления неинформативных составляющих и искажения информативных элементов для каждого конкретного изображения;

- независимость от опыта и интуиции, как разработчиков, так и пользователей средств обработки диагностических изображений.

Работа выполнена в рамках Государственного контракта №16.740.11.0041 (Заказчик – Министерство образования и науки РФ), выполняемого по Федеральной целевой программе «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 гг.

СПИСОК ЛИТЕРАТУРЫ

1. Вудс Р., Гонсалес Р. Цифровая обработка изображений. – М.: Техносфера, 2005. – 1072 с.
2. Прэтт Э. Цифровая обработка изображений. – М.: Мир, 1982. – 312 с.
3. Грузман И.С. Цифровая обработка изображений в информационных системах / И.С. Грузман, В.С. Киричук, В.П. Косых, Г.П. Перетягин, А.А. Спектор. – Новосибирск: НГТУ, 2000. – 168 с.
4. Павлидис Т. Алгоритмы машинной графики и обработки изображений. – М.: Радио и связь, 1990. – 396 с.
5. Лукин А. Введение в цифровую обработку сигналов (математические основы). – М.: МГУ, 2007. – 54 с.
6. Еременко В.Т., Линьков В.В. Методика выбора метода и параметров сжатия цифровых изображений в модульных структурах сбора и обработки данных АСУП // Известия ОрелГТУ, 2007.– №4/268(535). – С. 205-210.
7. Еременко В.Т. Модель адаптационной предварительной загрузки данных / В.Т. Еременко, Н.А. Кравцова, П.И. Потаракин, Д.В. Агарков // Известия ОрелГТУ, 2007. – №4-2/268(535) – С. 219-225.

8. Теория информации и информационных процессов: монография / В.Т. Еременко, И.С. Константинов, А.В. Коськин, В.А. Лобанова и др.; под ред. д.т.н. В.Т. Еременко, д.т.н. А.П. Фисуна. – Орел: ОГУ, ОрелГТУ, 2008. – 478 с.
9. Еременко В.Т. Способы и приемы оптимизации процесса оценки вида технического состояния объектов телекоммуникаций / В.Т. Еременко, А.Н. Орешин, Н.А. Орешин, А.М. Лабунец // «Вестник компьютерных и информационных технологий», 2008.– №6. – С. 40-47.

Еременко Владимир Тарасович
ФГОУ ВПО «Госуниверситет – УНПК», г. Орел
Доктор технических наук, профессор, зав. кафедрой «Электроника, вычислительная техника и информационная безопасность»
Тел.: (4862) 45-57-57
E-mail: wladimir@orel.ru

Тютякин Александр Васильевич
ФГОУ ВПО «Госуниверситет – УНПК», г. Орел
Кандидат технических наук, доцент, доцент кафедры «Электроника, вычислительная техника и информационная безопасность»
Тел.: (4862) 45-57-57
E-mail: avt@rbcmail.ru

Кондрашин Алексей Андреевич
ФГОУ ВПО «Госуниверситет – УНПК», г. Орел
Аспирант кафедры «Электроника, вычислительная техника и информационная безопасность»
Тел.: (4862) 45-57-57
E-mail: qaws@bk.ru

V.T. EREMENKO, A.V. TIUTIAKIN, A.A. KONDRASHIN

METHODOLOGICAL ASPECTS OF IMAGE PROCESSING IN AUTOMATED SYSTEMS OF DIAGNOSTICS

The article is devoted to the resolution of some tasks within the problem of image processing in the systems of technical and medical diagnostics. The applicability of known methods and algorithms of image processing for improving and restoration of graphic information in diagnostics systems is justified in the article. The elements of profiles, methods and algorithms of the automated image processing are defined. The basic principles of the choice of above-mentioned profiles are presented.

Keywords: *diagnostics; images processing; profile; choice of image processing profiles.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Vuds R., Gonsales R. Cifrovaya obrabotka izobrazhenij. – M.: Texnosfera, 2005. – 1072 s.
2. Pre`tt E`. Cifrovaya obrabotka izobrazhenij. – M.: Mir, 1982. 312 s.
3. Gruzman I.S. Cifrovaya obrabotka izobrazhenij v informacionny'x sistemax / I.S. Gruzman, V.S. Kirichuk, V.P. Kosy'x, G.P. Peretyagin, A.A. Spektor. – Novosibirsk: NGTU, 2000. – 168 s.
4. Pavlidis T. Algoritmy' mashinnoj grafiki i obrabotki izobrazhenij. – M.: Radio i svyaz', 1990. – 396 s.
5. Lukin A. Vvedenie v cifrovuyu obrabotku signalov (matematicheskie osnovy'). – M.: MGU, 2007. – 54 s.
6. Eryomenko V.T., Lin'kov V.V. Metodika vy'bora metoda i parametrov szhatiya cifrovy'x izobrazhenij v modul'ny'x strukturax sbora i obrabotki danny'x ASUP // Izvestiya OryolGTU, 2007. – № 4/268(535). – S. 205-210.
7. Eryomenko V.T. Model' adaptacionnoj predvaritel'noj zagruzki danny'x / V.T. Eryomenko, N.A. Kravcova, P.I. Potarakin, D.V. Agarkov // Izvestiya OryolGTU, 2007. – №4. – 2/268(535). – S. 219-225.
8. Teoriya informacii i informacionny'x processov: monografiya / V.T. Eryomenko, I.S. Konstantinov, A.V. Kos'kin, V.A. Lobanova i dr.; / pod red. d.t.n. V.T. Eryomenko, d.t.n. A.P. Fisuna. – Oryol: OGU, OryolGTU, 2008. – 478 s.
9. Eryomenko V.T. Sposoby' i priyomy' optimizacii processa ocenki vida texnicheskogo sostoyaniya ob``ektov telekommunikacij / V.T. Eryomenko, A.N. Oreshin, N.A. Oreshin, A.M. Labunec // «Vestnik komp'yuterny'x informacionny'x texnologij», 2008. – №6. – S. 40-47.

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

УДК 519.6

Е.Г. ЖИЛЯКОВ, С.П. БЕЛОВ, С.В. ТУЯКОВ, Д.В. УРСОЛ

О НАИЛУЧШЕМ ОРТОГОНАЛЬНОМ БАЗИСЕ ДЛЯ СУБПОЛОСНОГО АНАЛИЗА И СИНТЕЗА СИГНАЛОВ[1]

Показано, что для решения задач вычисления точных значений долей энергий сигналов, оптимальной фильтрации и синтеза сигналов с максимальной концентрацией энергии в заданном частотном интервале наилучшим является базис из ортогональных собственных функций соответствующих ядер, названных субполосными.

Ключевые слова: *анализ и синтез сигналов; частотные представления.*

It is shown that for solving the problems of calculation exact values of fractions the energies of the signals, optimal filtering and synthesis of signals with a maximum concentration of energy in a given frequency interval is the best basis of the orthogonal eigenfunctions of the corresponding kernels, called subband.

Keywords: *analysis and synthesis of signals; the frequency representation.*

ВВЕДЕНИЕ

В рамках данной работы под сигналом понимается функция времени, параметры которой содержат необходимую для решения вполне определенной задачи информацию.

В частности, сигналом является последовательность регистрируемых в процессе наблюдений значений неизвестной функции (эмпирических данных), содержащих информацию о закономерностях в поведении генерирующих их объекта.

Ясно, что для выявления и описания этих закономерностей необходимо на основе соответствующих принципов осуществить анализ эмпирических данных, успешность которого, прежде всего, определяется адекватностью используемых моделей целям исследований.

С другой стороны, эмпирические данные, например, изображения, часто с той или иной целью должны быть переданы по информационным коммуникациям на некоторое расстояние.

Для этого на передающей стороне с учетом специфики режима передачи формируются (синтезируются) специальные (информационные) сигналы, которые затем на приемной стороне подвергаются анализу с целью выделения (восстановления) передаваемых эмпирических данных.

Следует отметить, что и при передаче информации центральную роль играют модели, которые должны адекватно отражать специфику режима коммуникации с точки зрения синтеза и анализа информационных сигналов.

ПОСТАНОВКА ЗАДАЧИ

Одним из наиболее распространенных способов получения моделей анализа и синтеза сигналов служат так называемые частотные представления вида

$$f(t) = \int_{-\infty}^{\infty} F(\omega) e^{j\omega t} d\omega / 2\pi , \qquad (1)$$

где $f(t)$ – сигнал, область определения которого в дальнейшем предполагается

[1] Исследования выполнены при поддержке гранта РФФИ № 10-07-00326-а

конечной, то есть имеет место

$$t \in [0,T], T < \infty; \quad (2)$$

$F(\omega)$ – частотная характеристика, под которой чаще всего понимается трансформанта Фурье сигнала

$$F(\omega) = \int_0^T f(t) e^{-j\omega t} dt, \quad (3)$$

где ω – круговая частота.

В рамках данной работы (если противоположное не оговаривается) предполагаются выполненными условия сходимости [1] интегралов вида (1) и (3), а сигналы являются вещественнозначными непрерывными функциямм времени с ограниченной евклидовой нормой (пространство L_2), так что

$$\|f\|^2 = \int_0^T f^2(t) dt < \infty.$$

Поэтому [1], справедлива формула Парсеваля

$$\int_0^T f^2(t) dt = \int_{-\infty}^{\infty} |F(\omega)|^2 d\omega / 2\pi, \quad (4)$$

которая показывает, что с физической точки зрения трансформанта Фурье характеризует распределение энергии сигнала в области частот.

Соотношение (4) легко преобразовать к виду

$$\int_0^T f^2(t) dt = \sum_{r=1}^{\infty} P_r, \quad (5)$$

где P_r – части энергии (евклидовой нормы)

$$P_r = \int_{\omega \in \Omega_r} |F(\omega)|^2 d\omega / 2\pi, \quad (6)$$

попадающие в частотные интервалы вида

$$\Omega_r = [-\Omega_{2r}, -\Omega_{1r}) \cup [\Omega_{1r}, \Omega_{2r}), \quad (7)$$

причем выполняются равенства

$$\Omega_{2r} = \Omega_{1,r+1}, r = 1,2,\ldots,$$

которые, очевидно, гарантируют справедливость равенства (5).

Отметим, что при равной ширине частотных интервалов

$$\Delta\Omega_r = \Omega_{2r} - \Omega_{1r}$$

по значениям частей энергий (6) можно судить о наличии в сигнале квазипериодических компонент, если в каком-то из частотных интервалов наблюдается повышенная концентрация энергии.

В свою очередь, в задачах синтеза сигналов часто применяется принцип максимизации их энергии в отдельной полосе частот при заданной длительности [2, 3]. Рассмотрение свойств сигналов в соответствии с некоторой сеткой (распределением) частотных интервалов будем называть субполосным анализом и синтезом. Для реализации такого подхода целесообразно использовать адекватный математический аппарат, который и разрабатывается в данной работе.

СУБПОЛОСНЫЙ АНАЛИЗ СИГНАЛОВ

Представляется важным рассмотреть два основных аспекта субполосного

анализа, а именно – вычисление частей энергий вида (6) и разделение сигнала на аддитивные компоненты (фильтрация) в виде

$$f(t) = f_1(t) + f_2(t),$$

где трансформанта Фурье первой из них

$$F_1(\omega) = \int_0^T f_1(t) e^{-j\omega t} dt$$

в идеальном случае должна удовлетворять условию

$$\begin{aligned} &F_1(\omega) = F(\omega), \omega \in \Omega_r; \\ &F_1(\omega) \equiv 0, \omega \notin \Omega_r. \end{aligned}, \tag{8}$$

где Ω_r – некоторый определяемый соотношением (7) интервал оси частот ω.

Отметим, что непосредственные вычисления в соответствии с определением (6) неосуществимы ввиду невозможности вычислений на основе (3) значений трансформанты Фурье в континууме точек частотного интервала. Вместе с тем, подстановка правой части представления (3) в определение (6) позволяет получить соотношение, вполне пригодное для вычислений

$$P_r = \int_0^T \int_0^T A_r(t_1 - t_2) f(t_1) f(t_2) dt_1 dt_2, \tag{9}$$

где A_r – ядро, которое в дальнейшем называется субполосным

$$A_r(t_1 - t_2) = \frac{1}{2\pi} \int_{\omega \in \Omega_r} e^{-j\omega(t_1 - t_2)} d\omega. \tag{10}$$

В результате интегрирования нетрудно получить явное выражение

$$A_r(t_1 - t_2) = \frac{\sin[\Omega_{2r}(t_1 - t_2)] - \sin[\Omega_{1r}(t_1 - t_2)]}{\pi(t_1 - t_2)}, \tag{11}$$

после подстановки которого в (9) можно для вычисления интеграла применить ту или иную квадратурную формулу.

При решении задачи фильтрации представляется естественным использовать вариационный принцип минимизации меры погрешности аппроксимации условия (8)

$$S_r(f, f_1) = \min,$$

где S_r – функционал вида

$$S_r(f, f_1) = \frac{1}{2\pi} \int_{\omega \in \Omega_r} |F(\omega) - F_1(\omega)|^2 d\omega + \frac{1}{2\pi} \int_{\omega \notin \Omega_r} |F_1(\omega)|^2 d\omega, \tag{12}$$

а минимум ищется по всем непрерывным функциям f_1 с областью определения вида (2).

Нетрудно показать, что искомое оптимальное решение вариационной задачи (12) имеет вид

$$f_1(t) = \int_0^T A_r(t - t_1) f(t_1) dt_1, \tag{13}$$

то есть снова выражается с помощью субполосного ядра.

Ясно, что трансформанта Фурье вида (3) является аналитической функцией. Поэтому она не может быть равной тождественно нулю ни в каком сплошном интервале конечных размеров. Следовательно, интегралы вида (6) имеют положительные значения. Таким образом, из представления (9) следует, что субполосные ядра являются положительно определенными, а соотношение (11)

показывает, что они являются симметричными.

Поэтому [4] субполосное ядро может быть представлено в виде сходящегося в среднеквадратическом смысле ряда по собственным функциям

$$A_r(t_1 - t_2) = \sum_{k=1}^{\infty} \lambda_k^r q_k^r(t_1) q_k^r(t_2), \tag{14}$$

где λ_k, q_k – вещественные собственные числа и соответствующие им собственные функции ядра, так что выполняется условие

$$\lambda_k^r q_k^r(t) = \int_0^T A_r(t - t_1) q_k^r(t_1) dt_1, \tag{15}$$

причем ввиду положительной определенности субполосных ядер собственные числа являются положительными и предполагаются упорядоченными по убыванию, т.е.

$$\lambda_1^r > \lambda_2^r > \ldots > \lambda_J^r > \ldots > 0.$$

Известно также [4], что совокупность собственных функций симметричных и положительно определенных ядер представляет собой ортонормальный базис, т.е.

$$(q_k^r, q_i^r) = \int_0^T q_k^r(t) q_i^r(t) dt = \delta_{ik}, \tag{16}$$

который является полным в пространстве L_2.

Здесь δ_{ik} – символ Кронекера

$$\delta_{ik} = 1, i = k;$$
$$\delta_{ik} = 0, i \neq k.$$

Поэтому после подстановки разложения (14) в представление (9) и (13) нетрудно получить соотношения

$$P_r = \sum_{k=1}^{\infty} \lambda_k^r (\alpha_k^r)^2, \tag{17}$$

$$f_1(t) = \sum_{k=1}^{\infty} \lambda_k^r \alpha_k^r q_k^r(t), \tag{18}$$

где α_k^r – скалярные произведения вида

$$\alpha_k^r = (f, q_k^r) = \int_0^T f(t) q_k^r(t) dt. \tag{19}$$

Таким образом, естественным базисом для решения рассматриваемых задач субполосного анализа является совокупность ортонормальных собственных функций, соответствующих заданным частотным интервалам субполосных ядер.

Ниже будет показано, что этот базис естественным образом возникает и при рассмотрении задач оптимального субполосного синтеза сигналов на основе эмпирических данных. Поэтому представляет интерес более глубокое изучение свойств собственных чисел и собственных функций субполосных ядер.

Соотношение (14) при $t_1 = t_2 = t$ с учетом (11) дает

$$A(0) = \frac{\Omega_{2r} - \Omega_{1r}}{\pi} = \sum_{k=1}^{\infty} \lambda_k^r (q_k^r(t))^2.$$

Поэтому в результате интегрирования по интервалу (2) с учетом (16) нетрудно получить равенство для собственных чисел

$$\sum_{k=1}^{\infty} \lambda_k^r = 2(\nu_{2r} - \nu_{1r})T, \tag{20}$$

где ν_{ir} – частоты, определяемые соотношениями

$$\Omega_{ir} = 2\pi\nu_{ir}, i = 1,2.$$

Ввиду установленной раньше положительности собственных чисел из конечности правой части (20) следует, что большинство из них будет близко к нулю.

Вычисления показывают, что выполняется неравенство

$$1 - \frac{\sum_{k=1}^{J}\lambda_k}{2(\nu_{2r} - \nu_{1r})T} << 1,$$

где

$$J = 2\{(\nu_{2r} - \nu_{1r})T\} + 2 = M + 2,$$

символ $\{\ \}$ означает целую часть числа.

Таким образом, можно записать

$$\lambda_k \approx 0, k > J.$$

Тогда соотношения (17) и (18) принимают вид

$$P_r \approx \sum_{k=1}^{J}\lambda_k^r(\alpha_k^r)^2, \quad (21)$$

$$f_1(t) \approx \sum_{k=1}^{J}\lambda_k^r\alpha_k^r q_k^r(t). \quad (22)$$

Если в определение (15) подставить представление (10), то в результате интегрирования нетрудно получить

$$\lambda_k^r q_k^r(t) = \frac{1}{2\pi}\int_{\omega\in\Omega_r} Q_k^r(\omega)e^{j\omega t}d\omega, \quad (23)$$

где $Q_k^r(\omega)$ – трансформанта Фурье собственной функции.

Отметим, что ввиду свойства (16) справедливы соотношения

$$\frac{1}{2\pi}\int_{-\infty}^{\infty} Q_k^r(\omega)Q_i^{r*}(\omega)d\omega = \delta_{ik}, \quad (24)$$

где символ * означает комплексное сопряжение.

С другой стороны, умножив (23) слева и справа на $q_i^r(t)$ и интегрируя по t в пределах (2), имеем

$$\lambda_k^r = \frac{1}{2\pi}\int_{\omega\in\Omega_r}\left|Q_k^r(\omega)\right|^2 d\omega,$$

$$\int_{\omega\in\Omega_r} Q_k^r(\omega)Q_i^{r*}(\omega)d\omega = 0, i \neq k. \quad (25)$$

Таким образом, собственное число численно равно доле евклидовой нормы (энергии) собственной функции, которая приходится (попадает) на заданный частотный интервал. В свою очередь (24) и (25) означают, что трансформанты Фурье собственных функций ортогональны как на всей оси частот, так и на заданном частотном интервале (свойство двойной ортогональности [1]).

В свою очередь, подставив представление (10) в уравнение фильтрации (13), после интегрирования нетрудно прийти к соотношению

$$f_1(t) = \frac{1}{2\pi}\int_{\omega\in\Omega_r} F(\omega)e^{j\omega t}d\omega,$$

которое говорит о том, что получаемая функция полностью определяется отрезком

трансформанты Фурье исходного сигнала в заданном частотном интервале.

Указанное обстоятельство и оптимальность в смысле минимума евклидовой нормы погрешности (12) приближения к идеальному условию (8) определяют существенные преимущества фильтрации на основе соотношения (13) перед фильтрацией на основе вычисления сверток [2, 3].

Возможность на основе соотношений (17), (18) и (21), (22) вычислять для заданных частотных интервалов точные значения попадающих в них частей энергий и соответствующих аддитивных компонент сигналов позволяет утверждать, что ортонормальный базис собственных функций субполосных ядер является наилучшим для задач субполосного анализа.

СУБПОЛОСНЫЙ СИНТЕЗ СИГНАЛОВ НА ОСНОВЕ ЭМПИРИЧЕСКИХ ДАННЫХ

Пусть задан набор вещественнозначных эмпирических данных $e_1,...,e_M$, совокупность которого будем называть информационным вектором $\vec{e} = (e_1,..., e_M)^T$.

Рассмотрим следующую задачу. Синтезировать функцию времени $f\left(t,\vec{e}\right)$, $t \in [0,T]$, зависящую от эмпирических данных как от параметров, значения которых при отсутствии искажающих воздействий необходимо однозначно и точно вычислять на основе анализа получаемого сигнала. При этом должно выполняться вариационное условие

$$R(t) = \frac{P_r(t)}{\|f\|^2} = \max, \tag{26}$$

где максимум ищется по всему множеству непрерывных функций из пространства L_2 с областью определения (2):

$$P_r(t) = \int_0^T \int_0^T A_r(t_1 - t_2) f\left(t_1,\vec{e}\right) f\left(t_2,\vec{e}\right) dt .$$

Так как базис собственных функций субполосного ядра является полным в рассматриваемом пространстве [4], то (26) можно представить в виде

$$R(t) = \frac{\sum_{k=1}^{\infty} \lambda_k \alpha_k^2}{\sum_{k=1}^{\infty} \alpha_k^2} = \max, f \in L_2 ,$$

где α_k – скалярные произведения вида (19) (верхний индекс для простоты записей опущен).

Отсюда, имея в виду упорядоченность собственных чисел по убыванию, получаем неравенство

$$R(t) \le \lambda_1 , \tag{27}$$

где знак равенства достигается, когда искомая функция пропорциональна соответствующей собственной функции, т.е.

$$f(t) = c_1 q_1(t).$$

Заметим, что правая часть (27) определяет максимально достижимую концентрацию энергии среди всех функций из рассматриваемого пространства.

Таким образом, для случая

$$M = 1 \tag{28}$$

наилучший сигнал имеет вид

$$f(t,e_1)=e_1q_1(t), \tag{29}$$

при этом искомый параметр определяется из скалярного произведения

$$e_1=(f,q_1). \tag{30}$$

Построение оптимального в смысле (26) вектора для произвольного M основывается на следующем.

Утверждение. Для любого $M\geq 1$ выполняется неравенство

$$\frac{\sum_{k=1}^{M}\lambda_k\alpha_k^2}{\sum_{k=1}^{M}\alpha_k^2}\geq\frac{\sum_{i=1}^{M+1}\lambda_i\alpha_i^2}{\sum_{i=1}^{M+1}\alpha_i^2}. \tag{31}$$

Доказательство справедливости этого утверждения легко получить, если из левой части неравенства (31) вычесть правую и привести к общему знаменателю. В результате получим:

$$\frac{\sum_{k=1}^{M}\lambda_k\alpha_k^2}{\sum_{k=1}^{M}\alpha_k^2}-\frac{\sum_{i=1}^{M+1}\lambda_i\alpha_i^2}{\sum_{i=1}^{M+1}\alpha_i^2}=\frac{\alpha_{M+1}^2\sum_{k=1}^{M}\alpha_k^2(\lambda_k-\lambda_{M+1})}{\sum_{k=1}^{M}\alpha_k^2\sum_{i=1}^{M+1}\alpha_i^2}.$$

Очевидно, что в связи с упорядоченностью собственных чисел по убыванию правая часть последнего соотношения будет положительной, следовательно, неравенство (31) выполняется.

Утверждение говорит о том, что по аналогии со случаем (28), (29) и (30) оптимальный сигнал должен иметь вид

$$f(t,\vec{e})=\sum_{i=1}^{M}e_iq_i(t),$$

причем в виду ортонормальности собственных функций справедливы соотношения

$$e_i=(f,q_i),$$

которые позволяют определить компоненты информационного вектора на основе синтезированного сигнала.

ЗАКЛЮЧЕНИЕ

Таким образом, в работе показано, что эффективным средством решения задач субполосного анализа и синтеза сигналов является базис, состоящий из ортогональных собственных функций соответствующих субполосных ядер.

СПИСОК ЛИТЕРАТУРЫ

1. Хургин Я.И., Яковлев В.П. Финитные функции в физике и технике. – М.: Наука, 1971.
2. Френкс Л. Теория сигналов. – М.: Советское радио, 1974. – 344 с.
3. Цифровая обработка сигналов и изображений в радиофизических приложениях; под ред. В.Ф. Кравченко. – М.: ФИЗМАТЛИТ, 2007. – 544 с.
4. Смирнов В.И. Курс высшей математики. – М.: Наука, 1974. – Т.4, Ч.1. – 335 с.

Жиляков Евгений Георгиевич
Белгородский государственный университет, г. Белгород
Доктор технических наук, профессор, зав. кафедрой информационно-телекоммуникационных систем и технологий
Тел.: (4722) 30-13-92
E-mail: zhilyakov@bsu.edu.ru

Белов Сергей Павлович
Белгородский государственный университет, г. Белгород
Кандидат технических наук, профессор кафедры информационно-телекоммуникационных систем и технологий
Тел.: (4722) 30-13-50
E-mail: belov@bsu.edu.ru

Туяков Самат Валерьевич
Белгородский государственный университет, г. Белгород
Аспирант кафедры математического и программного обеспечения информационных систем
E-mail: student_pf@mail.ru

Урсол Денис Владимирович
Белгородский государственный университет, г. Белгород
Аспирант кафедры информационно-телекоммуникационных систем и технологий
E-mail: Ursol@bsu.edu.ru

E.G. ZILYAKOV, S.P. BELOV, S.V. TUYAKOV, D.V. URSOL

ABOUT THE BEST ORTHOGONAL BASIS FOR THE SUBBAND ANALYSIS AND SYNTHESIS OF SIGNALS

It is shown that for solving the problems of calculation exact values of fractions the energies of the signals, optimal filtering and synthesis of signals with a maximum concentration of energy in a given frequency interval is the best basis of the orthogonal eigenfunctions of the corresponding kernels, called subband.

Keywords: *analysis and synthesis of signals, the frequency representation.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Hurgin Ya.I., Yakovlev V.P. Finitny'e funkcii v fizike i texnike. – M.: Nauka, 1971.
2. Frenks L. Teoriya signalov. – M.: Sovetskoe radio, 1974. – 344 s.
3. Cifrovaya obrabotka signalov i izobrazhenij v radiofizicheskix prilozheniyax; pod red. V.F. Kravchenko. – M.: FIZMATLIT, 2007. – 544 s.
4. Smirnov V.I. Kurs vy'sshej matematiki. – M.: Nauka, 1974. – T.4, Ch.1. – 335 s.

УДК 001.57; 658.818; 681.3

М.В. МИХЕЛЕВ

ФОРМАЛИЗОВАНЫЙ МЕТОД ПРОЕКТИРОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ

Обсуждается возможность математического описания визуальных графоаналитических моделей с помощью алгебраического аппарата «пи-исчисления» Р. Милнера на примере моделей процессов управления наружным освещением в стандарте BPMN.

Ключевые слова: *визуальное графоаналитическое моделирование; BPMN; пи-исчисление; управление наружным освещением; бизнес-процесс.*

ВВЕДЕНИЕ

Любые организации, выходя на рынок или уже функционируя на нем, сталкиваются с очень серьезной для них проблемой – конкуренцией. Чтобы преодолеть данную проблему, им необходимо непрерывно улучшать свой бизнес, развивать новые отрасли своей деятельности, т.е. проводить непрерывную реорганизацию своего бизнеса, так как жесткая структура бизнеса в настоящее время не жизнеспособна. С другой стороны, по причине той же конкуренции любая организация не может функционировать без четкого описания своего бизнеса в виде должностных инструкций и положений о подразделениях. Это обеспечивается путем проведения регламентации бизнеса. Регламентация означает создание документации, определяющей ход, результаты процессов и порядок управления ими. Регламентация процессов начинается с определения того, какие процессы должны быть регламентированы. Затем проводится документирование процесса, его входов, выходов и подпроцессов по заранее разработанному шаблону. Регламентация необходима для более точного и корректного описания процесса, что позволит создать или откорректировать должностные инструкции, закрепить ответственность, укрепить нормативную базу организации.

Эта двухсторонняя и противоречивая по своей сути задача (обеспечение возможности непрерывной реорганизации бизнеса при его постоянной четкой регламентации) может быть решена только путем формализации бизнеса. Поэтому формализация бизнеса в настоящее время является бурно развивающейся отраслью системного анализа, организационного проектирования и управленческого консультирования. С одной стороны, формализованные бизнес-процессы легче изменять и модернизировать, с другой стороны, формализация процессов позволяет четко определить правила работы сотрудников и подразделений. Кроме того, формализация бизнес-процессов является хорошей основой для последующей информатизации и автоматизации бизнеса в организации.

В качестве основного средства формализации бизнеса используются компьютерные визуальные графоаналитические модели, создаваемые с помощью различных методов системного анализа. Они являются достаточно формальным описанием, позволяющим пошагово определять виды действия, участников и результаты, а также легко понимаемым всеми участниками бизнеса. При этом применяется несколько методологий и технологий такого моделирования, составляющих популярную информационную технологию, начавшую свое развитие в рамках так называемой CASE-технологии. Все они обладают как некоторыми достоинствами, так и определенными недостатками. Поэтому актуальными остаются исследования в области формализации визуальных графоаналитических моделей

бизнеса с помощью математических методов [1].

ВИЗУАЛЬНОЕ ГРАФОАНАЛИТИЧЕСКОЕ МОДЕЛИРОВАНИЕ БИЗНЕС-ПРОЦЕССОВ

В 2001-2004 годах организацией Business Process Management Initiative (BPMI) была разработана новая нотация визуального моделирования бизнес-процессов (BPMN) с учётом множества ранее существовавших нотаций. Основной целью данной разработки было получение нотации, легко понимаемой всеми пользователями: от бизнес-аналитика, создающего первые наброски описаний процессов, до технических специалистов, отвечающих за реализацию этих процессов, и, наконец, до людей бизнеса, которые управляют этими процессами и контролируют их работу. Только с появлением стандарта BPMN (доведение данной нотации до стандарта осуществил консорциум OMG) появилась возможность автоматизированного выполнения именно описаний бизнес-процессов, а не «программ», которые непрозрачным и непонятным способом разработаны другими людьми на основе этих прозрачных описаний.

Следует подчеркнуть, что одним из факторов развития BPMN является создание простого механизма для создания моделей бизнес-процессов, в то же время способного к управлению сложными бизнес-процессами. Способ решения проблемы сочетания этих двух противоречащих друг другу требований состоял в создании графических аспектов нотации по конкретным категориям. При этом совокупность категорий нотации получается небольшая, таким образом, читатель схемы BPMN может легко узнать основные типы элементов и понять схему. В рамках основных категорий элементов могут быть добавлены дополнительные изменения и информация для обеспечения соответствия требованиям сложности без значительных изменений основных ощущений и впечатлений от схемы.

Можно выделить четыре основные категории элементов нотации:

1) Объекты схемы – задача, событие, шлюз.

2) Артефакты – группа, аннотация, объект данных.

3) Области и дорожки – пул, дорожка, промежуточный этап.

4) Соединители – поток процесса, сопоставление, поток сообщений.

На рисунке 1 представлен бизнес-процесс, описывающий в нотации BPMN процедуру выполнения переключений уличного освещения в шкафу управления (ШУ). Диспетчеру, работающему в автоматизированной системе управления наружным освещением (АСУНО), поступает заявка на выполнение переключения ШУ [2].

Диспетчер обрабатывает заявку, выполняет поиск ШУ в системе и осуществляет удаленное переключение ШУ по команде. В случае успешного выполнения команды приходит подтверждение о выполненном переключении.

Весь бизнес-процесс разбит на действия, в терминах BPMN это задача или подзадача. Переходы между действиями показаны стрелками – это поток процесса, а документы, которые порождаются или используются каким-либо действием это объект данных. Также в бизнес-процессе присутствуют точки принятия решений, в которых поток процесса может быть продолжен по одному или нескольким альтернативным путям – это шлюзы.

Несмотря на то, что для решения ряда задач вполне достаточно графоаналитического представления процессов, существуют задачи, решение которых невозможно без более формального, т.е. математического их описания (например, задача верификации или имитационного моделирования).

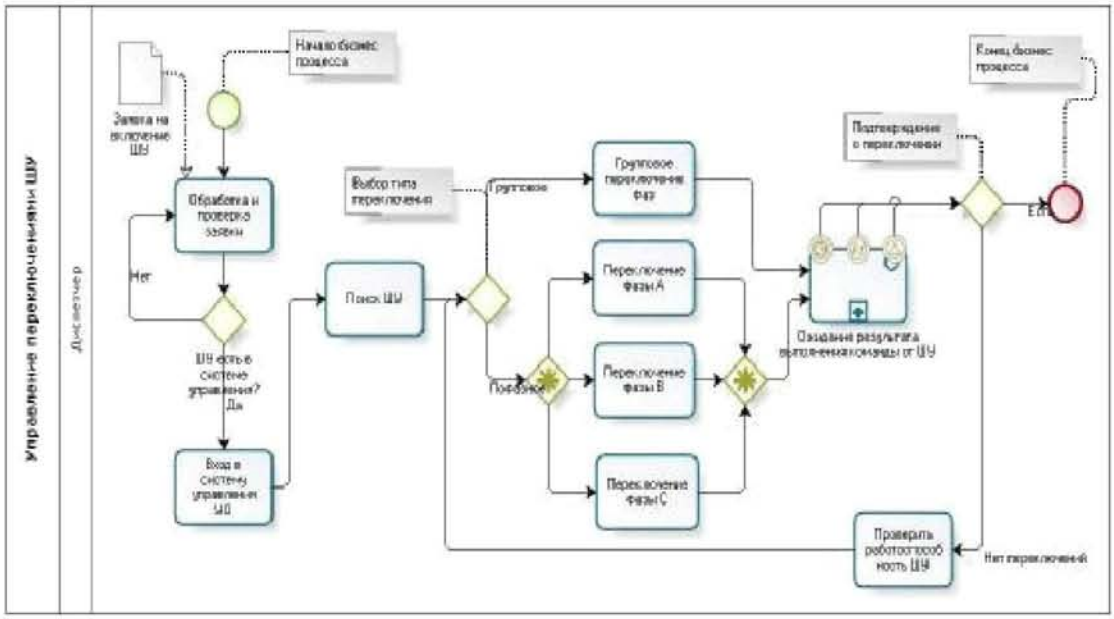


Рисунок 1 – Бизнес-процесс переключения освещения

МАТЕМАТИЧЕСКОЕ ОПИСАНИЕ БИЗНЕС-ПРОЦЕССОВ С ПОМОЩЬЮ ПИ-ИСЧИСЛЕНИЯ

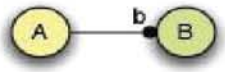
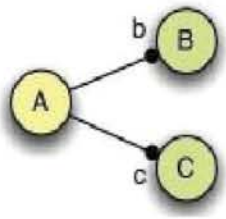
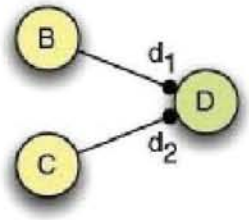
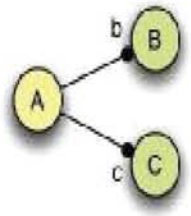
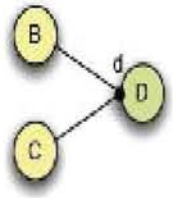
Для математического описания моделей бизнес-процессов будем использовать алгебраический аппарат, разработанный в 1989 году шотландским математиком Робертом Милнером, названный «пи-исчисление», являющийся расширением «исчисление взаимодействующих систем (CCS)» [3].

Пи-исчисления – современная алгебра процессов, которая описывает мобильные системы в широком смысле. Исчисление основывается на концепции мобильности, которое включает коммуникации и изменения. Связь осуществляется между различными процессами пи-исчислений. Структура процессов изменяется с течением времени по каналам коммуникаций, например, процесс может динамически включать в себя другие процессы, которые он получил с помощью каналов коммуникаций. Сами каналы коммуникаций основаны на концепции имен. Имя это собирательное название для предыдущих существующих концепций, таких как ссылки, указатели, идентификаторы и т.д., каждый из которых имеет сферу. Предполагается, что имя представляет собой ссылку на процесс, который в настоящее время обрабатывает процесс технологического маршрута (workflow), в это время границы имени включают в себя только активный процесс. Как только процесс завершится, границы имени переходят на процесс, который обрабатывает следующий блок технологического процесса.

На основании гибкости пи-исчисления появляется много различных возможностей формализовать модели бизнес систем. Каждый блок бизнес процесса, такой, как событие, условие, действие, описывается как самостоятельный процесс в терминах пи-исчисления. Эти процессы используют события через каналы коммуникаций для координирования поведения рабочего процесса. Некоторые процессы в совокупности образуют модель поведения, которая представляет собой модель технологического процесса.

В общем смысле, пи-исчисление – модель параллельных вычислений, основанная на посылке сообщений. В терминах пи-исчисления любой алгоритм представляется как последовательность посылки и принятия сообщений процессами. Посылка сообщений осуществляется с помощью канала.

Таблица 1 – Основные конструкции бизнес-процессов, описанные в нотации BPMN

1. Последовательность		$P = A \mid B;$ $A = \tau_A.\overline{b}\langle x\rangle.0;\ B = b(x).\tau_B.B'$
2. Параллельное разделение		$P = A \mid (B \mid C);$ $A = \tau_A.(\overline{b}\langle x\rangle.0 \mid \overline{c}\langle x\rangle.0);$ $B = b(x).\tau_B.B';$ $C = c(x).\tau_C.C'$
3. Синхронизация		$P = (B \mid C) \mid D;$ $B = \tau_B.\overline{d_1}\langle x\rangle.0;$ $C = \tau_C.\overline{d_2}\langle x\rangle.0;$ $D = d_1(x).d_2(x).\tau_D.D'$
4. Выбор		$P = A \mid (B + C);$ $A = \tau_A.(\overline{b}\langle x\rangle.0 + \overline{c}\langle x\rangle.0);$ $B = b(x).\tau_B.B';$ $C = c(x).\tau_C.C'$
5. Объединение		$P = (B + C) \mid D;$ $B = \tau_B.\overline{d}\langle x\rangle.0;$ $C = \tau_C.\overline{d}\langle x\rangle.0;\ D = d(x).\tau_D.D'$

Примитивными сущностями пи-исчисления являются имена. Их бесконечно много, они лишены внутренней структуры. Имена записываются как символьные строки, начинающиеся со строчной буквы.

Процесс P (выражение пи-исчисления) представляет собой одно из следующего списка:

1) – входной префикс, получение данных *x* из канала *c*.
2) – выходной префикс, передача данных *y* по каналу *c*.
3) – параллельный запуск двух процессов.
4) – репликация процесса.
5) – объявление канала и последующее выполнение процесса.
6) – внутреннее действие процесса.
7) 0 – пустой процесс.

Бизнес-процесс – это кортеж, состоящий из узлов, направленных ребер, типов и атрибутов. Формально описывается следующим образом:

$P = (N, E, T, A)$ – формальное описание процесса,

где N – набор узлов;

$E \subseteq (N \times N)$ – набор направленных ребер между узлами;

$T : N \to TYPE$ – функция;

$A \subseteq (N \times (KEY \times VALUE))$ – связи между узлами и значениями.

N представляет собой набор действий. E отвечает за маршрутизацию потока управления. T связывает узлы с шаблонами рабочего процесса модели. A описывает связь пары ключ/значение для узлов. Примечательно, что граф процесса описывает только статическую структуру, т.е. схему бизнес-процесса. Граф процесс может быть легко связан с графическим отображением подхода УФО.

Чтобы описать граф процесса с помощью семантики алгебры процессов, воспользуемся следующим алгоритмом:

Алгоритм 1. Описание графа процесса в семантике алгебры процессов.

Граф процесса $P = (N, E, T, A)$ представляется в виде элементов пи-исчисления следующим образом:

1. Все узлы процесса P соответствуют уникальным идентификаторам пи-исчисления $N1...N \mid P_N \mid$.

2. Все ребра процесса P соответствуют именам пи-исчисления $e1...e \mid P_E \mid$.

3. Внутреннюю деятельность процесса будем обозначать τ. Если граф процесса цикличный, то используется рекурсия для возможности многократного выполнения экземпляра деятельности.

4. Элемент $N \overset{def}{=} (ve1,...,e \mid P_E)(\prod_{i=1}^{|P_N|} N_i)$ описывает экземпляр процесса.

Любой бизнес-процесс можно представить как набор из основных конструкций Примитивными сущностями пи-исчисления являются имена. Их бесконечно много, они лишены внутренней структуры. Имена записываются как символьные строки, начинающиеся со строчной буквы.

Процесс P (выражение пи-исчисления) представляет собой одно из следующего списка:

1) – входной префикс, получение данных *x* из канала *c*.
2) – выходной префикс, передача данных *y* по каналу *c*.
3) – параллельный запуск двух процессов.
4) – репликация процесса.
5) – объявление канала и последующее выполнение процесса.
6) – внутреннее действие процесса.
7) 0 – пустой процесс.

Бизнес-процесс – это кортеж, состоящий из узлов, направленных ребер, типов и атрибутов. Формально описывается следующим образом:

$P = (N, E, T, A)$ – формальное описание процесса,

где N – набор узлов;

$E \subseteq (N \times N)$ – набор направленных ребер между узлами;

$T : N \to TYPE$ – функция;

$A \subseteq (N \times (KEY \times VALUE))$ – связи между узлами и значениями.

N представляет собой набор действий. E отвечает за маршрутизацию потока управления. T связывает узлы с шаблонами рабочего процесса модели. A описывает связь пары ключ/значение для узлов. Примечательно, что граф процесса описывает только статическую структуру, т.е. схему бизнес-процесса. Граф процесс может быть легко связан с графическим отображением подхода УФО.

Чтобы описать граф процесса с помощью семантики алгебры процессов, воспользуемся следующим алгоритмом:

Алгоритм 1. Описание графа процесса в семантике алгебры процессов.

Граф процесса $P = (N, E, T, A)$ представляется в виде элементов пи-исчисления следующим образом:

1. Все узлы процесса P соответствуют уникальным идентификаторам пи-исчисления $N1...N \mid P_N \mid$.

2. Все ребра процесса P соответствуют именам пи-исчисления $e1...e \mid P_E \mid$.

3. Внутреннюю деятельность процесса будем обозначать τ. Если граф процесса цикличный, то используется рекурсия для возможности многократного выполнения экземпляра деятельности.

4. Элемент $N \stackrel{def}{=} (\nu e1,..., e \mid P_E)(\prod_{i=1}^{|P_N|} N_i)$ описывает экземпляр процесса.

Любой бизнес-процесс можно представить как набор из основных конструкций. К основным конструкциям бизнес-процессов можно отнести [4] представленные в таблице 1.

На рисунке 2 представлен бизнес-процесс, ранее показанный на рисунке 1, в упрощенном виде. В данном случае все действия (задачи) представлены в виде процессов, переходы между действиями заменены именованными потоками процесса, шлюзы заменены блоками параллельного разделения, синхронизации и выбора.

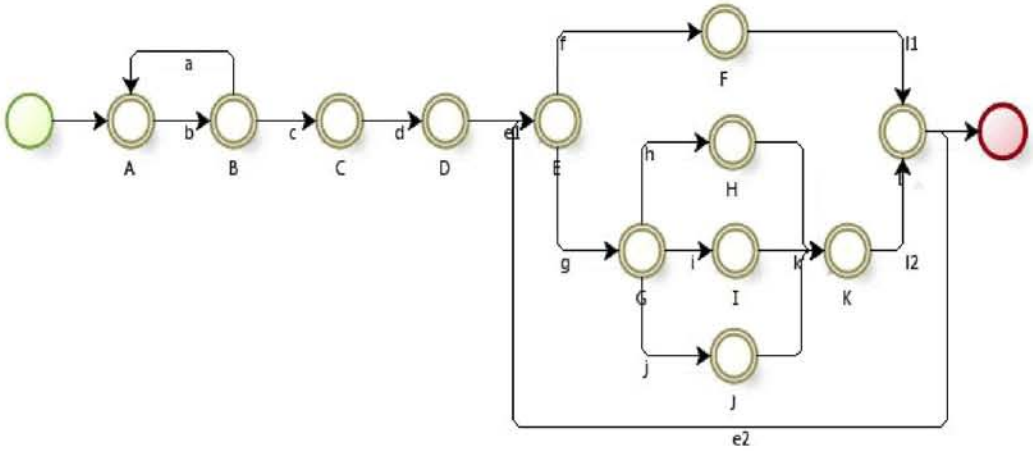


Рисунок 2 – Упрощенный вид бизнес-процесса переключения освещения

Процессы, показанные на рисунке 2, могут быть представлены в терминах пи-исчисления следующим образом:

$$A =! a(x).\tau_A.\overline{b}\langle x\rangle.0$$

$$B =! b(x).\tau_B.(\overline{a}\langle x\rangle.0 + \overline{c}\langle x\rangle.0)$$

$$C = c(x).\tau_C.\overline{d}\langle x\rangle.0$$

$$D = d(x).\tau_D.\overline{e}\langle x\rangle.0$$

$$E = e1(x).!e2(x).\tau_E.(\overline{f}\langle x\rangle.0 \mid \overline{g}\langle x\rangle.0)$$

$$F =! f(x).\tau_F.\overline{l1}\langle x\rangle.0$$

$$G =! g(x).\tau_G.(\overline{h}\langle x\rangle.0 + \overline{i}\langle x\rangle.0 + \overline{j}\langle x\rangle.0)$$

$$H =! h(x).\tau_H.\overline{k}\langle x\rangle.0$$

$$I = !i(x).\tau_I.\overline{k}\langle x\rangle.0$$

$$J = !j(x).\tau_J.\overline{k}\langle x\rangle.0$$

$$K = !k(x).\tau_K.\overline{l2}\langle x\rangle.0$$

$$L = (!l1(x) \mid l2(x)).\tau_L.(\overline{e2}\langle x\rangle.0 + 0)$$

Таким образом, весь бизнес-процесс переключения освещения может быть описан в виде следующих выражений.

$$P = A \mid B \mid (A + C) \mid D \mid E \mid (F \mid (G \mid H + I + J \mid K)) \mid L \mid (E + 0) \text{ или}$$

$$P = !a(x).\tau_A.\overline{b}\langle x\rangle.0 \mid !b(x).\tau_B.(\overline{a}\langle x\rangle.0 + \overline{c}\langle x\rangle.0) \mid (!a(x).\tau_A.\overline{b}\langle x\rangle.0) + (c(x).\tau_C.\overline{d}\langle x\rangle.0) \mid$$

$$d(x).\tau_D.\overline{e}\langle x\rangle.0 \mid e1(x).!e2(x).\tau_E.(\overline{f}\langle x\rangle.0 \mid \overline{g}\langle x\rangle.0) \mid (!f(x).\tau_F.\overline{l1}\langle x\rangle.0) \mid$$

$$(!g(x).\tau_G.(\overline{h}\langle x\rangle.0 + \overline{i}\langle x\rangle.0 + \overline{j}\langle x\rangle.0) \mid (!h(x).\tau_H.\overline{k}\langle x\rangle.0 + !i(x).\tau_I.\overline{k}\langle x\rangle.0 + !j(x).\tau_J.\overline{k}\langle x\rangle.0) \mid$$

$$!k(x).\tau_K.\overline{l2}\langle x\rangle.0)) \mid (!l1(x) \mid l2(x)).\tau_L.(\overline{e2}\langle x\rangle.0 + 0 \mid (e1(x).!e2(x).\tau_E.(\overline{f}\langle x\rangle.0 \mid \overline{g}\langle x\rangle.0 + 0)$$

ВЫВОДЫ

Моделирование бизнес-процессов – это эффективное средство поиска путей оптимизации, средство прогнозирования и минимизации рисков, возникающих на различных этапах управления процессами.

Использование BPMN в качестве нотации для моделирования бизнес-процессов является мощным и современным инструментом. Этот инструмент нацелен на бизнес-аналитиков, архитекторов и разработчиков программного обеспечения. Данная нотация создавалась как способ сделать более быстрой всю разработку деловых процессов от их проектирования до внедрения, такая гибкость и простота осуществляется за счет процессно-ориентированного подхода к моделированию приложений.

Использование пи-исчисления в качестве формального аппарата для описания моделей BPMN даёт возможность создавать средства имитационного моделирования бизнес-процессов и решать задачи верификации процессов.

Моделирование бизнес-процессов для управления уличным освещением с помощью BPMN-моделей и пи-исчисления позволило решить задачи мониторинга и диагностики сетей, управления переключениями и учета энергопотребления, а также более рационально организовать взаимодействие генерирующих компаний с конечными плательщиками электрической энергии.

СПИСОК ЛИТЕРАТУРЫ

1. Михелев М.В. Формализация бизнеса с помощью графоаналитических моделей / М.В. Михелев, С.И. Маторин // «Научные ведомости БелГУ». Сер. «Информатика». – Белгород, 2009. – №1(56). – Выпуск №9/1. – С. 86-94.
2. Михелев М.В. Моделирование бизнес-процессов в управлении наружным освещением / М.В. Михелев, С.И. Маторин // Журнал научных публикаций аспирантов и докторантов. – Курск, 2009. – №3. – С. 136-139.
3. R. Milner Communicating and Mobile Systems: the π-Calculus. Cambridge University Press, ISBN 052164320, 1999.
4. Михелев М.В. Формализация моделей процессов на основе пи-исчисления / М.В. Михелев, С.И. Маторин // «Научные ведомости БелГУ». Сер. «Информатика». – Белгород, 2009. – №9(64). – Выпуск 11/1 (третий выпуск).

Михелев Михаил Владимирович
Белгородский государственный университет, г. Белгород
Ассистент кафедры прикладной информатики
Тел.: (4722) 30-13-56
E-mail: mikhelevmv@gmail.com

M.V. MIKHELEV

FORMALIZED METHOD OF THE DESIGNING CONTROL SISTEM

Discuss capacity of the mathematical description of visual graphic-analytical models, by means of the algebraic device "pi-calculation" by R.Milner, on an example of models control processes of outward illumination in standard BPMN.

Keywords: *visual graphic-analytical design; automation of construction of diagrams; BPMN; pi-calculation; management outward illumination; business-process.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Mixelev M.V. Formalizaciya biznesa s pomoshh'yu grafoanaliticheskix modelej / M.V. Mixelev, S.I. Matorin // «Nauchny'e vedomosti BelGU». Ser. «Informatika». – Belgorod, 2009. – № 1(56). – Vy'pusk №9/1. – S.86-94.
2. Mixelev M.V. Modelirovanie biznes-processov v upravlenii naruzhny'm osveshheniem / M.V. Mixelev, S.I. Matorin // Zhurnal nauchny'x publikacij aspirantov i doktorantov. – Kursk, 2009. – №3. – S.136-139.
3. R. Milner Communicating and Mobile Systems: the π-Calculus. Cambridge University Press, ISBN 052164320, 1999.
4. Mixelev M.V. Formalizaciya modelej processov na osnove pi-ischisleniya / M.V. Mixelev, S.I. Matorin // «Nauchny'e vedomosti BelGU». Ser. «Informatika». – Belgorod, 2009. – №9 (64). – Vy'pusk 11/1 (tretij vy'pusk).

УДК 621.38

М.М. НЕЧИСТЯК, И.В. ФЕДОРЕНКО

МОДЕЛИРОВАНИЕ КАНАЛА ПЕРЕДАЧИ ИЗМЕРИТЕЛЬНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ПРОДУКТА ELECTRONICS WORKBENCH

Представлена модель канала передачи измерительной информации в виде зависимости выходного сигнала от входного воздействия, аппроксимируемой степенным полиномом. Получены выражения для коэффициентов аппроксимации в случае передачи импульсного испытательного сигнала и приведен пример их расчета по результатам компьютерного моделирования канала программными средствами Electronics Workbench.

***Ключевые слова**: модель канала; степенной полином; коэффициенты аппроксимации; амплитуды гармоник; компьютерное моделирование.*

Информация о состоянии сложных технических и промышленных объектов появляется на основе измерения сотен, а то и тысяч технологических параметров. Для обеспечения их измерения, а также дистанционной передачи на пункты диспетчерского управления используются системы контроля объектов, которые можно разбить на три группы: телеметрические системы; системы технологической сигнализации и информационно-измерительные системы.

В состав указанных систем входят каналы передачи измерительной информации, имеющие различные названия в зависимости от вида системы: каналы телеизмерений, каналы передачи извещений либо просто, измерительные каналы. Обобщенным для различных систем контроля является канал передачи измерительной информации (КПИИ), представляющий собой функционально объединенную совокупность средств измерений (СИ) и линии связи, по которым проходит один последовательно преобразуемый информативный сигнал, выполняющий законченную функцию измерения.

Разработка любого радиоэлектронного устройства сопровождается физическим или математическим моделированием. Физическое моделирование связано с большими материальными затратами, поскольку требуется изготовление макетов и их трудоемкое исследование. Поэтому на этапах проведения поисково-исследовательских работ прибегают к математическому моделированию с использованием средств и методов вычислительной техники.

Согласно [1], «математическая модель средства измерения – описание математическими средствами особенностей и свойств СИ, влияющих на результат измерения». К числу метрологических характеристик, предназначенных для определения результата измерения, относится функция преобразования СИ, определяемая как «зависимость информативного параметра выходного сигнала измерительного преобразователя от информативного параметра его входного сигнала» [2]. В [3] под математической моделью канала понимают указание характеристик его входных и выходных сигналов в их математической взаимосвязи. При этом должны быть заданы множество допустимых входных сигналов X, множество выходных сигналов Y и связывающее их отображение $X \Rightarrow Y$.

Часто требуется решение задачи моделирования в общем виде, не связанном с конкретными численными значениями параметров КПИИ, т.е. в виде формул,

отражающих связь воздействия X и реакции Y. В этом случае практикуется представление аналитической модели канала аппроксимирующей функцией в виде степенного полинома [1]:

$$Y = a_1 X + a_2 X^2 + a_3 X^3 + \ldots \quad (1)$$

где $a_1, a_2, a_3, \ldots$ – коэффициенты аппроксимации, значения которых определяют вид характеристики $Y = f(X)$. Для определения указанных коэффициентов целесообразно использовать современные вычислительные средства.

Целью статьи является разработка методики оценки коэффициентов аппроксимации зависимости $Y = f(X)$ в виде степенного полинома на основе сочетания методов аналитического и компьютерного моделирования.

Известные методы оценки амплитудных характеристик различных каналов с помощью измерителей уровня предполагают передачу по ним испытательных гармонических сигналов с прекращением передачи по каналам информационных сигналов [4]. Предлагается методика косвенного измерения коэффициентов аппроксимации $a_1, a_2, a_3, \ldots$ модели (1) по результатам оценки параметров, передаваемых по каналу импульсных сигналов.

Сигнал, представляющий собой последовательность импульсов с высотой (размахом) E, длительностью t_u и периодом следования T, может быть разложен в ряд Фурье [1, 4]:

$$x(t) = \frac{1}{2} \sum_{k=-\infty}^{\infty} A_k \exp(jk\Omega t), \quad (2)$$

где $A_k = \frac{2}{T} \int_{-t_u/2}^{t_u/2} E \exp(-jk\Omega t) dt = 2E \frac{t_u}{T} \sin c\left(\frac{k\Omega t_u}{2}\right)$ – комплексная амплитуда k–й гармоники; $\Omega = 2\pi/T$; $\sin c\alpha = \sin\alpha/\alpha$.

При скважности двухполярных импульсов $T/t_u = 2$, что соответствует передаче по каналу, так называемых «точек», используемых, например, при измерении краевых искажений дискретных сигналов; с учетом того, что комплексная амплитуда содержит только вещественную часть, ряд (2) приобретает вид [5]:

$$x(t) = E \sum_{k=1}^{\infty} \sin c(k\pi/2) \cdot \cos(k\Omega t), \quad (3)$$

а для амплитуд спектральных составляющих можно записать

$$A_k = 2E \left|\sin(k\pi/2)\right| / k\pi . \quad (4)$$

Таким образом, спектр рассматриваемого сигнала состоит лишь из нечетных гармоник. Взяв в формуле (4) отношение амплитуд гармоник с номерами k и l, находим, что $A_k / A_l = l/k$, т.е. имеет место пропорциональное уменьшение амплитуды с увеличением номера гармоники. Это означает, что первая гармоника характеризуется энергией в 9 раз большей, чем третья гармоника, и в 25 раз большей, чем пятая гармоника и т.д. В итоге на долю первой и третьей гармоник приходится около 95% энергии колебания. При этом можно получить достаточно хорошее воспроизведение формы колебания при сохранении в спектре лишь определенного количества составляющих (например, трех). В этом случае ряд (3) для сигнала со скважностью $T/t_u = 2$, ограниченный третьей гармоникой, имеет вид:

$$x(t) = x_1(t) + x_3(t) = A_1 \cos(\Omega t) + A_3 \cos(3\Omega t). \quad (5)$$

При прохождении сигнала $x(t)$ через канал, модель которого аппроксимируется полиномом (1) третьей степени, его выходной сигнал можно рассматривать как результат воздействия двух гармонических колебаний на нелинейный элемент:

$$y(t)=a_1[x_1(t)+x_3(t)]+a_2[x_1(t)+x_3(t)]^2+a_3[x_1(t)+x_3(t)]^3. \quad (6)$$

С учетом (5) преобразуем выражение (3) и получаем сумму гармонических составляющих:

$$y(t)=U_1\cos(\Omega t)+U_2\cos(2\Omega t)+U_3\cos(3\Omega t)+\dots, \quad (7)$$

где амплитуды гармонических составляющих выходного сигнала КПИИ [6]:

$$U_1=\left(a_1+14a_3E^2/3\pi^2\right)\frac{2E}{\pi};\quad U_2=10a_2E^2/3\pi^2;\quad U_3=\left(a_1+28a_3E^2/3\pi^2\right)\frac{2E}{3\pi}. \quad (8)$$

Решая систему уравнений (8) относительно a_1, a_2, a_3, находим коэффициенты аппроксимации для модели (1) канала:

$$a_1=\frac{\pi(2U_1-3U_3)}{2E};\quad a_2=\frac{\pi^2U_2}{10E^2};\quad a_3=\frac{3\pi^3(3U_3-U_1)}{28E^3}. \quad (9)$$

На основе полученных аналитических выражений (9) предлагается методика моделирования КПИИ, суть которой сводится к следующему. Исходными данными для расчета коэффициентов аппроксимации, представленных выражениями (9), являются высота импульсов (амплитуда – для однополярных импульсов) E входного сигнала и амплитуды спектральных составляющих U_1, U_2, U_3 сигнала на выходе канала. Для получения результатов измерения указанных параметров используем компьютерную программу схемотехнического моделирования Electronics Workbench (EWB) [7]. Особенностью программы является наличие в ней виртуальных контрольно-измерительных приборов, по внешнему виду, органам управления и характеристикам максимально приближенных к их промышленным аналогам. На рисунке 1 представлен пример компьютерного моделирования КПИИ средствами EWB.

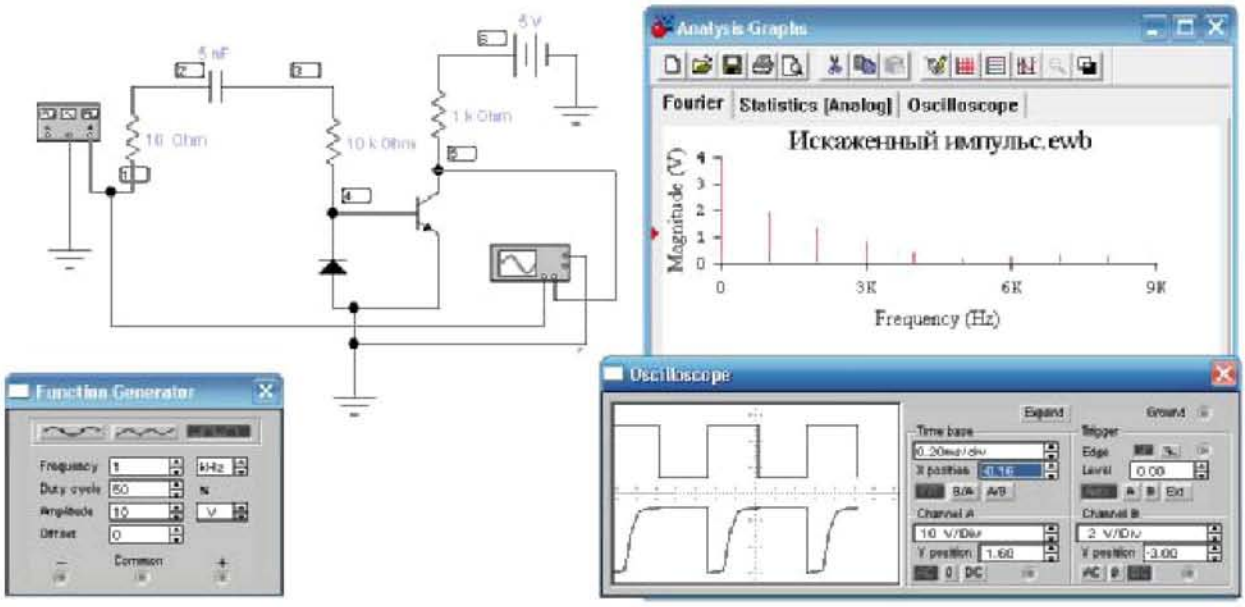


Рисунок 1 – Результат моделирования КПИИ средствами Electronics Workbench

В качестве источника испытательного сигнала используется функциональный генератор, формирующий двухполярный импульсный сигнал с амплитудой $\pm 10[V]$ и

размахом $E = 20\,[V]$ (верхние эпюры на экране осциллографа). Выходной сигнал исследуемого канала представляет собой последовательность искаженных импульсов (нижние эпюры на экране осциллографа) с амплитудами спектральных составляющих $U_1 = 1{,}9\,[V]$, $U_2 = 1{,}4\,[V]$, $U_3 = 0{,}8\,[V]$, отображенными на экране Analysis Graphs в режиме Фурье-анализа. Подставляя измеренные значения напряжений в выражение (9), рассчитываем коэффициенты аппроксимации a_1, a_2, a_3.

ВЫВОДЫ

Достоинством данной методики моделирования канала передачи измерительной информации является возможность оценки его характеристик непосредственно по значениям параметров выходного импульсного сигнала, отображаемых на виртуальных приборах программного продукта Electronics Workbench. Точность аппроксимации модели КПИИ определяется выбором числа учитываемых гармонических составляющих в выражении (3) и степени аппроксимирующего полинома (1). Наличие наглядного отображения результатов моделирования канала с помощью программного продукта EWB (на экране Analysis Graphs) позволяет подобрать ограничения на количество учитываемых гармоник выходного сигнала.

Результаты, представленные в статье, получены при выполнении НИР в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг.

СПИСОК ЛИТЕРАТУРЫ

1. Назаров Н.Г. Метрология. Основные понятия и математические модели. – М.: Высшая школа, 2002. – 348 с.
2. ГОСТ 8.009-84. Нормируемые метрологические характеристики средств измерений. – М.: Госстандарт СССР, 1984.
3. Галкин А.П., Лапин А.Н., Самойлов А.Г. Моделирование каналов систем связи. – М.: Связь, 1979. – 96 с.
4. Метрологическое обеспечение систем передачи; под ред. Б.П. Хромого. – М.: Радио и связь, 1991. – 392 с.
5. Солодовников А.И., Спиваковский А.М. Основы теории и методы спектральной обработки информации. – Л.: Изд-во ЛГУ, 1986. – 272 с.
6. Федоренко В.В., Боровлев И.И., Борисов С.Г. Аналитическая методика оценки амплитудной характеристики нелинейного канала передачи импульсных сигналов // Известия ВУЗов. Радиоэлектроника, 1994. – № 6. – С. 74-76.
7. Карлащук В.И. Электронная лаборатория на IBM PC. Лабораторный практикум на базе Electronics Workbench и MATHLAB. – М.: СОЛОН-Пресс, 2004. – 800 с.

Нечистяк Максим Михайлович
Северо-Кавказский государственный технический университет, г. Ставрополь
Аспирант кафедры информационных систем и технологий
Тел.: 8 918 862 36 35
E-mail: berlin7@rambler.ru

Федоренко Ирина Владимировна
Северо-Кавказский государственный технический университет, г. Ставрополь
Аспирант кафедры защиты информации
Тел.: 8 906 479 05 79
E-mail: fovin_25@mail.ru

M.M. NECHISTYAK, I.V. FEDORENKO

DESIGN CHANNEL OF TRANSMISSION INSTRUMENTATION WITH USING OF SOFTWARE PRODUCT ELECTRONICS WORKBENCH

The channel model of measuring information transfer is presented as a dependence of an output signal on an entrance influence, which is approximated by a power polynomial. The expressions for the approximation coefficients are received in the case of an impulsive test transmission and the example of their calculation with Electronics Workbench is presented.

Keywords: *channel model; sedate polynomial; approximation coefficients; amplitudes of harmonics; computer modeling.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Nazarov N.G. Metrologiya. Osnovny'e ponyatiya i matematicheskie modeli. – Vy'sshaya shkola, 2002. – 348 s.
2. GOST 8.009-84. Normiruemy'e metrologicheskie xarakteristiki sredstv izmerenij. – M.: Gosstandart SSSR, 1984.
3. Galkin A.P., Lapin A.N., Samojlov A.G. Modelirovanie kanalov sistem svyazi. – M.: Svyaz', 1979. – 96 s.
4. Metrologicheskoe obespechenie sistem peredachi; pod red. B.P. Xromogo. – M.: Radio i svyaz', 1991. – 392 s.
5. Solodovnikov A.I., Spivakovskij A.M. Osnovy' teorii i metody' spektral'noj obrabotki informacii. – L.: Izd-vo LGU, 1986. – 272 s.
6. Fedorenko V.V., Borovlyov I.I., Borisov S.G. Analiticheskaya metodika ocenki xarakteristiki nelinejnogo kanala peredachi impul'sny'x signalov // Izvestiya VUZov. Radioe`lektronika, 1994. – №6. – S.74-76.
7. Karlashhuk V.I. E'lektronnaya laboratoriya na IBM PC. Laboratorny'j praktikum na baze Electronics Workbench и MATHLAB. – M.: SOLON-Press, 2004. – 800 s.

УДК 004.891

М.А. САЗОНОВ, С.И. ФОМИН

МЕТОД ФОРМИРОВАНИЯ ЭКСПЕРТНОЙ ГРУППЫ В УСЛОВИЯХ НЕПОЛНЫХ ВХОДНЫХ ДАННЫХ

В статье представлен метод формирования экспертной группы по тематике проблемной ситуации и определена роль подсистемы формирования экспертной группы в распределенной системе сбора и обработки экспертных данных. Приводится порядок формализации проблемной ситуации и представления ее в виде кортежа, состоящего из векторов и точечных значений. Авторами метода разработан алгоритм формализации тематики проблемной ситуации. Он основан на едином классификаторе с учетом приоритета экспертов и ранжирования их для формирования компетентной группы ограниченного состава для конкретной ситуации.

Ключевые слова: *эксперт; экспертная группа; проблемная ситуация; классификатор; тематика; ЛПР; рейтинг; уровень знаний; область знаний; степень соответствия области знаний заданной тематике.*

ВВЕДЕНИЕ

В настоящее время высокие темпы внедрения информационных технологий привели к существенному росту объемов хранимой и передаваемой информации различных форматов. Её разнородность, сложность релевантного поиска и обработки затрудняют формирование у лица, принимающего решение, своевременного, точного и актуального представления о конкретной предметной области. Кроме того, лицо, ответственное за принятие решения (ЛПР), не может обладать всем спектром знаний в объеме, достаточном для принятия оптимального решения в различных сферах деятельности. Это требует привлечения групповых оценок экспертов хотя бы на этапе выработки альтернативных решений [1].

Примером простой задачи отбора экспертной группы является формирование заявки на закупку технического оборудования для организации. В этом случае в экспертную группу, как правило, войдут сотрудники отдела технического обеспечения и их выбор будет безальтернативным, что свойственно для принятия решений на нижних уровнях управления. В иных ситуациях, когда проблема носит нестандартный комплексный характер, задача выбора компетентных экспертов (формирования оперативного штаба) уже не будет тривиальной. К таким, например, относятся сложные техногенные чрезвычайные ситуации, требующие немедленного разрешения и принятия мер по минимизации и устранению последствий. В этом случае время формирования экспертной группы ограничено, поскольку проблема требует скорейшего разрешения. Численно состав также ограничен, так как работа с большой группой снижает оперативность сбора информации, усложняет поиск согласованного решения и затрудняет одновременное представление мнений большого количества специалистов.

Процесс поиска решения легче организовать в таких условиях, когда множество проблемных ситуаций имеют узкий тематический спектр. Например, при решении узкоспециализированных задач, где множество входных данных ограничено, а цель хорошо формализована, или на нижних уровнях управления, когда перечень типовых задач четко определен и пути их решения в достаточной степени проработаны. С повышением уровня иерархии управления и расширением спектра тематического охвата сложность проблемы формирования альтернативных решений и выбора наилучшего из них возрастает.

Таким образом, принятие решений на уровне руководства предприятия или организации характеризуется:

– широким спектром и неоднородной тематикой выполняемых задач;

– высокой неопределенностью процесса поиска альтернатив принятия решений и выбора наилучшей из них;

– уникальностью условий множества проблемных ситуаций;

– отсутствием полного набора типовых решений;

– вероятностным характером результатов принятых решений.

В таких условиях наиболее распространенным способом поиска и выбора решений является экспертный подход, предполагающий привлечение специалистов, задача которых состоит в выработке альтернатив и снижении неопределенности последствий принятых решений. Реализация такого подхода требует предварительной подготовки и привлечения нескольких специалистов, компетентных в рассматриваемой тематике, так как традиционно полагается, что мнение группы надежнее, чем мнение одного специалиста (эксперта) [2]. Последовательность реализации экспертного оценивания представлена на рисунке 1. Этап формирования экспертной группы является промежуточным, но от его эффективности в значительной степени зависит качество информации, используемой при выработке альтернатив принятия решений.

Существуют различные способы организации экспертного оценивания, начиная с простейших, таких, как метод «мозгового штурма», заканчивая более сложными процедурами, такими, как методы Дельфи или Терстоуна [3]. Однако ни один из них не гарантирует поиск оптимального решения, если состав экспертной группы недостаточно компетентен в необходимом спектре тематик предметных областей разрешаемой проблемы. Соответственно, в состав группы должны входить специалисты с уровнем компетентности, обеспечивающим выработку наилучшего решения в сложившейся ситуации.

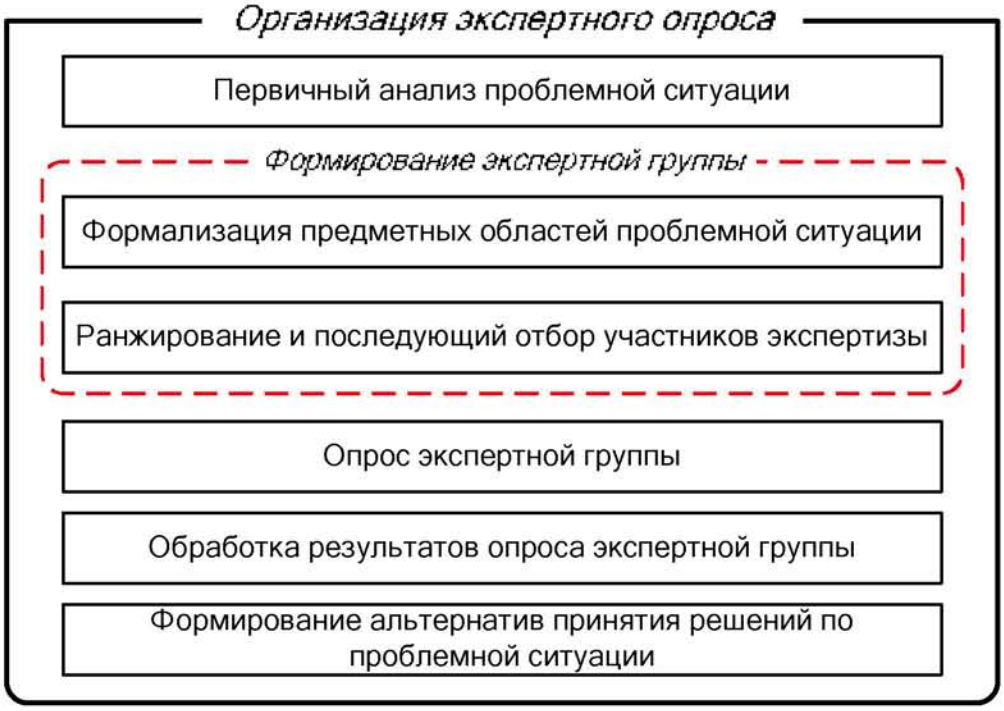


Рисунок 1 – Основные этапы экспертного оценивания

ОСНОВНАЯ ЧАСТЬ

Постановка задачи формирования экспертной группы

Суть идеи отбора экспертов основана на следующих утверждениях:

– каждая проблемная ситуация характеризуется набором тематик (отдельных областей знаний) и интенсивностью их включения (весовыми коэффициентами);

– тематики задаются в соответствии с классификационным принципом покрытия и являются классами толерантности;

– каждый эксперт характеризуется компетентностью в различных областях знаний и её глубиной;

– множество экспертов может пополняться;

– гипотетическое множество проблемных ситуаций содержит все возможные тематики;

– множество тематик конечно и определено.

– С учетом вышесказанного разработана модель формирования экспертной группы, представленная на рисунке 2.

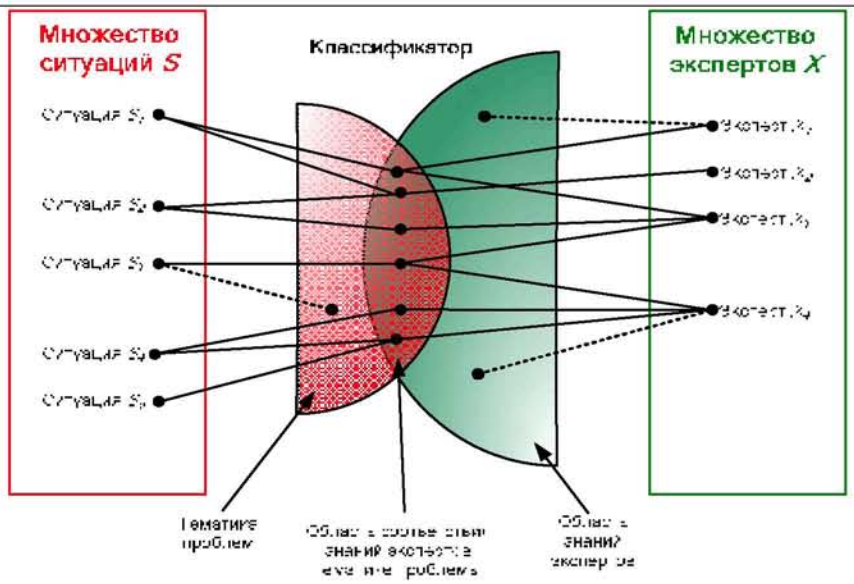


Рисунок 2 – Модель отбора для формирования экспертной группы

Экспертные группы по ситуациям:

S_1 для $K_1^{\{S_1\}} : w_{K_1^{\{X_2\}}}, w_{K_1^{\{X_3\}}} > 0$

для $K_2^{\{S_1\}} : w_{K_1^{\{X_2\}}} > 0$

S_2 для $K_1^{\{S_2\}} : w_{K_1^{\{X_3\}}} > 0$

для $K_2^{\{S_2\}} : w_{K_2^{\{X_3\}}} > 0$

S_3 для $K_1^{\{S_3\}} : w_{K_3^{\{X_3\}}}, w_{K_1^{\{X_4\}}} > 0$

S_4 для $K_1^{\{S_4\}} : w_{K_2^{\{X_4\}}} > 0$

для $K_2^{\{S_4\}} : w_{K_3^{\{X_4\}}} > 0$

S_5 для $K_1^{\{S_5\}} : w_{K_3^{\{X_4\}}} > 0$

В основе моделируемого процесса лежит классификатор K, объединяющий области знаний экспертов и формулировку проблемной ситуации, что позволяет производить отбор экспертов для их опроса в рамках сформулированной проблемы. Структура классификатора имеет иерархический вид.

Используя теоретико-множественный подход, представим модель в виде выражения:

$$\forall\left(K_j^{\{S_i\}} \in S\right)\exists\left(K_p^{\{X_i\}} \in X\right) : w_{K_p^{\{X_i\}}} > 0,$$

где X – множество экспертов;

$K_p^{\{X_i\}}$ – области знаний эксперта;

$K_j^{\{S_i\}}$ – области знаний, которые затрагивает ситуация;

$w_{K_p^{\{X_i\}}}$ – уровень компетентности эксперта в области знаний;

S – множество ситуаций;

S_i – конкретная ситуация, характеризуемая набором областей знаний.

Приведенный на рисунке 2 пример позволяет наблюдать, что для принятия решения по ситуациям сформированы соответствующие экспертные группы.

Таким образом, решение задачи формирования экспертной группы производится с учетом следующих допущений:

– *в исходную выборку входят эксперты, перечень компетенций которых перекрывает тематику рассматриваемых проблемных ситуаций;*

– *о каждом эксперте имеется полная актуальная информация, позволяющая определить уровень его компетентности по отдельной тематике;*

и ограничений:

– *численность экспертной группы ограничена некоторым заранее заданным числом (численность оперативного штаба, заданное количество респондентов и т.д.);*

время формирования группы ограничено.

Структура метода формирования экспертной группы

Для формирования экспертной группы с учетом указанных допущений и ограничений предложен способ, позволяющий учитывать тематику проблемной ситуации. Концептуальное представление работы указанного способа представлено на рисунке 3. В его основе лежит сопоставление в единимом классификаторе описания проблемной ситуации и взвешенного формализованного представления о компетенциях эксперта в известных областях знаний. Специалист анализирует формулировку проблемной ситуации, производит ее формализацию и передает в модуль ранжирования. В него же поступает заранее подготовленная формализованная информация о компетенциях экспертов. Затем на основе векторного сравнения с учетом весовых коэффициентов производится расчет рейтинга экспертов. По результатам расчета генерируются ранжированные списки, на основе которых ЛПР формирует итоговую группу компетентных экспертов.

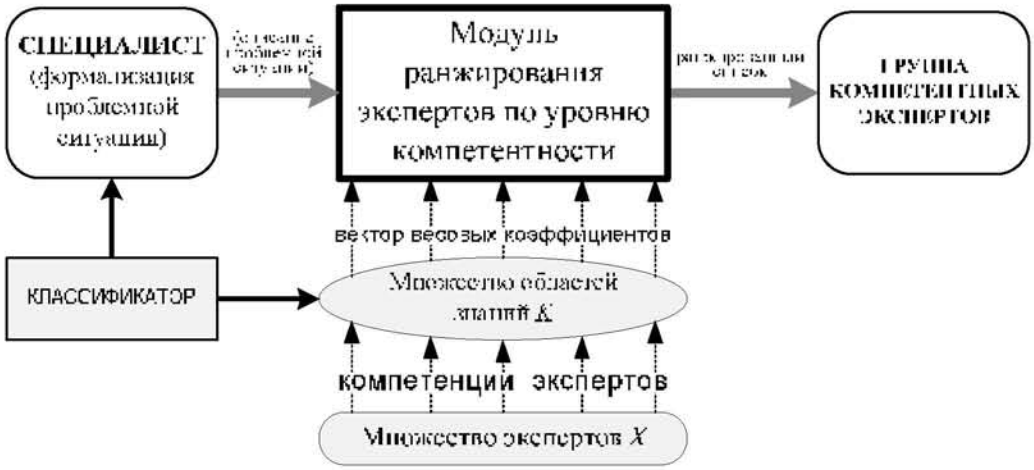


Рисунок 3 – Структура метода формирования экспертной группы

Комплекс моделей

Для решения задачи формирования экспертной группы используются модели ситуации, эксперта и процесса формирования экспертной группы.

1. Модель ситуации:

$$S_i = \left\langle K^{\{S_i\}}, P^{\{S_i\}}, G^{\{S_i\}}, M^{\{S_i\}} \right\rangle,$$

где $K^{\{S_i\}} = \bigcup_{j=1}^{n} \left[k_j^{\{S_i\}}; w_j^{\{S_i\}} \right]$ – области знаний, которые затрагивает ситуация;

$k_j^{\{S_i\}}$ – предметная область ситуации на низшем уровне иерархии;

$w_j^{\{S_i\}}$ – весовой коэффициент предметной области $k_j^{\{S_i\}}$ в ситуации S_i;

$G^{\{S_i\}}$ – географическое местоположение исследуемой ситуации;

$M^{\{Y_i\}}$ – масштаб ситуации, множество значений.

2. Модель эксперта:

$$X_i = \left\langle K^{\{X_i\}}, J^{\{X_i\}}, N^{\{X_i\}}, U^{\{X_i\}}, E^{\{X_i\}} \right\rangle,$$

где X_i – модель эксперта;

$J^{\{X_i\}}$ – место работы эксперта;

$N^{\{X_i\}} = \bigcup_{j=1}^{n} \left[kn_j^{\{X_i\}}; wn_j^{\{X_i\}} \right]$ – научные работы и публикации эксперта;

$kn_j^{\{X_i\}}$ – область знаний научной работы на низшем уровне иерархии;

$wn_j^{\{X_i\}}$ – степень соответствия области знаний $kn_j^{\{X_i\}}$ тематике научной работы;

$U^{\{X_i\}} = \left[uzv^{\{X_i\}}, ust^{\{X_i\}} \right]$ – научные результаты эксперта;

$ust^{\{X_i\}} = \bigcup_{j=1}^{n} \left[kust_j^{\{X_i\}}; wust_j^{\{X_i\}} \right]$ – ученая степень эксперта;

$kust_j^{\{X_i\}}$ – область знаний ученой степени на низшем уровне иерархии (в соответствии с паспортом специальности, утвержденным ВАК России);

$wust_j^{\{X_i\}}$ – степень соответствия области знаний $kust_j^{\{X_i\}}$ направлению ученой степени $ust^{\{X_i\}}$;

$uzv^{\{X_i\}}$ – ученое звание эксперта;

$E^{\{X_i\}} = \bigcup_{j=1}^{n} \left[Y_j, R_j^{\{X_i\}} \right]$ – экспертизы, в которых эксперт принимал участие;

$R_j^{\{X_i\}}$ – значение рейтинга эксперта в *j*-й экспертизе;

$K^{\{X_i\}} = \bigcup_{j=1}^{n} \left[k_j^{\{X_i\}}; w_j^{\{X_i\}} \right]$ – области знаний эксперта, здесь *n* – количество областей знаний;

$k_j^{\{X_i\}}$ – предметная область знаний эксперта на низшем уровне иерархии;

$w_j^{\{X_i\}}$ – уровень знаний эксперта по предметной области $k_j^{\{X_i\}}$, рассчитываемый по формуле:

$$w_j^{\{X_i\}} = \sum_k wn_k^{\{X_i\}} + \sum_p R_p^{\{X_i\}} + \sum_l wust_l^{\{X_i\}}.$$

3. Модель процесса формирования экспертной группы:

$$Y_i = \left\langle T^{\{Y_i\}}, S^{\{Y_i\}}, X^{\{Y_i\}} \right\rangle,$$

где Y_i – модель отбора экспертной группы;

$T^{\{Y_i\}}$ – текстуальная формулировка проблемы для обсуждения экспертной группой;

$S^{\{Y_i\}}$ – модель ситуации, по которой формируется экспертная группа для принятия решения;

$X^{\{Y_i\}}$ – компетентная группа экспертов.

Структура системы сбора и обработки экспертных данных

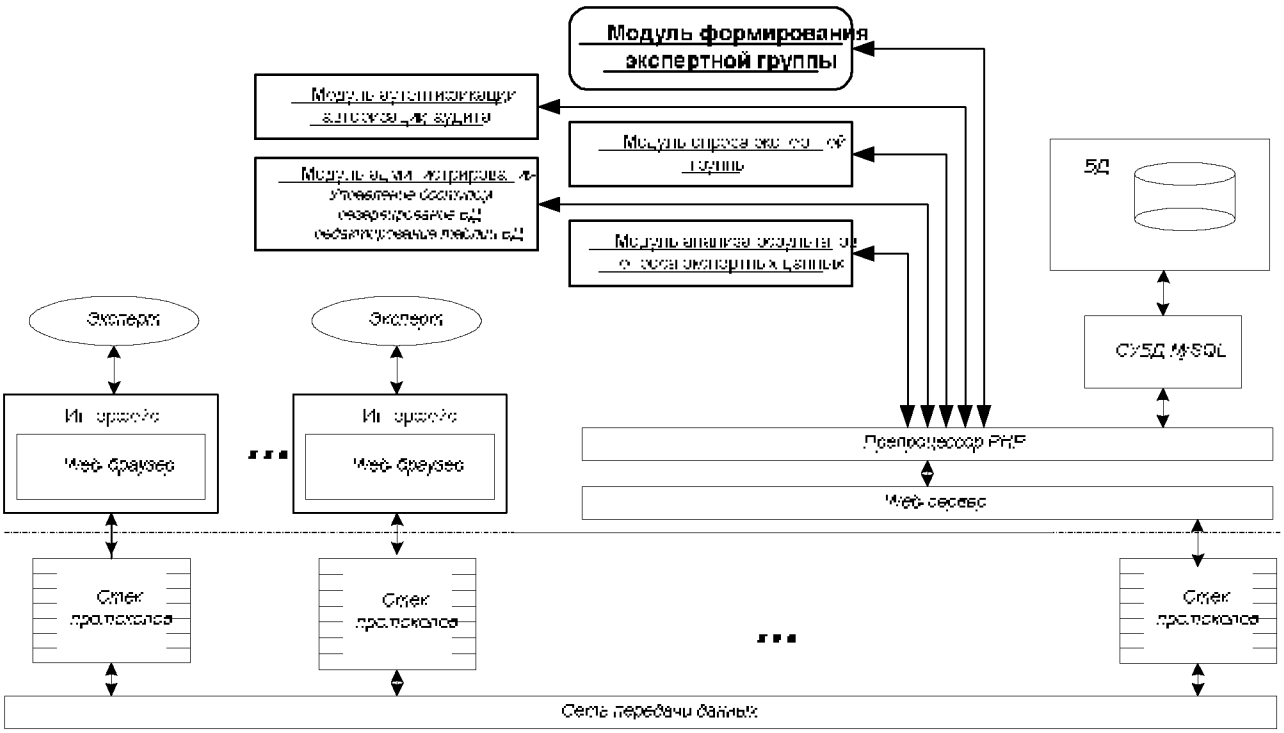


Рисунок 4 – Распределенная система сбора и обработки экспертных данных

Работа системы формирования экспертной группы происходит непосредственно после задания (формализации) специалистом формулировки проблемной ситуации при наличии базы данных экспертов, заполненной с учетом указанных допущений. Работа специалиста начинается с ввода в текстовое поле формулировки проблемной ситуации. Затем выбираются предметные области, затрагиваемые ситуацией, и экспертно указывается степень их соответствия тематике проблемной ситуации.

На первом этапе анализа определяется степень соответствия знаний экспертов $w_j^{\{X_i\}}$ тематике сформулированной проблемной ситуации $S^{\{Y_i\}}$. Рейтинг экспертов составляется на основе аддитивной нормированной свертки полученных значений функции соответствия для знаний эксперта по проблеме. Также фиксируется количество и наименования областей знаний проблемы, которые известны каждому эксперту. По результатам первого этапа в первом приближении возможно сделать вывод о целесообразности привлечения каждого конкретного эксперта в группу для решения проблемы на основе ранжированного списка.

Лицо, ответственное за организацию и проведение экспертного опроса,

получив ранжированные списки, формирует итоговую экспертную группу с учетом возможных ограничений и оповещает выбранных экспертов. Процедура экспертного опроса должна обеспечивать удаленный вызов и доступ экспертов к подсистеме сбора и обработки экспертных данных, также являющейся частью системы экспертного опроса, вариант которой представлен на рисунке 4.

Эксперты получают доступ к системе через интерфейс, который должен функционировать на основе соответствующих протоколов безопасности. Результаты каждого экспертного опроса сохраняются в базе данных и в дальнейшем определяют рейтинг каждого эксперта, привлекавшегося к экспертизе.

ВЫВОДЫ

Внедрение современных технологий автоматизации в процессы управления уже сейчас позволяет существенно снизить рутинную нагрузку на аппарат управления. Работа руководителя все чаще состоит в формировании управленческого решения или его выборе из нескольких альтернатив. Но в определенных условиях, когда проблемная ситуация носит нетривиальный характер, а ошибочное решение может иметь крайне негативные, а иногда и катастрофические последствия, возникает необходимость проведения экспертного оценивания. В этом случае задача формирования экспертной группы является крайне актуальной, определяет результат всей процедуры экспертного опроса и существенно влияет на качество принятого решения. Исходя из этого, процедура формирования группы экспертов должна:

- учитывать специфику конкретной ситуации;
- работать в условиях ограничений, представленных в постановке задачи;
- обеспечивать формирование компетентной экспертной группы при условии выполнения допущений, представленных в постановке задачи.

Предложенный метод формирования экспертной группы позволяет выполнить эти требования за счет формализации тематики ситуации на основе единого классификатора, возможности автоматизации разработанного способа с использованием известных информационных технологий, и использовании детерминированного математического аппарата при формировании ранжированных списков экспертов.

Внедрение описанного метода в дальнейшем позволит реализовать распределенную систему сбора и обработки экспертных данных с возможностью формирования экспертной группы для каждой ситуации с ограничением по численности количеством экспертов. При необходимости сбор информации у представителей выбранной экспертной группы может быть осуществлен дистанционно при условии обеспечения соответствующего уровня конфиденциальности, требуемого как при защите коммерческой информации, так и при защите персональных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С. Системный анализ в управлении: учеб. пособие / А.А. Емельянов, А.А. Кукушкин. – М.: Финансы и статистка, 2009. – 368 с.
2. Сазонов М.А. Проблемы разработки модели процесса принятия решения руководителем подразделения / В.И. Козачок, И.А. Сенотрусов // Информатизация и информационная безопасность правоохранительных органов: XIII Международная науч. конф. 25-26 мая 2003 г. – М.: Академия управления МВД России, 2004. – С.43-45.

3. Джексон Питер. Введение в экспертные системы. – М.: Издательский дом «Вильямс», 2003. – С. 18-29, 211 стр.

Сазонов Михаил Анатольевич
Академия ФСО России, г. Орел
Кандидат технических наук, преподаватель кафедры №32
Тел.: 8 (4862) 40-83-58
E-mail: sma77@list.ru

Фомин Сергей Игоревич
Академия ФСО России, г. Орел
Курсант
Тел.: 8 920 281 76 51
E-mail: xoma686@mail.ru

M.A. SAZONOV, S.I. FOMIN

THE METHOD OF EXPERT GROUP BUILD-UP UNDER INCOMPLETE INPUT DATA CIRCUMSTANCES

The article represents the method of expert group build-up on problem situation subject-matter and the expert group build-up system's place in distributed expert data collection and processing system is defined. The precedence rule of a problem situation formalization and declaration it as a tuple, comprising vectors and point wise values, is outlined. Problem situation subject-matter formalization algorithm was developed by method's authors. It's based on integrated situation classifier which considerates expert's priorities and ranking them to build-up the most qualified group of limited membership for specific situation.

Keywords: *expert; expert group; problem situation; classifier; subject-matter; PTD; rating; knowledge level; area of knowledge; area of knowledge compliance degree to problem situation subject-matter.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Anfilatov V.S. Sistemny'j analiz v upravlenii: ucheb. posobie / A.A. Emel'yanov, A.A. Kukushkin. – M.: Finansy' i statistika, 2009. – 368 s.
2. Sazonov M.A. Problemy' razrabotki modeli processa prinyatiya resheniya rukovoditelem podrazdeleniya / V.I. Kozachok, I.A. Senotrusov// Informatizaciya i informacionnaya bezopasnost' pravooxranitel'ny'x organov: XIII Mezhdunarodnaya nauch. konf. 25-26 maya 2003 g. – M.: Akademiya MVD Rossii, 2004. – S.43-45.
3. Dzhekson Piter. Vvedenie v e`kspertny'e sistemy'. – M.: Izdatel'skij dom «Vil'yams», 2003. – S.18-29, 211 str.

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

УДК 65.011.56

М.П. МАСЛАКОВ

ИСПОЛЬЗОВАНИЕ СЕТЕЙ ПЕТРИ ПРИ МОДЕЛИРОВАНИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ СОСТАВЛЕНИЯ (ПРИГОТОВЛЕНИЯ) СТЕКОЛЬНОЙ ШИХТЫ

Рассмотрены вопросы автоматизации управления составлением (приготовлением) шихты на предприятиях стекольной промышленности. Разработана структурная схема единой автоматизированной системы управления технологическим процессом составления шихты. Построены сети Петри для отдельных этапов технологического процесса составления шихты. Разработана сеть Петри для всего технологического процесса составления шихты.

Ключевые слова: *система управления составлением шихты; моделирование сетями Петри; моделирование технологического процесса.*

Технологический процесс составления (приготовления) стекольной шихты можно разделить на три этапа:

1. Заготовка сырьевых материалов (ЗСМ);
2. Дозирование обработанных сырьевых материалов (ОСМ);
3. Смешивание ОСМ.

На сегодняшний день не существует единой (комплексной) автоматизированной системы управления, которая объединяла бы все три этапа технологического процесса приготовления шихты. Рассмотрим структурную схему системы управления технологическим процессом приготовления шихты, на примере ОАО «Иристонстекло» РСО-Алания г. Владикавказ (рис.1).

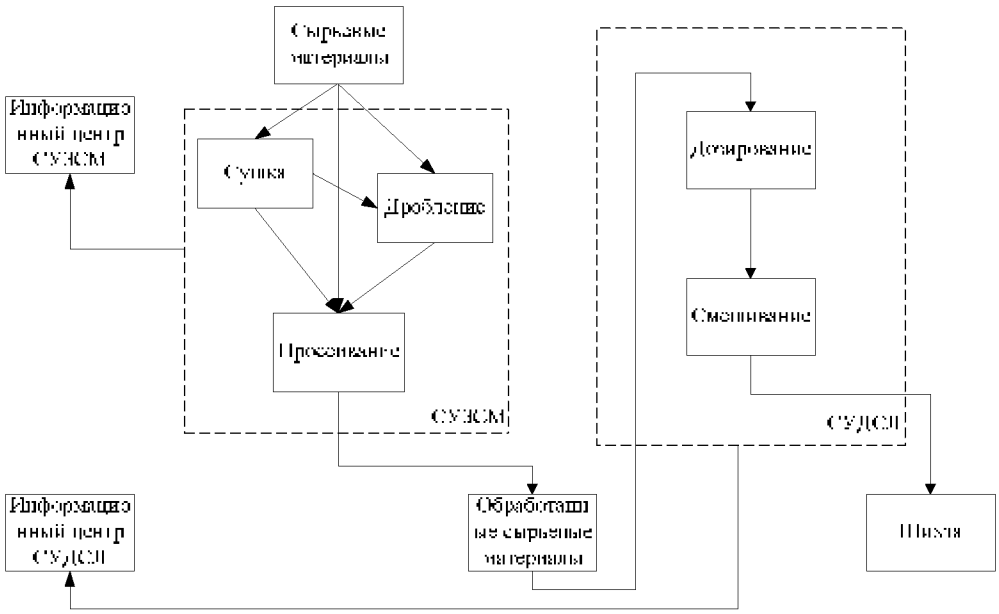


Рисунок 1 – Структурная схема системы управления приготовлением шихты

Данная структурная схема системы управления технологическим процессом приготовления шихты, включающим в себя основные операции – сушка, дробление,

просеивание для сырьевых материалов и дозирование, смешивание – для обработанных сырьевых материалов [2]. В данной системе управления технологическим процессом составления шихты (ТПСШ) этап обработки сырьевых материалов имеет свою систему управления, а также и этап дозирования и смешивания – у него своя система управления (СУДСЛ). Две системы управления СУЗСМ (система управления заготовкой сырьевых материалов) и СУДСЛ (система управления дозировочно-смесительной линией) – это отдельно функционирующие системы, события (операции), происходящие в них, не взаимосвязаны, нет единого контролирующего органа, аварийные ситуации, произошедшие в одной системе, приводящие к ее останову, никак не влияют на работу другой. Основные проблемы при таком роде управления – это либо нехватка сырьевых материалов на этапе дозирования и смешивания, либо слеживание сырьевых материалов из-за избыточности их заготовки. Поэтому целесообразнее и выгоднее использовать единую систему управления всем технологическим процессом приготовления шихты, а не отдельно его этапами, с целью непосредственного контроля наполняемости бункеров (рис. 2).

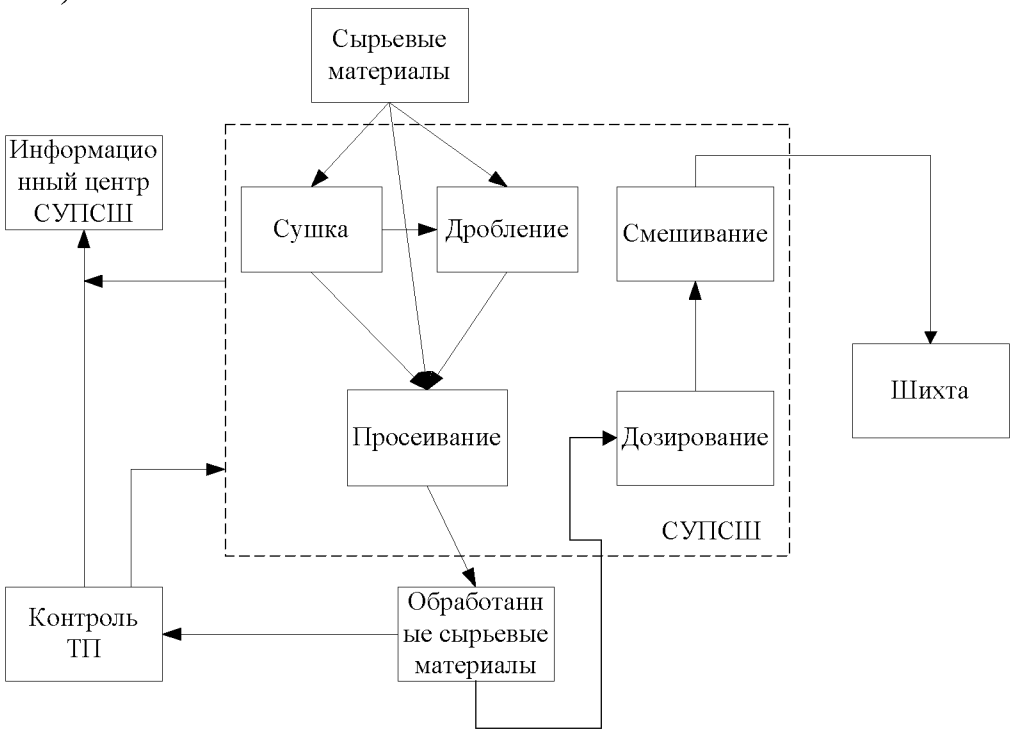


Рисунок 2 – Структурная схема единой АСУ ТП составления (приготовления) шихты

Из данной структурной схемы видно, что все операции технологических этапов приготовления шихты охвачены единой АСУТП составления (приготовления) шихты (СУПСШ). В разработанной АСУТП предусмотрен единый контролирующий орган, осуществляющий наблюдение за наполняемостью бункеров в соответствии с рецептурой на отвесы. Аварийные ситуации в какой-либо технологической операции вызывают цепную реакцию останова взаимосвязанного оборудования процесса в последующей и предыдущей операциях, если нет запаса сырья, для продолжения приготовления шихты. Слёживание компонентов в данной СУ исключается за счет того, что заготавливается столько сырьевого материала, сколько необходимо для нормальной работы СУДСЛ.

Используя структурную схему единой автоматизированной системы управления технологическим процессом приготовления шихты, аппарат сетей Петри

[1] и сам технологический процесс приготовления (его операции), который используется на стекольном заводе ОАО «Иристонстекло», разработаем сеть Петри для единой системы управления технологическим процессом составления шихты.

Изначально построим сети Петри для заговительного этапа технологического процесса приготовления шихты. Этот этап включает заготовку семи сырьевых материалов (песок, мел, доломит, сода, глинозем, содосульфатная смесь, селитра). Сети Петри для каждого компонента выглядят так, как представлено на рисунке 3.

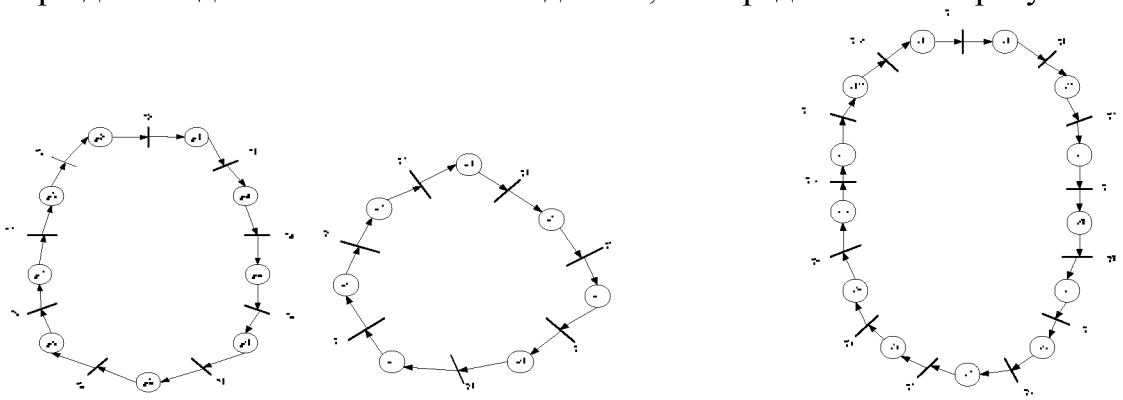


Рисунок 3 – Сеть Петри для заготовки сырьевых материалов
а) – для песка, глинозема, селитры, сульфатно-содовой смеси, мела;
б) – для соды; в) – для доломита

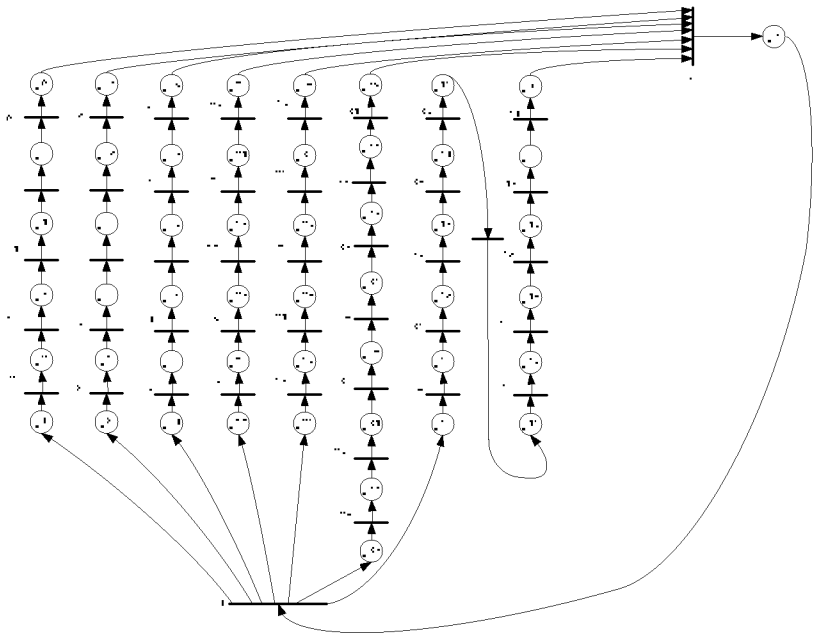


Рисунок 4 – Сеть Петри заготовительного этапа составления (приготовления) шихты

На рисунке 3(а) – типовая сеть Петри для процесса заготовки песка, глинозема, селитры, сульфатно-содовой смеси, мела; они имеют одинаковое количество позиций и переходов, конечно значение для каждого сырья позиций и переходов свои. На рисунке 3(б) – сеть Петри для процесса заготовки соды, (в) – для доломита.

Все процессы заготовки сырьевых материалов асинхронные и осуществляются параллельно друг другу для уменьшения времени на заготовку. Единственное, что их объединяет – это то, что они влияют на 2-ой этап приготовления шихты (дозирование), а точнее на наполняемость бункеров ОСМ, из которых происходит

дозирование СМ. Используя сети Петри, представленные на рисунке 3, выделив сопряженные состояния (в модели (а) это позиция p9, в (б) – это p7, а в (в) – это p13.), строим сеть Петри для всего заготовительного этапа технологического процесса приготовления шихты (рис.4). Сеть Петри заготовительного этапа приготовления шихты, представленная на рисунке 4, включает в себя одновременную заготовку семи сырьевых материалов.

Для построения сети Петри дозирования и смешивания обработанных сырьевых материалов воспользуемся технологией работы дозировочно-смесительной линии Составного цеха №2 ОАО «Иристонстекло», представленной в таблице 1.

Таблица 1 – Технология дозирования сырьевых материалов (компонентов) в Составном цехе №2 ОАО «Иристонстекло», г. Владикавказ

Номер дозатора	Компонент	Очередность выгрузки (группировка)
1	песок	1
2	песок	1-1
3	глинозем	2
4	сода	2,3-1
5	доломит	1-1-1
6	селитра	2,3-1
7	сульфат	2,3-1
8	мел	3
9	мелкие добавки	1-2

В таблице 1 представлена очередность выгрузки компонентов шихты из дозаторов или же очередность загрузки компонентов шихты в смеситель, необходимая для получения шихты с требуемыми характеристиками (однородность, влажность, хим. состав). Сеть Петри для этапов дозирования и смешивания обработанных сырьевых материалов представлена на рисунке 5. При ее разработке также использовались принципы параллельной работы дозаторов для уменьшения времени на приготовление отвеса шихты.

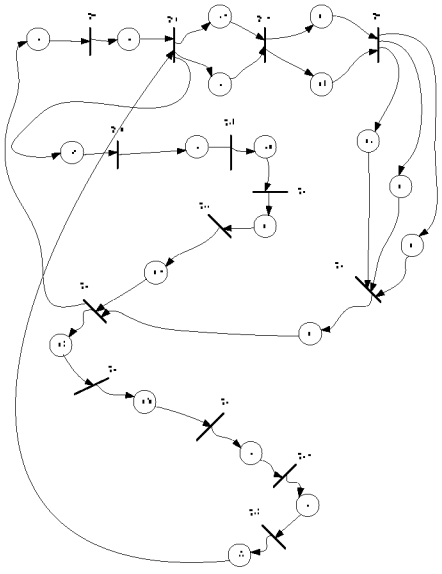


Рисунок 5 – Сеть Петри для этапов дозирования и смешивания ОСМ

Далее, объединив сеть Петри ЗСМ с сетью Петри для дозирования и смешивания ОСМ, получаем сеть Петри единой АСУ ТП составления (приготовления) шихты, которая позволит контролировать и управлять всеми этапами и их процессами приготовления шихты, сократит простои оборудования, уменьшит брак и аварийные ситуации из-за несогласованности систем управления различных этапов. Модель такой АСУ технологическим процессом приготовления шихты представлена на рисунке 6.

Описание состояний и переходов моделей, представленных на рисунках 4, 5 и 6, представлено в таблице 2.

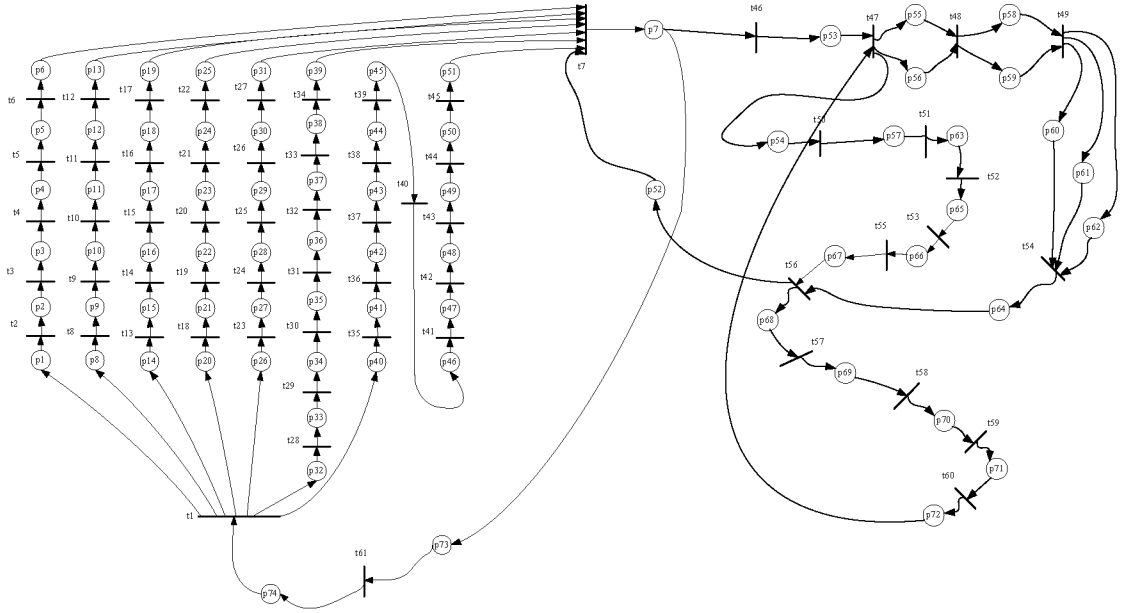


Рисунок 6 – Сеть Петри технологического процесса составления шихты от заготовки до складирования

Таблица 2 – Описание состояний и переходов моделей на сетях Петри, представленных на рисунках 4, 5 и 6

Позиция	Переход
1	2
P1 – осуществляется загрузка песка в сушильный барабан	t1 – загрузка начата
P2 – ожидание сушки песка	t2 – окончание загрузки
P3 – осуществляется сушка песка	t3 – сушка начата
P4 – сушка окончена, ожидание выгрузки	t4 – окончание сушки
P5 – осуществляется выгрузка	t5 – выгрузка начата
P6 – выгрузка в БЗМ окончена, ожидание дозирования	t6 – выгрузка окончена
P8 – осуществляется загрузка на сито	t7 – дозирование начато
P9 – загрузка окончена, ожидание просеивания	t8 – окончание загрузки
P10 – осуществляется просеивание	t9 – просеивание начато
P11 – просеивание окончено, ожидание загрузки в БЗМ	t10 – окончание просеивания
P12 – осуществляется загрузка	t11 – загрузка начата

Продолжение таблицы 2

1	2
Р13 – загрузка окончена, ожидание дозирования	t12 – окончание загрузки
Р32 – осуществляется загрузка соды в дробилку	t28 – окончание загрузки
Р33 – конец загрузки, ожидание дробления	t29 – дробление начато
Р34 – осуществляется дробление	t30 – окончание дробления
Р35 – дробление окончено, ожидание просеивания	t31 – просеивание начато
Р36 – осуществляется просеивание	t32 – окончание просеивания
Р37 – просеивание окончено, ожидание загрузки в БЗМ	t33 – загрузка в БЗМ начата
Р38 – осуществляется загрузка в БЗМ	t34 – окончание загрузки в БЗМ
Р39 – загрузка окончена, ожидание дозирования	t35 – окончание загрузки
Р40 – осуществляется загрузка в дробилку	t36 – дробление начато
Р41 – загрузка окончена, ожидание дробления	t37 – окончание дробления
Р42 – осуществляется дробление	t38 – просеивание начато
Р43 – дробление окончено, ожидание просеивания	t39 – окончание просеивания
Р44 – осуществляется просеивание	t40 – мелкое дробление начато
Р45 – просеивание окончено, ожидание дробления мелкого доломита	t41 – окончание мелкого дробления
Р46 – осуществляется мелкое дробление	t42 – просеивание начато
Р47 – дробление окончено, ожидание просеивания	t43 – окончание просеивания
Р48 – осуществляется просеивание	t44 – загрузка начата
Р49 – просеивание окончено, ожидание загрузки в БЗМ	t45 – окончание загрузки в БЗМ
Р50 – осуществляется загрузка в БЗМ	t13 – окончание загрузки в протирочное устройство
Р51 – окончена загрузка, ожидание дозирование	t14 – протирка начата
Р14 – осуществляется загрузка в протирочное устройство селитры	t15 – окончание протирки
Р15 – окончена загрузка, ожидается протирка	t16 – загрузка в БЗМ начата
Р16 – осуществляется протирка	t17 – окончание загрузки
Р17 – протирка окончена, ожидание загрузки в БЗМ	t18 – окончание загрузки
Р18 – осуществляется загрузка в БЗМ	t19 – просеивание начато
Р19 – загрузка окончена, ожидание дозирования	t20 – окончание просеивания
Р20 – осуществляется загрузка на сито сульфата	t21 – загрузка в БЗМ начата
Р21 – загрузка окончена, ожидание просеивания	t22 – загрузка окончена в БЗМ
Р22 – осуществляется просеивание	t23 – окончание загрузки

Продолжение таблицы 2

1	2
P23 – просеивание окончено, ожидание загрузки в БЗМ	t24 – просеивание начато
P24 – осуществляется загрузка	t25 – окончание просеивания
P25 – окончена загрузка в БЗМ, ожидается дозирование	t26 – загрузка в БЗМ начата
P26 – осуществляется загрузка на сито мела	t27 – окончание загрузки
P27 – загрузка окончена, ожидание просеивания	t46 – окончание дозирования, линия включена
P28 – просеивание осуществляется	t47 – выгрузка начата
P29 – просеивание окончено, ожидание загрузки в БЗМ	t50 – окончание выгрузки песка1
P30 – осуществляется загрузка в БЗМ	t48 – окончание выгрузки мела и глинозема
P31 – загрузка окончена, ожидается дозирование	t51 – начата выгрузка песка2 и мд
P7 – осуществляется наполнение (дозирование материала в весы), включение транспортной линии	
P53 – контрольное взвешивание, ожидание выгрузки компонентов	t49 – начата выгрузка ССС
P54 – осуществляется выгрузка песка1	t52 – окончание выгрузки песка2 и мд
P55 – осуществляется выгрузка мела	t54 – окончание выгрузки ССС
P56 - осуществляется выгрузка глинозема	t53 – выгрузка начата доломита
P57 – окончена выгрузка песка1, ожидание выгрузки песка2 и мд	t55 – окончание выгрузки доломита
P58 –окончена выгрузка мела, ожидание выгрузки ССС(сода, селитра, сульфат)	t56 – смешивание и увлажнение компонентов начато
P59 – окончена выгрузка глинозема, ожидание выгрузки ССС	t57 – оканчивается смешивание и увлажнение
P63 – осуществляется выгрузка песка2 и мд	t58 – линия включена
P60 – осуществляется выгрузка соды	t59 – выгрузка в БЗШ начата
P61 – осуществляется выгрузка селитры	t60 – окончание выгрузки в БЗШ
P62 – осуществляется выгрузка сульфата	t61 – дозирование осуществляется
P65 – окончена выгрузка песка2 и мд, ожидание выгрузки доломита	
P64 – окончена выгрузка ССС, ожидается смешивание и увлажнение	
P66 – осуществляется выгрузка доломита	
P67 – окончена выгрузка доломита, ожидается смешивание и увлажнение	
P68 – осуществляется смешивание и увлажнение	
P69 – ожидается включение транспортной линии склада	
P70 – смешивание окончено, ожидается выгрузка в БЗШ	

Продолжение таблицы 2

1	2
Р71 – осуществляется выгрузка шихты в БЗШ	
Р72 – выгрузка окончена, ожидание загрузки компонентов	
Р52 – весы пусты, ожидание дозирования	
Р73 – дозирование начато, ожидание включения заготовительного оборудования	
Р74 – оборудование включено, ожидание загрузки сырьевых материалов	

При моделировании данной сети в программе VisualPetri были получены следующие данные: 1) сеть ограниченная – 3; 2) безопасная; 3) живая; 4) обратимая; 5) правильная; 6) класс сети – автомат; 7) пассивных переходов нет.

Это свидетельствует о том, что созданная сеть Петри технологического процесса приготовления шихты, объединившая все три этапа (заготовка, дозирование и смешивание ОСМ) является пригодной для проектирования единой АСУ ТП приготовления шихты.

СПИСОК ЛИТЕРАТУРЫ

1. Лескин А.А., Мальцев П.А., Спиридонов А.М. Сети Петри в моделировании и управлении. – Ленинград: «Наука», 1989. – 133 с.
2. Китайгородский И.И., Качалов Н.Н. и др. Технология стекла; под общей ред. Китайгородского И.И. – М.: Стройиздат, 1967. – 564 с.

Маслаков Максим Петрович
Северо-Кавказский горно-металлургический институт (СКГТУ), г. Владикавказ
Ассистент, аспирант кафедры «Промышленная электроника»
Тел.: (8672) 57-42-79
E-mail: kalbash1@mail.ru

M.P. MASLAKOV

USE OF NETWORKS PETRI AT MODELLING OF THE AUTOMATED CONTROL SYSTEM BY TECHNOLOGICAL PROCESS OF DRAWING UP (PREPARATION) GLASS SHIHTY

Questions of automation of management by drawing up (preparation) shihty at the enterprises of the glass industry are considered. The block diagramme of the uniform automated control system by technological process of drawing up shihty is developed. Networks of Petri for separate stages of technological process of preparation shihty are constructed. The network of Petri is developed for all technological process of drawing up shihty.

Keywords: *control system of drawing up shihty; modelling by networks of Petri; modelling of technological process.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Leskin A.A., Mal'cev P.A., Spiridonov A.M. Seti Petri v modelirovanii i upravlenii. – Leningrad: «Nauka», 1989. – 133 s.
2. Kitajgorodskij I.I., Kachalov N.N. i dr. Texnologiya stekla. Pod red. Kitajgorodskogo I.I. – M.: Strojizdat, 1967. – 564 s.

УДК 621.74.06-048.35:[658.52:681.586'3]

С.Ю. РАДЧЕНКО, А.Ю. МЕЛЬНИКОВ

АНАЛИЗ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ МНОГОФАКТОРНЫМИ ПРОЦЕССАМИ

С применением системного подхода формируются требования, предъявляемые к системам автоматизированного управления с учетом многофакторности управляемого процесса, позволяющие выявить источники аварийных ситуаций; выработаны рекомендации по их предотвращению.

Ключевые слова: *автоматизированная система управления; аварийные ситуации; датчики.*

ВВЕДЕНИЕ

В настоящее время на многих предприятиях используется морально и функционально устаревшее оборудование, которое, несмотря на удовлетворение параметров технологического процесса, в остальных аспектах (переналадка, смена технологического процесса, корректировка процесса во время работы и др.) не позволяет добиться необходимых результатов быстродействия, точности результата технологического процесса, отказоустойчивости и других параметров [1,3]. В таком технологическом оборудовании основным ядром возникающих проблем и аварийных ситуаций является устаревшая, работающая по жесткому алгоритму система управления, не позволяющая адекватно реагировать на отклонение технологического процесса от идеального (требуемого). Механическая, гидравлическая, пневматическая и другие системы технологического оборудования в большой степени удовлетворяют параметрам технологического процесса, а в некоторых системах или их составных частях изначально заложен более высокий технологический потенциал. Для решения проблемы модернизации производства есть два варианта: покупка нового, более совершенного технологического оборудования или установка новой системы управления на имеющееся технологическое оборудование, которая отвечала бы всем современным требованиям. Покупка нового производственного оборудования – наиболее затратный способ, он предполагает наращивание производства для скорейшей окупаемости, что не всегда возможно либо нецелесообразно. В рамках модернизации, автоматизации производственного оборудования (линий) экономически целесообразно произвести частичную модернизацию, такую, как установка новой автоматизированной, отвечающей всем современным требованиям системы управления. Наиболее предпочтительными в данном случае являются контроллерные системы управления.

При постройке новых систем управления действующим технологическим оборудованием необходимо учитывать, что на нем отсутствуют (полностью или частично) необходимые контролирующие элементы (датчики), необходимые для функционирования построенной системы управления. Для более точной и адекватной работы оборудования в процессе управления им необходимо учитывать как параметры технологического процесса и возможности оборудования, так и рассмотрение всех уязвимых мест в алгоритме работы основного рабочего цикла технологического процесса.

АНАЛИЗ АВАРИЙНЫХ СИТУАЦИЙ СИСТЕМЫ УПРАВЛЕНИЯ МНОГОФАКТОРНЫМИ ПРОЦЕССАМИ

Варианты уязвимых мест и пути их нейтрализации рассмотрим на примере литьевой машины термопластичных материалов, пройдя по алгоритму её работы. В качестве объекта исследования принимаем литьевую машину термопластичных

материалов типа ДА3128-63 с силой прижатия полуформ 50 тс. Выбор литьевой машины обоснован наличием в её работе большого числа переходных процессов (многофакторность процесса). Алгоритм работы исполнительных механизмов различных машин литья термопластичных материалов практически не отличается друг от друга и состоит из следующих этапов [2]:

1. Гранулированная или порошкообразная пластмасса из бункера поступает в загрузочную часть нагревательного цилиндра, захватывается вращающимся шнеком и транспортируется по цилиндру в его переднюю часть. На данном этапе возможны следующие аварийные ситуации:

- засор в цилиндре либо в его загрузочной части;
- отсутствие материала;
- отсутствие вращения шнека.

2. Продвигаясь по цилиндру, пластмасса пластицируется (размягчается) за счет тепла от внешних нагревателей и тепла, выделяющегося при её деформации в витках шнека. Накапливаемый в передней части цилиндра расплав отодвигает шнек назад – возникает противодавление при пластикации. На данном этапе возможны следующие аварийные ситуации:

- недогрев либо перегрев пластмассы;
- отсутствие вращения шнека.

Причинами возникновения перечисленных аварийных ситуаций могут являться: проблемы в системе нагрева, проблемы с приводом гидромотора, проблемы с системой питания гидромотора.

3. Под действием давления, развиваемого гидроцилиндром смыкания, подвижная плита прессового узла перемещается вперед, и полуформы смыкаются. На данном этапе возможны следующие аварийные ситуации:

- заклинивание механизма смыкания (в том числе, вследствие попадания инородных тел);
- недоход полуформ.

Причинами возникновения перечисленных аварийных ситуаций могут являться: отсутствие либо нахождение вне допустимых пределов давления рабочей жидкости в приводе смыкания, попадание инородных тел в область полуформ и др.

4. После закрытия формы с заданной силой запирания инжекционный цилиндр под действием силы, развиваемой гидроцилиндром подвода сопла, перемещается вперед, и сопло прижимается к форме. На данном этапе возможны следующие аварийные ситуации:

- заклинивание системы подвода-отвода сопла (в том числе вследствие попадания инородных тел);
- недостаточный прижим либо зазор между соплом и формой;
- недостаточная скорость подвода сопла.

Причинами возникновения перечисленных аварийных ситуаций могут являться: отсутствие либо нахождение вне допустимых пределов давления рабочей жидкости в приводе смыкания, попадание инородных тел в область полуформ и др.

5. Далее, под действием силы, развиваемой гидроцилиндром впрыска, шнек движется вперед, и подготовленная при пластикации доза расплава подается в форму. На данном этапе возможны следующие аварийные ситуации:

- недоход шнека до крайней точки инжекционного цилиндра;
- недогрев либо перегрев пластмассы;
- отклонение скорости впрыска от заданного.

Причинами возникновения перечисленных аварийных ситуаций могут являться: отсутствие либо нахождение вне допустимых пределов давления в системе

гидроцилиндра впрыска, проблемы в системе нагрева и др.

6. В форме в течение заданного промежутка времени пластмасса выдерживается под давлением. При выдержке под внешним давлением из инжекционного цилиндра в форму поступают новые порции расплава для компенсации усадки пластмассы в результате охлаждения. На данном этапе возможны следующие аварийные ситуации:

- недостаточная выдержка под давлением;
- недостаточное охлаждение полуформ либо их переохлаждение.

Причинами возникновения перечисленных аварийных ситуаций могут являться: проблемы с системой охлаждения полуформ, нештатная работа блока задания времени выдержки под давлением.

7. По окончании выдержки под давлением сопло отводится от формы. На данном этапе возможны следующие аварийные ситуации:

- заклинивание системы подвода-отвода сопла (в том числе, вследствие попадания инородных тел);
- недостаточная скорость отведения сопла от полуформ.

Причинами возникновения перечисленных аварийных ситуаций могут являться: отсутствие либо нахождение вне допустимых пределов давления рабочей жидкости в приводе отвода-подвода сопла, попадание инородных тел в область механизма отвода-подвода сопла и др.

8. Сразу по окончании выдержки либо через некоторое время (зависит от режима литья) начинается вращение шнека. На данном этапе аварийные ситуации повторяют п.2:

9. По окончании охлаждения пластмассы в форме подвижная плита под действием давления, развиваемого в штоковой полости гидроцилиндра, отходит назад, и форма раскрывается. На данном этапе аварийные ситуации:

- заклинивание механизма смыкания-размыкания полуформ (в том числе попадания инородных тел);
- недостаточная скорость размыкания полуформ;
- нештатная работа системы питания гидроцилиндра.

Причинами возникновения перечисленных аварийных ситуаций могут являться: отсутствие либо нахождение вне допустимых пределов давления рабочей жидкости в приводе смыкания-размыкания полуформ, попадание инородных тел в область полуформ и др.

10. Отлитая деталь извлекается из формы. На данном этапе возможны следующие аварийные ситуации:

- «залипание» отливки в форме;
- застревание отливки при выходе из формы (к лотку);
- деформация отливки при выходе из формы и при движении по лотку.

Причиной возникновения перечисленных аварийных ситуаций может являться отклонение от нормы параметров системы управления, в том числе системы извлечения отливки.

ВЫРАБОТКА РЕКОМЕНДАЦИЙ ПО ПРЕДОТВРАЩЕНИЮ ВОЗНИКНОВЕНИЯ АВАРИЙНЫХ СИТУАЦИЙ

Для отслеживания перечисленных нештатных ситуаций предлагается установка соответствующих датчиков в «уязвимые» места. При определении мест установки датчиков необходимо учитывать, что для некоторых этапов алгоритма будут задействованы одни и те же чувствительные элементы, что позволит сократить их количество.

1. При перемещении гранулированной или порошкообразной пластмассы по

бункеру происходит заполнение инжекционного цилиндра без выдавливания поршня. Для предотвращения аварийных ситуаций необходимо отслеживать наличие пластмассы в бункере, отсутствие либо недостаточное число оборотов шнека, вращаемого гидромотором, а также проходимость канала цилиндра и канала от бункера до цилиндра.

Наиболее простой и частично решенной проблемой из числа перечисленных является слежение за наличием материала в бункере. В рассматриваемой литьевой машине за состоянием наличия материала в бункере следит оператор через специальное окно. С введением новой автоматизированной системы управления отслеживать уровень материала необходимо с помощью датчиков. Есть несколько вариантов определения наличия материала с помощью датчиков: оптическим и емкостным датчиком. Применение оптического датчика менее предпочтительно, т.к. высока вероятность засора окна датчика и, как следствие, возникновение ошибок и неполадок в работе машины. В отличие от оптического, емкостной датчик позволяет следить непосредственно за самой средой вокруг датчика.

В рассматриваемой литьевой машине не была установлена сигнализация отсутствия вращения шнека и работа этого узла определялась оператором лишь по остановке машины при работе. При установке новой системы управления предотвратить приведенный сбой возможно несколькими способами: слежением за частотой вращения гидромотора, а также контролем давления в системе питания гидромотора. Для определения частоты вращения гидромотора применяется датчик угловых перемещений, установленный на валу гидромотора. Принцип работы датчика не имеет значения, т.к. в основном такие датчики выполнены в герметичных корпусах, что исключает их повреждение окружающей средой.

При прохождении материала по инжекционному цилиндру может произойти налипание полурасплавленного материала на шнеке и его непроходимость для следующих порций расплава. К такому виду непредвиденной ситуации можно также отнести засор канала подачи материала из бункера в цилиндр. Данная ситуация не является аварийной, однако может повлечь за собой остановку машины. Для предотвращения необходимо заложить в алгоритм работы новой системы управления подачу сигнала через время, достаточное для прохождения материала и уплотнения его в цилиндре при отводе шнека. Контролировать отвод шнека возможно установкой концевых датчиков положения шнека.

2. В процессе наполнения инжекционного цилиндра происходит расплав материала, а при повороте шнека его сдвиг назад. Для предотвращения описанных для этой стадии неполадок необходимо следить за вращением шнека, а также контролировать температуру инжекционного цилиндра. На рассматриваемой литьевой машине установлены термодатчики, отслеживающие температуру цилиндра в нескольких зонах, что позволяет контролировать весь процесс прогрева и нагрева материала и делать вывод о готовности его для впрыска в форму. Установленные термодатчики удовлетворяют параметрам технологического процесса и могут быть использованы в новой системе управления литьевой машины.

Вращение шнека предполагается производить аналогично предыдущей части алгоритма. Отвод и дальнейшее перемещение шнека можно отследить при помощи концевых выключателей (предпочтительно применение оптических щелевых, перекрывающихся в крайних положениях), на рассмотренной литьевой машине такие датчики установлены, однако необходима их замена на более современные.

3. При смыкании формы происходит перемещение подвижной полуформы к неподвижной. Для предотвращения аварийных ситуаций в процессе смыкания полуформ необходимо отслеживать перемещение механизма смыкания, а также силу,

развиваемую в системе гидропривода в процессе сведения. Необходимо также отслеживать весь процесс смыкания, поскольку в большинстве литьевых машин применяется сведение полуформ в несколько этапов (смыкание, прижатие и т.д.).

При слежении за перемещением подвижной формы возможны несколько вариантов определения ее положения: косвенный и прямой. Один из вариантов определения положения – это косвенный, он основан на рассмотрении взаимного расположения элементов механизма смыкания, однако он менее предпочтителен в связи с невозможностью определения реального положения подвижной полуформы. Другой вариант является более предпочтительным, т.к. установка датчика положения (одного или нескольких) позволит наиболее точно определить положение подвижной формы. Датчик положения может применяться нескольких типов, предпочтительным является оптический датчик, основой работы которого является отсчет времени испускания, отражения и возврата пучка света, отраженного от светоотражающего маяка, установленного на подвижной полуформе, при этом необходимо исключить возможность попадания посторонних предметов в рабочее поле датчика (например, путем установки защитного кожуха). Для слежения за крайними положениями полуформы целесообразно применить тензодатчики, при помощи которых возможно контролировать не только крайние положения полуформы, но и относительную величину прижатия полуформ друг к другу, достаточную для совершения последующих операций. При попадании инородного тела в межформенное пространство движение полуформ может продолжиться, однако это уже является аварийной ситуацией, для ее предотвращения необходимо следить посредством датчика давления за состоянием давления в системе гидропривода смыкания полуформ перед гидроцилиндром, что позволит мгновенно определить аварийную ситуацию и прекратить смыкание полуформ.

Проводя анализ данных, полученных от датчика положения, а также давления в гидросистеме смыкания, можно выявить соответствие работы механизма смыкания заданному алгоритму, что позволит предотвратить возможные неполадки.

4. При подводе сопла происходит перемещение всей системы впрыска до литьевой формы. Для предотвращения аварийных ситуаций на данном этапе необходимо отслеживать положение системы впрыска (в том числе, крайние положения), силу перемещения, а также давление в гидросистеме подвода сопла.

Отслеживать положение системы впрыска возможно таким же способом, что и при смыкании полуформ (п.3), однако в связи с меньшим давлением в системе подвода сопла, достаточно отслеживать только крайние положения, а также следить за силой прижима сопла установкой одного тензодатчика. При заклинивании системы (попадание в её пространство инородных предметов) целесообразно отслеживать давление в гидросистеме (датчиком давления) перед гидроцилиндром, что позволит вовремя остановить перемещение сопла к форме.

5. При впрыске расплава в полость формы происходит перемещение (линейное) шнека по инжекционному цилиндру в сторону сопла. Для предотвращения аварийных ситуаций, а также для исключения отклонения от параметров заданного технологического процесса, необходимо следить за перемещением шнека, отслеживать его крайние положения, следить за температурой инжекционного цилиндра.

Положение и состояние шнека достаточно отслеживать аналогично процессу отвода шнека (п.2), однако необходимо дополнить процесс слежением за положением шнека, определением давления в процессе впрыска, т.к. попадание инородных тел можно определить скачком давления в гидросистеме.

Температуру цилиндра достаточно определять аналогично п.2.

6. На этапе выдержки под давлением происходит долив горячего расплава, а так же предварительное охлаждение отливки. Для исключения появления брака необходимо отслеживать температуру формы, учитывая, что чем ближе к поверхности, взаимодействующей с расплавом, тем более точнее можно сделать вывод о готовности отливки.

Применение временного интервала для определения готовности менее предпочтительно, т.к. это не является адекватным в начальное время работы машины.

7. При отводе сопла возможны аварийные ситуации, аналогичные п.4, следовательно, меры по предотвращению неполадок являются также аналогичными.

8. В этой части алгоритма происходит повторный забор материала в полость цилиндра, что полностью соответствует п.2, следовательно, все принимаемые меры также подобны.

9. При размыкании полуформ происходит процесс, обратный п.3, что позволяет применить те же меры по предотвращению аварийных ситуаций, а также применить такие же отслеживающие устройства.

10. При извлечении детали из формы возможно застревание отливки в форме, а также на пути к лотку. Для предотвращения аварийных ситуаций необходимо установить датчик (оптический на просвет либо емкостной), позволяющий отследить прохождение объекта по каналу от разомкнутых полуформ к лотку. Оптический датчик менее предпочтителен в связи с возможным засором оптической линии. Емкостной датчик более предпочтителен, т.к. в нем отсутствуют видимые чувствительные каналы. Для исключения появления брака необходимо отслеживать состояние отлитых заготовок, попавших в лоток. Наиболее простым способом определения деформированных отливок является визуальный контроль оператором.

ВЫВОДЫ

1. В данной статье был определен объект модернизации: машина для литья термопластичных материалов типа ДА3128-63 с силой прижатия 500 КН. Выбор обоснован наличием в работе оборудования большого числа переходных процессов.

При анализе вариантов модернизации было выявлено, что наиболее целесообразно использовать частичную модернизацию посредством установки новой системы управления.

2. Определены параметры и места установки датчиков для реализации новой системы управления:

- установка емкостного датчика на бункер;
- установка датчика угловых перемещений на шкив гидромотора;
- установка концевых датчиков положения шнека;
- установка оптического датчика положения механизма смыкания полуформ (для измерения удаления интересующей точки – подвижной полуформы);
- установка концевых датчиков положения системы впрыска;
- установка датчика температуры литьевой формы (максимально близко к поверхности контакта с отливкой;
- установка емкостного датчика в местах выхода отливок из формы.

3. Используя новую систему управления, можно повысить качество получаемых изделий, производительность технологического оборудования, а также его надежность, отказоустойчивость и безопасность. Новая система управления дает возможность применения современных подходов к работе производственного оборудования.

4. При установке новой автоматизированной системы управления неоспоримым преимуществом перед новым оборудованием является возможность настроить технологический процесс с учетом различных факторов, а также сохранять

и применять в дальнейшем его параметры. Кроме того, модернизированное технологическое оборудование может обмениваться информацией с оператором через удаленное рабочее место, что позволяет уберечь оператора от вредных воздействий технологического процесса, т.к. установка новой автоматизированной системы управления позволяет вывести пульт оператора за границы воздействия вредных факторов. Кроме того, применение сетевого управления технологическим процессом позволяет вывести на пульт оператора не одну, а несколько единиц технологического оборудования и тем самым повысить производительность линии.

5. Применение подобной автоматизированной системы управления возможно на широком спектре оборудования, что позволяет построить оконченную производственную линию, управляемую с одного пульта оператора.

6. Стоимость элементов новой системы автоматизированного управления технологического оборудования в десятки раз дешевле покупки нового производственного оборудования, что позволяет поднять морально и технологически устаревшее оборудование на новый потенциальный и технологический уровень с наименьшими финансовыми затратами.

СПИСОК ЛИТЕРАТУРЫ

1. Беккер М.Л. Литье под давлением. – М.: Машиностроение, 1990.
2. Калинчев Э.Л., Калинчева Е.И., Саковцева М.Б. Оборудование для литья пластмасс под давлением: расчет и конструирование. – М.: Машиностроение, 1985.
3. Освальд Т.А., Тунг Л.Ш., Грэманн П.Дж. Литье под давлением; под ред. Э.Л. Калиничева – СПб.: Профессия, 2006.

Радченко Сергей Юрьевич
ФГОУ ВПО «Госуниверситет – УНПК», г. Орел
Доктор технических наук, проректор, профессор
Тел.: (4862) 43-71-25
E-mail: sur@ostu.ru

Мельников Анатолий Юрьевич
ФГОУ ВПО «Госуниверситет – УНПК», г. Орел
Аспирант
Тел.: (4862) 41-98-35
E-mail: tollik1986@yandex.ru

S.YU. RADCHENKO, A.YU. MELNIKOV

ANALYSIS AUTOMATED MANAGERIAL SYSTEM MUCH FACTORIAL PROCESS

With use the system approach, is formed requirements presented for reception managerial system with provision for several factorial processes of management showing sources emergencies and creation to recommendations upon their prevention.

Keywords: *automated managerial system; emergencies; sensors.the wavelet transform; the wavelet techniques; the simulation; the transform theory.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Bekker M.L. Lit'yo pod davleniem. – M.: Mashinostroenie, 1990.
2. Kalinchev E`.L., Kalincheva E.I., Sakovceva M.B. Oborudovanie dlya lit'ya plastmass pod davleniem: raschyot i konstruirovanie. – M.: Mashinostroenie, 1985.
3. Osval'd T.A., Tung L.Sh., Gre'mann P.Dzh. Lit'yo pod davleniem; pod red. E`.L. Kalincheva. – SPb.: Professiya, 2006.

ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И КОМПЬЮТЕРНЫЕ СЕТИ

УДК 621.394.20

Д.В. ГАЙЧУК, А.В. БЕЛОКОНЬ, Л.В. БЕЛОКОНЬ, А.О. КРИВОНОЖКИН

ПЕРЕДАЮЩАЯ ЧАСТЬ СМЕШАННОЙ СИСТЕМЫ УПЛОТНЕНИЯ ДЛЯ РАДИОЛИНИЙ ДЕКАМЕТРОВОГО ДИАПАЗОНА

Повышение пропускной способности радиоканала декаметрового диапазона может быть достигнуто с помощью использования двух или большего числа независимых каналов для передачи одного сообщения, т.е. должна быть применена система уплотнения. Целью статьи является разработка передающей части смешанной системы уплотнения для радиолиний декаметрового диапазона, сочетающей комбинационное уплотнение, уплотнение по форме сигнала и частотное уплотнение.

Ключевые слова: *пропускная способность; фазоразностный модулятор; фазовый модулятор; комбинационное уплотнение; уплотнение по форме сигнала и частотное уплотнение; система уплотнения.*

ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ ПРИМЕНЕНИЯ СМЕШАННЫХ СИСТЕМ УПЛОТНЕНИЯ В КАНАЛАХ РАДИОСВЯЗИ ДКМ ДИАПАЗОНА

В настоящее время в теории и практике передачи дискретной информации наиболее важными являются два направления: повышение помехоустойчивости системы связи и повышение скорости информационного обмена при передаче сообщений.

Второе направление особенно актуально для радиолиний декаметрового диапазона, так как увеличение пропускной способности радиоканала декаметрового диапазона не может быть достигнуто простым повышением скорости модуляции в данном канале. Это объясняется тем, что многолучевое распространение радиоволн вызывает наложение соседних элементов сигнала друг на друга, то есть приводит к межсимвольной интерференции. Кроме того, особенности помеховой обстановки в КВ канале, при которых начальная фаза принимаемого сигнала и коэффициент передачи канала изменяются по случайному закону, налагают ограничения на возможность применения современных скоростных методов модуляции.

Поэтому повышение пропускной способности радиоканала декаметрового диапазона может быть достигнуто с помощью использования двух или большего числа независимых каналов для передачи одного сообщения, то есть должна быть применена система уплотнения. Одним из используемых в настоящее время устройств преобразования сигналов в ДКМ диапазоне является изделие АТ-3004Д, являющееся примером смешанной системы уплотнения. В изделии используется 12 частотных диапазонов, размещенных в спектре канала тональной частоты, при этом для передачи информации при помощи двойной относительной фазовой модуляции используются только 10 частотных каналов (u=10).

Возьмем за основу указанное изделие и рассмотрим возможность повышения эффективности системы связи без расширения спектра. Одним из способов решения указанной задачи является использование уплотнения по форме [1, 5], когда для организации индивидуальных каналов используются «почти» ортогональные или квазиортогональные сигналы, приближенно удовлетворяющие условию

$$\rho_{ij} = \frac{1}{T}\int_0^T x_i(t)x_j(t)dt = \begin{cases} 0, & \text{при } i \neq j, \\ P_c, & \text{при } i = j, \end{cases} \quad (1)$$

Такой ансамбль сигналов представляют прямоугольной матрицей размера m на

u

$$p = \frac{m}{u}\ ,\ p > 1,$$

где m > u *u* – размерность исходного ансамбля ортогональных сигналов,

m – число различных сигналов в ансамбле индивидуальных квазиортогональных сигналов,

p определяет кратность уплотнения.

Например, для u=4, m=5 ансамбль дискретных сигналов может быть представлен матрицей вида

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} \\ x_{21} & x_{22} & x_{23} & x_{24} & x_{25} \\ x_{31} & x_{32} & x_{33} & x_{34} & x_{35} \\ x_{41} & x_{42} & x_{43} & x_{44} & x_{45} \end{pmatrix}, \qquad (2)$$

а коэффициент *p* = 1,25.

В каждом из n частотных каналов осуществляется уплотнение по форме на основе использования ансамбля квазиортогональных сигналов без расширения спектра по отношению к исходной системе, т.е. $\tau = T_{AT}$. Этот способ уплотнения предполагает одновременную передачу m сигналов длительностью $T=u\cdot\tau$, например, при m=5, u=4 одновременно передается 5 сигналов с длительностью, в 4 раза большей, чем в исходной системе.

Применив двойную относительную манипуляцию фазы в каждом индивидуальном канале, получим скорость передачи информации в каждом индивидуальном канале:

$$V_1 = 2\frac{1}{T},$$

а используя *m* индивидуальных сигналов, скорость передачи информации определяется:

$$V_m = m \cdot V_1 = 2\frac{m}{T} = 2\frac{up}{u\tau} = 2\frac{p}{\tau},\ \text{бит/с}. \qquad (3)$$

Анализируя выражение (3) видно, что скорость передачи информации определяется видом модуляции, длительностью элемента сигнала τ, а также коэффициентом p, показывающим, во сколько раз было увеличено количество сигналов в ансамбле. Дальнейшее повышение эффективности системы связи обеспечивается использованием частотного уплотнения. Тогда скорость передачи будет определяться так:

$$V_{общ} = n\cdot V_m. \qquad (4)$$

Взяв за основу изделие АТ-3004Д, имеем T_{AT} = 8,33 мс, число частотных каналов при этом – n = 10. Подставив выражение (3) в (4), получим

$$V_{общ} = n\cdot V_m = 10\cdot 2\cdot p/0{,}00833 = 2400\cdot p,\ \text{бит/с}.$$

Таким образом, предлагаемая система уплотнения обеспечивает выигрыш в скорости передачи в *p* раз.

Рассмотрим далее особенности построения передающей части предлагаемой системы уплотнения.

РАЗРАБОТКА СТРУКТУРНОЙ СХЕМЫ ПЕРЕДАЮЩЕЙ ЧАСТИ СМЕШАННОЙ СИСТЕМЫ УПЛОТНЕНИЯ

Рассмотрим основные задачи, выполняемые передающей частью системы

уплотнения:

-преобразование исходной информационной последовательности из последовательной формы в параллельную по 2·m·n информационных импульса;

-последовательное выполнение двойной относительно фазовой (фазоразностной), фазовой (или, в зависимости от вида сигналов, амплитудно-фазовой) и частотной модуляции;

- алгебраическое сложение полученных сигналов;

- передача сигналов в канал тональной частоты.

Таким образом, структура передающей части системы уплотнения имеет вид, представленный на рисунке 1.

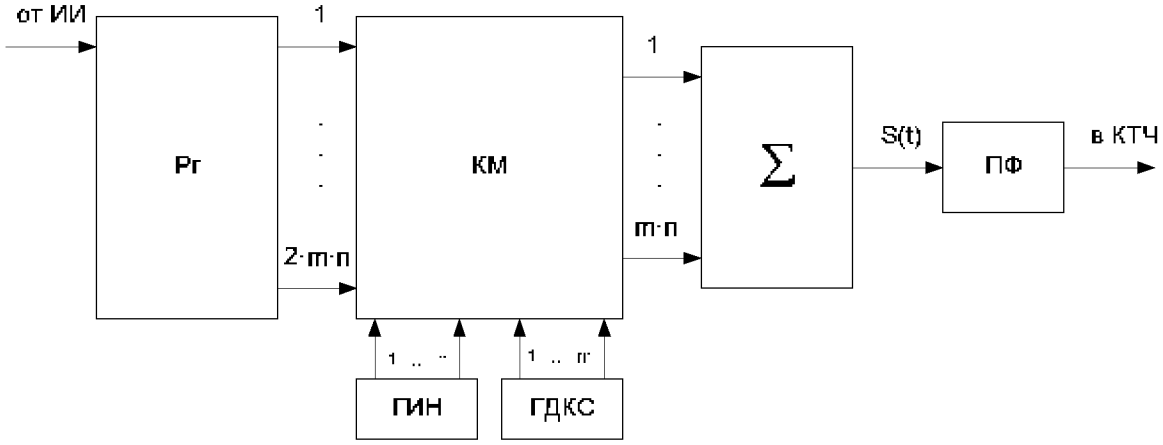


Рисунок 1 – Структура передающей части системы уплотнения

Рг – регистр, КМ – комплексный модулятор, ∑ – сумматор, ПФ – полосовой фильтр, ГИН – генератор индивидуальных несущих, ГДКС – генератор дискретных квазиортогональных сигналов, ИИ – источник информации, КТЧ – канал тональной частоты

Дальнейшим направлением работы является разработка функциональной схемы передающей части смешанной системы уплотнения.

РАЗРАБОТКА ФУНКЦИОНАЛЬНОЙ СХЕМЫ ПЕРЕДАЮЩЕЙ ЧАСТИ СМЕШАННОЙ СИСТЕМЫ УПЛОТНЕНИЯ

На основе структурной схемы, приведенной в разделе 2, была разработана функциональная схема передающей части системы уплотнения (рис. 2).

Устройство работает следующим образом. От источника информации ИИ передаваемая информационная последовательность поступает на последовательный вход регистра RG. С параллельных выходов регистра информация по два бита (дибиты) поступают на входы устройств M_i , $i = 1...n$. Блок M_i содержит модулятор ФРМ, выполняющий функцию двойной относительно фазовой модуляции и модулятор ФМ (АФМ), выполняющий функцию классической модуляции сигнала $S_{фрмi}(t)$. В качестве несущего колебания для модулятора ФРМ используется один из n сигналов генератора индивидуальных несущих. Полученный в результате фазоманипулированный сигнал $S_{фрмi}(t)$ используется в качестве несущего колебания для модулятора ФМ (АФМ). В качестве модулирующего сигнала в модуляторе ФМ (АФМ) используется один из m сигналов генератора дискретных квазиортогональных сигналов. Таким образом, блок M_i последовательно выполняет комбинационное уплотнение, уплотнение по форме сигнала, а частотное уплотнение выполняется выбором одного из n сигналов ГИН, частоты которых кратны $\frac{1}{\tau}$.

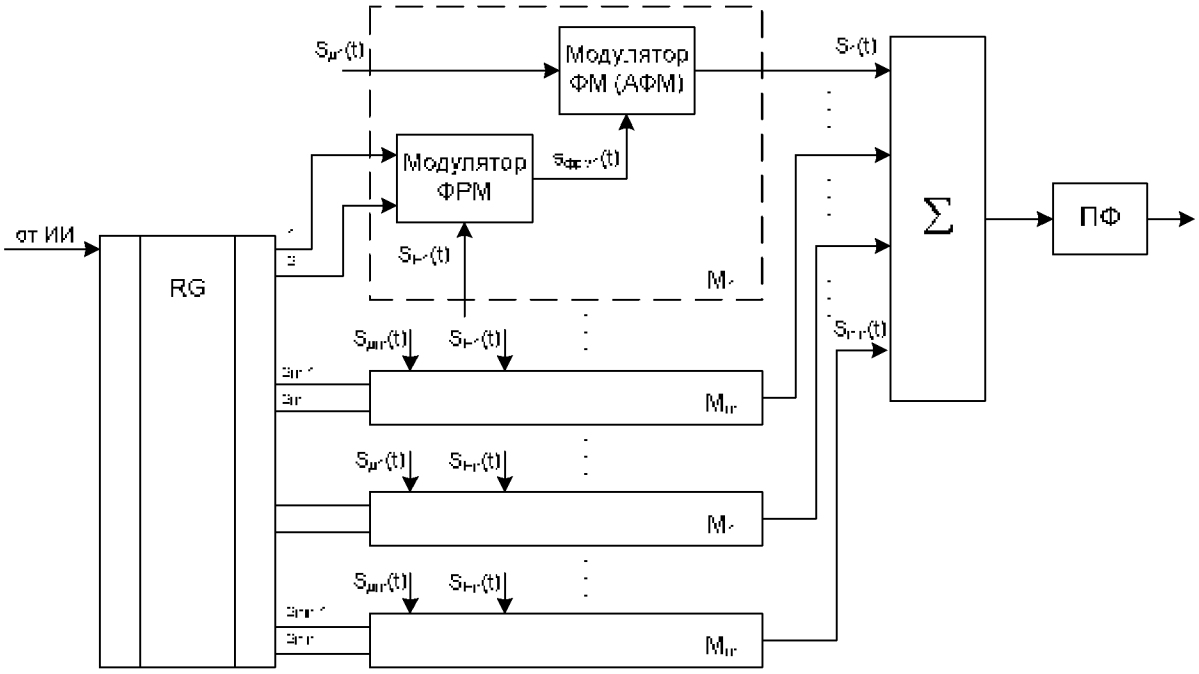


Рисунок 2 – Функциональная схема передающей части системы уплотнения

Передающая часть системы содержит: последовательно-параллельный регистр RG, m·n блоков идентичных M, выполняющих функцию комплексной модуляции, сумматор, выполняющий функцию объединения модулированных сигналов, полосовой фильтр

Модулированные сигналы $S_i(t)$, несущие информацию о передаваемых «дибитах», поступают на сумматор, формирующий вид передаваемого группового сигнала. Далее групповой сигнал через полосовой фильтр ПФ подается в канал тональной частоты.

Предложенное устройство может быть реализовано на цифровой элементной базе.

СПИСОК ЛИТЕРАТУРЫ

1. Варакин Л.Е. Теория систем сигналов. – М.: Советское радио, 1978. – С. 303.
2. Финк Л.М. Теория передачи дискретных сообщений. – М.: Советское радио, 1970. – 728 с.
3. Хмельницкий Е.А. Оценка реальной помехозащищенности приема сигналов в КВ диапазоне. – М.: Связь, 1975. – 354 с.
4. Андронов И.С., Финк Л.М. Передача дискретных сообщений по параллельным радиоканалам. – М.: Советское радио, 1971. – 406 с.
5. Кловский Д.Д. Передача дискретных сообщений по радиоканалам. – М.: Связь, 1969. – 376 с.
6. Кловский Д.Д. Теория передачи сигналов.– М.: Связь, 1973. – 376 с.
7. Гайчук Д.В., Белоконь А.В., Белоконь Л.В. Разработка требований к ансамблям сигналов-переносчиков информации в двухлучевых ДКМ радиоканалах // Двойные технологии. – 2009. – Выпуск №4. – С. 56-58.
8. Белоконь Л.В., Белоконь А.В., Самус М.В. Использование трансортогональных сигналов в низкоскоростных радиоканалах с кодовым уплотнением // Актуальные проблемы и инновации в экономике, управлении, образовании, информационных технологиях: материалы международной научной конференции. – 2009. – Том IV. – Выпуск №5. – С. 23-24.
9. Гайчук Д.В., Самус М.В., Белоконь А.В. Система уплотнения для радиолиний декаметрового диапазона // Современное состояние и приоритеты развития фундаментальных и прикладных наук на физико-математическом факультете: материалы 54-й научно-методической конференции преподавателей и студентов СГУ «Университетская наука – региону». – Ставрополь, 2009. – С. 238-241.

Гайчук Дмитрий Викторович
Ставропольский военный институт связи ракетных войск, г. Ставрополь
Кандидат технических наук, доцент, начальник кафедры систем и комплексов связи РВСН Тел.: 8 962 741 54 80

Белоконь Александр Викторович
Ставропольский военный институт связи ракетных войск, г. Ставрополь
Старший преподаватель кафедры систем и комплексов связи РВСН
Тел.: 8 903 409 17 44

Белоконь Людмила Владимировна
Ставропольский государственный университет, г. Ставрополь
Кандидат технических наук, доцент кафедры высшей алгебры и геометрии
Тел.: 8 903 409 17 43

Кривоножкин Антон Олегович
Ставропольский военный институт связи ракетных войск, г. Ставрополь
Курсант факультета сетей связи и систем коммутации
Тел.: 8 918 881 84 38

D.V. GAJCHUK, A.V. BELOKON, L.V. BELOKON, A.O. KRIVONOGKIN

TRANSFERRING PART OF THE MIXED SYSTEM OF CONSOLIDATION FOR RADIO LINES DECAMETER A RANGE

Increase of throughput of a radio channel decameter a range can be reached by means of use of two or many numbers of independent channels for transfer of one message, i.e. the consolidation system should be applied. Article purpose is working out of a transferring part of the mixed system of consolidation for radio lines decameter a range, combining combinational consolidation, consolidation under the form of a signal and frequency consolidation.

Keywords: *throughput; phase difference the modulator; the phase modulator; combinational consolidation; consolidation under the form of a signal and frequency consolidation; consolidation system.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Varakin L.E. Teoriya sistem signalov. – M.: Sovetskoe radio, 1978. – S. 303.
2. Fink L.M. Teoriya peredachi diskretny'x soobshhenij. – M.: Sovetskoe radio, 1970. – 728 s.
3. Xmel'nickij E.A. Ocenka real'noj pomexozashhitnosti priyoma signalov v KV diapazone. – M.: Svyaz', 1975. – 354 s.
4. Andronov I.S., Fink L.M. Peredacha diskretny'x soobshhenij po parallel'ny'm radiokanalam. – M.: Sovetskoe radio, 1971. – 406 s.
5. Klovskij D.D. Peredacha diskretny'x soobshhenij po radiokanalam. – M.: Svyaz', 1969. – 376 s.
6. Klovskij D.D. Teoriya peredachi signalov. – M.: Svyaz', 1973. – 376 s.
7. Gajchuk D.V., Belokon' A.V., Belokon' L.V. Razrabotka trebovanij k ansamblyam signalov-perenoschikov informacii v dvuxluchevy'x DKM radiokanalax // Dvojny'e texnologii. – 2009. – Vy'pusk №4. – S. 56-58.
8. Belokon' L.V., Belokon' A.V., Samus M.V. Ispol'zovanie transortogonal'ny'x signalov v nizkoskorostny'x radiokanalax s kodovy'm uplotneniem // Aktual'ny'e problemy' i innovacii v e`konomike, upravlenii, obrazovanii, informacionny'x texnologiyax: materialy' mezhdunarodnoj nauchnoj konferencii. – 2009. – Tom IV. – Vy'pusk №5. – S. 23-24.
9. Gajchuk D.V., Samus M.V., Belokon' A.V. Sistema uplotneniya dlya radiolinij dekametrovogo diapazona // Sovremennoe sostoyanie i prioritety' razvitiya fundamental'ny'x i prikladny'x nauk na fiziko-matematicheskom fakul'tete: materialy' 54-j nauchno-metodicheskoj konferencii prepodavatelej i studentov SGU «Universitetskaya nauka – regionu». – Stavropol', 2009. – S.238-241.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.05

Д.А. КАРАУЛАНОВ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЗАДАЧИ ПЕЛЕНГАЦИИ ИСТОЧНИКА РАДИОИЗЛУЧЕНИЯ, ЗАКРЫТОГО ДЛЯ ПРЯМОЙ РАДИОВИДИМОСТИ

В статье рассмотрены основные принципы работы программы RadioReflex 1.0, использующей методику пеленгации источника радиоизлучений, закрытого для прямой радиовидимости.

Ключевые слова: *пеленгация; радиоизлучение; карта; математическая модель; программа расчета.*

Определение местоположения источника радиоизлучения (ИРИ) является одной из основных задач, решаемых пунктами радиоконтроля (ПРК). В условиях густонаселенного городского массива или горной местности, когда отсутствует прямая «радиовидимость» между ИРИ и ПРК, решение данной задачи усложняется. В этом случае определить местоположение ИРИ можно только по отраженным от зданий либо горных массивов радиолучам. Для решения указанной задачи в автоматическом режиме разработана программа RadioReflex 1.0, предполагающая использование цифровых карт местности.

В режиме обучения на карте фиксируются точки расположения ИРИ и ПРК, после чего определяются зоны прямой радиовидимости посредством трассировки радиоволн (рис. 1).

Рисунок 1 – Экранная форма программы RadioReflex 1.0. Расчет зон прямой видимости объектов

Диагональ прямоугольника, стороны которого равны разрешению изображения карты по горизонтали W_P и вертикали H_P, представляется как радиус трассировки:

$$R_{tr} = \sqrt{W_P^2 + H_P^2}. \quad (1)$$

Объект может излучать радиоволны как во все стороны, так и в заданном направлении, которое указывается в виде сектора окружности при помощи параметров: азимута A и величины угла сектора θ_A.

Обнаружение предметов, отражающих радиоволны, производится путем

анализа состояния пикселей изображения за некоторое количество итераций двух циклов (рис. 2).

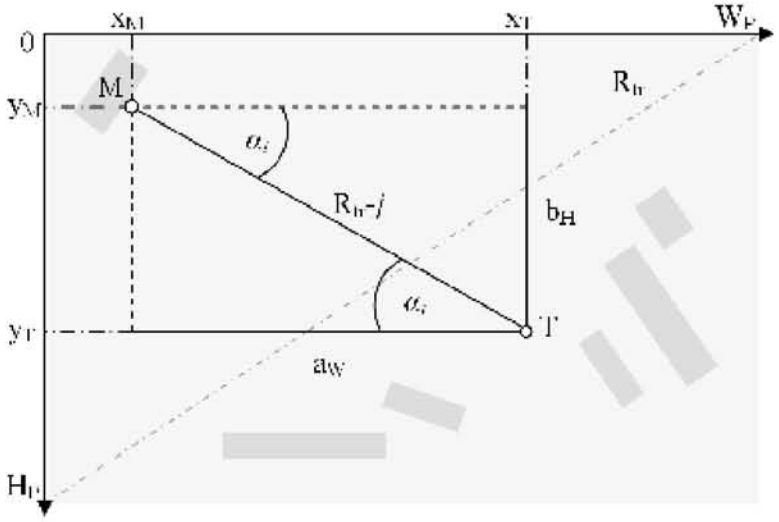


Рисунок 2 – Вычисление координат пикселя

Первый цикл (внешний) в ходе i-ой итерации $(i = \overline{1,Q})$ вычисляет направление α_i движения луча от источника:

$$\alpha_i = \pi \frac{\theta_A \cdot i + Q \cdot (A - 90)}{180 \cdot Q}. \quad (2)$$

На втором цикле (внутренний) при перемещении в i-ом направлении попиксельно обеспечивается вычисление на каждой j-ой итерации $(j = \overline{R_{tr},1})$ координаты каждой точки из прямоугольного треугольника, катет которого a_W определяется по формуле:

$$a_W = \cos(\alpha_i) \cdot (R_{tr} - j). \quad (3)$$

Аналогично определяется второй катет треугольника b_H:

$$b_H = \sin(\alpha_i) \cdot (R_{tr} - j). \quad (4)$$

Заметим, что значения величин катетов могут быть отрицательными. В этом и состоит идея их использования для вычисления положения точки $M(x_M,y_M)$. Используя формулы (2) и (3), определяются горизонтальная x_M и вертикальная y_M координаты:

$$x_M = a_W + x_T; \quad (5)$$

$$y_M = b_H + y_T. \quad (6)$$

После нахождения координат анализируем яркость пикселя, используя аддитивную цветовую модель RGB. Изображение в данной модели состоит из трех каналов: красного (R), зеленого (G) и синего (B). Для расчета яркости L_M каналов RGB используется следующая эмпирическая формула, учитывающая вклад каждого цветового канала:

$$L_M = 0{,}2125 \cdot R + 0{,}7154 \cdot B + 0{,}0721 \cdot B, \quad (7)$$

где значения R, G, B = 0 .. 255.

Если L_M меньше определенного уровня яркости, задаваемого через параметрическое поле на форме программы, то данный пиксель является препятствием для дальнейшего прямолинейного распространения радиоволны, при этом координаты пикселя x_M и y_M являются номерами строки и столбца соответственно для бинарного элемента матрицы $K_{W_P \times H_P}$, в который заносится 1 в случае обнаружения препятствия.

После этого внутренний цикл завершается, не достигнув минимального значения счетчика. Если программа не обнаружила в данном направлении препятствия, то цикл завершится при достижении границы изображения.

Чтобы определить общие точки отражения радиоволн для ИРИ и ПРК, необходимо сначала для каждого объекта вычислить собственные матрицы $K^{(ИРИ)}$ и $K^{(ПРК)}$. Затем производится логическое умножение элементов матрицы с одинаковыми порядковыми номерами строки и столбца: $k_{ij}^{(ИРИ\&ПРК)} = k_{ij}^{(ИРИ)} \& k_{ij}^{(ПРК)}$. Если полученная матрица $K^{(ИРИ\&ПРК)}$ является нулевой, то делаем вывод о невозможности дальнейших вычислений в силу отсутствия у ИРИ и ПРК общих точек отражения радиоволн. В ином случае сумма элементов матрицы даст количество общих точек отражения: $S = \sum_{i=1}^{W_P} \sum_{j=1}^{H_P} k_{ij}^{(ИРИ\&ПРК)}$.

Объекты ИРИ и ПРК не должны находиться в зоне прямой видимости друг друга, т.е. между ними должно быть препятствие. Поскольку нам известны координаты ИРИ и ПРК, мы можем найти уравнение прямой, проходящей через точки ($x_{ИРИ}$, $y_{ИРИ}$) и ($x_{ПРК}$, $y_{ПРК}$), определив угловой коэффициент

$$k = \frac{y_{ИРИ} - y_{ПРК}}{x_{ИРИ} - x_{ПРК}}, \tag{8}$$

при условии, что $x_{ИРИ} - x_{ПРК} \neq 0$, и смещение прямой по вертикали

$$b = y_{ПРК} - y_0, \tag{9}$$

где $y_0 = k \cdot x_{ИРИ}$.

Осуществляя перемещение по пикселям карты от ИРИ к ПРК, необходимо учитывать абсолютную величину углового коэффициента. Если $|k|<1$, то счетчик цикла i принимает значения $(i = \overline{x_{ИРИ}, x_{ПРК}})$ и шаг цикла вычисляется по формуле $\delta = \frac{x_{ПРК} - x_{ИРИ}}{|x_{ПРК} - x_{ИРИ}|}$. Промежуточные точки имеют координаты: $M_i(i, k \cdot i + b)$. В случае, если $|k|\geq 1$, счетчик цикла i принимает значения $(i = \overline{y_{ИРИ}, y_{ПРК}})$ и шаг цикла: $\delta = \frac{y_{ПРК} - y_{ИРИ}}{|y_{ПРК} - y_{ИРИ}|}$. Координаты точки в этом случае вычисляются следующим образом: $M_i(\frac{i-b}{k}, i)$. Цикл завершается при нахождении препятствия либо при достижении другого объекта. Поиск препятствия осуществляется при помощи формулы (7), определяющей яркость пикселя в точке M_i. В случае, если ни одна из точек не находится ниже порога яркости, принимается решение о нахождении ИРИ и ПРК в зоне прямой видимости друг друга и дальнейшие расчеты нецелесообразны.

Как только найдены общие точки отражения в условии отсутствия прямой видимости между объектами, можно выполнять расчет местоположения ИРИ. Постоянство произведения величин $a^2(U_{вх}) = R_{ИО} \cdot R_{ОП}$, где $R_{ИО}$ – расстояние от ИРИ до отражающего объекта, $R_{ОП}$ – расстояние от отражающего объекта до ПРК для некоторых фиксированных значений $U_{вх}$, следует из математической модели зоны формирования отраженных лучей (ЗФОЛ) «закрытого» ИРИ в виде линий Кассини в случае наличия информации о неизменных значениях параметров передатчика ИРИ (мощности $P_И$; коэффициента усиления $G_И$; высоты передающей антенны h_1; коэффициента полезного действия (КПД) тракта от передатчика к антенне $\eta_И$), приемника ПРК (входного сопротивления $\omega_{вх}$; коэффициента усиления $G_П$; высоты приемной антенны h_2; КПД передачи тракта от приемной антенны к приемнику $\eta_П$) и

высоты отражающего объекта h_0 [1]:

$$R_{ИО} \cdot R_{ОП} = \sqrt{\left(h_1^2 + h_0^2\right)\left(h_2^2 + h_0^2\right)\frac{\sqrt{P_И G_И \eta_И G_П \eta_П \omega_{вх}}}{U_{вх}}} = const\left(R_{ИО} \cdot R_{ОП}\right) \quad . \qquad (10)$$

Значение $R_{ОП}$ известно, т.к. точка отражения находится в зоне видимости ПРК. Расстояние $R_{ИО}$ от точки отражения до предполагаемого места расположения ИРИ определяется по формуле [1]: $R_{ИО} = \frac{a^2\left(U_{вх}\right)}{R_{ОП}}$. Выбирая некоторое количество n точек из матрицы $K^{(ИРИ\&ПРК)}$ строим вокруг них окружности с индивидуально вычисленным радиусом $R_{ИОi}, (i = \overline{1,n})$. Пересечения окружностей позволяют выделить область неопределенности искомого ИРИ.

Для уменьшения погрешности определения местоположения ИРИ воспользуемся методом построения радикальной оси [2], т.е. прямой, равноудаленной от двух окружностей и перпендикулярной к линии их центров. Покажем нахождение радикальной оси на примере двух окружностей M_1 и M_2 с известными радиусами R_1, R_2 и координатами их центров: $M_1(x_{M1},y_{M1})$ и $M_2(x_{M2},y_{M2})$ соответственно. Подобно формулам (8) и (9) находим уравнение прямой, проходящей через центры окружностей:

$$y = k_{M_1M_2} \cdot x + b_{M_1M_2} \quad . \qquad (11)$$

Аналогично формуле (1) по теореме Пифагора находим расстояние между центрами окружностей:

$$C_{M_1M_2} = \sqrt{\left(x_{M_1} - x_{M_2}\right)^2 + \left(y_{M_1} - y_{M_2}\right)^2} \quad . \qquad (12)$$

Вычислим расстояние от центра окружности M_1 до точки пересечения W линии центров окружностей M_1 и M_2 с радикальной осью:

$$L_W = \frac{R_1^2 - R_2^2 + C_{M_1M_2}^2}{2 \cdot C_{M_1M_2}} \quad . \qquad (13)$$

Величина L_W дает возможность найти координаты точки W:

$$x_W = \frac{L_W \cdot \left(x_{M_2} - x_{M_1}\right)}{\left|x_{M_2} - x_{M_1}\right| \cdot \sqrt{1 + k_{M_1M_2}^2}} \quad . \qquad (14)$$

В соответствии с формулой (11) определяется ордината точки W:

$$y_W = k_{M_1M_2} \cdot x_W + b_{M_1M_2} \quad . \qquad (15)$$

Определив координаты точки $W(x_W,y_W)$, через которую проходит радикальная ось двух окружностей, несложно получить уравнение прямой радикальной оси, используя угловой коэффициент из формулы (11) и координаты точки W из формулы (14) и (15). Угловой коэффициент перпендикулярной прямой составит $\frac{-1}{k_{M_1M_2}}$, а смещение относительно оси ординат будет равно $y_W + \frac{x_W}{k_{M_1M_2}}$. Отсюда определяется уравнение прямой радикальной оси:

$$y = \frac{x_W - x}{k_{M_1M_2}} + y_W \quad . \qquad (16)$$

Построив окружность M_3, при условии, что она пересекается с M_1 и M_2, можно, используя формулу (16), определить координаты радикального центра этих окружностей $Z(x_z,y_z)$, взяв, например, радикальные оси M_1M_2 и M_2M_3, найдем абсциссу

x_z:

$$x_Z = \frac{k_{M_2M_3} - k_{M_1M_2}}{k_{M_2M_3}\left(k_{M_1M_2}\left(y_{W23} - y_{W12}\right) - x_{W12}\right) + x_{W23}k_{M_1M_2}} \quad . \qquad (17)$$

Используя формулу (16), находим ординату y_z. В ходе работы программы рекомендуемым является определение отрезка масштаба и указание его длины ψ в метрах (рис. 1). При известной длине отрезка p в пикселях масштаб μ вычисляется по формуле:

$$\mu = \frac{\psi}{p} \qquad (18)$$

В обобщенном виде алгоритм работы программы можно представить в виде блок-схемы (рисунок 3).

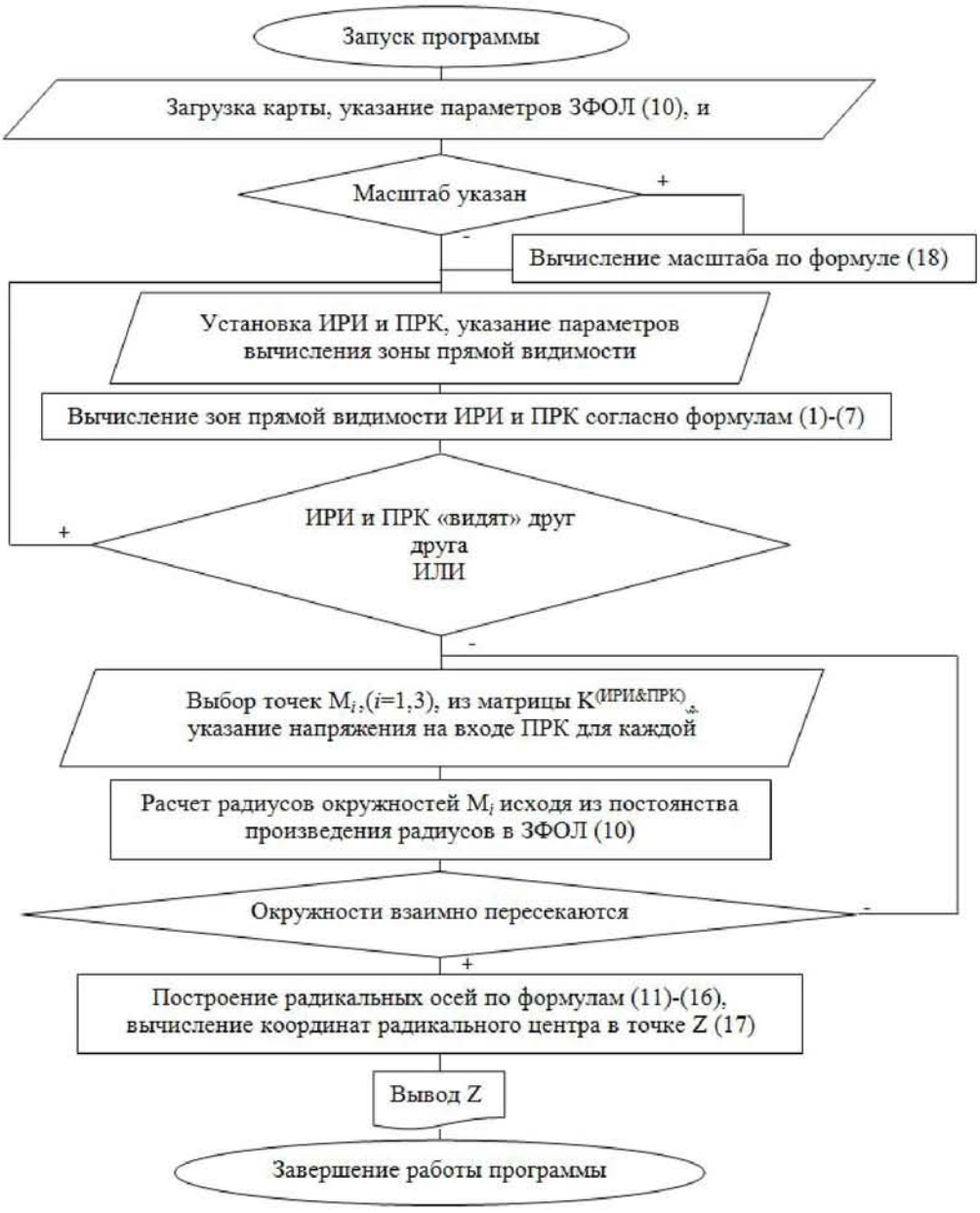


Рисунок 3 – Алгоритм работы программы RadioReflex 1.0

Точка Z является наиболее вероятным местонахождением пеленгуемого ИРИ при определенных типовых условиях.

В ходе проведения эксперимента в программе RadioReflex 1.0 на цифровой

карте одного из спальных районов города Ставрополя были получены следующие результаты: среднеквадратическая погрешность – 165 м, погрешность менее 170 м имеет 50% измерений, погрешность менее 200 м имеет 67% измерений. В настоящее время самым распространенным методом определения местоположения передатчика в системах сотовой связи является метод идентификатора соты, использующий несколько базовых станций, который имеет погрешность от 500 м до 10 км и более. Очевидно, что предлагаемая методика имеет намного меньшую погрешность и позволяет определять координаты априори идентифицированного объекта с помощью одного стационарного пункта радиоконтроля. Вместе с тем, данная методика дает лишь приближенную оценку местоположения ИРИ. Для повышения точности пеленгации ИРИ необходимо учитывать большое число факторов, влияющих на распространение радиоволн, т.е. обеспечить адекватность модели зоны формирования отраженных лучей [1] реальным условиям распространения радиоволн, что и является направлением дальнейших исследований.

Программа создана на основе методики, предложенной в работе «Решение задачи радиоконтроля на основе использования методов планиметрии» [1], с помощью среды программирования Microsoft Visual Basic 2008 Express Edition.

СПИСОК ЛИТЕРАТУРЫ

1. Корниенко С.А., Сивакозов А.И., Федоренко В.В. Решение задачи радиоконтроля на основе использования методов планиметрии // Известия Института инженерной физики, 2007. – №1. – С.16-18.
2. Коксетер Г.С.М., Грейтцер С.П. Новые встречи с геометрией. – М.: Наука, 1978. – 224 с.
3. Лукин С.Н. Понятно о Visual Basic. NET. – М.: Диалог-МИФИ, 2005. – 853 с.

Карауланов Дмитрий Александрович
Северо-Кавказский государственный технический университет, г. Ставрополь
Аспирант
Тел.: 8 919 734 96 09
E-mail: mr.hawk@mail.ru

D.A. KARAULANOV

THE SOFTWARE FOR TASK OF DIRECT FINDING OF SOURCE OF RADIO WAVES EMISSION, CLOSED FOR DIRECT RADIOVISIBILITY

There is consideration of the basic mechanism of working of the RadioReflex 1.0 software, that uses method of direct finding of source of radio waves emission, closed for direct radiovisibility. hierarchies.

Keywords: *direct finding; radio waves emission; map; mathematical model; calculation program.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Kornienko S.A., Sivakozov A.I., Fedorenko V.V. Reshenie zadachi radiokontrolya na osnove ispol'zovaniya metodov planimetrii // Izvestiya Instituta inzhenernoj fiziki, 2007. – №1. – S.16-18.
2. Kokseter G.C.M., Grejtcer S.P. Novy'e vstrechi s geometriej. – M.: Nauka, 1978. – 224 s.
3. Lukin S.N. Ponyatno o Visual Basic.NET. – M.: Dialog-MIFI, 2005. – 853 s.

УДК 004.942

В.В. КОМАШИНСКИЙ, Т.А. НГУЕН

АЛГОРИТМ ОБНАРУЖЕНИЯ ЗАПРЕЩЕННЫХ ДАННЫХ ВО ВХОДНОМ WEB-ПОТОКЕ НА ОСНОВЕ МЕТОДА КУМУЛЯТИВНЫХ СУММ

В статье рассматривается возможность применения алгоритма кумулятивных сумм для обнаружения фрагментов запрещенных данных во входном web-потоке от публичных серверов. Для принятия решения используется распределение размера http-ответов. Данное распределение получается эмпирически для двух случаев: размера http-ответов всех типов и размера графических http-ответов.

Ключевые слова: *алгоритм кумулятивных сумм; размер http-ответов; входной web-поток; фильтрация, обнаружение.*

МЕТОД КУМУЛЯТИВНЫХ СУММ ДЛЯ ОБНАРУЖЕНИЯ РАЗЛАДКИ

Пусть дана случайная последовательность (одно- или многомерная) $x_1,\ldots,x_N$, далее $\{x_1^N\}$, которая в момент t_0 скачком меняет свои свойства, однозначно определяемые вектором параметров θ. Это значит, что до момента t_0-1 включительно $\theta=\theta_1$, а начиная с t_0 вектор $\theta=\theta_2$. Наблюдая $\{x_1^N\}$, необходимо обнаруживать момент разладки t_0.

Для решения поставленной задачи Е.С. Пейджем в работе [4] был предложен метод кумулятивных сумм, который не использует априорное распределение момента t_0 и представляет собой многократно применяемый последовательный анализ А. Вальда [3, 5], а конкретно – последовательный критерий отношения вероятностей для двух простых гипотез H_1 (нет разладки): $\theta=\theta_1$ и H_2 (есть разладка): $\theta=\theta_2$, где θ – скалярный параметр плотности распределения вероятностей $f(x_t/\theta)$ наблюдения x_t. Кумулятивная сумма определяется по выражению:

$$S_t = S_{t-1} + \ln\frac{f(x_t/\theta_2)}{f(x_t/\theta_1)}. \qquad (1)$$

Один из вариантов трактовки метода заключается в следующем. Так как до разладки сумма S_t в среднем дрейфует вниз (рис. 1), а после разладки вверх, то предлагается на каждом шаге t вычислить разность

$$\Delta S_t = S_t - \min_{i\le t} S_i, \qquad (2)$$

и как только она станет значимой, т.е. превысит некоторое пороговое значение h, подать сигнал о разладке [1].

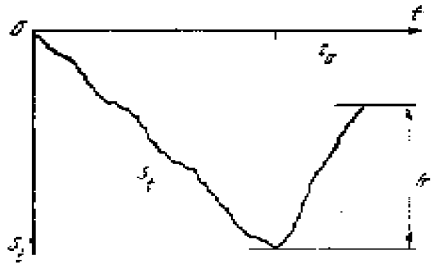


Рисунок 1 – Типичное поведение

Для метода кумулятивной суммы, как и для других методов решения задачи последовательного обнаружения разладки, характерна некоторая задержка τ, которая определяется, как

$$\tau = t_a - t_0 + 1, \qquad (3)$$

где t_a – момент подачи сообщения о разладке, $t_a \ge t_0$.

Применительно к задаче обнаружения фрагментов запрещенных данных во входном web-потоке отсутствию разладки соответствует случай, когда во входном web-потоке нет запрещенных данных. Наличию разладки соответствует случай, когда во входном web-потоке содержатся данные от запрещенных web-сайтов. В качестве

параметра x предлагается рассматривать две величины: *размер http-ответов* и *размер графических http-ответов*. Графическим http-ответом называется http-ответ, в котором содержатся графические данные.

Предполагается, что запрещенные данные во входном web-потоке приходят с ограниченной длиной и многократно. Следовательно, существует возможность определения моментов начала и прекращения поступления запрещенных данных. Для этого нужно сформулировать задачу обнаружения запрещенных данных во входном web-потоке на основе метода кумулятивных сумм следующим образом.

Пусть с момента t_{i_0} входной web-поток переходит в состояние «отсутствия запрещенных данных» (рис. 2).

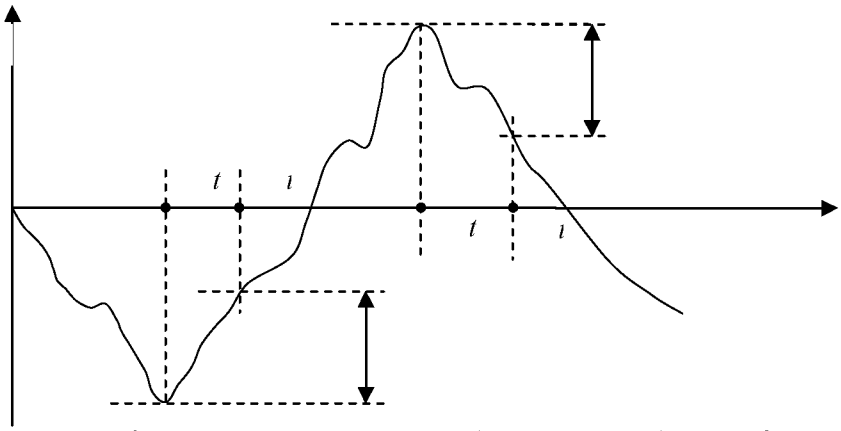


Рисунок 2 – Обнаружения фрагментов запрещенных данных во входном web-потоке методом кумулятивных сумм

На каждом шаге t вычисляется разность ΔS_t:

$$\Delta S_t = S_t - \min_{i_0<i\le t} S_i . \qquad (4)$$

Как только ΔS_t превысит некоторое пороговое значение h, подается сигнал о начале в потоке фрагмента запрещенных данных. При этом состояние входного web-потока будет называться «наличие запрещенных данных».

Пусть с момента t_{i_0} входной web-поток переходит в состояние «наличие запрещенных данных». На каждом шаге t вычисляется разность ΔS_t:

$$\Delta S_t = \min_{j_0<j\le t} S_j - S_t . \qquad (5)$$

Как только ΔS_t превысит некоторое пороговое значение h, подается сигнал о прекращении в потоке фрагмента запрещенных данных. Состояние входного web-потока называется «отсутствием запрещенных данных».

Поскольку метод является параметрическим, требующим априорных функций плотности распределения вероятностей величины x до и после разладки $f(x/\theta_1)$ и $f(x/\theta_2)$, необходимо предварительно определить эти функции.

ОЦЕНКА ФУНКЦИИ ПЛОТНОСТИ РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ ПО ЭМПИРИЧЕСКИМ ДАННЫМ

В рамках исследования экспертным путем были определены две выборки web-сайтов – G_1 и G_2. В первую выборку (G_1) входят только деловые (разрешенные) web-сайты, а именно, научно-технические web-сайты, электронные газеты на русском, вьетнамском и английском языках. Во вторую выборку (G_2) входят web-сайты преимущественно на английском языке, содержащие порнографические (запрещенные) изображения.

С помощью специального программного обеспечения были получены

фрагменты потоков http-ответов – совокупности $R_1 = \{r_{11}, r_{12}, ..., r_{1N_1}\}$ от G_1 и $R_2 = \{r_{21}, r_{22}, ..., r_{2N_2}\}$ от G_2. Каждый http-ответ характеризуется своим размером (в байтах) и типом. Тип http-ответа в данном контексте определяется содержимым в нем данных и может быть как неграфический, так и графический (JPEG, GIF, PNG,…). Совокупность R_1 состоит из $N_1 \approx 68.000$ http-ответов, в том числе, $N_1^{г} \approx 68.000$ графических. Совокупность R_2 состоит из $N_2 \approx 65.000$ http-ответов, в том числе, $N_2^{г} \approx 56.000$ графических. Выше было определено, что основными анализируемыми параметрами будут являться *размер http-ответов* и *размер графических http-ответов*.

В качестве оценки функции плотности распределения вероятностей величины x используется так называемая *диаграмма*, количество столбцов которой определяется по формуле Стерджесса [2]:

$$k = k(N) = 1 + \log_2 N. \quad (6)$$

Гистограмма строится по группированным данным. Предполагаемая область значений случайной величины x делится независимо от выборки на k интервалов (не обязательно одинаковых). Пусть $A_1, A_2, \ldots, A_k$ – интервалы на прямой, называемые интервалами группировки. Обозначим для $j = \overline{1..k}$ через n_j число элементов выборки, попавших в интервал A_j:

$$n_j = \{\text{число } x_i \in A_j\} = \sum_{i=1}^{N} I(x_i \in A_j), \text{ здесь } \sum_{j=1}^{k} n_j = N. \quad (7)$$

На каждом из интервалов A_j строят прямоугольник, площадь которого пропорциональна n_j. Общая площадь всех прямоугольников должна равняться единице. Пусть l_j – длина интервала A_j. Высота f_j прямоугольника над A_j равна

$$f_j = n_j / N l_j. \quad (8)$$

Полученная фигура называется гистограммой.

В случае, когда в качестве величины x выступает *размер http-ответов*, имеем:

$$\log_2 N_1 = \log_2 68000 \approx 16;$$
$$\log_2 N_2 = \log_2 65000 \approx 16;$$

следовательно, $k = 1+16 = 17$.

Полученная по данной методике выборочная оценка плотности распределения вероятностей размеров http-ответов во входном web-потоке представлена на рисунке 3. На оси абсцисс – размер http-ответов [кбайт]. Сплошной линией изображается плотность распределения вероятностей размеров http-ответов для совокупности R_1. А пунктирной линией – плотность распределения вероятностей размеров http-ответов для совокупности R_2. Можно заметить, что последний интервал (от 47 и более) выбран намного длиннее, чем все остальные, которые имеют одинаковую длину.

В случае, когда в качестве величины x выступает *размер графических http-ответов*, имеем:

$$\log_2 N_1^{г} = \log_2 21000 \approx 14; \qquad \log_2 N_2^{г} = \log_2 56000 \approx 16.$$

Результат оценки плотности распределения вероятностей должен позволять вычислить кумулятивные суммы (1). Поэтому нужно выбрать единое общее количество интервалов k для двух выборок R_1 и R_2. Предлагается выбрать $k = 1+(14+16)/2 = 16$.

Полученная по данной методике выборочная оценка плотности распределения вероятностей размеров графических http-ответов во входном web-потоке представлена на рисунке 4. На оси абсцисс – размер http-ответов [кбайт]. Сплошной линией изображается плотность распределения вероятностей размеров графических http-ответов для со R_1, пунктирной линией – плотность распределения вероятностей размеров графических http-ответов для R_2. Как и в предыдущем случае, последний интервал выбран намного длиннее, чем все остальные, которые имеют одинаковую длину.

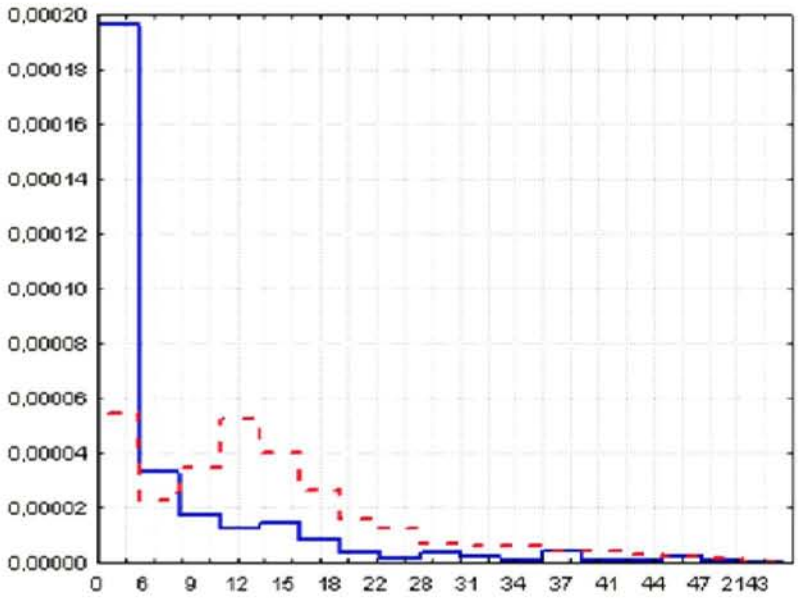


Рисунок 3 – Выборочная оценка плотности распределения вероятностей размеров http-ответов во входном web-потоке

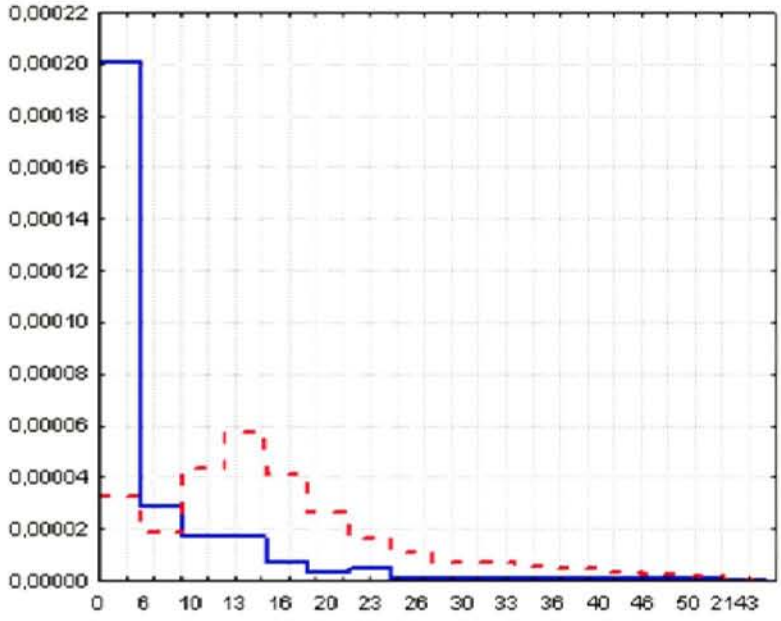


Рисунок 4 – Выборочная оценка плотности распределения вероятностей размеров графических http-ответов во входном web-потоке

Из рисунков 3, 4 видно:

- http-ответы и графические http-ответы во входном web-потоке, приходящем от web- сайтов выборки G_1, с большей вероятностью имеют незначительный размер (< 10 кбайт);
- http-ответы и графические http-ответы во входном web-потоке, приходящем от web- сайтов выборки G_2, с большей вероятностью имеют значительный размер;
- http-ответы с незначительным размером более вероятно относятся к совокупности R_1.

Выявленная разница в распределении размеров http-ответов двух совокупностей R_1 и R_2 позволит использовать метод кумулятивных сумм для обнаружения во входном web-потоке фрагментов запрещенных данных. Оценки

плотности распределения размеров http-ответов, представленные в графическом виде на рисунках 3,4, наглядно показывает возможность применения метода кумулятивной суммы. Для вычисления кумулятивных сумм (1) необходимо аналитическое задание оценки $f(x)$.

Пусть дана выборка $\{ x_1^N \}$. Соответствующий ей вариационный ряд делится на k участков с границами $X_0,X_1,\ldots,X_k$ и длинами $A_0,A_1,\ldots,A_k$, где $A_i = X_i - X_{i-1}$, $i = \overline{1..k}$. По выражениям (6,7,8) определяются k значений f_i, Тогда $f(x)$ определяется следующим образом:

$$f(x) = f_i, \text{ если } X_{i-1} \le x < X_i, \tag{7}$$

причем $i = \overline{1..k}$ и $f(X_k) = f_k$.

АЛГОРИТМ ОБНАРУЖЕНИЯ ФРАГМЕНТОВ ЗАПРЕЩЕННЫХ ДАННЫХ ВО ВХОДНОМ WEB-ПОТОКЕ НА ОСНОВЕ МЕТОДА КУМУЛЯТИВНЫХ СУММ

Задача обнаружения фрагментов запрещенных данных во входном web-потоке методом кумулятивной суммы может быть сформулирована следующим образом:

Пусть даны $R_1 = \{r_{11}, r_{12}, \ldots, r_{1N_1}\}$ от выборки разрешенных web-сайтов G_1 и $R_2 = \{r_{21}, r_{22}, \ldots, r_{2N_2}\}$ от выборки запрещенных web-сайтов G_2, а также допустимая задержка $\tau^{\text{доп}}$.

Требуется построить алгоритм обнаружения фрагментов запрещенных данных во входном web-потоке с минимальной вероятностью ложной тревоги $P_{\text{лож}}$ при обеспечении

$$\bar{\tau} \le \tau^{\text{доп}}, \tag{8}$$

где $\bar{\tau}$ – среднее значение τ, и $P_{\text{лож}}$ определяется как

$$P_{\text{лож}} = L/N, \tag{9}$$

где L – общая длительность ложных тревог, измеряемая количеством разрешенных http-ответов, ложно принимаемых за запрещенные;

N – общее количество разрешенных http-ответов.

Из рисунка 2 видно, что задержка τ и вероятность ложной тревоги $P_{\text{лож}}$ зависят от поведения кумулятивной суммы S_t и выбранного порогового значения h. Поведение кумулятивной суммы S_t в свою очередь зависит от $f(x/\theta_1)$ и $f(x/\theta_2)$, которые уже определены свойствами R_1 и R_2. Следовательно, поставленная задача сводится к определению порогового значения h, при котором обеспечиваются минимизация $P_{\text{лож}}$ и выполнение условия (8).

Задача определения требуемого значения h решается в два этапа. На первом этапе определяется верхняя граница значений h (нижняя граница считается равной нулю). На втором этапе осуществляется поиск требуемого h в пределах его значений.

Верхняя граница значений h определяется максимальной разностью кумулятивной суммы ΔS_t (2) при отсутствии запрещенных данных в R_1 (рис. 5,6).

Очевидно, что если порог h не меньше максимального значения ΔS_t, то согласно используемому методу, разладки в R_1 не будет, что и означает отсутствие ложной тревоги. В результате имеем оценку:

$$0 < h \le \max \Delta S_t. \tag{10}$$

Для потока R_1, полученного в ходе экспериментального исследования, было определено: если x – размер http-ответов, то $\max \Delta S_t = 226$, то есть

$$0 < h \le 226; \tag{10'}$$

если же x – размер графических http-ответов, то $\max \Delta S_t = 70$, то есть

$$0 < h \le 70. \tag{10"}$$

На втором этапе предлагается осуществить поиск значения h в найденной области по некоторому шагу Δh. Очевидно, чем больше h, тем больше τ. Поэтому поиск предлагается начать с верхней границы $h = \max \Delta S_t$. На каждом шаге значение h уменьшается на величину Δh, вычисляется средняя задержка $\bar{\tau}$ и проверяется условие (8). Искомым считается первое (максимальное) значение h, при котором выполняется условие (8).

Результат исследования заданных выборок на предмет зависимости порога срабатывания и ложных тревог от допустимой средней задержки представлен в таблице 1.

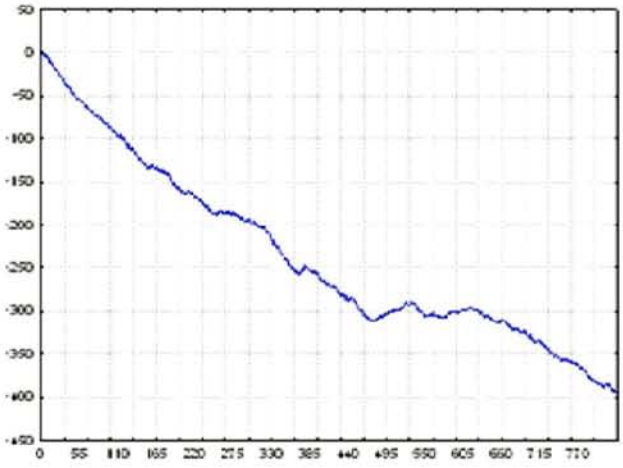


Рисунок 5 – Поведение кумулятивной суммы S_t для отрезка реальных данных потока R_1

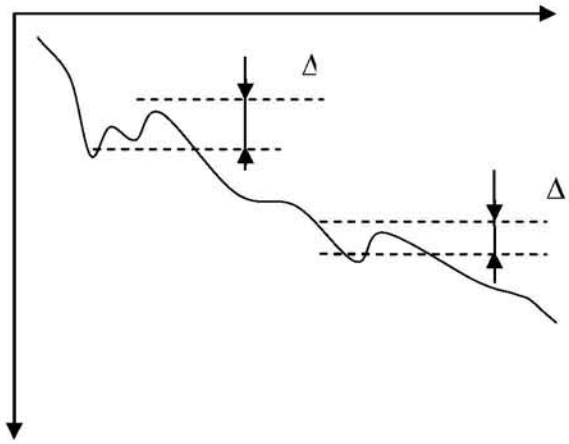


Рисунок 6 – Определение верхней границы значений h

В таблице 1 $\bar{\tau}^{\text{доп}}$ – допустимая средняя задержка, которая определяет значения $h_{\text{общ}}$ – порог срабатывания для случая, когда в качестве величины x выступает *размер http-ответов* (всех типов), и $h_{\text{г}}$ – порог срабатывания для случая, когда в качестве величины x выступает *размер графических http-ответов*. Пороги $h_{\text{общ}}$ и $h_{\text{г}}$ в свою очередь определяют общие длительности ложных тревог $L_{\text{общ}}$, $L_{\text{г}}$ и соответствующие вероятности ложной тревоги $P_{\text{лож}}^{\text{общ}}$, $P_{\text{лож}}^{\text{г}}$. Согласно (9):

$$P_{\text{лож}}^{\text{общ}} = \frac{L_{\text{общ}}}{N_1}; \qquad P_{\text{лож}}^{\text{г}} = \frac{L_{\text{г}}}{N_1^{\text{г}}}. \tag{11}$$

Таблица 1 – Зависимость порога срабатывания и ложных тревог от допустимой средней задержки

$\bar{\tau}^{\text{доп}}$	$h_{\text{общ}}$	$L_{\text{общ}}$	$P_{\text{лож}}^{\text{общ}}$	$h_{\text{г}}$	$L_{\text{г}}$	$P_{\text{лож}}^{\text{г}}$	$\bar{\tau}^{\text{доп}}$	$h_{\text{общ}}$	$L_{\text{общ}}$	$P_{\text{лож}}^{\text{общ}}$	$h_{\text{г}}$	$L_{\text{г}}$	$P_{\text{лож}}^{\text{г}}$
1	2	3	4	5	6	7	8	9	10	11	12	13	14
20	6	6981	0,10	16	736	0,03	40	20	2316	0,03	37	455	0,02
21	7	4895	0,07	17	684	0,03	41	20	2316	0,03	38	451	0,02
22	7	4895	0,07	18	669	0,03	42	21	2223	0,03	40	371	0,02
23	8	3330	0,05	20	618	0,03	43	22	2192	0,03	41	365	0,02
24	10	2714	0,04	21	661	0,03	44	23	1992	0,03	42	367	0,02
25	11	2575	0,04	21	661	0,03	45	23	1992	0,03	43	314	0,01
26	11	2575	0,04	22	649	0,03	46	24	1956	0,03	44	317	0,01
27	12	2551	0,04	23	609	0,03	47	24	1956	0,03	45	314	0,01
28	13	2426	0,04	24	629	0,03	48	25	1950	0,03	46	319	0,02
29	13	2426	0,04	25	562	0,03	49	26	1863	0,03	47	326	0,02
30	14	2404	0,03	27	560	0,03	50	26	1863	0,03	48	327	0,02

Продолжение таблицы 1.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
31	14	2404	0,03	28	544	0,03	51	27	1844	0,03	50	326	0,02
32	15	2424	0,04	29	529	0,02	52	27	1844	0,03	51	325	0,02
33	15	2424	0,04	30	516	0,02	53	28	1852	0,03	52	323	0,02
34	15	2424	0,04	31	483	0,02	54	29	1749	0,03	53	244	0,01
35	16	2380	0,03	32	489	0,02	55	29	1749	0,03	55	241	0,01
36	16	2380	0,03	32	489	0,02	56	30	1675	0,02	56	240	0,01
37	17	2233	0,03	33	484	0,02	57	31	1653	0,02	57	239	0,01
38	18	2189	0,03	34	506	0,02	58	32	1698	0,02	59	221	0,01
39	19	2334	0,03	36	518	0,02	59	32	1698	0,02	60	222	0,01

Диапазон исследуемых значений $\bar{\tau}^{\text{доп}}$ выбирается из соображений того, что для web-сайтов выборки G_1 каждая web-страница в среднем содержит 54 встроенных объекта (изображения, javascript, css, flash…). При использовании браузером кэширования на каждую web-страницу в потоке приходится в среднем 27 таких объектов. В расчетах не учитываются http-ответы, кэшированные браузером. Обнаружение фрагментов запрещенных данных в рамках эксперимента есть обнаружение фрагментов данных R_2 (в смешанном потоке), поэтому в выборе $\bar{\tau}^{\text{доп}}$ учитывается только свойства R_2.

Для потока R_2 среднее отношение количества графических http-ответов к общему количеству http-ответов составляет:

$$\frac{N_2^{\text{г}}}{N_2} = \frac{56169}{65097} = 0{,}86\,. \qquad (11)$$

Это означает, что задержке $\bar{\tau}^{\text{доп}}$ в случае, когда в качестве величины x выступает *размер http-ответов* (всех типов), соответствует задержка $0{,}86 \cdot \bar{\tau}^{\text{доп}}$ в случае, когда в качестве величины x выступает *размер графических http-ответов*. То есть, чтобы сравнить эти две величины по возможности обнаружения запрещенных данных (в рамках поставленной задачи), необходимо сравнить тройку ($h_{\text{общ}}$, $L_{\text{общ}}$, $P_{\text{лож}}^{\text{общ}}$) при $\bar{\tau}^{\text{доп}}$ с тройкой ($h_{\text{г}}$, $L_{\text{г}}$, $P_{\text{лож}}^{\text{г}}$) при $0{,}86 \cdot \bar{\tau}^{\text{доп}}$.

Очевидно, что качество обнаружения определяется не порогом срабатывания h, а длительностью ложных тревог L и соответствующей ей вероятностью ложной тревоги $P_{лож}$. Чем меньше L и $P_{лож}$, тем лучшим считается качество обнаружения. По данным таблицы 1 видно, что при эквивалентной допустимой средней задержке использование параметра «*размер графических http-ответов*» позволяет с лучшим качеством обнаружить запрещенные фрагменты во входном web-потоке.

ВЫВОДЫ

Результат исследования позволяет сделать вывод о возможном применении метода кумулятивных сумм для формирования алгоритма обнаружения запрещенных данных во входном web-потоке. При этом результативность алгоритма выше при использовании параметра «*размер графических http-ответов*».

СПИСОК ЛИТЕРАТУРЫ

1. Никифоров И.В. Последовательное обнаружение изменения свойств временных рядов. – М.: Наука, 1983. – 198 с.
2. Чернова Н.И. Лекции по математической статистике [Электронный ресурс].– URL: http://nsu.ru/mmf/tvims/chernova/ms/lec/node4.html.

3. Вальд А. Последовательный анализ. – М.: Физматгиз, 1960. – 328 с.
4. Page E.S. Continuous inspection schemes. // Biometrika, 1954, 41, N1, p.100-115.
5. Ghosh B.K. Sequential tests of statistical hypotheses. Reading (Mass.): Addison-Wesley, 1970. – 454 p.
6. Jeongeun Julie Lee, Maruti Gupta. «A new traffic model for current user web browsing behavior», Intel Corporation 2007.
7. Choi H., Limb J. «A behavioral model of web traffic» in International conference of networking protocol'99 (ICNP 99), September 1999.
8. Mah B.A. «An empirical model of HTTP network traffic», in Proceedings of INFOCOM'97, April 7-11, Kobe, Japan.

Комашинский Владимир Владимирович
Академия ФСО России, г. Орел
Сотрудник
Тел.: (4862) 40-83-59
E-mail: vladkom-orel@rambler.ru

Нгуен Туан Ань
Академия ФСО России, г. Орел
Сотрудник
Тел.: 8 920 822 51 28
E-mail: summerlant@gmail.com

V.V. KOMASHINSKY, T.A. NGUYEN

AN ALGORITHM BASED ON CUMULATIVE SUM METHOD FOR DETECTING ILLEGAL DATA IN INCOMING WEB TRAFFIC

The application of the cumulative sum method for detecting fragments of illegal data in incoming web traffic is considered. The distribution of http-response size is used for decision-making. The distribution is calculated empirically in two cases: distribution of general http-response size and distribution of graphic http-response size. In the paper modern information systems problems of functional safety are stated and the ways selection method of functional safety mechanisms realization for critical sociotehnical systems on the basis of radicals is considered.

Keywords: *cumulative sum; http-response size; incoming web traffic; filtering; detection.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Nikiforov I.V. Posledovatel'noe obnaruzhenie izmeneniya svojstv vremenny'x ryadov. – M.: Nauka, 1983. – 198 s.
2. Chernova N.I. Lekcii po matematicheskoj statistike. [E`lektronny'j resurs]. URL: http://nsu.ru/mmf/tvims/chernova/ms/lec/node4.html
3. Val'd A. Posledovatel'ny'j analiz. – M.: Fizmatgiz, 1960. – 328 s.
4. Page E.S. Continuous inspection schemes. // Biometrika, 1954, 41, N1, p.100-115.
5. Ghosh B.K. Sequential tests of statistical hypotheses. Reading (Mass.): Addison-Wesley, 1970. – 454 p.
6. Jeongeun Julie Lee, Maruti Gupta. «A new traffic model for current user web browsing behavior», Intel Corporation 2007.
7. Choi H., Limb J. «A behavioral model of web traffic» in International conference of networking protocol'99 (ICNP 99), September 1999.
8. Mah B.A. «An empirical model of HTTP network traffic», in Proceedings of INFOCOM'97, April 7-11, Kobe, Japan.

УДК 004

А.И. ТИТОВ, Н.И. КОРСУНОВ

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ ШИФРОВАНИЯ ДАННЫХ

В данной статье рассмотрена модификация алгоритма шифрования данных, основанная на методе Вижинера, с применением маски шифрования. Маска шифрования – это хеш-функция, для различных файлов является различной. Разобран пример формирования маски шифрования. Представлена методика модифицированного шифрования.

Ключевые слова: *метод Вижинера; маска шифрования; хеш-функция.*

Цель – разработка метода шифрования данных, позволяющего использовать модификации шифра Вижинера.

Для достижения поставленной цели предлагается использовать многократную итерацию. Итеративный алгоритм шифрования – это такой алгоритм шифрования, для которого соответствующие алгоритм зашифрования и алгоритм расшифрования состоят из последовательных однотипных циклов шифрования.

Подобные алгоритмы относительно просто реаизуются и позволяют обеспечивать, в частности, свойство перемешивания, свойство рассеивания и свойство усложнения. Алфавит для шифрования любого типа файлов, очевидно, имеет разрядность n=256. Это объясняется тем, что файл – это набор байт, а, как мы знаем, байт имеет значение от 0 до 255. В отличие от шифра Вижинера и известных модификаций, предложен блочный подход, который позволяет при частичном дешифровании шифр текста начать передачу данных. Так как задача дешифрования следующего байта не зависит от значения предыдущего, следовательно, момент трансляции открытого текста может идти параллельно дешифрованию.

Шифрование производится блочно по одному байту и, независимо от количества итераций, алгоритм шифрования и дешифрования имеет следующий вид.

Для шифрования необходимо два параметра: i – один байт шифруемого файла, j – один байт ключа шифрования. Результатом шифрования является один байт шифрованного файла. Выражения, используемые для шифрования, выведены аналитически из таблицы 1. По этой таблице легко проверить, что эти выражения справедливы для всех наборов значении байта.

```
crypt(i,j:byte):byte;
begin
  if j<(256-i) then
    crypt:=i+j
  else
    crypt:=j-(256-i)
end;
```

Таблица 1 – таблица Виженера для шифрования любого файла

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24……	253	254	255
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24……	253	254	255	0
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24……	253	254	255	0	1
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24……	253	254	255	0	1	2
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24……	253	254	255	0	1	2	3
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24……	253	254	255	0	1	2	3	4
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24……	253	254	255	0	1	2	3	4	5
7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24……	253	254	255	0	1	2	3	4	5	6

……
……
254 255 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24…….253
255 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24…….253 254

Дешифрование работает аналогично шифрованию – вычисляется байт открытого файла. Входные данные: байт ключа, байт шифрованного файла.

```
decrypt(i,x:byte):byte;
begin
  if x>(i-1) then
    decrypt:=x-i
  else
    decrypt:=x+(256-i)
end;
```

При однократном шифровании, зная алфавит и шифрованный текст, криптоаналитик, используя метод протяжки известного слова, может подобрать ключ шифрования**.** Метод протяжки вероятного слова – метод криптографического анализа, состоящий в последовательном опробовании места в шифрованном тексте, соответствующего вероятному фрагменту открытого текста. При истинном варианте опробования возможно составление и решение уравнений относительно неизвестного ключа. Для устранения этого предлагается использовать многократный итерационный метод при шифровании и дешифровании. Причем для увеличения криптостойкости необходимо смещать ключ шифрования на втором и последующих шагах итерации. Для вычисления смешения будем пользоваться остатком ключа с предыдущей итерации.

Прямолинейный процесс шифрования-дешифрования представляется следующей последовательностью шагов.

Первый шаг шифрования

Ключ	1	21	31	41	51	61	31	1	21	31	41	51	61
Открытый файл	121	145	0	18	35	43	0	0	9	15	5	6	3
Шифрованный файл	122	166	31	59	86	104	31	1	30	46	46	56	64

Второй шаг шифрования

Ключ	31	1	21	31	41	51	61	31	1	21	31	41	51
Шифрованный файл 1 шага	122	166	31	59	86	104	31	1	30	46	46	56	64
Шифрованный файл	153	167	52	90	127	155	92	32	31	67	77	97	115

Третий шаг шифрования

Ключ	61	31	1	21	31	41	51	61	31	1	21	31	41
Шифрованный файл 2 шага	153	167	52	90	127	155	92	32	31	67	77	97	115
Шифрованный файл	214	198	53	111	158	196	143	93	62	68	98	128	156

Четвертый шаг шифрования

Ключ	51	61	31	1	21	31	41	51	61	31	1	21	31
Шифрованный файл 3 шага	214	198	53	111	158	196	143	93	62	68	98	128	156
Шифрованный файл	9	3	82	112	179	227	184	144	123	99	99	149	187

После четвертого шага шифрования сравним открытый файл и шифрованный файл

Ключ	1	21	31	41	51	61	31	1	21	31	41	51	61
Открытый файл	121	145	0	18	35	43	0	0	9	15	5	6	3
Шифрованный файл	9	3	82	112	179	227	184	144	123	99	99	149	187

Стоит заметить, что при сравнительно коротком ключе 7 байт мы получаем стойкий шифр к методу протяжки известных слов и частотному анализу. Оба метода способны получить только маску шифрования (хеш-функцию ключа для данного файла), но не способны получить сам ключ шифрования. Для полноценного взлома необходимо получить несколько безошибочных масок шифрования (хеш-функций для различных файлов) и уже в них выявлять зависимости для получения конечного ключа, что естественно приведёт к увеличению времени взлома.

Может показаться, что для N-итерационного шифрования необходимо проходить исходный файл N раз. При прямолинейном подходе это действительно так, но при этом теряется возможность использования данного алгоритма для блочного шифрования. Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа.

Для организации блочного шифра можно заменить многократный проход исходного файла на шифрование блоками по одному байту, независимо от остальных байт в файле.

При этом каждый блок будет шифроваться в несколько проходов с использованием различных байт ключа, позиции которых вычисляются с помощью следующих выражений.

Для получения выражений используем отсутствие первоначального смещения на первом шаге шифрования.

Вычисление начального смещения для второго шага шифрования происходит следующим образом (рис. 2).

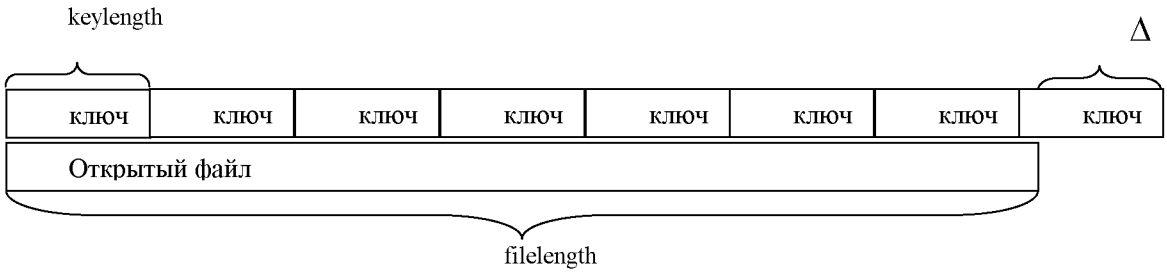


Рисунок 2 – Вычисление смещения для второго шага шифрования

$\Delta = filelength \bmod keylength$,

где filelength – количество байт в открытом файле;

keylengt – количество байт в ключе шифрования;

Δ – величина смещения ключа на втором шаге итерации.

На рисунке 2 проиллюстрирован остаток ключа, который переходит на следующую итерацию и отождествляет смещение ключа шифрования.

Вычисления смещения на любом шаге приведено на рисунке 3 .

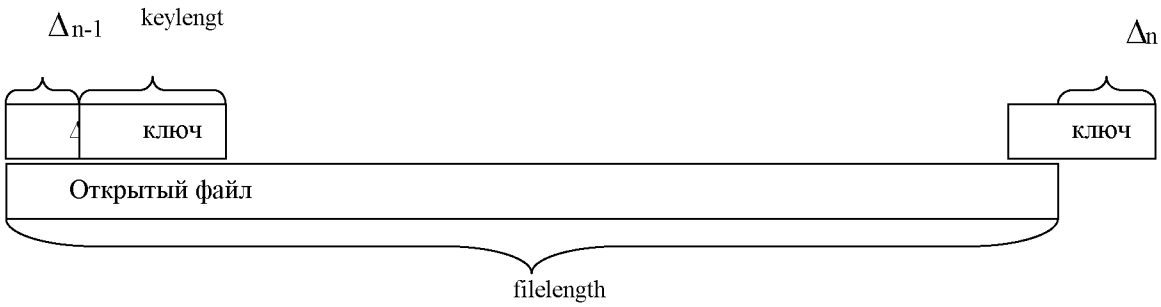


Рисунок 3 – Вычисление смещения для следующих за вторым шагом шифрования

Отсюда следует, что вычисление смещения на любом шаге шифрования представляется в виде.

$$\Delta_n = (filelength - (keylength - \Delta_{n-1})) \bmod keylength ,$$

где Δ_n – вычисляемая величина смещения ключа на шаге n;

Δ_{n-1} – величина смещения ключа на предыдущем шаге (n-1).

Так как длина ключа не регламентирована, то

filelength mod keylengt = 0.

Для того, чтобы вторая и последующие итерации не проходили впустую, необходимо смещать ключ на n байт. Число n – величина, задаваемая администратором в момент настройки криптосистемы.

ПРИМЕР:

Необходимо зашифровать открытый файл

Открытый файл	121	145	0	18	35	43	0	0	9	15	5	6	3

При помощи ключа

Номер байта	1	2	3	4	5	6	7
Ключ	1	21	31	41	51	61	31

Количество итераций 4

Filelength = 13

Keylength = 7

Δ1=(13 mod 7);

Δ1=6;

Δ2=(13-(7-6)) mod 7

Δ2=5;

Δ3=(13-(7-5)) mod 7

Δ3=4;

Значения смещений вычисляются однократно и используются при шифровании всего файла.

Номер байта открытого файла N=0;

Байт открытого файла	121	Номер байта ключа Nb	Значение ключа
Итерация 1	122	(N mod Keylength)+1= 1	1
Итерация 2	153	(1+6) = 7	31

Итерация 3	214	(1+5) = 6	61
Итерация 4	9	(1+4) = 5	51
Шифрованный байт	9		

N=1;

При вычислении номера байта ключа на каждом из шагов итерации будем пользоваться правилом

If ((Nb+ Δi) > Keylength) then Nbi=(Nb+ Δi) mod Keylength
else Nbi=(Nb+ Δi);

Байт открытого файла	145	Номер байта ключа Nb	Значение ключа
Итерация 1	145	2	21
Итерация 2	166	(2+6) mod Keylength = 1	1
Итерация 3	167	2+5 = 7	31
Итерация 4	198	2+4 = 6	61
Шифрованный байт	198		

N=2;

Байт открытого файла	0	Номер байта ключа Nb	Значение ключа
Итерация 1	31	3	31
Итерация 2	52	(3+6) mod Keylength = 2	21
Итерация 3	53	(3+5) mod Keylength = 1	1
Итерация 4	82	3+4 = 7	31
Шифрованный байт	82		

И так далее…

ВЫВОД

Предложенный алгоритм, основанный на варьировании количества итерации со смещением ключа, позволяет усложнить процесс, увеличить временную сложность взлома. Так как для получения первичного ключа необходимо применение частотных методов, позволяющих вычислить маски шифрования (хеш-функции для различных файлов), после получения достаточного количества верных масок возможен анализ полученных данных для выявления первичного ключа.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия. // Старый Оскол: ООО «ТНТ» (тонкие научные технологии), 2005. – 448 с.
2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник // СПб.:БХВ-Петербург, 2009. – 576 с.: ил.
3. Альферов А.П. Основы криптографии: учебное пособие // Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. // 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002. – 480 с.; ил.
4. Thomas W. Cusick, Pantelimon Stanica. «Cryptographic Boolean Functions and Applications» // Academic Press is an imprint of Elsevier 525 B Street, Suite 1900, San Diego, CA 92101-4495, USA Linacre House, Jordan Hill, Oxford OX2 8DP, UK. First edition, 2009. Новости науки: AllScience.ru – Российский научный портал. –URL: http://www.allscience.ru/News/?ID=7092 – Философия криптографии: возможности гомоморфизма.
5. Зубов А.Ю. Совершенные шифры. – М.: Гелиос АРВ, 2003. – 160 с., ил.
6. Криптография и алгоритмы шифрования [Электронный ресурс]. – URL: http://vse-shifri.ru.

Корсунов Николай Иванович
Белгородский государственный университет, г. Белгород
Доктор технических наук, профессор, профессор кафедры «Математическое и программное обеспечение информационных систем»
Тел.: (84722) 30-13-51
E-mail: korsunov@intbel.ru

Титов Алексей Иванович
Белгородский государственный технологический университет им. В.Г. Шухова, г. Белгород
Аспирант
Тел.: 8 908 785 39 28
E-mail: titov@programist.ru

N.I. KORSUNOV, A.I. TITOV

MODIFIED DATA ENCRYPTION ALGORITHM

In this paper the modification of the data encryption algorithm based on the method Vizhinera with the use of encryption masks. Mask encryption is a hash function for a variety of files is different. Analyzed example of formation of the encryption mask. The technique of modified encryption.

Keywords: *the method Vizhinera; encryption masks; the hash function.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Ignat'ev V.A. Informacionnaya bezopasnost' sovremennogo kommercheskogo predpriyatiya // Stary'j Oskol: OOO «TNT» (tonkie nauchny'e texnologii), 2005. – 448 s.
2. Panasenko S.P. Algoritmy' shifrovaniya. Special'ny'j spravochnik // SPb.: BXV-Peterburg, 2009. – 576 s.: il.
3. Al'ferov A.P. Osnovy' kriptografii: uchebnoe posobie / Zubova A.Yu., Kuz'min A.S., Cheryomushkin A.V. // 2-e izd., ispr. i dop. – M.: Gelios ARV, 2002. 480 s.; il.
4. Thomas W. Cusick, Pantelimon Stanica. Cryptographic Boolean Functions and Applications» // Academic Press is an imprint of Elsevier 525 B Street, Suite 1900, San Diego, CA 92101-4495, USA Linacre House, Jordan Hill, Oxford OX2 8DP, UK. First edition, 2009.
5. Zubov A.Yu. Sovershenny'e shifry'. – M.: Gelios ARV, 2003. – 160 s.; il.
6. Kriptografiya i algoritmy' shifrovaniya / [E'lektronny'j resurs] URL: http://vse-shifri.ru.

УДК 004.056.53

В.В. ЛЫСЫХ

ОБФУСКАЦИЯ КОДА В КОНТЕКСТЕ ПРОБЛЕМЫ ЗАЩИТЫ ПРОГРАММНЫХ ПРОДУКТОВ

Проводится классификация современных методов защиты программных продуктов. Даётся понятие процесса обфускации. Сравниваются методы запутывания и методы анализа программ. Формулируются свойства, которыми должен обладать запутанный программный продукт. Предлагается метод запутывания, удовлетворяющий перечисленным свойствам.

Ключевые слова: *обфускация программ; защита программных продуктов.*

Одним из важных направлений деятельности в области обеспечения информационной безопасности является защита программных продуктов от вредоносных воздействий на информацию в процессе функционирования компьютерных систем.

Существующие способы защиты программных продуктов можно разделить на способы, реализуемые с помощью **аппаратных и программных и средств защиты** [3,5].

К аппаратным относятся средства, использующие специальное оборудование [1] или физические особенности носителей, чтобы идентифицировать оригинальную версию программы и защитить продукт от нелегального использования. Такие методы наиболее удобны для производителя программного обеспечения, так как легко можно защитить уже полностью готовый и оттестированный продукт.

Программные средства защиты реализуются программным путем без использования физических характеристик носителей информации, специального оборудования и т.п. Под программными методами защиты информации понимается комплекс специальных алгоритмов и компонентов общего программного обеспечения вычислительных систем, предназначенных для выполнения функций контроля, разграничения доступа и исключения несанкционированного доступа [2,6].

К программным методам защиты программных продуктов относится использование «водяных знаков» (software watermark), «отпечаток пальца» (software fingerprint), установка подлинности кода (tamper-proofing), шифрование программного кода (enciphering) и запутывание программ (obfuscated program) [1, 4].

Обфускация (obfiiscation – запутывание) – это один из методов защиты программного кода, который позволяет усложнить процесс реверсивной инженерии кода защищаемого программного продукта [8,9].

Суть процесса заключается в том, чтобы запутать программный код и устранить большинство логических связей в нем, то есть трансформировать его так, чтобы он был очень труден для изучения и модификации посторонними лицами.

Запутывание как метод защиты программных продуктов можно считать сравнительно новым и перспективным. Обфускация соответствует принципу экономической целесообразности, так как ее использование незначительно увеличивает стоимость программного продукта и позволяет при этом снизить потери от пиратства, а также плагиата в результате кражи уникального алгоритма работы защищаемого программного продукта [10].

Запутывающие преобразования позволяют обеспечить скрытность деталей

реализации программных продуктов. Такой подход существенно усложняет процесс реверсивной инженерии кода защищаемого программного продукта.

Определим понятия «запутывающие преобразования», «запутанная программа», «процесс запутывания».

Запутывающие преобразования (obfuscating transformations) – это преобразования, в результате применения которых к исходной программе изменяется ее структура или код, но при этом она остается работоспособной и выполняет те же функции.

Запутанной (obfuscated) программой называется программа, которая после применения запутывающих преобразований на всех допустимых для исходной программы входных данных выдаёт тот же самый результат, что и оригинальная программа, но является более трудной для анализа, понимания и модификации [11]. Временные затраты на «распутывание» запутанной программы должны быть эквивалентны времени потраченному на создание аналогичной программы «с нуля». Для оценивания эффективности процесса запутывания используются три величины:

1. Устойчивость – указывает на степень сложности осуществления реверсивной инженерии над кодом, прошедшим процесс обфускации.

2. Эластичность – указывает на то, насколько хорошо данный процесс обфускации, защитит программный код от применения деобфускаторов.

3. Стоимость преобразования – позволяет оценить, насколько больше требуется системных ресурсов для выполнения кода, прошедшего процесс обфускации, чем для выполнения оригинального кода программы.

Процесс запутывания – это процесс трансформации исходной программы с помощью запутывающих преобразований, после которого программа становится запутанной.

Запутывающие преобразования можно разделить на несколько групп:

• **преобразования форматирования исходного кода** (лексическое запутывание) – преобразования, которые изменяют только внешний вид программы. К этой группе относятся преобразования, удаляющие комментарии, отступы в тексте программы или переименовывающие идентификаторы;

• **преобразования структур данных**, изменяющие структуры данных, с которыми работает программа. К этой группе относятся преобразования, изменяющие иерархию наследования классов в программе, или преобразования, объединяющие скалярные переменные одного типа в массив;

• **преобразования потока управления программы**, которые изменяют структуру её графа потока управления, такие, как развёртка циклов, выделение фрагментов кода в процедуры и другие;

• **превентивные преобразования**, нацеленные против определённых методов декомпиляции программ или использующие ошибки в определённых инструментальных средствах декомпиляции.

Рассмотрим методы, которые применяются при анализе программ в компиляторах. Цель таких методов – выявление зависимостей между компонентами программы, что даёт возможность применить определённые оптимизационные преобразования или накладывает ограничения на проводимые оптимизационные преобразования.

Методы анализа программ могут быть разделены на 4 группы:

• синтаксические – методы, основанные только на результатах лексического, синтаксического и семантического анализа программы;

- статические – методы анализа потоков управления и данных и методы, основанные на результатах анализа потоков управления и данных. Статические методы анализа работают с программой, не используя информацию о работе программы на конкретных начальных данных;
- динамические – основаны на использовании информации, полученной в результате наблюдения за работой программы на конкретных входных данных;
- статистические – методы, использующие информацию, собранную в результате значительного количества запусков программы на большом количестве наборов входных данных.

Запутывающие преобразования процесса форматирования исходного кода не устойчивы к методам синтаксического анализа, т.к. программы обладают открытой семантикой. Для анализа таких программ достаточно изучения семантики программы, что дает возможность определить внесенные изменения в программу. Также для программ, реализованных на языках высокого уровня программирования, всегда можно использовать инструменты автоматического переформатирования, поэтому использовать такие преобразования необходимо для программ с низкой стоимостью, не требующих высокого уровня защиты, либо комбинировать эти преобразования с другими методами.

Запутывание преобразованием структур данных можно проанализировать статистическим и динамическим анализом потока данных. Анализ потока данных основывается на изучении того, как в процессе работы программы изменяются в ней данные (переменные, массивы). Также достаточно легко провести анализ содержимого регистров, временных переменных, в том числе, определение возвращаемых функциями значений, распространение типов данных.

Преобразования потока управления не устойчивы к методам статического и статистического анализа, т.к. всегда есть возможность визуализации графа потока управления.

Можно провести сравнение трасс, полученных на одном и том же наборе входных данных, осуществить алгебраические упрощения для определения непрозрачных предикатов, статическое и динамическое устранение мертвого кода.

Исходя из вышесказанного, можно сделать вывод о том, что запутывающее преобразование называется устойчивым относительно некоторого класса методов анализа программ, если методы этого класса не позволяют надёжно раскрыть данное запутывающее преобразование.

Для некоторых видов запутывающих преобразований требуемые инструменты анализа (синтаксические, статические, статистические и динамические) зависят от того, каким способом было реализовано преобразование.

Поскольку теория запутывания программ находится в стадии активного формирования, существует потребность в создании новых методов запутывания.

Создаваемый **метод обфускации** должен приводить программный продукт к виду, который будет удовлетворять следующим свойствам:

- запутывание должно быть замаскированным. То, что к программе были применены запутывающие преобразования, не должно выявляться при поверхностном анализе;
- запутывание не должно быть регулярным. Регулярная структура запутанной программы или её фрагмента позволяет отделить запутанные части и даже идентифицировать алгоритм запутывания;

• применение стандартных синтаксических и статических методов анализа программ не должно давать существенных результатов.

Для создания эффективного метода защиты предлагается использовать комбинирование запутывающих преобразований потока управления, преобразования структур данных, преобразования форматирования.

Разработанный метод обфускации состоит их следующих этапов:

• Построение графа потока управления и выделение базовых блоков программы. На этом этапе выполняется построение исходного графа с использованием теории графов и проводится оптимизационный анализ.

• Преобразование графа потока управления, изменение структуры циклов, введение меток (указателей) и их перемешивание, добавление новых переходов от одного базового блока к другому. Изменение порядка операций в исходном тексте программы и переименование меток (использование не связанных между собой названий меток).

• Введение массива для хранения переменных одного типа.

• Переприсваивание и перевычисление переменных. Присвоение различным переменным одних и тех же значений и использование этих переменных в различных участках программы.

• Создание блока «мертвого кода». Такое преобразование должно осуществляется таким образом, чтобы в процессе работы программы к этому блоку были постоянные обращения. Данный блок может работать в качестве «маршрутизатора».

• Введение связности между блоками основного и мертвого кода с помощью указателей. Учитывая стойкость каждого из использованных запутывающих преобразований к конкретным средствам анализа, можно утверждать, что применение их в совокупности позволит создать метод, устойчивый как к синтаксическому и статическому, так и к динамическому анализу.

Для **теоретического обоснования устойчивости метода** используется аппарат дискретной математики, машин Тьюринга [7]. Дадим определения и теоремы, сформулированные А.В. Черновым [8].

Пусть $S = \{0,1\}$, $poly(n)$ – произвольный многочлен от переменной n.

Определение 1. Пусть $f : S^m \to S^n, m = poly(n)$. Функция f (отображение) называется односторонней функцией, если для любого $x \in S^m$ существует полиномиальный алгоритм вычисления значений $f(x)$ и не существует полиномиального алгоритма инвертирования функции f. Для любой полиномиальной вероятностной машины Тьюринга Pr_T выполнено следующее:

$$P\{f(A(f(x))) = f(x)\} < 1/poly(m).$$

Вероятность здесь определяется случайным выбором x и случайными величинами, которые Pr_T использует в своей работе.

Определение 2. Взаимно однозначная односторонняя функция $f : S^n \to S^n$ называется односторонней перестановкой.

Определение 3. ε-приближённым алгоритмом решения оптимизационной задачи называется алгоритм, находящий решение не более, чем в ε раз хуже оптимального решения.

Пример. Задача M минимизации некоторого функционала f.

Пусть A – ε-приближённый алгоритм нахождения решения задачи M. Пусть для некоторой реализации задачи оптимальное значение функционала равно X. Тогда алгоритм A найдёт решение задачи, при котором значение f равно Y, причём будет справедливо неравенство $X \le Y \le PX$.

Определение 4. Пусть $f : S^m \to S^n$, $x = (x_1,...,x_m)$, $y = (y_1,...,y_n)$, $y = f(x)$. Переменная x_k называется существенной, если существуют $(x_1,...,x_{k-1},x_{k+1},...,x_m) \in S$ и $j \in \{1,...,n\}$ такие, что выполняется условие: $f_j(x_1,...,x_{k-1},0,x_{k+1},...,x_m) \neq f_j(x_1,...,x_{k-1},1,x_{k+1},...,x_m)$.

Теорема 1. Пусть $f : S^m \to S^n, f$ записана как система булевых формул в базисе $\{\cup,\cap,\neg\}, 1 \le k \le m$. Задача проверки существенности переменной x_k NP-полна [8].

Доказательство.

Пусть $e_1 \neq e_2 \equiv (e_1 \cap \overline{e_2}) \cup (\overline{e_1} \cap e_2)$, где e_1, e_2 – булевы формулы.

Обозначим $\bar{x} = (x_1,..., x_m), \bar{y} = (y_1,..., y_n)$ и $\bar{x}|_{i=\sigma} = (x_1,...,x_{i-1},\sigma,x_{i+1},...,x_m)$.

1. Задача существенности находится в классе NP. Если переменная существенна, то существует такой вектор $\bar{x}$, для которого $g(\bar{x}) = 1$. Если переменная не существенна, то на всех наборах $\bar{x}$: выполняется $g(\bar{x}) = 0$. И наоборот, если $g(\bar{x})$ принадлежит языку «выполнения» (выполняется), то переменная x_k существенна. Если $g(\bar{x})$ не принадлежит языку «выполнения», то x_k – не существенна.

Таким образом, задача проверки существенности сведена к задаче проверки выполнимости булевой формулы. Последняя находится в классе NP. Следовательно, и задача проверки существенности находится в классе NP, как показано в работе Чернова А.В. [8].

2. Задача выполнения, которая является NP-полной, полиномиально сводится к задаче существенности.

Пусть $g(\bar{x})$ – некоторая формула в базисе $\{\cup,\cap,\neg\}$. Тогда формула, реализующая функцию $f \equiv 1$, принадлежит языку «выполнения», но ни одна переменная в такой формуле не является существенной.

В формуле, реализующей функцию $f \equiv 0$, которая не принадлежит языку «выполнения», также нет существенных переменных. Все прочие формулы принадлежат языку «выполнения» и хотя бы одна переменная в них является существенной. Таким образом, формула не принадлежит «выполнению», если её значение на любом битовом наборе равно 0, и в ней нет существенных переменных.

Для проверки выполнимости формулы нужно проверить её значение в одной точке и m раз проверить существенность переменных формулы. Следовательно, задача выполнения полиномиально по Тьюрингу сводится к задаче существенности, что доказывает NP-полноту последней.

Определение 5. Пусть $f : S^m \to S^n$, $\bar{x} = (x_1,..., x_m), \bar{y} = (y_1,..., y_n)$, $\bar{y} = f(\bar{x})$. Пусть множество I – это множество индексов компонент $\bar{y}$.

Переменная x_k называется существенной относительно множества I, если существуют такие $(x_1,...,x_{k-1},1,x_{k+1},...,x_m) \in S$ и такая $j \in I$, что выполняется условие $f_j(x_1,...,x_{k-1},0,x_{k+1},...,x_m)$

Теорема 2. *Пусть даны* $m,n, f : S^m \to S^n, I \notin 2^{(1,...,n)}, k$.

Задача проверки существенности переменной x_k относительно множества I NP – полна [8].

Доказательство принадлежности задачи к классу NP аналогично доказательству теоремы 1.

Пусть $I = \{1,...,n\}$ задача существенности является частным случаем для доказательства NP.

Определение 6. Задача анализа зависимостей по данным определяется как задача нахождения такого минимального множества переменных $W_{in} \subseteq V_{in}$, что переменные из множества $V_{in} - W_{in}$ несущественны относительно W_{out}, где $V = \{v_1,...,v_k\}$ – множество переменных запутанной программы, $f : S^m \to S^n$ – базовый блок, представляющий вычисление булевой функции над переменными из V_{in};

$V_{in} \subseteq V, |V_{in}| = m$ – переменные, значения которых используются при вычислении f;

$V_{out} \subseteq V, |V_{out}| = n$ – переменные, которые получают новые значения в результате вычисления, если для некоторой переменной $v \in V_{in}$ и $v \in V_{out}$ при вычислении используется старое значение переменной;

$W_{out} \subseteq V_{out}$ – множество «существенных» переменных на выходе из базового блока.

Теорема 3. Задача ЗАВ NP – полна[8].

Доказательство.

Принадлежность задачи классу NP следует из того, что для каждого такого i, что $(1 \le i \le k)$ можно найти решение задачи существенности относительно множества (то есть определить, принадлежит ли множеству V_{in}). Далее за полиномиальное время проверяется, что $|W_{in}| \le l$, число l такое, что $(0 \le l \le k)$..

Определение 7. «Мёртвые» инструкции – это инструкции, которые относятся к вычислению несущественных переменных.

Из доказанного выше следует, что задача выявления «мёртвого» кода в программе, состоящей из одного базового блока, NP – полна, и, более того, не существует ε-приближённого полиномиального алгоритма выявления «мёртвого» кода.

Переменные произвольных целых типов могут рассматриваться как набор переменных булева типа.

Устойчивость запутанной программы к автоматическому анализу обосновывается следующим:

- При статическом анализе массивов невозможно сделать анализ с точностью до каждого элемента массива. Следовательно, такой анализ окажется не эффективным.
- При использовании разработанного метода защиты программных средств с запутыванием кода программы появляется избыточность, то есть увеличение количества операций. Таким образом, при анализе зависимости по данным и для анализа указателей потребуется большое количество ресурсов и такой анализ окажется не эффективным.

Устойчивость запутанной программы к ручному анализу *обосновывается следующими соображениями:*

- Использование меток представляет большую трудность для анализа программы.
- «Мертвый блок» кода программы работает в качестве маршрутизатора и имеет непосредственную связность с основным блоком программы, следовательно, распутывание требует анализа всего кода программы.
- В результате применения метода, даже для относительно простых алгоритмов сортировок, увеличивается объем кода программы в 1,5 раза, следовательно, увеличивается количество операндов и машинных команд, что делает сложным ручной анализ программы. При этом незначительно понижается производительность программы вследствие возрастания требований к системным ресурсам.
- В результате преобразования графа потока управления появляются дополнительные переходы, что приводит к запутанности графа. Графическое отображение графа управления, трассировка переходов программы делает такой анализ сложным как в ручном, так и в автоматическом режиме.

СПИСОК ЛИТЕРАТУРЫ

1. Бабенко Л.К., Ищуков С.С., Макаревич О.Б. Защита информации с использованием смарт-карт и электронных брелков. – М.: Гелиос, 2003. – 352 с.
2. Дерявин П.Н. Теоретические основы компьютерной безопасности: учеб. пособие для ВУЗов и др. – М.: Радио и связь, 2000. – 192 с.
3. Красовский В.И., Храмов А.В. Аппаратно-программные средства телекоммуникационных сетей фирмы OST: учеб. пособие. – М.: МИФИ, 1996. – 68 с.
4. Наумович Г., Мемон Н. Предотвращение пиратства, обратной инженерии и незаконного использования компьютеров. – Computer IEEE Computer Society, v. 36, no. 6, 7, June 2003. – P. 64-71.
5. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса; под ред. действительного члена РАЕН, д.т.н., проф. В.А. Минаева. – М.: Гелиос АРВ, 2002. – 432 с.
6. Стенг Д., Мун С. Секреты безопасности сетей. – К.: «Диалектика», 1996. – 543 с.
7. Blum M., Luby M., Rubinfeld R. Self-testing correcting with applications to numerical problems II Proc 22th ACM Symposium on Theory of Computing. - 1990. - P. 73 - 83.
8. Chernov A. New Program Obfuscation Method. II In Proceedings of the Adrei Ershov Fifth International Conference «Perspectives of Systems Informatics». International Workshop on Program Understanding, Novosibirsk, July 14-16, 2003. Springer LNCS № 2890.
9. Collberg C., Thomborson C., Low D. Taxonomy of Obfuscating Transformations II Department of Computer Science. The University of Auckland.
10. Lynn B., Prabhakaran M., Sahai A. Positive results and techniques for obfuscation. IIEUROCRYPT, 2004. – P. 20-39.
11. Zakharov V.A., Varnovsky N.P. On the possibility of provably secure obfuscating programs. II Proc. 5th Conf. Perspectives of System Informatics, 2003. – P.71-78.

Лысых Владимир Витальевич
Белгородский государственный университет, г. Белгород
Аспирант кафедры математического и программного обеспечения информационных систем
E-mail: lysykh_vl@mail.ru

V.V. LYSYKH

CODE OBFUSCATION IN THE CONTEXT OF SOFTWARE PROTECTION

The paper covers the modern software protection methods classification. The concept of the obfuscation process is given. Code analysis and code obfuscation methods are compared. The features of an obfuscated software product are suggested. An obfuscation method is proposed that meets the features offered.

Keywords: *program obfuscation; software protection.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Babenko L.K., Ivashhukov S.S., Makarevich O.B. Zashhita informacii s ispol'zovaniem smart-kart i e'lektronny'x brelkov. – M.: Gelios, 2003. – 352 s.
2. Deryavin P.N. Teoreticheskie osnovy' komp'uternoj bezopasnosti: ucheb. posobie dlya VUZov i dr. – M.: Radio i svyaz', 2000. – 192 s.
3. Krasovskij V.I., Xramov A.V. Apparatno-programmny'e sredstva telekommunikacionny'x setej firmy' OST: ucheb. posobie. – M.: MIFI, 1996. – 68 s.
4. Naumovich G., Memon N. Predotvrashhenie piratstva, obratnoj inzhenerii i nezakonnogo ispol'zovaniya komp'uterov. – Computer IEEE Computer Society, v. 36, no. 6, 7, June 2003. – P. 64-71.
5. Pyarin V.A., Kuz'min A.S., Smirnov S.N. Bezopasnost' e'lektronnogo biznesa; pod red. dejstvitel'nogo chlena RAEN, d.t.n., prof. V.A. Minaeva. – M.: Gelios ARV, 2002. – 432 s.
6. Steng D., Mun S. Sekrety' bezopasnosti setej. – K.: «Dialektika», 1996. – 543 s.
7. Blum M., Luby M., Rubinfeld R. Self-testing correcting with applications to numerical problems II Proc 22th ACM Symposium on Theory of Computing. – 1990. – P. 73-83.
8. Chernov A. New Program Obfuscation Method. II In Proceedings of the Adrei Ershov Fifth International Conference «Perspectives of Systems Informatics». International Workshop on Program Understanding, Novosibirsk, July 14-16, 2003. Springer LNCS № 2890.
9. Collberg C., Thomborson C., Low D. Taxonomy of Obfuscating Transformations II Department of Computer Science. The University of Auckland.
10. Lynn B., Prabhakaran M., Sahai A. Positive results and techniques for obfuscation. IIEUROCRYPT, 2004. – P. 20-39.
11. Zakharov V.A., Varnovsky N.P. On the possibility of provably secure obfuscating programs. II Proc. 5th Conf. Perspectives of System Informatics, 2003. – P. 71-78.

УДК 004.056

Д.А. СВЕЧНИКОВ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ, ИСПОЛЬЗУЕМЫХ В СЕТЯХ ОБЩЕГО ПОЛЬЗОВАНИЯ

Безопасность удостоверяющих центров, используемых в сетях общего пользования, может быть достигнута только путем решения взаимосвязанной совокупности задач защиты. Основными из них являются: обеспечение конфиденциальности, целостности, доступности информации и подотчетности всех пользователей системы. Для решения этих задач в рамках системы удостоверяющих центров должна быть создана комплексная система обеспечения безопасности, которая объединит административное управление, криптографические средства защиты, алгоритмическое, математическое, программное, информационное и иное обеспечение, а также персонал, отвечающий за реализацию в системе требуемой политики безопасности. Ключевым аспектом решения проблемы безопасности удостоверяющих центров, используемых в сетях общего пользования, является выработка системы требований, критериев и показателей для определения необходимой степени их защищенности и оценки уровня безопасности.

Ключевые слова: *информационная безопасность; удостоверяющий центр; модель нарушителя; система требований по информационной безопасности; система защиты информации удостоверяющего центра.*

На современном этапе развития информационно-телекоммуникационных систем наблюдается активное внедрение систем электронного документооборота во многие сферы деятельности государства и жизни общества. Важной особенностью подобных распределенных информационно-телекоммуникационных систем является наличие в них процессов обработки, подлежащей защите конфиденциальной информации, и решение вопросов обеспечения юридической значимости электронных документов.

Одним из ключевых понятий, введенных в Федеральном законе «Об электронной цифровой подписи» от 10.01.2002 №1-ФЗ, является понятие удостоверяющего центра (УЦ) – базовой компоненты инфраструктуры открытых ключей, занимающейся выпуском и обеспечением актуальности сертификатов открытых ключей ЭЦП [1]. Удостоверяющий центр также является своего рода информационно-телекоммуникационной системой, обрабатывающей информацию ограниченного распространения (например, ключевая информация, регистрационные данные пользователей и т.д.). Обеспечение информационной безопасности УЦ является необходимым условием, при котором ЭЦП в электронном документе может быть признана юридически равнозначной собственноручной подписи в документе на бумажном носителе. Кроме этого, основополагающим фактором при организации юридически значимого электронного документооборота является доверие к технологии, реализующей инфраструктуру открытых ключей.

Очевидно, что средства ЭЦП функционируют в некотором окружении, которое может влиять на их информационную безопасность (ИБ) и правильность работы. Данные обстоятельства определяют необходимость реализации комплекса организационно-технических мер, обеспечивающих безопасность функционирования средств ЭЦП и комплексов технических средств, реализующих функциональное назначение УЦ.

Важным и перспективным направлением по обеспечению информационной

безопасности УЦ является разработка типовых компонент комплекса, обладающих заданными функциональными свойствами и свойствами по безопасности. Решения, обеспечивающие класс защиты УЦ на уровне, достаточном для использования в сетях общего пользования, востребованы в государственных информационных системах и ряде крупных коммерческих организаций, обеспечивающих функционирование региональных УЦ. В частности, в соответствии с требованиями ФЗ «при создании ключей ЭЦП для использования в информационной системе общего пользования должны применяться только сертифицированные средства ЭЦП».

В соответствии с Указом Президента РФ № 611 от 12 мая 2004 г. «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» обязательным условием подключения УЦ к сетям общего пользования является использование сертифицированных для таких сетей средств защиты информации, в том числе, и криптографических средств.

Вместе с тем, данные мониторинга безопасности ряда важных информационных ресурсов показывают высокую активность атак из глобальной сети Internet, разнообразность методов, реализующих попытки негативного воздействия, повышенный интерес хакерского сообщества к критически важным информационным ресурсам (например, сайт Президента РФ, сайты министерств РФ, ресурсы сети RSNet и т.д.).

Важным обстоятельством, которое необходимо учитывать при подключении УЦ к сетям общего пользования, является наличие потенциальных нарушителей – как внешних, так и внутренних, располагающих значительными возможностями по осуществлению различных деструктивных воздействий.

Для УЦ можно выделить следующие основные категории (типы) нарушителей безопасности: $H1$ – внешний по отношению к системе удостоверяющих центров (СУЦ) нарушитель; $H2$ – пользователи СУЦ; $H3$ – обслуживающий персонал СУЦ; $H4$ – группа администраторов СУЦ.

Нарушители всех категорий (типов) могут обладать следующей исходной информацией: данными об организации работы, структуре и используемом оборудовании УЦ, технической и эксплуатационной документацией; сведениями об открытой информации и формате сертификатов открытых ключей.

Нарушители могут располагать указанными средствами и документацией в объеме, зависящем от реализованных в УЦ режимных, организационно-технических и технических мер, направленных на предотвращение и пресечение несанкционированных действий. При этом нарушители типа $H1$, $H2$ могут получить указанную информацию только из открытых источников и в результате анализа перехвата данных, передаваемых по доступным каналам связи СУЦ. Нарушители типа $H3$ и $H4$ могут располагать данной информацией в полном объеме.

При обработке данных о функционировании УЦ нарушители всех типов могут:

– выделять каналы связи, относящиеся к СУЦ;

– выделять возможные служебные сигналы, передаваемые по каналам и линиям связи в незашифрованном виде;

– выделять и использовать все проявляющиеся в каналах связи нарушения правил эксплуатации и неисправности в работе УЦ.

Кроме этого, нарушители $H4$ могут в полном объёме:

– блокировать аппаратные и/или программные компоненты УЦ;

– модифицировать программные механизмы УЦ;

– внедрять в технические средства УЦ дополнительные программные

механизмы;

– применять методы, основанные на наблюдении в канале связи ответных реакций технических средств УЦ на активные воздействия.

Таким образом, нарушители типа *H*1, *H*2 и *H*3 потенциально имеют наименьшее количество возможностей реализации угроз ИБ УЦ. Однако данные нарушители могут реализовывать компьютерные атаки и вирусные заражения, основанные на использовании уязвимостей и недокументированных возможностей программного обеспечения (ПО) и, в частности, операционных систем (ОС). Результатом таких действий может являться НСД к ключевой и служебной информации, блокировка или модификация программных средств УЦ, внедрение в технические средства УЦ дополнительных программных механизмов, осуществляющих различные деструктивные воздействия или приводящих к утечке информации. Только при соответствующей реализации в УЦ технических мер, направленных на предотвращение и пресечение несанкционированных действий, данные нарушители могут быть практически полностью лишены возможности привести в действие какую-либо угрозу.

Наибольшие опасения вызывают нарушители типа *H*4 (группа администраторов), так как они фактически имеют полный доступ ко всей СУЦ. Частичное решение этой задачи возможно за счет разделения обязанностей администратора на две роли: администратора выдачи сертификатов и администратора безопасности. В обязанности первого входит контроль формирования сертификатов, при этом он не должен иметь доступ к журналу аудита событий и к общему наблюдению за системой. Второй отвечает только за контроль над системой и за её общую безопасность.

Ключевым аспектом решения проблемы обеспечения ИБ УЦ является выработка системы требований, критериев и показателей для оценки уровня их безопасности [2]. За выбор и обоснование требований отвечает ФСТЭК и ФСБ. Такие требования определяются на основе используемых классов защищенности автоматизированных систем и в соответствии с ГОСТ Р ИСО/МЭК 15408-2002, ГОСТ Р ИСО/МЭК 17799-2005, а также ГОСТ Р ИСО/МЭК 27001-2005.

В настоящее время требование по обязательной сертификации предъявляются к УЦ, предназначенным для использования на территории Российской Федерации, в части защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну. Кроме этого, все УЦ, предоставляющие услуги любым органам государственной власти, независимо от их ведомственной и территориальной принадлежности, должны быть аккредитованы в соответствии с порядком, установленным Правительством Российской Федерации.

При формировании требований по ИБ УЦ учитываются следующие основные аспекты:

– необходимая степень защищенности УЦ;

– категорирование обрабатываемой и хранимой информации с целью определения необходимого уровня защиты для каждой категории;

– модели нарушителя и модель угроз.

В системе требований по ИБ выделяют следующие группы:

– требования к средствам криптографической защиты информации (СКЗИ);

– требования по защите от НСД;

– требования по защите от утечки информации;

– требования по надежности и устойчивости функционирования;

– требования к информационным объектам УЦ.

Подсистема требований к СКЗИ включает и требования к ключевой информации. Требования к СКЗИ предполагают определение класса безопасности УЦ и использование СКЗИ соответствующего класса (КС-2 или КС-1) по «Требованиям к средствам криптографической защиты конфиденциальной информации». Для криптографической защиты должны использоваться только отечественные и сертифицированные ФСБ криптоалгоритмы, в частности, удовлетворяющие стандартам ГОСТ 28147-89, ГОСТ 34.11-94, ГОСТ 34.10-2001. Требования к ключевой информации определяют условия и варианты хранения секретных ключей, применяемых для формирования ЭЦП, и ключей шифрования. При этом особые требования предъявляются к защите секретных ключей центов регистрации и сертификации УЦ.

Подсистема требований по защите от НСД включает требования по регистрации, аутентификации, вариантам разграничения доступа (дискреционному, мандатному, ролевому), требования к аудиту. Согласно руководящим документам ФСТЭК, аттестация автоматизированных систем, предназначенных для обработки конфиденциальной информации, должна производится по классу «1Г» или «1Д» и предусматривать выполнение требований по разграничению и контролю доступа, учету носителей информации и обеспечению ее целостности.

Поскольку технологической платформой УЦ является локальный или территориально распределенный программно-аппаратный комплекс, то требования защиты от НСД распространяются и на программное, и на аппаратное обеспечение УЦ. Составными элементами типового УЦ являются:

– доверенные операционные системы, под управлением которых функционируют компоненты УЦ;

– доверенное прикладное программное обеспечение компонентов УЦ;

– доверенное аппаратное обеспечение компонентов УЦ.

Для доверенного ПО (ОС) обязательна проверка того, что:

– реализованные в ПО (ОС) алгоритмы соответствуют декларированным функциям;

– ПО (ОС) не содержит недекларированных функций;

– любая последовательность выполнения декларированных функций не приводит к нарушению информационной безопасности ПО (ОС).

Доверенность ПО (ОС) гарантирует отсутствие уязвимостей, используемых для внедрения дополнительных программных механизмов, осуществляющих различные деструктивные воздействия или приводящих к утечке ключевой и служебной информации.

Доверенность ПО (ОС) устанавливается путем проведения статического и динамического анализа исходных кодов исследуемого ПО (ОС).

В ходе статического анализа:

– восстанавливаются основные маршруты вызовов процедур и функций;

– проверяется соответствие выполняемых действий целевым функциям ПО (ОС);

– проводится поиск недокументированных возможностей ПО (ОС) и т.д.

В ходе динамического анализа исходных кодов ПО (ОС) производится идентификация фактических маршрутов выполнения вызовов процедур и функций с последующим сопоставлением маршрутам, построенным в ходе статистического анализа.

Разработка защищенных технических средств на базе доверенного ПО,

обладающего необходимыми средствами управления разграничением доступа и прошедшего соответствующие проверки оборудования, позволяет обеспечить требуемый для использования в сетях общего пользования режим защиты.

Доверенность аппаратных средств УЦ подразумевает отсутствие в них негативных функциональных возможностей, позволяющих модифицировать или искажать алгоритм работы технических средств УЦ. Анализ аппаратных средств должен проводиться специализированными организациями, имеющими лицензию на деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах.

Подсистема требований по защите от утечки информации регламентирует исключение утечки открытой, критической и/или опасной информации в канал связи, величины пороговых соотношений сигнал/помеха, нормированные значения помех для защиты от утечки информации по ПЭМИН.

Подсистема требований по надежности, устойчивости и своевременному восстановлению функционирования УЦ регламентируют параметры корректности работы, диагностического контроля, мониторинга правильности функционирования, требования к резервному копированию и архивированию. Основные требования этой подсистемы определяют допустимые значения вероятностей неисправностей и сбоев, не приводящие к отключению или опасной модификации реализованных в УЦ механизмов защиты от несанкционированного доступа к ключевой и другой конфиденциальной информации. Требования к резервному копированию и восстановлению определяют такие условия, при которых данные, сохраненные при резервном копировании, являются достаточными для восстановления УЦ (в том числе, и возможность резервного копирования секретного ключа и сертификата центра сертификации). Требования по архивированию включают варианты защиты архивных данных соответствующими алгоритмами и средствами.

В подсистеме требований к хранению, формированию, обновлению и выдаче информационных объектов определяются требования к структуре сертификата и списку отозванных сертификатов, требования к реестру сертификатов, обеспечению доступа к нему и вариантам поиска, требования к проверке ЭЦП в сертификате. Общий регламент распространяется на обеспечение защиты информации в сетевом справочнике и базах данных ЦС и ЦР посредством применения алгоритмов ЭЦП. Требования к изданию и отзыву сертификатов регламентируют абсолютные и относительные значения временных показателей в сертификатах и в списке отозванных сертификатов.

Исходя из перечисленных требований, предъявляемых к УЦ, обосновываются задачи по обеспечению ИБ и класс защищенности УЦ, а также выбор средств защиты информации.

Основными задачами по обеспечению ИБ УЦ являются:

– защита конфиденциальной информации (ключевой информации, служебной и личной информации, охраняемой в соответствии с действующим законодательством, секретных ключей УЦ, парольной информации и информации аудита и т.п.) при ее хранении, обработке и передаче;

– контроль целостности конфиденциальной и открытой информации (информации о владельцах, входящей в состав сертификатов, информации об отозванных сертификатах и т.п.);

– контроль целостности программных и аппаратных компонент комплекса УЦ;

– обеспечение безотказной работы компонент комплекса УЦ.

В соответствии с современными требованиями, УЦ должен быть высокозащищенным комплексом, сертифицированным по соответствующим требованиям ИБ, и эксплуатироваться как доверенная, замкнутая, не модифицируемая автоматизированная система. Под замкнутостью понимается невозможность воздействия на состав и компоненты системы иным способом, кроме как определенным регламентом образом. Под не модифицируемостью понимается отсутствие в системе средств разработки, прямо или косвенно влияющих на функциональную однозначность выполняемых процедур.

Вопросы обеспечения безопасного функционирования УЦ во всех режимах должны быть определены в Регламенте УЦ и политике безопасности УЦ [3]. В них отражаются обязанности субъектов системы УЦ, протоколы работы, принятые форматы объектов системы, основные организационно-технические мероприятия, необходимые для безопасной работы системы, в том числе:

– определение необходимой степени защищенности;

– категорирование обрабатываемой и хранимой информации с целью определения необходимого уровня защиты для каждой категории;

– разработка моделей нарушителя и угроз;

– перечень технических средств, используемых для защиты компонентов УЦ;

– аттестация УЦ для подтверждения его соответствия требуемой степени защищенности;

– разработка инструкций по соблюдению правил обеспечения защиты информации как для персонала, так и для пользователей;

– ознакомление пользователей УЦ с Регламентом, получение от них обязательства на выполнение требований Регламента;

– ознакомлением пользователей УЦ с информацией о политике применения выдаваемых сертификатов ключей подписей.

Учитывая требования по обеспечению ИБ, в состав системы защиты информации УЦ должны входить следующие подсистемы:

– защиты информации от НСД, включающую программные и/или программно-аппаратные средства аутентификации и разграничения доступа администраторов и пользователей УЦ;

– межсетевого экранирования. При этом межсетевые экраны (МЭ) должны быть сертифицированы не менее чем по 4 классу защиты в соответствии с требованиями к межсетевым экранам ФСТЭК России;

– криптографической защиты и обеспечения целостности информации, включающую программные и/или программно-аппаратные СКЗИ сертифицированные ФСБ России для использования в сетях общего пользования;

– защиты криптографических ключей (секретного ключа администратора и пользователей) УЦ;

– антивирусной защиты компонентов УЦ;

– обнаружения, предупреждения и защиты от компьютерных вторжений;

– активного аудита информационной безопасности УЦ;

– резервного копирования и архивирования данных;

– контроля целостности компонентов УЦ;

– обеспечения безотказной работы комплекса;

– защиты оборудования комплекса от утечки информации по техническим и побочным каналам;

– обеспечения защиты информации от НСД режимными и организационно-

техническими мерами.

Реализация перечисленного выше комплекса мер защиты позволит обеспечить защиту технических средств УЦ от воздействий внешних и внутренних нарушителей. Достаточность принятых мер для конкретной реализации УЦ и его степень защищенности должна подтверждаться результатами тематических исследований и экспертным заключением организации выполняющей сертификацию.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «Об электронной цифровой подписи» от 10.01.2002 № 1-ФЗ.
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие. – М.: ИД «Форум»: ИНФРА-М, 2010. – 592 с.
3. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. – М.: Горячая линия-Телеком, 2004. – 248 с.

Свечников Дмитрий Александрович
Академия ФСО России, г. Орел
Кандидат технических наук, доцент
Тел.: (4862)54-99-33
E-mail: mhm57@yandex.ru

D.A. SVECHNIKOV

PROVIDING INFORMATION SECURITY OF CERTIFICATION AUTHORITY USED IN PUBLIC DATA NETWORKS

Safety of certification authority (CA) used in Public Data Networks can be achieved only by solving the interrelated protection problems. The basic task is to provide privacy, integrity of information and auditing of all system users. To solve these problems a complex system of providing security is to be created. This system is to include administrative management, cryptographic protection, and software. To control the system highly qualified personnel is required. The key solution of CA security problem is to develop requirements, criteria and characteristics to determine the necessary degree of protection and to access security level.

Keywords: *information security; certification authority; model of the infringer; requirements of information security; complex system of providing security certification authority.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Federal'ny'j zakon «Ob e'lektronnoj cifrovoj podpisi» ot 10.01.2002 № 1-FZ.
2. Shan'gin V.F. Kompleksnaya zashhita informacii v korporativny'x sistemax: ucheb. posobie. – M.: ID «Forum»: INFRA-M, 2010. – 592 s.
3. Gorbatov V.S., Polyanskaya O.Yu. Osnovy' texnologii PKI. – M.: Goryachaya liniya-Telekom, 2004. – 248 s.

УДК 681.324

О.В. ТРЕТЬЯКОВ, А.В. КРИКУНОВ

ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ПРОБЛЕМЫ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

В статье рассмотрены философские и исторические аспекты развития информационных технологий. Авторы исследуют угрозы безопасности, возникающие в результате информационно-телекоммуникационной революции, рассматривают методологические проблемы современного информационного противоборства.

Ключевые слова: *информационные технологии; информационное общество; информационное противоборство; информационный терроризм.*

ПОСТАНОВКА ЗАДАЧИ ИССЛЕДОВАНИЯ

Произошедшие в результате глобальной информатизации огромные технологические и социально-экономические изменения стали общепризнанными. Как отмечается в Стратегии развития информационного общества в Российской Федерации, современное общество «характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти» [1].

Парадоксальность ситуации заключается в том, что, с одной стороны, парадигма постиндустриального (информационного) развития общества уже стала реальностью социально-политической практики в большинстве развитых стран Америки и Европы (включая Россию), с другой – анализ событий начала XXI века позволяет сделать вывод о том, что большинство оптимистичных прогнозов теоретиков информационного общества не реализованы. Все более значимым фактором становится информационное противоборство (не только в публицистике, но и в научных изданиях всё чаще употребляется не совсем строгие термины «информационная война» и «информационная борьба»).

Выявление сущности, содержания и особенностей современного информационного противоборства предполагает комплексное решение ряда теоретико-методологических проблем:

– рассмотрение феномена современного информационного противоборства в контексте развития науки и техники;

– выявление масштаба и уровней ведения информационного противоборства;

– выяснение соотношения информационно-технической и информационно-психологической составляющих в ходе информационного противоборства;

– раскрытие причин резкого повышения эффективности средств информационного воздействия на рубеже XX–XXI веков.

ГЕНЕРАТИВНАЯ СИТУАЦИЯ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Феномен современного информационного противоборства является результатом определенных процессов в социально-политической практике, интеллектуальной деятельности, технико-технологической сфере. Представляется возможным выделить несколько «линий», определяющих содержание генеративной ситуации современного информационного противоборства.

Первую линию образует комплекс определенных философских идей и установок, складывавшихся и получивших распространение на протяжении столетий. Конкретный анализ методологических основ обеспечения информационной безопасности в различных исторических условиях дан в трудах многих выдающихся

мыслителей прошлого (Платона, Аристотеля, Аврелия Августина, Ф. Аквинского, Н. Макиавелли, Ф. Бэкона, Т. Гоббса, Дж. Локка, Ш. де Монтескье и др.). Синкретичный характер философских учений делает возможным выявление идей, касающихся рассматриваемого вопроса. Представляет интерес положение о том, что условия, при которых возникают информационные угрозы, четко не определены, а причины, порождающие их, многочисленны. Часть из них находится в сфере неурегулированных внутригосударственных и социально-политических отношений, выражаемых морально-правовой категорией «справедливость». Уже Аристотель указывал на то, что справедливость есть представление о должном, связанное с исторически меняющимися взглядами на неотъемлемые права человека [2]. Информационные угрозы безопасности коренятся и в социально-экономических условиях жизни общества и государства. Один из первых теоретиков гражданского общества Г.В.Ф. Гегель характеризовал его как общество, в котором «каждый для себя – цель, все остальное для него ничто» [3]. Именно информационное содержание рефлексии самосознания гражданского общества формирует определенное умонастроение, что четко выражено в известном марксистском тезисе об овладевших умами масс идеях как материальной силе.

Выделение обеспечения информационной безопасности в самостоятельный, относительно независимый от других вид общественно-политической и духовно-практической деятельности происходит лишь во второй половине XX века, когда «…возникает целый ряд социально-философских и методологических проблем, связанных с новой социальной ролью знаний… Выявляется, что использование знаний может иметь не только положительные, но и отрицательные последствия, что увеличивает степень возникающего при их применении риска» [4].

Вторая линия представляет собой развивавшиеся с XIX века исследования в области физиологии высшей нервной деятельности, психологии мышления и познания. Было доказано, что информация может оказывать психологическое воздействие на сознание людей, их мышление, волю и эмоции. В.М. Бехтерев описал явление массового внушения под влиянием «психического заражения», вторжение в сознание посторонней идеи без прямого и непосредственного участия в этом акте «Я» субъекта [5]. К настоящему времени разработана система теорий и прикладных практик скрытого информационного принуждения личности. К их числу, в первую очередь, можно отнести манипулятивное воздействие, рефлексивное управление, нейро-лингвистическое программирование.

Тесно связана с вышеописанными третья линия – теоретические и прикладные разработки в области политтехнологий и PR (от англ. Public Relations – связи с общественностью). По сути, это информационные технологии – технологии управления информацией для достижения политических или иных целей. Ключевая стратегия в рамках политтехнологий и PR – убеждение, поставленное на научную основу. В настоящее время разработаны модели и методы действий в открытом информационном пространстве, распространяется «сетевая» идеология.

Четвертая линия – становление и развитие теории информации, основу которой составили результаты Р. Хартли, К. Шеннона, а также несколько более поздние работы А.Н. Колмогорова, А.А. Харкевича, Р.Л. Стратоновича. Отметим интересную особенность сложившегося в рамках теории информации апостериорного подхода. Он позволяет, наряду с полезной информацией, рассматривать (и количественно оценивать) «дезинформацию», поступающую в систему. Поступление «дезинформации» проявляется в таких действиях, которые ухудшают положение системы.

Примером может быть модель, которую можно считать крайним упрощением ситуации, в которой движущийся объект имеет ограниченный временной ресурс.

Пусть объект за один шаг может переместиться из точки k в точку k+1 или и k-1 (k – целое); исходное положение – точка k = 0; цель есть точка m > 0; эта точка должна быть достигнута не более, чем за n ($n \geq m$) шагов. При отсутствии информации переходы из k в k+1 и k-1 равновероятны.

Целесообразность управления (и ценность информации, на основе которой оно выбрано) легко подсчитывается. Заметим, что значение целесообразности здесь зависит не только от текущей координаты, но и от номера шага (т.е. от количества оставшегося временного ресурса; в более сложных случаях – от всей истории движения объекта). Если, например, n = 3, а m = 1, то целесообразность перемещения из точки 0 в точку -1 на первом шаге равна

$$\log_2 \frac{1/4}{(1/2)+(1/2)^2} \approx -1{,}32 \; бит ,$$

что соответствует, как и следовало ожидать, случаю дезинформации.

Теория информации обеспечила значительное расширение поля исследуемых объектов, открывая пути к освоению сложных саморегулирующихся систем.

Пятая линия генеративной ситуации современного информационного противоборства связана с процессами в технико-технологической сфере.

Реальностью и общемировым явлением современности стала ускоренная информатизация всех сторон общественного бытия. Она включает в себя три взаимосвязанных процесса: медиатизацию, компьютеризацию, интеллектуализацию. Ускоренная информатизация стала одним из результатов информационно-телекоммуникационной революции последней трети XX века.

Другое следствие информационно-телекоммуникационной революции – начало процесса создания и развития нового типа информационных сетей, которым свойственны следующие черты:

– информационные сети становятся все более взаимосвязанными. Благодаря разработке общих стандартов возможно свободное «перетекание» сообщений из одной сети в другую;

– телекоммуникационные сети имеют глобальный характер;

– сети становятся все более «персональными» (могут удовлетворять информационные потребности отдельных разнообразных групп пользователей);

– сети становятся интеллектуальными. Они «понимают» информационные потребности индивидуальных пользователей, могут автоматически искать необходимую информацию, обеспечивать доступ к различным информационным ресурсам;

– информационные услуги стали качественно новыми (интегрированными, мультимедиа, мобильными).

Таким образом, происходит становление электронной коммуникационной среды, в принципе позволяющей человеку получить (почти) любую информацию в (почти) любое время и в (почти) любом месте.

Именно это является объективным фактором упрочения в общественном сознании парадигмы постиндустриального (информационного) развития общества.

В субъективном плане она зиждется в первую очередь на новом подходе к оценке места и роли интеллектуально-духовной сферы человека: информатизация трактуется как развитие информационно-коммуникативных процессов в обществе на базе новейшей компьютерной и телекоммуникационной техники и как качественное совершенствование (с помощью современных информационно-технологических

средств) когнитивных социальных структур и процессов.

Информатизация порождает феномены совершенно новой природы, технически осязаемые, поддающиеся формализации и модельному представлению, но ранее на планете не встречавшиеся и не имеющие в прошлом даже теоретических аналогов. Привлечение к их анализу аппарата общей теории систем, синергетики, теории больших систем и т.п. достаточно продуктивно, но потенциально может сузить восприятие необычности этих явлений, отодвигая на время момент окончательного краха «доинформационного» мировоззрения.

ВЫСОКОТЕХНОЛОГИЗИРОВАННОЕ СОЦИОИНФОРМАЦИОННОЕ ПРОСТРАНСТВО В СУБЪЕКТ-ОБЪЕКТНЫХ ОТНОШЕНИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Противоборство в информационной сфере присуще человечеству с момента его возникновения. Информационная сфера трактуется нами как фрагмент реальности, в котором объективизируется идеальное индивидуальное, аккумулируется и транслируется идеальное внеиндивидуальное.

На рубеже XX–XXI веков технические средства информационного обмена функционируют в рамках глобальной многоуровневой социотехнической системы.

Последнее является основой для формирования высокотехнологизированного социоинформационного пространства, под которым понимается многомерная сеть, построенная из сложнопереплетенных прямых и обратных связей субъектов информационных взаимодействий (единиц и областей). Социоинформационное пространство в принципе разрешает существование любого типа информации, в чем реализуются его отличия от пространства физического плана.

В организационно-техническом аспекте социоинформационное пространство составляет совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем, сетей, приложений и организационных структур, функционирующих на основе определенных принципов и по установленным правилам, обеспечивающим информационное взаимодействие пользователей, а также удовлетворение их информационных потребностей.

В состав технологических и организационных компонентов социоинформационного пространства в обобщенном варианте входят:

– информационно-телекоммуникационная инфраструктура – территориально распределенные в стране (странах, мире) компьютеры, связанные между собой в сети средствами связи и телекоммуникации;

– информационные ресурсы на машинных носителях, прежде всего специализированные информационные массивы в виде автоматизированных баз данных, а также информационные ресурсы, распределенные по Web-сайтам в сети Internet;

– методы и средства прикладной математики – алгоритмы и программные средства (комплексы), обеспечивающие функционирование аппаратных платформ (систем);

– организационные меры, обеспечивающие функционирование компонентов информационного пространства;

– правовые меры (нормы);

– рынок информационных технологий, средств связи, информатизации и телекоммуникаций, информационных продуктов и услуг.

Социоинформационное пространство включает в себя:

1. Антропосоциальные «единицы» информационного пространства:

а) генерирующие информацию (групповые коммуникаторы, ньюсмейкеры (от англ. newsmaker – букв. «творец новостей»);

б) лидеры общественного мнения;

в) эксперты (интерпретаторы);

г) лидеры мнений (под ними понимаются достаточно активные люди, в отличие от вышеперечисленных категорий не завязанные на определенные каналы распространения информации, имеющие совокупную потребность в распространении информации в малых и средних социальных группах);

д) производители специальной информации (театр, кино, реклама во всех ее проявлениях вне СМИ, мода, товары, архитектура и т.п.).

2. Каналы коммуникаций.

3. Области, которые в социальных системах формируются по определенным социально-психологическим принципам, включаются в определенную сеть (информационные каналы). Области, включенные в определенные каналы в данный момент времени, могут пересекаться; различают также области, не включенные в информационные каналы, но находящиеся под влиянием контекста, общего ритма информационных процессов и синхронизирующиеся через вторичные воздействия.

Переход от социоинформационного пространства к реальному пространству (или наоборот) опирается на ряд закономерностей функционирования объектов. Происходят определенные трансформации объекта при его смещении из одного типа пространства в другое.

Современное социоинформационное пространство (в том числе, российское) характеризуется слабой управляемостью, наличием большого числа субъектов, многообразием процессов информационных воздействий, а также противоречием между уровнем развития информационных технологий и возможностью доступа к ним.

Корпорацией РЭНД был проведен ряд международных научных конференций и семинаров, в ходе которых изучалось и оценивалось мнение ведущих экспертов по проблемам трансформации общества в условиях информационно-телекоммуникационной революции. Результаты работы были обобщены экспертами РЭНД в ряде отчетов [6]. Представляются достаточно интересными некоторые наблюдения и выводы, относящиеся к рассматриваемой нами проблематике:

– глобальная информатизация всех сфер жизни общества не повышает, а понижает степень его безопасности;

– ускорение научно-технического прогресса увеличивает вероятность применения террористами в качестве средств поражения сугубо мирных технологий, причем возможность «двойного» их использования зачастую не только не предусматривается, но и не осознается создателями технологии;

– «цифровое неравенство» и появление «проигравших» информационную гонку стран (Laggard Countries) могут послужить причиной для поиска новых методов и средств информационного противоборства, нового витка террористической активности;

– терроризм все более активно использует достижения глобальной информатизации и информационно-телекоммуникационной революции, поскольку, во-первых, террористы все шире применяют возможности современных информационно-телекоммуникационных систем для связи и сбора информации, пропаганды своих идей, пополнения ресурсов, поиска источников финансирования и т.д., во-вторых, реалией наших дней становится так называемый «кибертерроризм», в-третьих, большинство террористических актов сейчас рассчитаны не только на

нанесение материального ущерба и угрозу жизни и здоровью людей, но и на информационно-психологический шок, воздействие которого на большие массы людей создает благоприятную обстановку для достижения террористами своих целей.

Информационные воздействия представляют собой новую форму глобального противостояния, проходящего на разных уровнях, охватывающего все элементы информационного пространства. Эти воздействия носят целенаправленный характер и основываются на использовании информационного превосходства в виде контролируемого влияния на информацию, информационные процессы и информационно-телекоммуникационную инфраструктуру.

Устойчивое функционирование общества невозможно без целенаправленного процесса информатизации, а также без обеспечения безопасности информационного пространства от деструктивных информационных воздействий.

Цель деструктивного информационного воздействия – посредством формирования мнений, представлений, знаний, аттитюдов, ценностных ориентаций наполнить индивидуальное и массовое сознание определенным содержанием, которое будет служить базисом прогнозируемого поведения.

Феномен скрытого деструктивного информационного воздействия принадлежит к числу глобальных проблем, свойственных всем социально значимым сторонам общественной жизни.

В информационном обществе скрытое воздействие преобладает над силовыми методами. Возрастание эффективности скрытого деструктивного информационного воздействия связано с революционным научно-техническим прогрессом, повлекшим за собой стремительное развитие средств массовой коммуникации.

Ведущий методологический подход при решении задач обеспечения информационно-психологической безопасности и защиты от информации – рассмотрение человека, общества и государства как саморазвивающиеся и обменивающиеся с внешним миром информацией самообучающиеся системы.

Вместе с тем, в настоящее время возникает необходимость решения ряда новых аспектов рассматриваемой проблемы. Информатизация общества создает ситуацию дефицита времени на осознание факта информационного нападения, повышается вероятность принятия ошибочных решений под воздействием деструктивной информации. Появляется необходимость в синтезе информационно-психологической и информационно-технической безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия развития информационного общества в Российской Федерации // Российская газета, 2008, 16 февраля.
2. Аристотель. Сочинения: в 4 т. Т. 4. Политика. – М.: Мысль, 1984. – С. 375-644.
3. Гегель Г.В.Ф. Философия права. – М.: Мысль, 1990. – С. 228-230.
4. Горохов В.Г. Научно-техническая политика в обществе незнания // Вопросы философии, 2007. – № 12. – С. 65.
5. Бехтерев В.М. Внушение и его роль в общественной жизни. – СПб: Ленинградское издательство, 2009. – 286 с.
6. Gatune J. Navigating the Information Revolution. Choices for Laggard Countries. – Santa Monica: RAND Corporation, 2006. – 172 p.; Don B. W., Frelinger D. R. & oth. Network Technologies for Networked Terrorists. – Santa Monica: RAND Corporation, 2007. – 80 p.; Libicki M. & oth. Regaining information superiority against 21st-century insurgents. – Santa Monica: RAND Corporation, 2007. – 159 p.; Terrorist Groups and the Exchange of New Technologies. – Santa Monica: RAND Corporation, 2007. – 114 p.; Al-Qaida: Terrorist

Selection and Recruitment. – Santa Monica: RAND Corporation, 2007. – 89 p.

Третьяков Олег Владимирович
Академия ФСО России, г. Орел
Кандидат исторических наук, доцент, доцент кафедры гуманитарных и социально-экономических дисциплин
Тел.: (4862)54-99-41
E-mail: oleg020862@mail.ru

Крикунов Александр Владимирович
Институт Востоковедения РАН, г. Москва
Аспирант
Тел.: (495)623-15-91
E-mail: cpc72@list.ru

O.V. TRETYAKOV, A.V. KRIKUNOV

THEORETICAL AND METHODOLOGICAL PROBLEMS OF THE MODERN INFORMATION CONFRONTATION

Philosophical and historical impacts of information technologies are described in the article. The author exams previews and premises a modern information society, studies ontological and methodological backgrounds this phenomenon. The author emphasizes the necessity to minimize the considered negative influences of information technologies.

Keywords: *information technologies; information society; information warfare; information terrorism.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Strategiya razvitiya informacionnogo obshhestva v Rossijskoj Federacii //Rossijskaya gazeta, 2008, 16 fevralya.
2. Aristotel'. Sochineniya: v 4 t. T. 4. Politika. – M.: My'sl', 1984. – S. 375-644.
3. Gegel' G.V.F. Filosofiya prava. – M.: My'sl', 1990. – S. 228-230.
4. Goroxov V.G. Nauchno-texnicheskaya politika v obshhestve neznaniya // Voprosy' filosofii, 2007. – № 12. – S. 65.
5. Bexterev V.M. Vnushenie i ego rol' v obshhestvennoy zhizni. – SPb: Leningradskoe izdatel'stvo, 2009. – 286 s.
6. Gatune J. Navigating the Information Revolution. Choices for Laggard Countries. Santa Monica: RAND Corporation, 2006. – 172 p.; Don B. W., Frelinger D. R. & oth. Network Technologies for Networked Terrorists. Santa Monica: RAND Corporation, 2007. – 80 p.; Libicki M. & oth. Regaining information superiority against 21st-century insurgents. Santa Monica: RAND Corporation, 2007. – 159 p.; Terrorist Groups and the Exchange of New Technologies. Santa Monica: RAND Corporation, 2007. – 114 p.; Al-Qaida: Terrorist Selection and Recruitment. Santa Monica: RAND Corporation, 2007. – 89 p.

УДК 34.342

А.П. ФИСУН, Ю.А. БЕЛЕВСКАЯ

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ПУТЕМ РАЗВИТИЯ ТЕОРИИ ИНФОРМАЦИОННОГО ПРАВА

Изложены результаты анализа особенностей информационно-телекоммуникационных технологий (ИКТ), обусловивших необходимость дальнейшего совершенствования эффективного инструментария их развития. Одним из путей такого совершенствования является развитие теории информационного права как важнейшего инструментария, обеспечивающего процессы создания, применения, поддержания в актуальном состоянии, модернизации и совершенствования ИКТ и информационной сферы, а также определяющего компонента правового регулирования конституционных прав и свобод человека и гражданина в информационной сфере и сфере обеспечения их информационной безопасности. Уточнен ряд принципов формирования структуры теоретических основ информационного права и ее компонентов.

Ключевые слова: *информационно-коммуникационные технологии; информация; информационная сфера; информационная безопасность; теория информационного права.*

Анализ состояния, особенностей и проблем информационно-телекоммуникационных технологий (ИКТ) позволил выделить ряд значащих факторов, которые обуславливают и актуализируют необходимость дальнейшего развития одного из важных инструментариев совершенствования ИКТ – теории информационного права. К таким факторам относятся:

– устойчивая тенденция внедрения практически во все сферы и виды деятельности личности, общества и государства современных ИКТ, в том числе, глобальных, национальных, региональных и локальных информационных систем;

– динамичное развитие рынка ИКТ и производимых ими информационных продуктов и услуг, лежащих в основе развития материально-энергетического мирового и национального производств, социально-политического, экономического, научного развития мирового сообщества;

– формирование и динамичное развитие международного информационного пространства, сближающего и объединяющего национальные информационные сферы;

– повышение требований обеспечения информационной безопасности личности, общества и государства и используемых ими ИКТ в условиях лавинообразного возрастания объемов информационных потоков не только полезной, но и разрушающей информации;

– качественное и количественное изменения объемов и содержания задач управления органов публичной власти (ОПВ), вызванные переходом к информационному обществу и обусловившие необходимость повышения эффективности деятельности ОПВ и соответствующего совершенствования их информационного обеспечения;

– усложнение внутринациональных и межнациональных социальных, экономических, политических, научно-технических и иных процессов, видов и сфер

деятельности личности, общества и государств, в основе которых лежат производство и потребление интеллекта, знаний, и информационные процессы, обуславливающие возникновение новых информационных общественных отношений;

– широкое использование во всех сферах и видах деятельности личности, общества и государства современных ИКТ, обуславливающих формирование новых, устойчивых закономерностей развития информационного общества;

– повышение роли информации как объекта правоотношений во всех сферах и видах материально-энергетической деятельности личности, общества, государства, а также сложность и неопределенность объективной оценки ее свойств;

– возрастание угроз информации ИКТ, обусловленных лавинообразным развитием и широким использованием самих ИКТ во всех сферах и видах деятельности современного общества, в развивающихся национальных и международных информационных пространствах;

– необходимость предоставления и обеспечения достоверной, полной, своевременной и безопасной информации как основы эффективной деятельности личности, общества, государства, используемых ими ИКТ и обеспечения их информационной безопасности;

– недостаточное развитие современного научно-методологического инструментария для решения проблем повышения качества информационного обеспечения материально-энергетических сфер и видов деятельности развивающегося информационного общества;

– закономерности формирования, развитие фундаментальной, прикладной информационной и юридической наук, их интеграция в части исследования и использования общих и единых объектов общественных отношений – информации и ИКТ.

С учетом вышеназванных факторов решение проблемы развития и формирования теории информационного права (ТИП), фактически теоретических основ информационного права как эффективного и важнейшего инструментария, обеспечивающего процессы создания, применения, поддержания в актуальном состоянии, модернизации и совершенствования ИКТ, а также определяющего компонента правового регулирования конституционных прав и свобод человека и гражданина в информационной сфере и сфере обеспечения их информационной безопасности, состоит в решении следующих первоочередных задач:

– уточнение и формирование понятия, структуры ТИП как основы эффективного регулирования и развития ИКТ, широко используемых во всех сферах и видах деятельности современного общества;

– уточнение и формирование обобщенного содержания понятийного базиса ТИП и последующее определение содержания центрального понятия искомой теории;

– обоснование подхода формирования содержания объекта, предмета и концепции ТОИП.

Решение этих первоочередных задач, основанное на учете развития современных ИКТ и их безусловного практического интегрирования во все сферы и виды деятельности современного общества, позволит выявить особенности, уточнить и осмыслить роль и место ТИП как в системе юридических наук, так и в системе информационных наук, в том числе, теоретической, прикладной информатике,

информационно-коммуникационных технологиях, являющихся сегодня важнейшим инструментарием, основой информационного обеспечения и эффективного регулирования и развития практически всех материально-энергетических сфер и видов деятельности личности, общества, государства и информационной сферы.

Прежде, чем решать задачу формирования конкретного содержания самого понятия и направлений развития ТИП, необходимо определить особенности формирования его структуры. В настоящее время в силу значительного разнообразия существующих и формирующихся информационных общественных отношений, взглядов и подходов на формирование информационного права и его теории как отраслевой, частной теории юридической науки, неоднозначности толкования ряда норм действующего нормативного правового базиса искомой сферы, возникают сложности в однозначном определении относительно полной структуры ТИП. Однако с учетом состояния современной теории права, теоретической информатики и других информационных теорий [11-14] авторами предлагается рассматривать содержание ТИП, которая в общем виде может быть представлена известными в теории права составными компонентами отрасли и законодательства информационного права, которые в настоящее время находятся на стадии развития. При этом, такая развивающаяся структура отрасли информационного права, как, впрочем, и любая самостоятельная научная теория, должна формироваться на основании известных основных принципов и требований [1-7, 9, 11-14], в том числе:

– перехода к широкому пониманию содержания информации;

– широкого использования методов системологии;

– первоочередного решения задачи выбора базовой концепции информации и информатизации с учетом развития прикладных задач развития ИКТ;

– учета полной реализации нормативной правовой базы, обеспечивающей поддержку существующих видов деятельности, органов публичной власти органов управления в информационной сфере, а также создание, применение и развитие ИКТ;

– комплексного и дифференцированного учета гуманитарных и социально-экономических, мировоззренческих, морально-психологических и этических аспектов разработки, использования и совершенствования ИКТ, развития информационной сферы, обеспечения их информационной безопасности;

– ориентации не только на формальные, но и на неформальные математические методы и естественные науки;

– обязательного и первоочередного уточнения, формирования однозначного содержания объекта и предмета искомой науки;

– возможности использования известных или разработки новых методов и методик формирования, уточнения и получения новых знаний о свойствах объекта общественных информационных отношений;

– формирования, уточнения или развития концепции искомой отрасли, дающей относительно полное представление о природе изучаемого объекта;

– наличия методов оценки эффективности процесса получения новых знаний в искомой сфере и другие.

Анализ научных результатов известных исследований информационной сферы, ИКТ, в том числе, представленных в [11-14], позволил выявить то, что особенности формирования содержания структуры ТИП обуславливаются содержанием, характеристиками и особенностями тех элементов, признаков и особенностей, которые характерны для ИКТ и всей информационной сферы. На основании этих выводов авторы предлагают новый подход к формированию структуры ТИП,

который, прежде всего, основан на необходимости выделения и определения первоочередной роли и значимости информации не только как объекта современных ИКТ, сложившегося и продолжающего формироваться в отечественном и зарубежном информационном законодательстве и отрасли информационного права как узкой, частной отрасли, но и как объекта общей теории права и государства, а также практически всех частноправовых и публично-правовых отраслей отечественного и международного права. С учетом этого подхода вполне логичен и тривиален последующий этап формирования структуры ТИП, сущность которого состоит в том, что прежде, чем формировать структуру искомой теории, необходимо определиться с выбором содержания понятия «теория» и связанными с ней производными, частными и составляющими понятиями.

Анализ содержания известных понятий «теория» позволил сделать вывод о том, что, несмотря на их значительное разнообразие [1-7, 9, 11] и кажущуюся сложность применения к исследуемой отрасли, эти понятия могут при некотором обосновании использоваться для формирования содержания искомого понятия и последующей структуры ТИП. Так, «теория» в переводе с греческого означает рассмотрение, исследование. Другое понятие «теория» рассматривается в двух аспектах: как система основных идей в отрасли знаний и как форма научного знания, дающая целостное представление о закономерностях и существенных связях действительности [7,8]. Используя содержание этих понятий теории, авторы применили их к формируемому содержанию понятия ТИП и предложили следующее определение.

Теория информационного права:

– система взглядов, идей, знаний, опыта об информационной сфере (среде), ИКТ, характеризующих логическую взаимозависимость элементов этой сферы, ИКТ, дающих целостное представление о содержании и закономерностях существующих и развивающихся частноправовых и публично-правовых общественных информационных отношениях и соответствующих отраслях права, регулирующих создание, использование, совершенствование ИКТ, развитие информационной сферы;

– знания о существенных связях с другими отраслями знаний, прежде всего, с теоретической информатикой, теорией и практикой информационно-коммуникационных технологий, информационной безопасностью социотехнических систем.

С учетом такого понимания содержания определения ТИП, а также указанных выше принципов, была уточнена и сформирована структура ТИП, представляющая новый взгляд, вариант концептуальных направлений, определяющих пути развития и содержание ТИП, являющейся эффективным инструментарий регулирования и развития информационной сферы и ее ИКТ (рис.1).

Предложенные авторами определение и структура ТИП, а также опыт известных ученых [9, 11-14], дают основания утверждать, что дальнейшее развитие искомой теории предполагает в качестве первоочередной задачи уточнение и развитие понятийного базиса ТИП, что обусловлено следующими факторами:

– новизной постановки искомой проблемы, решение которой осуществляется с позиции определяющей роли информации, ИКТ как основных объектов практически всех сфер и видов деятельности современного общества, и, следовательно, возникающих и развивающихся в нем правоотношений;

– неоднозначностью и многообразием содержания информации, как основного

объекта всех видов и сфер деятельности личности, общества и государства, используемых ими ИКТ, в том числе, обеспечения их информационной безопасности и возникающих при этом общественных информационных отношений, связанных с содержанием как информации, так и ее производных понятий.

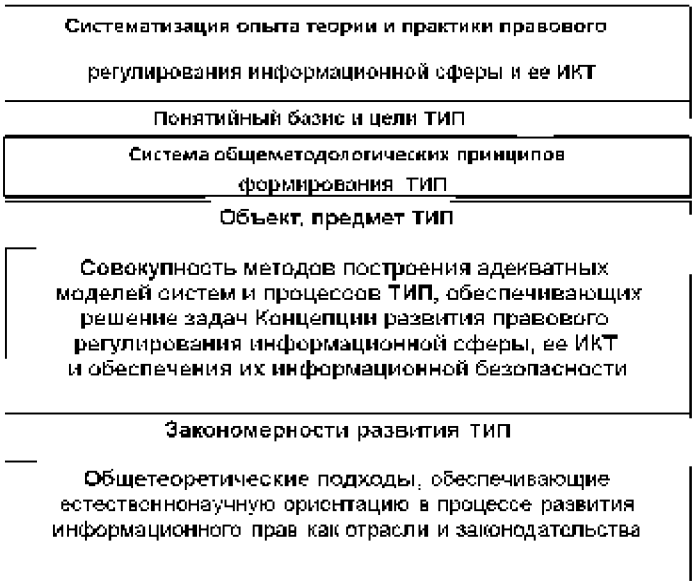


Рисунок 1 – Структура теории информационного права

Предложенные авторами определение и структура ТИП, а также опыт известных ученых [9, 11-14], дают основания утверждать, что дальнейшее развитие искомой теории предполагает в качестве первоочередной задачи уточнение и развитие понятийного базиса ТИП, что обусловлено следующими факторами:

– новизной постановки искомой проблемы, решение которой осуществляется с позиции определяющей роли информации, ИКТ как основных объектов практически всех сфер и видов деятельности современного общества, и, следовательно, возникающих и развивающихся в нем правоотношений;

– неоднозначностью и многообразием содержания информации, как основного объекта всех видов и сфер деятельности личности, общества и государства, используемых ими ИКТ, в том числе, обеспечения их информационной безопасности и возникающих при этом общественных информационных отношений, связанных с содержанием как информации, так и ее производных понятий.

С учетом этих факторов в рамках рассматриваемого содержания ТИП неотъемлемым элементом структуры ТИП будет являться *понятийный базис*, включающий следующие основные понятия: информация, информационные правоотношения, информационная сфера (среда), информационно-коммуникационные технологии, информационная безопасность (ИБ) личности, общества и государства, ИБ ИКТ, ИБ информационных систем, ИБ социотехнических систем, обеспечение ИБ, безопасность информации и другие. При формировании этого понятийного базиса ТИП необходимо придерживаться принципа относительной полноты и открытости его перечня. То есть, необходимо отметить, что этот понятийный базис развиваемой ТИП не может иметь законченной, статичной структуры, а является динамичным в силу динамичного развития основного базиса, информационно-коммуникационных технологий современного общества, которые обуславливают формирование новых и развитие существующих правоотношений в

информационной сфере, а последние, в свою очередь, обуславливают как образование очередных новых понятий, так и развитие, уточнение существующих, которые должны быть включены в структуру ТИП.

Следующими важными элементами структуры являют однозначно определенные *объект и предмет* ТИП. Их содержание определяет назначение теории и позволяет формулировать последующие ее компоненты, обеспечивает эффективное развитие информационного права как отрасли и законодательства и качественно новую возможность правового регулирования развития ИКТ.

Известно, что объект теории определяется как теоретический образ, представляющий источник мысленного получения знаний без непосредственного обращения к объекту. Предмет теории сосредотачивается в рамках понятий концепции и теории, содержание которых составляют знания об объекте, представляемые в известных формах, в целостном, интегрированном виде как предмет данной науки, а также суммой разрозненных фактологических, несвязных знаний об объекте данных на уровне явлений [3].

В общем виде предметом науки являются знания об объекте исследования, доведенные до целостного и глубокого представления о нем. При этом необходимо помнить, что целостность знаний не равнозначна полноте отражения сущности объекта, которая характеризуется степенью односторонности при высоком уровне детальности представлений об этой стороне, а также степенью всесторонности при низкой детализации знаний о каждой из сторон. В зависимости от соотношений этих характеристик определяется целостность знаний. Так, чем выше степень проникновения в сущность познаваемого объекта, тем больше целостность связана со всесторонностью знаний об объекте, что дает основания целостное знание называть понятием об объекте как отражении его сущности.

С учетом известных взглядов на метод как инструмент, которым исследуется объект и представляется предмет, в исследуемой ТИП, также при использовании множества методов образуется и несколько вариантов интеграции знаний об объекте, представленных в виде нескольких самостоятельных предметов, даже для одного объекта, которым является информация. Это обусловлено важнейшими особенностями информации и соответствующими возникающими общественными информационными отношениями, которые имеют двойственный частно- и публично-правовой характер. С учетом этих особенностей в зависимости от уровня развития методологии науки предметы ТИП могут быть представлены независимыми и несовместимыми, отрицающими друг друга, частично перекрывающимися, взаимодополняющими. Последнее представление допускает реализацию очередного этапа интегрирования и создания предмета более высокого уровня, в рамках которого остальные будут представлять частные случаи. И этот уровень будет более полно отражать сущность изучаемого объекта ТИП.

По мнению же В.С. Нерсесянца [9], объектом является то, что еще подлежит научному изучению с помощью познавательных средств, в процессе которого появляются новые знания об объекте, его сущностных, отличительных свойствах, закономерностях. Эти сущностные свойства объекта, по мнению ученого, будут являться предметом соответствующей науки. Такое же мнение было высказано В.М. Сырых, который определяет объект и предмет науки как начальный и конечный результат познания [10]. С учетом этих взглядов, а также проведенных авторами исследований направлений развития информатики, ИКТ, правового регулирования

информационной сферы [11-14], которые отличаются разнообразием формы и содержания, можно утверждать, что *предмет* исследования ТИП формируется в рамках нескольких областей юридических наук, которые сегодня должны учитывать реальное состояние развития современного общества, ИКТ. Базовой является конституционное право, которое находится в постоянном развитии и обуславливает внешние факторы, влияющие на формирование ТИП.

Однако в силу неоднозначности и многозначности содержания объекта информационного права, неопределенности знаний о нем, содержание правового регулирования информационной сферы, не позволяют однозначно сформулировать достаточно обобщенное, содержание предмета ТИП. С учетом этого, направления формирования предмета ТИП могут быть представлены векторами, определяющими, с одной стороны, состояние предмета отрасли информационного права, с другой стороны – состояние предмета других отраслей права, других наук и практики их применения, в зависимости от разработанности которых будет формироваться конечный относительно полный объект ТИП (рис.2). Эта модель формирования объекта ТИП, как составного компонента методологического базиса искомой теории позволяет ответить на вопрос: «Что изучается, исследуется в ИКТ и в информационной сфере в целом?»

Таким образом, в качестве варианта, представляющего содержание объекта ТИП будем понимать информационное право как отрасль права, а содержанием предмета будет выступать содержание информационного законодательства и закономерности его развития, обеспечивающие эффективное регулирование ИКТ. Такое законодательство, а именно его нормативные правовые акты, регулируя различные виды правоотношений, позволяют анализировать, изучать объект теории и являются средством получения новых знаний.

Помимо этого, уяснение понимания предмета изучаемого объекта позволяет сформулировать общее понятие концепции ТИП как определенного предмета и всех факторов, приемов и методов его обоснования. Отсюда следует, что любая наука может представлять свои знания в форме нескольких концепций и соответствующих им предметов.

Понятие «концепция» тесно связано с понятием «теория». Одной из причин такой взаимосвязи является отождествление этих понятий, что является не совсем корректным. В широком смысле, теория представляет собой множество феноменологических знаний, не вошедших ни в одну концепцию, знаний о методах и методиках получения знаний и методологии данной науки. Теория в узком понимании включает в себя концептуальные, понятийные и фактологические знания, методологию и методы получения знаний. Если мы рассматриваем методологию и методы в форме особого вида знаний и доводим все знания об объекте исследования до уровня единой концепции, понятия теории и концепции совпадут. Если же для объяснения свойств объекта используется несколько концепций, то эти понятия будут составлять содержание теории, а любая из предложенных концепций окажется одной из концепций данной теории. Поэтому в проводимом исследовании по формированию ТИП ее содержание будет пониматься шире и будет содержать не только фактологические знания, но и инструментарий, обеспечивающий

формирование новых знаний.

Эти новые знания, в свою очередь, будут выполнять функцию предвидения и уточнения достоверности гипотетических посылок без непосредственного эмпирического опыта, определять направления дальнейшего совершенствования правового регулирования информационной сферы, возникающих в ней общественных отношений, в том числе, прав и свобод личности.

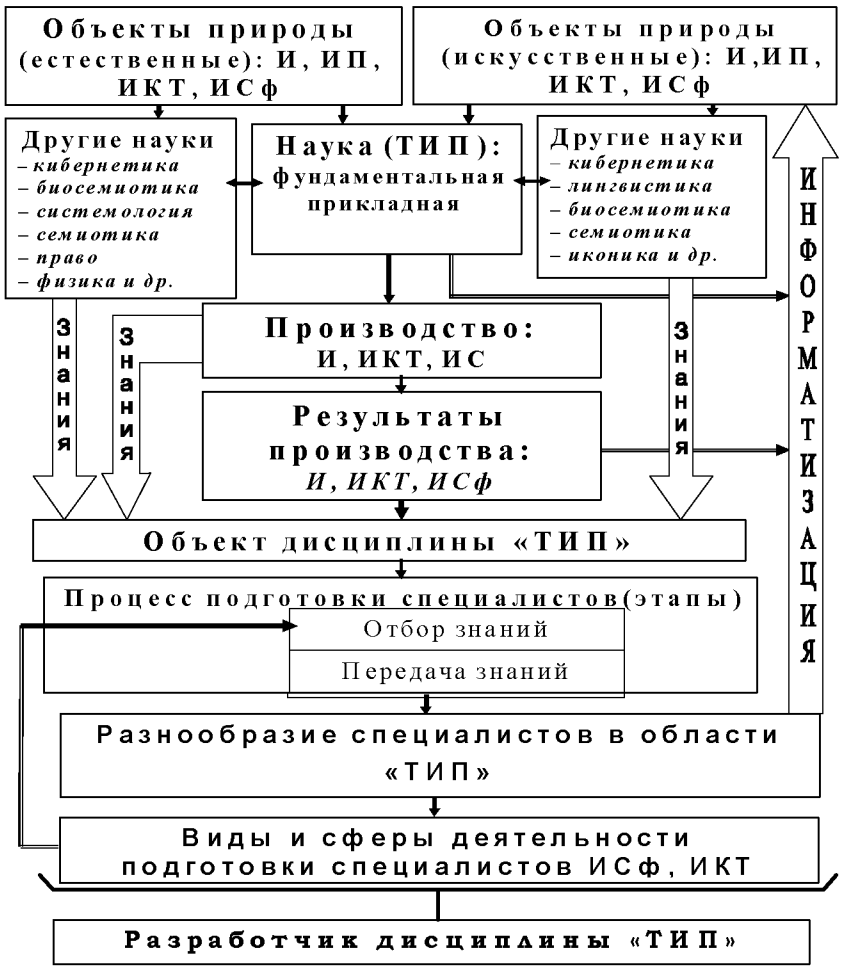


Рисунок 2 – Логическая модель формирования содержания объекта ТИП

Дальнейшее развитие ТИП и его научно-методологического базиса предполагает:

– определение совокупности таких компонентов методологического базиса, как методы, обеспечивающие углубленное изучение и исследование содержания объекта и предмета теории;

– решение задач анализа, синтеза при регулировании развития ИКТ, результаты которых обеспечивают функциональную связь между теорией и практикой развития инструментария правового регулирования информационной сферы;

– уточненные и формулирование цели, задачи и функции ТИП.

Таким образом, в качестве одного из направлений дальнейшего совершенствования информационной сферы, повышения эффективности создания, применения и развития ее ИКТ может быть предложено развитие теории информационного права, осуществляемое на основе предложенного авторами

содержания понятия ТИП, подхода и выделенных особенностей формирования ее структуры, выделенного общего содержания понятийного базиса, содержания объекта и предмета. При этом формирование развернутого содержания ТИП будет осуществляться на основе системного изложения имеющихся знаний, накопленных теорией права, частноправовыми и публично-правовыми отраслями права и законодательства, теоретической информатикой, теорией и практикой ИКТ, отражающих развитие и возникновение новых информационных отношений. В свою очередь, теория информационного права будет представлять эффективный инструментарий решения прикладных задач правового регулирования эффективного развития современных ИКТ.

СПИСОК ЛИТЕРАТУРЫ

1. Бэкон Ф. О достоинстве и преумножении наук // Сочинения в 2-х томах. – Том 1. – М.: «Мысль», 1997.– 567 с.
2. Баженов Л.Б. Строение и функции естественнонаучной теории. – М.: Наука, 1978. – 231 с.
3. Овчинский Н.Ф. Методологические принципы в истории научной мысли. – М.: Эдиториал УРСС, 1997. – 296 с.
4. Рузавин Г.И. Научная теория. Логико-методологический анализ. – М.: Мысль, 1978. – 244 с.
5. Зиновьев А.А. Основы логической теории научных знаний. – М.: Наука, 1967. – 261 с.
6. Мельников Г.П., Преображенский С.Ю. Методология лингвистики: учеб. пособие. – М.: Изд-во УДН, 1989. – 84 с.
7. Печенкин А.А. Обоснование научной теории. – М.: Наука, 1991. – 184 с.
8. Советский энциклопедический словарь / Гл. ред. Прохоров. – Изд. 4, испр. и дополн. – М.: Советская энциклопедия, 1989. – 1632 с.
9. Нерсесянц В.С. Общая теория права и государства. – М., 1999. – С. 18.
10. Сырых В.М. Теория государства и права. – М., 1998. – С. 491.
11. Фисун А.П., Минаев В.А., Саблин В.Н. и др. Теоретические основы информатики и информационная безопасность. – М.: Радио и связь, 2000. – 468 с.
12. Фисун А.П., Белевская Ю.А., Минаев В.А. и др. Правовое обеспечение информационной безопасности объектов информатизации и регулирование конституционных прав личности в информационной сфере: монография; под ред. д.т.н. А.П. Фисуна, к.ю.н. Ю.А. Белевской. – Орел: ОГУ, ОрелГТУ, 2008.– 428 с.
13. Фисун А.П. Теоретическая информатика – фундаментальный базис формирования информационной культуры современного общества, развития информационной науки и технологий. – Известия ОрелГТУ. Серия «Фундаментальные и прикладные проблемы техники и технологии». Научный журнал ОрелГТУ № 2/270 (545), 2008.
14. Фисун А.П., Белевская Ю.А. Информационная теория и информационное право как основной инструментарий обеспечения информационной безопасности и противодействия информационному терроризму. – Научно-технический журнал «Информационные системы и технологии» – № 5(61) 2010. – Орел, 2010. – С. 142-144.

Фисун Александр Павлович
Орловская региональная академия государственной службы, г. Орел
Доктор технических наук, профессор, профессор кафедры административного и финансового права
Тел.: 8 910 307 00 81
E-mail: fisun@orel.ru

Белевская Юлия Александровна
Орловская региональная академия государственной службы, г. Орел
Кандидат юридических наук, доцент, доцент кафедры конституционного и муниципального права
Тел.: (4862) 40-86-75
E-mail: furiya_ua@mail.ru

A.P. FISUN, JU.A. BELEVSKAYA

PERFECTION OF INFORMATION-COMMUNICATION TECHNOLOGIES BY DEVELOPMENT THEORIES OF THE INFORMATION RIGHT

Results of the analysis of features of information-telecommunication technologies (ITT), caused necessity of the further perfection of effective toolkit of their development are stated. One of ways of such perfection is development theory the information right, as the major toolkit providing processes of creation, application, maintenance in an actual condition, modernization and perfection ITT and information sphere, and also a defining component of legal regulation of constitutional laws and freedom of the person and the citizen in information sphere and sphere of maintenance of their information safety. A number of principles of formation of structure of theoretical bases of the information right of its components is specified.

Keywords: *information-communication technologies; the information; information sphere; information safety; the theory of the information right.*

BIBLIOGRAPHY (TRANSLITERATED)

1. Be'kon F. O dostoinstve i preumnozhenii nauk // Sochineniya v 2-x tomax. – Tom 1. – M.: «My'sl'», 1997. – 567 s.
2. Bazhenov L.B. Stroenie i funkcii estestvennonauchnoj teorii. – M.: Nauka, 1978. – 231 s.
3. Ovchinskij N.F. Metodologicheskie principy' v istorii nauchnoj my'sli. – M.: E'ditorial URSS, 1997. – 296 s.
4. Ruzavin G.I. Nauchnaya teoriya. Logiko-metedologicheskij analiz. – M.: My'sl', 1987. – 244 s.
5. Zinov'ev A.A. Osnovy' logicheskoj teorii nauchny'x znanij. – M.: Nauka, 1976. – 261 s.
6. Mel'nikov G.P., Preobrazhenskij S.Yu. Metodologiya lingvistiki: ucheb. posobie. – M.: Izd-vo UDN, 1989. – 84 s.
7. Pechyonkin A.A. Obosnovanie nauchnoj teorii. – M.: Nauka, 1991. – 184 s.
8. Sovetskij e`nciklopedicheskij slovar' / Gl. red. Proxorov. – Izd. 4, ispr. i dopoln. – M.: Sovetskaya e`nciklopediya, 1989. – 1632 s.
9. Nersesyanc V.S. Obshhaya teoriya prava i gosudarstva. – M.: 1999. – S.18.
10. Sy'ry'x V.M. Teoriya gosudarstva i prava. – M.: 1998. – S.491.
11. Fisun A.P., Minaev V.A., Sablin V.N. i dr. Teoreticheskie osnovy' informatiki i informacionnaya bezopasnost'. – M.: Radio i svyaz', 2000. – 468 s.
12. Fisun A.P., Belevskaya Yu.A., Minaev V.A. i dr. Pravovoe obespechenie informacionnoj bezopasnosti ob''ektov informatizacii i regulirovanie konstitucionny'x prav lichnosti v informacionnoj sfere: monografiya ; pod red. d.t.n. A.P. Fisuna, k.yu.n. Yu.A. Belevskij. – Oryol: OGU, OryolGTU, 2008. – 428 s.
13. Fisun A.P. Teoreticheskaya informatika – fundamental'ny'j bazis formirovaniya informacionnoj kul'tury' sovremennogo obshhestva, razvitiya informacionnoj nauki i texnologij. – Izvestiya OryolGtu. Seriya «Fundamental'ny'e i prikladny'e problemy' texniki i texnologii». Nauchny'j zhurnal OryolGTU №2/270 (545), 2008.
14. Fisun A.P., Belevskaya Yu.A. Informacionnaya teoriya i informacionnoe pravo kak osnovnoj instrumentarij obespecheniya informacionnoj bezopasnosti i protivodejstviya informacionnomu terrorizmu. – Nauchno-texnicheskij zhurnal OryolGTU «Informacionny'e sistemy' i texnologii». – №5 (61) 2010. – Oryol: OryolGTU, 2010. – S.142-44.

УДК 004.491.22

А.Н. ХАЛЮЗЕВ

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЯВЛЕНИЯ МНОЖЕСТВЕННЫХ ВИРУСНЫХ ЗАРАЖЕНИЙ УЗЛОВ КОМПЬЮТЕРНОЙ СЕТИ

В статье представлена математическая модель проявления множественных вирусных заражений узлов компьютерной сети (КС) с установленными на них ОС семейства Windows. Модель позволяет определять количество зараженных узлов в КС на заданном интервале времени в условиях распространения неизвестных сетевых вирусов. К неизвестным относятся вирусы, сигнатуры которых отсутствуют в базах данных антивирусных средств пользователей. Основой модели является определение множественных запусков схожих между собой программ. Определение сходства между программами осуществлялось путем сравнения соответствующих трасс как совокупности генерируемых ими системных функций Native API. Кроме того, была введена метрика сравнения – расстояние Хэмминга, и определены параметры модели (пороговое значения, длина трасс).

Ключевые слова: *сетевой вирус; множественные заражения; компьютерная сеть; сетевой узел; трассы программ; модель.*

Массовое распространение компьютерных вирусов в настоящее время приобрело гигантские масштабы и привело к тому, что вопрос о создании средств противодействия и защиты от данной угрозы приобретает новое качество. В условиях ведения глобальной информационной войны компьютерные вирусы становятся средством кибертерроризма. Наряду с этим бурное и повсеместное развитие как локальных, так и глобальных вычислительных сетей (в частности, Интернета), а также появление высокоскоростной транспортной составляющей при объединении разнородных сетей, расположенных в различных географических регионах, вывело на первый план уже не борьбу с компьютерными вирусами, а борьбу с эпидемиями, вызываемыми компьютерными вирусами. Наибольшую угрозу при этом представляют эпидемии неизвестных КВ, сигнатур которых нет в базах данных пользователей на узлах КС. В этих условиях следует отметить значительный масштаб и высокую скорость поражения информационных систем. При этом объектами эпидемий могут стать информационно-телекоммуникационные системы, компьютерные сети, а также индивидуальные пользователи.

В связи с этим особую актуальность приобретает задача разработки эффективных механизмов противодействия угрозе возникновения и развития эпидемий неизвестных компьютерных вирусов в компьютерных сетях.

Источниками возникновения вирусных эпидемий в КС являются сетевые вирусы. Проведенный анализ [1] указанного класса вирусов позволяет сделать вывод, что наиболее опасным с точки зрения возникновения и развития вирусных эпидемий в КС является автономный сетевой вирус. Вирус данного типа может распространяться по КС без участия человека. В случае применения эффективной техники сканирования и многопоточности скорость их распространения может быть настолько высокой, чтобы в считанные минуты поразить компьютерную сеть, состоящую из десятков тысяч и более узлов.

Задача противодействия угрозе возникновения и развития вирусных эпидемий в компьютерных сетях предполагает решение нескольких частных подзадач:

– контроля динамики развития вирусной эпидемии, заключающегося в определении основных параметров ее развития;

– принятие решения о возникновении эпидемии;

– построение модели эпидемии с целью прогноза ее дальнейшего развития;

– оповещение узлов КС о распространении эпидемии;

– принятие мер по реагированию, т.е. противодействию дальнейшему распространению эпидемии по КС.

В любом случае первичной, а, следовательно, наиболее приоритетной, является задача контроля динамики развития вирусной эпидемии в компьютерных сетях, как локальных, так и глобальных. Под указанным понятием в данной работе понимается определение основных параметров эпидемии в определенные моменты времени $t_1, t_2, t_3 \ldots$, например, количества зараженных узлов в КС.

Современные КВ, способные заражать элементы КС, имеют высокую скорость распространения: от сотен до тысяч узлов КС в секунду [1, 6]. Ввиду этого особое значение в процессе контроля имеет время, необходимое на сбор информации о развитии эпидемии, ее обработку и принятие решения о противодействии ей в рамках защищаемой КС.

Следует отметить, что в настоящее время научная база в области мониторинга вирусных эпидемий, в целом, развита недостаточно. Единственным российским ученым, проводившим исследования в данной области, является С.В. Новиков [2]. В большей степени исследования проводились зарубежными учеными: M.M. Williamson, J. Léveillé, J.O. Kephart, S.R. White, C.C. Zou, L. Gao, W. Gong, D. Towsley, T. Vogt, Z. Chen, L. Gao, K. Kwiat, D.J. Malan и др.

Основными направлениями исследований в области вирусных эпидемий являются:

1. Моделирование процесса распространения вирусных эпидемий с позиций получения механизма прогноза динамики их развития [2-5];
2. Исследование сетевых вирусов и различных техник сканирования IP-адресов заражаемых узлов [6-8];
3. Исследование механизмов обнаружения сетевых вирусов [1,6];
4. Исследование превентивных механизмов защиты от эпидемий компьютерных вирусов [9].

Наиболее близким к задаче обеспечения контроля развития вирусных эпидемий является первое направление. Анализ подходов к разработке модели процесса распространения вирусных эпидемий в КС показал, что все существующие эпидемические модели можно классифицировать по 3-м признакам: учету случайных факторов, характеру времени, учету особенностей сетевых вирусов. Установлено, что детерминированные модели применяются в том случае, когда влияние случайных факторов приводит к незначительным колебаниям характеристик моделей и вследствие этого ими можно пренебречь. Стохастические модели применяются, когда необходимо учесть случайные факторы, как правило, в малых компьютерных сетях. Моделирование показывает, что применение стохастических подходов для больших сетей дает тот же самый результат, что и детерминированный. По второму признаку модели делятся на непрерывные и дискретные. По 3-му признаку модели делятся на: модели роста популяций, классические эпидемические модели и модели, адаптированные к процессу распространения компьютерных вирусов. Первые два класса моделей без каких-либо изменений заимствованы из биологии и

эпидемиологии. Модели роста популяций позволяют определять темп роста эпидемии, а также ее размер (количество зараженных узлов в любой момент времени). Эпидемические модели также определяют условие возникновения эпидемии в виде эпидемиологического предела (теорема Кермака-МакКендрика). Данный предел – это условие, при соблюдении которого эпидемия может начаться. Модели, относящиеся к третьему классу, не были в чистом виде заимствованы из биологии. Их основа – классические модели – однако при разработке они были модифицированы с учетом особенностей сетевых вирусов и их распространения по компьютерным сетям.

Существующие эпидемические модели описывают процесс развития эпидемий КВ с учетом различных факторов. Позволяют на их основе осуществлять прогнозирование характеристик эпидемий в различное время, но не учитывают методы обнаружения КВ, т.е. оперируют с фактами заражений. Кроме того, их построению предшествует этап сбора информации о количестве зараженных узлов в КС – контроля. На практике целесообразно рассматривать не модели процесса эпидемии, а механизмы и модели контроля динамики развития эпидемий. На основе последних осуществляется дальнейшая идентификация и оценка параметров эпидемических моделей.

При осуществлении контроля необходимо выполнять требования по своевременности и достоверности. Это, в свою очередь, напрямую зависит от 3-го направления – исследования механизмов обнаружения сетевых вирусов. Среди них можно выделить два кардинально различных класса – сигнатурный и поведенческий.

С точки зрения обеспечения достоверности контроля наиболее предпочтительным является класс сигнатурных методов обнаружения. Вероятность обнаружения вирусов посредством данного класса равна 1. Это справедливо для случая, когда вирус является известным. При распространении неизвестного КВ вероятность обнаружения изначально равна нулю. После разработки соответствующей сигнатуры экспертом антивирусного центра данная вероятность становится равной единице, но происходит это с некоторой задержкой. Таким образом, существенным недостатком данного метода обнаружения является длительность времени, необходимого для разработки соответствующей сигнатуры и ее распространения по всем узлам КС. Сейчас примерное время выработки сигнатуры экспертом антивирусного центра составляет от нескольких часов до нескольких дней. Данное обстоятельство существенно снижает своевременность контроля при распространении неизвестных вирусов в КС.

Поведенческие методы инвариантны к обнаружению известных или неизвестных вирусов. Однако они характеризуются наличием определенного числа ошибок первого и второго рода. Вследствие этого вероятность обнаружения как известных, так и неизвестных вирусов посредством данных методов меньше единицы. Таким образом, достоверность поведенческих методов ниже достоверности сигнатурных методов. Однако поведенческие методы не требуют разработки сигнатур, поэтому время обнаружения неизвестных КВ для данных методов существенно ниже, чем для сигнатурных методов, а вследствие этого они обеспечивают лучшую своевременность.

При решении задачи контроля развития эпидемии неизвестного вируса в КС наиболее существенным является требование по обеспечению своевременности. Это связано с высокой скоростью распространения современных сетевых вирусов в КС. Ввиду этого для решения указанной задачи сигнатурные методы обнаружения не

подходят. Необходимо применять существующие или разрабатывать новые поведенческие методы.

Существенным недостатком современных поведенческих методов обнаружения вирусов является то, что они не адаптированы к контролю вирусного распространения по КС. Данные методы разрабатывались в целях обнаружения одиночных зараженных узлов в КС, а не множественных их заражений. Они не приспособлены к массовому распространению вирусов по КС и не способны оценивать количество зараженных узлов в масштабах всей сети.

Для устранения данного недостатка предлагается математическая модель проявления множественных вирусных заражений узлов компьютерной сети на основе обнаружения сходства в их поведении. При этом необходимо определить модель поведения конкретного узла в компьютерной сети.

Распространение сетевого вируса по компьютерной сети характеризуется последовательным запуском его исполняемого кода на каждом из узлов данной сети. Таким образом, модель поведения узла можно определить в виде списка запускаемых на определенном интервале времени приложений (1):

$$Node_{j\Delta t} = \{Programm_1, Programm_2, Programm_3 ...\}, \quad (1)$$

где j – номер узла в КС.

В свою очередь, любое системное или пользовательское приложение в ходе своей работы, потребляя некоторые ресурсы путем обращения к низкоуровневым средствам операционной системы (ОС), генерирует определенные наборы системных вызовов. Сетевой вирус, как и любой другой вирус, представляет собой приложение, т.е. исполняемый код. Таким образом, одной из моделей исполняемого кода вируса является представление его последовательностью вызовов системных функций (СФ), которую назовем трассой программы (2).

$$Tr = F_1^i F_2^i F_3^i ... F_n^i ... \ , \quad (2)$$

где F_i – переменная, соответствующая вызову i-ой СФ;

i – индекс или имя СФ;

n – порядковый номер вызова СФ в трассе.

Эксперимент по мониторингу вызовов СФ при запуске нормальных программ и сетевых вирусов показал, что из всего множества (порядка 2-3 тыс. СФ) на практике встречаются лишь 126. Например, такие, как: NtOpenFile, NtOpenKey, NtOpenKeyedEvent, NtOpenSection, NtQuerySystemInformation, NtAllocateVirtualMemory, NtAllocateVirtualMemory и др. Таким образом, совокупность отслеживаемых СФ можно представить в виде множества F:

$$F = \{F^i\},\ i \in \{1,2,3,... ,126\} \quad . \quad (3)$$

Для случая исполняемого кода сетевого вируса $n \to \infty$. Это связано с тем, что данный тип вируса постоянно сканирует компьютерную сеть с целью поиска новых жертв заражения. Другими словами, последовательность вызова системных функций, соответствующая сетевому вирусу, будет бесконечной. Представление исполняемого кода бесконечной последовательностью не имеет физического смысла и является бесполезным на практике. В связи с этим необходимо ограничить данную последовательность определенной длиной. При таком условии выражение (2) преобразуется к виду:

$$Tr = F_1^i F_2^i F_3^i ... F_n^i,\ n = N,\ i \in \{1,2,3,..,126\}\ , \qquad (4)$$

где N – длина последовательности вызовов СФ.

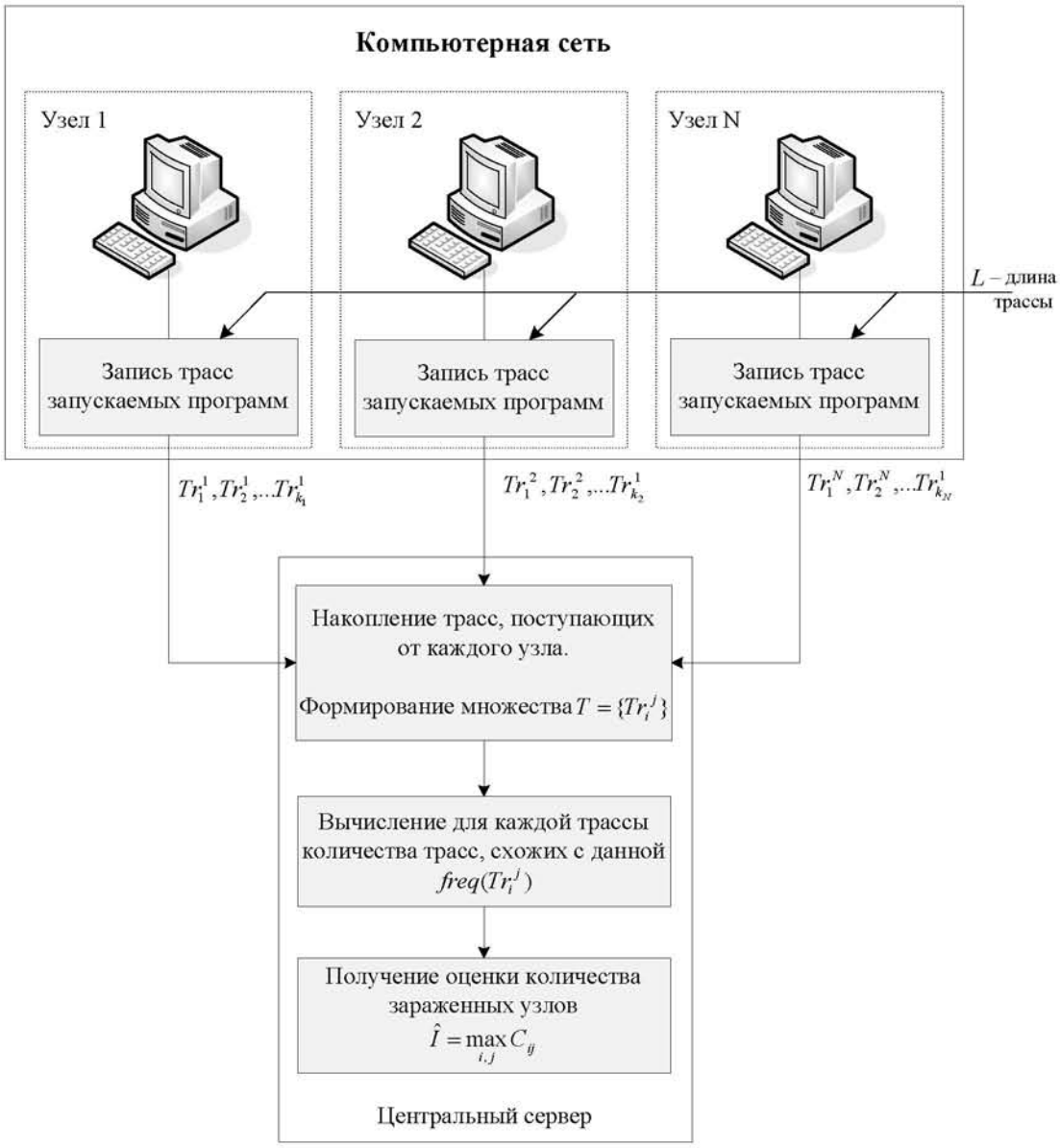


Рисунок 1 – Модель проявления множественного заражения в КС

Формальное описание модели:

Распространение сетевого вируса по КС характеризуется главным свойством – запуском своих копий на узлах КС. Это означает появление в модели поведения зараженных узлов трасс, соответствующих запускам данного вируса. В компьютерной сети в данном случае будет проявляться множественное заражение. Данное проявление, как уже было сказано в предыдущем пункте, будет характеризоваться появлением множества схожих между собой трасс, количество которых и будет являться оценкой количества зараженных узлов в КС на определенном интервале времени.

Общий вид модели проявления множественного заражения в КС на интервале времени представлен на рисунке 1, а ее сущность состоит в следующем:

На каждом узле осуществляется отслеживание запуска всех приложений и запись трасс, соответствующих им. Все трассы имеют одинаковую длину, заранее предопределенную и равную L. Записанные трассы последовательно в асинхронном

режиме передаются на центральный сервер (ЦС), который осуществляет обработку поступающих трасс и определение по ним количества зараженных узлов в КС.

От каждого узла поступают трассы, которые могут соответствовать как нормальным программам, так и вирусам. В результате образуется множество трасс T:

$$T = \begin{Bmatrix} \{Tr_1^1 & Tr_2^1 & \dots & Tr_{k_1}^1\} \\ \{Tr_1^2 & Tr_2^2 & \dots & Tr_{k_2}^2\} \\ \{Tr_1^3 & Tr_2^3 & \dots & Tr_{k_3}^3\} \\ \{Tr_1^N & Tr_2^N & \dots & Tr_{k_N}^N\} \end{Bmatrix} . \quad (5)$$

Для нахождения схожих между собой трасс необходимо каждую трассу, поступающую от одного узла, сравнить со всеми трассами, поступающими от всех других узлов. При этом для начала преобразуем матрицу T к следующему виду (выражение 6):

Для каждой ij – ой трассы Tr_i^j, при всех $j = 1...N$: $i = 1...k_j$, где N – количество узлов в КС, а k_j – количество трасс поступивших от j – го узла, определим множество P:

$$P = \begin{Bmatrix} \{pr(Tr_1^1) & pr(Tr_2^1) & \dots & pr(Tr_{k_1}^1)\} \\ \{pr(Tr_1^2) & pr(Tr_1^2) & \dots & pr(Tr_{k_2}^2)\} \\ \{pr(Tr_1^3) & pr(Tr_1^3) & \dots & pr(Tr_{k_3}^3)\} \\ \{pr(Tr_1^N) & pr(Tr_1^N) & \dots & pr(Tr_{k_N}^N)\} \end{Bmatrix}, \quad (6)$$

где каждый элемент $pr(Tr_i^j)$ представляет собой тоже множество, образующееся следующим образом:

1. Вначале первая трасса, поступившая от первого узла, сравнивается со всеми трассами, поступившими от всех других узлов. Для каждой пары вычисляется индикаторная функция $cor(Tr_i, Tr_j)$, определяющая наличие или отсутствие сходства между данными трассами, согласно выражению (7):

$$cor(Tr_i, Tr_j) = \begin{cases} 1, \text{если } Sim(Tr_i, Tr_j) \ge h \\ 0, \text{если } Sim(Tr_i, Tr_j) < h \end{cases}, \quad (7)$$

где $Sim(Tr_i, Tr_j)$ – функция расстояния или метрики, определяющая степень сходства (различия) между трассами, а h – пороговое значение метрики, при котором принимается решение о наличии или отсутствии сходства между трассами. В результате получим множество $pr(Tr_1^1)$, представленное в выражении (8):

$$pr(Tr_1^1) = \begin{Bmatrix} \{cor(Tr_1^1, Tr_1^2), cor(Tr_1^1, Tr_2^2), \dots, cor(Tr_1^1, Tr_{k_2}^2)\} \\ \{cor(Tr_1^1, Tr_1^3), cor(Tr_1^1, Tr_2^3), \dots, cor(Tr_1^1, Tr_{k_3}^3)\} \\ \dots \\ \{cor(Tr_1^1, Tr_1^N), cor(Tr_1^1, Tr_2^N), \dots, cor(Tr_1^1, Tr_{k_N}^N)\} \end{Bmatrix}. \quad (8)$$

Элементы указанного множества принимают значения 0 или 1 в зависимости от того, существует сходство между трассами или нет.

2. Вторая трасса, поступившая от первого узла, сравнивается со всеми трассами, поступившими от всех других узлов. Аналогично пункту 1 и выражению (7) вычисляется функция $cor(Tr_i, Tr_j)$ для указанных пар трасс. В результате получим

множество $pr(Tr_2^1)$, представленное в выражении (9):

$$pr(Tr_2^1)=\begin{Bmatrix}\{cor(Tr_2^1,Tr_1^2),cor(Tr_2^1,Tr_2^2),...,cor(Tr_2^1,Tr_{k_2}^2)\}\\ \{cor(Tr_2^1,Tr_1^3),cor(Tr_2^1,Tr_2^3),...,cor(Tr_2^1,Tr_{k_3}^3)\}\\ ...\\ \{cor(Tr_2^1,Tr_1^N),cor(Tr_2^1,Tr_2^N),...,cor(Tr_2^1,Tr_{k_N}^N)\}\end{Bmatrix}. \quad (9)$$

3. Таким образом, получаются элементы $pr(Tr_i^1)$, $i=1...k_1$ для всех трасс, поступивших от 1-го узла.

4. Аналогично п. 1-3 находятся элементы $pr(Tr_i^2)$, $i=1...k_2$ для всех трасс, поступивших от 2-го узла.

5. В конечном счете находятся элементы $pr(Tr_i^N)$, $i=1...k_N$ для всех трасс, поступивших от N – го узла. В частности, находится последний элемент $pr(Tr_{k_N}^N)$, представленный в выражении (10):

$$pr(Tr_{k_N}^N)=\begin{Bmatrix}\{cor(Tr_{k_N}^N,Tr_1^1),cor(Tr_{k_N}^N,Tr_1^1),...,cor(Tr_{k_N}^N,Tr_{k_1}^1)\}\\ \{cor(Tr_{k_N}^N,Tr_1^2),cor(Tr_{k_N}^N,Tr_2^2),...,cor(Tr_{k_N}^N,Tr_{k_2}^2)\}\\ ...\\ \{cor(Tr_{k_N}^N,Tr_1^{N-1}),cor(Tr_{k_N}^N,Tr_2^{N-1}),...,cor(Tr_{k_N}^N,Tr_{k_{N-1}}^{N-1})\}\end{Bmatrix}. \quad (10)$$

Далее, посредством полученных множеств $pr(Tr_i^j)$, для каждой поступившей трассы необходимо получить значения счетчиков $freq_i^j$, определяющих количество трасс, схожих с данной. Указанная операция выполняется посредством суммирования всех элементов множеств $pr(Tr_i^j)$. Например, для 1-ой трассы, поступившей от 1-го узла, данная сумма будет определяться выражением (11):

$$freq_1^1=\sum_{i,j} pr(Tr_1^1)(i,j), \quad (11)$$

где (i,j) – индекс соответствующего элемента множества $pr(Tr_1^1)$. Таким образом, получим множество счетчиков схожих трасс C (выражение (12)):

$$C=freq(pr(Tr_i^j))\begin{Bmatrix}\{freq(Tr_1^1) & freq(Tr_2^1) & ... & freq(Tr_{k_1}^1)\}\\ \{freq(Tr_1^2) & freq(Tr_1^2) & ... & freq(Tr_{k_2}^2)\}\\ & ... & & \\ \{freq(Tr_1^N) & freq(Tr_1^N) & ... & freq(Tr_{k_N}^N)\}\end{Bmatrix}. \quad (12)$$

Количеством зараженных узлов согласно данной модели, а точнее, его оценкой, будет являться элемент матрицы C с максимальным значением плюс единица (выражение (13)), что соответствует наихудшему случаю. Единица добавляется вследствие того, что осуществляется сравнение пар трасс.

$$I=\max_{i,j} C_{ij}+1 \quad . \quad (13)$$

В идеальном случае, когда не существует ошибки распознавания схожих между собой пар трасс, оцененное значение количества зараженных узлов равно его реальному значению (выражение (14)):

$$I=I_{реальн.} \quad . \quad (14)$$

В том случае, когда существует ошибка распознавания оцененное значение количества зараженных узлов будет равно реальному, но с некоторой ошибкой (выражение (15)). Данная ошибка будет определяться суммарной ошибкой неправильного распознавания схожих трасс.

$$I = I_{реальн.} + \varepsilon \ . \qquad (15)$$

Основой разработанной модели является расчет индикаторной функции для пар трасс, показывающей наличие или отсутствие сходства между ними. Для этого необходимы выбор метрики сравнения трасс и определение основных параметров модели. К ним относятся: длина трасс L и соответствующее ей пороговое значение индикаторной функции $cor(Tr_i, Tr_j)$. Для полного и окончательного определения модели проявления множественных заражений необходимо определить значения указанных параметров. При этом необходимо минимизировать суммарную ошибку неправильного распознавания, т.е. неправильного определения несхожих трасс как схожих и неправильного определения схожих трасс как несхожих.

Для определения порогового значения была поставлена и решена задача одномерного 2-хклассового статистического распознавания образов. При решении задачи распознавания руководствовались принципом минимизации суммарной ошибки неправильной классификации, представляемой суммой ошибок 1-го и 2-го рода. В случае определения количества зараженных узлов в КС через количество схожих между собой трасс обе ошибки нежелательны. Это связано с тем, что наличие ошибки 1-го рода приведет к завышению количества схожих трасс, следовательно, и к завышению количества зараженных узлов в КС. Наличие ошибки 2-го рода, наоборот, приведет к занижению количества схожих трасс. Кроме того, при выборе критерия в расчет бралось отсутствие априорных вероятностей появления классов и информации о матрице потерь от неправильной классификации. В связи с этим для принятия решения по распознаванию был выбран критерий максимального правдоподобия.

Для определения качества распознавания была определена суммарная ошибка неправильной классификации. Сделан вывод, что наименьшая ошибка достигается при длине трасс $L = 400$, а соответствующий ему порог $h = 72{,}77$.

Разработанная модель проявления множественного вирусного заражения с учетом определенных параметров позволяет определять количество зараженных узлов в КС на заданном интервале времени. Основным достоинством данной модели является ее применимость в условиях распространения неизвестных вирусов, т.е. на стадии так называемого «нулевого дня».

СПИСОК ЛИТЕРАТУРЫ

1. URL: http://www.viruslist.com
2. Новиков С.В. Модель распространения вирусных атак в сетях передачи данных общего пользования на основе расчета длины гамильтонова пути. Дис. канд. техн. наук, С-Пб, 2007.
3. Ризниченко Г.Ю., Рубин А.Б. Математические модели биологических продукционных процессов. – М.: Изд. МГУ, 1993.
4. Matthew M. Williamson, Jasmin Léveillé Epidemic Spreading in Technological Networks, Iformation Infrastructure Laboratory HP Laboratories Bristol HPL-2003-39, February 27th , 2003.
5. Kephart J.O., White S.R. Directed-Graph epidemiological models of computer viruses.
6. Nazario J. Defense and Detection Strategies against Internet Worms, J. Nazario, 2004.
7. Weaver N., Slaniford S., Paxson V. Very Fast Containment of Scanning Worms, August 2004.
8. Tom Vogt Simulating and optimising worm propagation algorithms, 9th September 2003.

9. David Moore, Colleen Shannon, Geoffrey M. Voelker, Stefan Savage Internet Quarantine: Requirements for Containing Self-Propagating Code, University of California, San Diego, 2004.

Халюзев Алексей Николаевич
Академия ФСО России, г. Орел
Адъюнкт Академии ФСО России
Тел.: 8 960 64332 92

A.N. HALYUZEV

MATHEMATIC MODEL OF MULTIPLE VIRAL INFECTIONS APPEARANCE OF NETWORKS NODES

The mathematic model of multiple viral infections appearance of networks nodes with Windows's family installed operation system is given. Model allows to define number of infected hosts in computer networks on the set interval of time in the conditions of unknown virus spreading. Unknown viruses is a viruses which signatures are absent in databases of anti-virus means of users. Model basis is definition of plural starts of programs similar among themselves. Similarity definition between programs was carried out by comparison of corresponding lines, as sets of Native API system functions generated by them. Besides, the comparison metrics – distance of Hemminga has been entered, and model parameters (threshold values, length of lines) are defined.

Keywords: *network virus; infection; multiple infections; computer networks; network node; program traces; model.*

BIBLIOGRAPHY (TRANSLITERATED)

1. URL: http://www.viruslist.com
2. Novikov S.V. Model' rasprostraneniya virusny'x atak v setyax peredachi danny'x obshhego pol'zovaniya na osnove raschyota dliny' gamil'tonova puti. Dis. kand. texn. nauk, S-P, 2007.
3. Riznichenko G.Yu., Rubin A.B. Matematicheskie modeli biologicheskix produkcionny'x processov. – M.: Izd. MGU, 1993.
4. Matthew M. Williamson, Jasmin Léveillé Epidemic Spreading in Technological Networks, Iformation Infrastructure Laboratory HP Laboratories Bristol HPL-2003-39, February 27th , 2003.
5. Kephart J.O., _White S.R. Directed-Graph epidemiological models of computer viruses.
6. Nazario J. Defense and Detection Strategies against Internet Worms, J. Nazario, 2004.
7. Weaver N., Slaniford S., Paxson V. Very Fast Containment of Scanning Worms, August 2004.
8. Tom Vogt Simulating and optimising worm propagation algorithms, 9th September 2003.
9. David Moore, Colleen Shannon, Geoffrey M. Voelker, Stefan Savage Internet Quarantine: Requirements for Containing Self-Propagating Code, University of California, San Diego, 2004.