МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

В І С Н И К

Східноукраїнського національного університету імені Володимира Даля

№ 9(103)

Науковий журнал
Частина І

Видавництво СНУ ім. В. Даля
Луганськ - 2006

ВІСНИК
СХІДНОУКРАЇНСЬКОГО
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ
№ 9(103) 2006
НАУКОВИЙ ЖУРНАЛ
ЗАСНОВАНО У 1996 РОЦІ
ВИХІД З ДРУКУ –ДВАНАДЦЯТЬ РАЗІВ
НА РІК

ЗАСНОВНИК
Східноукраїнський національний університет

Журнал зареєстровано Міністерством України у справах преси та інформації **Свідоцтво** про державну реєстрацію **серія КВ № 2411 від 19.12.96 р.**

VISNIK
OF THE EAST UKRAINIAN
NATIONAL UNIVERSITY
NAMED IN MEMORY OF
VLADIMIR DAL
№ 9(103) 2006
SCIENTIFIC JOURNAL
WAS FOUNDED IN 1996
IT IS ISSUED TWELVE TIMES A YEAR

FOUNDER
East Ukrainian National University

Registered by the ministry of ukraine for press and information registration **gertificate** **KB № 2411 dated 19.12.96**

Журнал включено до Переліків наукових видань ВАК України № 2 (Бюл. ВАК №5 (13) 1999 р.), №3 (Бюл. ВАК №6 (14) 1999 р.) та № 4 (Бюл. ВАК №2 (16) 2000 р.), в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук з технічних, історичних та економічних наук відповідно.

Відповідальний за випуск: Петров О.С.

До журналу увійшли статті студентів, аспірантів і докторантів Східноукраїнського національного університету, вищих учбових закладів України, Росії та закордонних країн.

Журнал підготовлено кафедрою комп'ютерних систем та мереж Східноукраїнського національного університету імені Володимира Даля.

Рекомендовано до друку Вченою радою Східноукраїнського національного університету імені Володимира Даля (протокол № 11 від 30.06.2006 р.)

Матеріали номера друкуються мовою оригіналу.

ЗМІСТ
CONTENTS

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056

Голубенко А.Л., Хорошко В.А., Петров А.С., Белозеров Е.В.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КИБЕРПРЕСТУПНОСТЬ

Описаны основные методы и цели киберпреступников. Определены акценты развития киберпреступности и пути обеспечения безопасности.

Развитие человечества последовательно приводит к новым формам коммуникации и распространения информации, наиболее популярными из которых в настоящее время являются различные телекоммуникационные сети. Использование этих сетей в различных отраслях деятельности человека естественно привлекает внимание преступников. Причем в последнее время развитие киберпреступности уже преобретает формы организованной преступности.

Информационные технологии изменяют принципы взаимодействия в обществе, поэтому неудивительно, что они также изменяют понятие преступности как таковое. Компьютеры, компьютерные сети, и Internet становятся составной частью бизнеса и социальной активности. Объем информации, доступной с помощью компьютеров и компьютерных сетей привлекает преступников, и эта привлекательность будет только расти по мере того, как информационные технологии будут приобретать новые формы.

В 2004 году FBI оценил стоимость последствий киберпреступлений в 400 млрд.дол. при общем объеме электронной коммерции в 70млрд.дол., в 2005 году – 540 млрд.дол. и 90,5млрд.дол. соответственно. Если в 2003 году исследователи McAfee Inc. [1] обнаруживали ежемесячно 300 потенциальных вредоносных угроз, то в 2005 году цифра выросла до 2000. Если еще несколько лет назад целью 90% вирусов было нарушение нормальной работы телекоммуникационных сетей и не ставило своей целью получение наживы, то в настоящее время 85% создаваемого вредоносного ПО используется для получения наживы. Изменился и стиль преступлений – взламываемые пользовательские системы и сети теперь зачастую служат для совершения атак на более привлекательные цели (таблица 1).

Можно выделить следующие аспекты привлекательности телекоммуникационных сетей для преступников:

- Растет интеграция сервисов для осуществления банковской и коммерческой деятельности в телекоммуникационных сетях;
- Возрастают количества и суммы транзакций;
- Большинство сервисов коммуникационных сетей позволяют пользователям работать относительно конфиденциально и анонимно;
- Существует возможность использования специальных роботов (bots) для снижения временных затрат на преступную деятельность;
- Киберпреступления сложно отследить и собрать доказательства;
- Пострадавшие склонны замалчивать киберпреступления;
- Меньший риск в сравнении с обычными видами преступлений и более высокая эффективность;
- Возможность совершения преступлений через границы стран и континентов;
- Не требуется физического присутствия;

Неудивительно, что современные формы преступности постепенно перемещаются в область киберпространства и требуют все более глубокого изучения с целью эффективного предотвращения. Согласно оценок [2-6] возможно только 5% киберпреступниковв настоящее время могут быть пойманы и осуждены.

Согласно отчета по информационной безопасности компании McAfee Inc.[1] прослеживается следующая аналогия между традиционной и киберпреступностью:

- Традиционный рэкет / Электронный рэкет;
- Ограбление банков / Хакерство;
- Кражи кредитных карт / Кражи электронных баз кредитных карт личных банковских данных пользователей;
- Аферы с акциями / Электронный «Pump-and-Dump»;
- Фиктивные звонки / Фишинг;
- Отмывание денег;
- Вымогательство/вымогательство (чаще с угрозой причинения вреда репутации компании);
- Мошенничество/мошенничество (предложение принять участие в отмывании денег, поддельные электронные магазины (схожие www-имена), поддельные аукционы и проч.);
- Воровство с использованием отвлекающего маневра / Вирусы, использующие back door;

Необходимо отметить, что описанные выше преступления присущи не только зарубежному информационному сообществу и в Украине реализуется большая часть из этого спектра преступлений. Так например, длительное время существовал целый набор сайтов с изменениями в названии в 1-2 символа, имитирующих работу известного украинского банка. В результате выполнения стандартных банковских операций потребитель размещал запрос на платеж, а преступник получал не только деньги от транзакции, но и полные банковские реквизиты потребителя с требуемыми параметрами доступа.

Уровень ущерба, нанесенного компьютерными преступлениями в Украине, уже сейчас составляет десятки миллионов гривен [8]. Преступления в сфере использования телекоммуникаций неоднократно создавали разные предпосылки для возникновения в Украине чрезвычайных ситуаций, в том числе на объектах жизнеобеспечения. В Украине чаще всего в суде рассматриваются уголовные дела, возбуждаемые по ст. 361 УК Украины – незаконное вмешательство в работу электронно-вычислительных машин (компьютеров) систем, компьютерных сетей и сетей электросвязи. По данным МВД Украины, в 2005 году зарегистрировано 271 таких правонарушений, что почти в два раза больше по сравнению с 2004 годом (197). Однако данная статистика, по мнению большинства экспертов, не отражает реальную картину с киберпреступностью на Украине. Как известно, латентность компьютерных преступлений – это признак, который отображает существование в стране той реальной ситуации, когда определенная часть преступности остается неучтенной. Во всех государствах фактическая преступность превышает то количество преступлений, которые зарегистрированы их органами.

Таблица 1

Результаты исследования CSI/FBI Computer Crime and Security Survey
(на основании изучения деятельности 530 компаний)

Вид действий	**2005**	**2003**	
Вирусные атаки	$42 млн	$27 млн	+ 55%
Неавторизованный доступ	$31 млн	$0,5 млн	+ 6300%
Кража информации	$31 млн	$70 млн	- 56%
Отказ в обслуживании	$7 млн	$65 млн	- 89%
Кража лаптопов	$4 млн	$7 млн	- 42%

Проведенный анализ преступлений по всему миру показывает, что самыми многочисленными являются нарушения, связанные с неправомерным доступом (табл.1). Это прежде всего связано с тем, что данный вид преступлений, как правило, является чаще всего подготовкой к более серьезным киберпреступлениям.

На основании отчета CSI/FBI Computer Crime and Security Survey в среднем международные компании тратят на обеспечение информационной безопасности около 500 у.е. на 1 работающего при этом 5% бюджета телекоммуникационных систем идет на обеспечение безопасности. По данным прессы в Украине на развитие информационной инфраст-

руктуры различного типа организации тратят от 1% (машиностроение) до 15% (финансовый сектор) своих бюджетов. Учитывая некоторое отставание Украины в понимании проблем актуальности защиты информации, можно предположить, что данные статьи составляют порядка 0,5-0,8% затратной части бюджетов.

Рассмотрение ближайшего будущего киберпреступности показывает:

1. Наиболее реальными целями вскоре будут персональные мобильные средства телекоммуникации, процесс совершенствования и развития которых в настоящее время, чрезвычайно динамичен. Развитие функций мобильных устройств уже вскоре позволит их превратить в достойных конкурентов стационарных телекоммуникационных систем. Кроме того, развитие телекоммуникационных систем, реализующих IP-телефонию и прочие голосовые сервисы неминуемо приведет к попыткам киберпреступников реализовать уязвимости данного сервиса для реализации незаконного доступа. В феврале 2005 года было объявлено об обнаружении уязвимостей в системе голосового сервиса Skype, однако к моменту обнаружения уже целый ряд компаний, использующих данный сервис, понесли убытки в результате незаконного проникновения.

2. Вредоносные коммуникационные сообщения в настоящий момент являются бичом практически всех телекоммуникационных систем и согласно прогнозам объем этих преступлений в общем количестве киберпреступлений будет сохраняться. Однако многие аналитики уже в настоящее время рассматривают снижение роли электронной почты, как средства доставки вредоносного кода на компьютеры, и рассматривают реальную возможность создания более изощренных систем для реализации данных функций.

3. Использование безпроводных методов коммуникации уже сейчас привлекает значительное количество киберпреступников, однако учитывая, что подобные сети в нашей стране пока не получили массового распространения, рост киберпреступности, реализующией возможности данных методов еще впереди.

4. Привлекательность для киберпреступников банковских систем будет в дальнейшем все больше возрастать, а соответветственно возрастать и использование уязвимостей, направленных на получение банковских и идентификационных параметров пользователей. Однако в ближайшем будущем возможна реализация систем биометрической идентификации пользователей, что возможно поможет повысить безопасность идентификации.

Прогнозируя будущее индустрии электронной безопасности можно выделить следующие тенденции:

1. Совершенствование сетевого оборудования - защитных сервисных коммутаторов, с помощью которых появится возможность оказывать корпоративным клиентам широкий спектр услуг по обеспечению безопасности в компьютерных сетях;

2. Формирование рынка услуг по защищенной доставке цифрового контента и рынка технологий такой доставки;

3. Произойдет возрастание объемов рынка управляемых услуг безопасности, при этом лидирующее положение на нем будут занимать провайдеры, учитывающие интересы электронной коммерции, пользователей услуг Web-хостинга и виртуальных частных сетей на основе IP;

4. Специалистами прогнозируется формирование нового рынка услуг удаленной "точечной" сетевой защиты в рамках виртуальных частных сетей на основе IP - его участники будут обеспечивать защиту удаленных компьютерных систем, которые клиенты будут использовать для работы в интернете;

5. Увеличение объемов рынка интеллектуальных услуг сетевой защиты по мере того, как его участники будут превращать адаптивное управление безопасностью сетей из реактивного в предупреждающий процесс, предоставляя пользователям возможность защититься от хакеров, пытающихся проникнуть в их IT-системы;

6. Интеграция систем управления безопасностью с платформами для управления сетями и расширение применения биометрических систем аутентификации для повышения достоверности электронных документов и придания им юридической силы;

7. Возрастет спрос на консалтинговые услуги в части подготовки концепций информационной безопасности, проектирования комплексных информационных систем с учетом требований защиты, построения систем управления информационной безопасностью.

Информационная безопасность относится к числу дисциплин, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс информационных технологий, так и постоянное противоборство нападающих и защищающихся.

Однако только комплексный, систематический, современный подход на уровне каждого пользователя способен успешно противостоять нарастающим угрозам.

Литература

1.http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet;

2. Berinato, Scott. "After the Storm, Reform." CIO Magazine, Dec. 15, 2003.http://www.cio.com/archive/121503/securityfuture.html;

3. Starr, Randy; Newfrock, Jim; & Delurey, Michael. "Enterprise Resilience: Managing Risk in the Networked Economy." Strategy & Business, Spring 2003. http://www.strategy-business.com;

4. Mimoso, Michael S. "Measuring Security ROI a Tall Order." SearchSecurity.com, April 15, 2002. http://www.searchsecurity.com;

5. WordNet. Cognitive Science Laboratory, Princeton University. http://www.cogsci.princeton.edu;

6. ISO (2005) ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management;

7. Mitnick, K.D., Simon, W.L. (2002) The Art of Deception: Controlling the Human Element of Security, Wiley Publishing Inc., Indianalpois, Indiana;

8. Ахтырская Н. О совершенствовании уголовного законодательства Украины в сфере борьбы с киберпреступностью http://www.crime-research.org\articles;

9. А. В. Соколов, О. М. Степанюк «Защита от компьютерного терроризма» - СПб.: БХВ-Петербург; Арлит – 2002. – 496 с;

10. Безопасность информационных технологий. Методология создания систем защиты Домарев В. В. – К.: ООО «ТИД «ДС», 2001. – 688 с;

11. Методы и средства защиты информации / Под ред. Ю. С. Ковтанюка – К.: Издательство Юниор, 2003,. – 504 с.

УДК 621.391:681.3.06

Дудикевич В.Б., Пархуць Л.Т., Хорошко В.О.

ЕВРИСТИЧНІ АЛГОРИТМИ ЗНАХОДЖЕННЯ Р-МЕДІАНИ ГРАФА ДЛЯ ОПТИМІЗАЦІЇ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ МЕРЕЖ

У статті розглянуто питання розвитку теорії графів для оптимізації побудови захищених інформаційних мереж.

Подання структури захищеної інформаційної мережі у вигляді сукупності і способів взаємодії елементів, що входять до її складу, передбачає задання конфігурації мережі зв'язку, через яку проходить обмін інформацією між елементами мережі. При цьому, конфігурація мережі в основному визначається її топологією, просторовим розташуванням джерел та користувачів інформації, а конфігурація і вид мережі зв'язку є важливою структурною характеристикою її [1]. Для певного класу мереж, зокрема, систем зв'язку, систем збереження і розподілу інформації, під структурою мережі переважно розуміють саме конфігурацію мережі зв'язку. Саме таке топологічне представлення структури мережі зв'язку успішно застосовується при рішенні багатьох практичних задач [2,3].

Для оптимізації побудови захищеної інформаційної мережі зручно використовувати апарат теорії графів, який дозволяє реалізувати алгоритм впорядкованого перебору при

пошуку оптимальної структури. Тому розвиток теорії графів стосовно структури інформаційних мереж зв'язку є актуальною задачею [4,5].

Важливе прикладне значення при виборі областей обслуговування і розміщення джерел передачі та отримання інформації в мережі з метою мінімізації трафіку та забезпечення надійного захисту від несанкціонованого доступу має і узагальнення задачі про медіану графа – задача про р-медіану.

У цьому випадку мережу представимо у вигляді сильно зв'язного графа $G=(X,Y)$, $|X|=n$, кожній дузі $u\in U$ якого приписана довжина $l(u)>0$, а кожній вершині $x\in X$ поставлено у відповідність число $q(x)>0$. Припустимо, що для будь-якого шляху $P(x,y)$ (що йде з вершини х в у) визначена його довжина як сума довжин дуг, що йому належать, а для будь-яких вершин $x,y\in X$ знайдено відхилення $d(x,y)$ вершини у від х як довжина найкоротшого шляху $P(x,y)$ з х в у, враховуючи $d(x,y)=0 \quad \forall x\in X$.

Позначимо

$$d(Y,x)=\min_{y\in Y} d(y,x),$$

де $x\in X$, а Y – довільна власна підмножина множини X, і визначимо функціонал

$$F_G(Y)=\sum_{x\in X} d(y,x)\cdot q(x).$$

Необхідно знайти підмножину $Y^*\subset X, |Y^*|=p$, для якої

$$F_G(Y^*)=\min_{Y\subset X,|Y|=p} F_G(Y).$$

При р=1 цю задачу можна вирішити методом перебору варіантів, затративши на це порядку O(n3) дій.

В загальному випадку для знаходження р-медіани графа повний перебір вимагає розгляду $\binom{n}{p}$ варіантів. Оскільки при великих п число варіантів достатньо велике, то для вирішення багатьох практичних задач доцільніше застосовувати евристичні алгоритми.

Нижче будуть запропоновані два такі алгоритми. В обох приведених алгоритмах будується кінцева послідовність підмножин $X^0,X^1,X^2,...,X^k,X^{ii}\subset X$, $|X^i|=p$, $i=1,2,...,k(X^i=\{x^i_j, j=1,2,...,p\})$, де кожну наступну підмножину X^{i+1} отримуємо на підставі попередньої X^i і де як розв'язок береться множина або X^k, або X^{k-1}; за X^0 візьмемо довільну підмножину з X множини $|X^0|=p$.

Перший алгоритм

Отже, опишемо процес побудови множини X^{i+1} при першому алгоритмі в припущенні, що побудована множина X^i.

Множину *X* розбиваємо на класи $X^i_1,X^i_2,...,X^i_p(x^i_j\in X^i_j)$ з дотриманням лише тієї умови, що якщо вершина $x\in X^i_{j_1}$, то $y\neq x$ не може потрапити в клас $X^i_{j_1}$ у разі, коли існує вершина $x^i_{j_2}\in X^i_{j_2}$ така, що $d(x^i_{j_1},y)>d(x^i_{j_2},y)$.

Кожна з множин $X_j^i, j = 1,2,...,p,$ породжує в G зв'язний підграф $G_j^i = (X_j^i, U_j^i), U_j^i \subset U.$ Для кожного з G_j^i вирішуємо аналогічну задачу з $p=1$ і знаходимо одну з вершин $x_j^{i+1} \in X_j^i,$ мінімізуючих $\sum_{z \in X_j^i} q(z)d(x,z).$ Утворюємо множину $X^{i+1} = \{x_j^{i+1}, j = 1,2,...,p\}.$

Якщо $F_G(X^{i+1}) < F_G(X^i),$ то переходимо до побудови множини X^{i+2}, в протилежному випадку процес припиняємо і як рішення беремо множину X (або X^{i+1}).

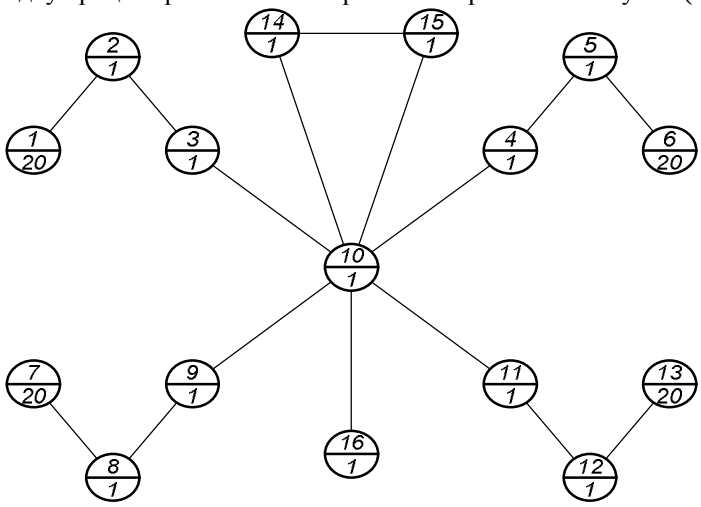


Рис. 1.

Проте зазначимо, що рішення, отримане на основі такого підходу, багато в чому залежить від того, як була вибрана множина X^0. Іноді, при невдалому її виборі рішення може виявитися далеко не оптимальним. Підтвердженням сказаному може служити приклад для неорієнтованого графа, зображеного на рис.1 (випадок орієнтованого сильно зв'язного графа можна отримати, якщо кожне ребро представити як пару протилежно направлених дуг).

В кружечку, що зображає вершину неорієнтованого графа, записаний дріб, чисельником якого є номер вершини, а знаменником – відповідне q(x); довжини l(и) всіх ребер (дуг) передбачаються рівними одиниці.

Неважко переконатися, що якщо як X^0 при $p=4$ вибрати множину {10, 14, 15, 16}, то рішенням, отриманим на основі викладеного алгоритму, виявиться також множина {10, 14, 15, 16}, яка є далеко не оптимальною.

Більшість таких випадків отримуємо через те, що вершини множини X^0 вибираються досить „близько" одна від одної. Тому дуже часто, щоб уникнути таких ситуацій доцільно як X^0 вибирати множину Z^0, що є p-центром графа.

Другий алгоритм

Викладемо тепер другий алгоритм знаходження p-медіани, графа.

Знову припускатимемо, що побудована множина X^i, і покажемо спосіб побудови X^{i+1}:

а) утворюємо множину $Z = X \setminus X^i$;

б) перевіримо, чи виконана умова $Z = ø$. Якщо так, то процес припиняємо і як рішення беремо множину X^i, в протилежному випадку переходимо до в);

в) беремо довільну вершину $x \in Z$;

г) перевіримо, чи існує в множині X^i така вершина y_i що $F_G((X^i U\{x\})\setminus\{y\}) < F_G(X^i)$. Якщо так, то як X^{i+1} беремо $(X^i U\{x\})\setminus\{y\}$ і переходимо до побудови множини X^{i+2}, в протилежному випадку Z замінюємо на $Z\setminus\{x\}$ і переходимо до б).

Розгляд ряду практичних прикладів та їх аналіз на персональному комп'ютері показав, що другий алгоритм в деяких випадках дає рішення краще за перший, проте кількість ітерацій може бути значно більшою. Приведені алгоритми знаходження р-медіани графа в поєднанні з іншими елементами теорії графів дозволяють покращити якість оптимального проектування інформаційних мереж.

Література

1. Кудинов В.А., Пархуць Л.Т., Хорошко В.А. Оптимизация структуры информационной сети. Науково-технічний журнал «Захист інформації», № 3, 2004. – с.44-49;
2. Конеев И.Р., Беляева А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. –752с;
3. Ирвин Дж., Харль Д. Передача данных в сетях: инженерный подход. – СПб.: БХВ-Петербург, 2003. –448с;
4. Пархуць Л.Т., Хорошко В.О. Рішення задачі Вебера для оптимального розміщення комп'ютерів в інформаційній мережі. Збірник наукових праць Національного гірничого університету, № 19, т.2, Дніпропетровськ, НГУ, 2004. – с.157-160;
5. Пархуць Л.Т. Пошук дисперсійної медіани графа. Міжвідомчий збірник наукових праць "Відбір і обробка інформації", 2005, № 23 (99), – с.143-147.

УДК 519.7

Скрыпник Л. В., Ковальчук Л. В.

ТЕСТ ФЕРМА - ЛУКАСА РАСПОЗНАВАНИЯ ПОЛИНОМОВ ГАЛУА НАД КОЛЬЦАМИ ГАЛУА

Предложены вероятностные алгоритмы генерации и распознавания неприводимых полиномов над конечными полями и полиномов Галуа над кольцами Галуа. Показано, что данные алгоритмы могут быть более эффективными, чем классические детерминированные алгоритмы. Оценивается вероятность успеха алгоритмов и среднее время работы до успеха.

Вступление

В данной работе будут рассмотрены алгоритмы распознавания полиномов Галуа над кольцами Галуа. Следует отметить, что полиномы Галуа являются обобщением неприводимых полиномов над конечными полями и играют ту же роль, что и неприводимые полиномы – они используются для построения расширений Галуа колец Галуа так же, как неприводимые полиномы используются для построения расширения полей. Полиномы Галуа и кольца Галуа являются важными объектами, имеющими достаточно много приложений как в теории кодирования ([1]), так и в криптографии, например, в задачах разделения секрета, шифрования, цифровой подписи ([2, 3]).

Эта работа является продолжением работы [4] и в некотором смысле её обобщением. В [4] были построены вероятностные алгоритмы тестирования неприводимости полиномов, являющиеся обобщениями соответствующих вероятностных алгоритмов для тестирования простоты чисел. Было показано, что помимо аналогов тестов Соловея-Штрассена и Миллера-Рабина, для тестирования неприводимости полиномов может быть использован тест Ферма. Были представлены условия, при которых вероятность ошибки

данного теста не превосходит ½. Также было показано, что для тестирования неприводимости полиномов достаточно больших степеней (порядка 100 и более), приведенные вероятностные тесты являются более быстродействующими, чем классический детерминированный алгоритм. При этом вероятность ошибки тестов может быть сделана как угодно малой (например, порядка 2×10^{-10}).

Все эти тесты оказываются применимыми и для распознавания полиномов Галуа над кольцами Галуа.

В настоящей работе построено несколько дополнительных тестов, которые также являются вероятностными и могут использоваться как для проверки неприводимости полинома над конечным полем, так и для распознавания полинома Галуа над кольцом Галуа.

Основные определения и теоретические сведения

Введем ряд определений и обозначений, а также приведём перечень основных теоретических сведений, которые будут использоваться в дальнейшем изложении.

Определение 1 ([1])

Кольцом Галуа называется конечное коммутативное кольцо R с единицей e, в котором множество всех делителей нуля имеет вид pR для некоторого простого числа p.

Кольцо Галуа определено однозначно (с точностью до изоморфизма) количеством элементов и характеристикой.

Пусть R - кольцо Галуа характеристики p^n. Соответствующее поле $\overline{R} = R/pR$ называется его полем вычетов. Естественный эпиморфизм колец $R \to \overline{R}$ индуцирует эпиморфизм соответствующих колец полиномов

$$R[X] \to \overline{R}[X] \cong R[X]/pR[X].$$

Образ полинома $f(x) \in R[X]$ при этом эпиморфизме обозначим $\bar{f}(x) \in \overline{R}[X]$.

Определение 2 ([1])

Унитарный полином $f(x) \in R[X]$ называется полиномом Галуа, если $\bar{f}(x) \in \overline{R}[X]$ неприводим над $\overline{R}$.

Следовательно, проверка того, является ли данный полином полиномом Галуа, сводится к проверке неприводимости соответствующего полинома.

Как уже упоминалось, полиномы Галуа играют важную роль при построении расширений колец Галуа. А именно, справедлива следующая теорема.

Теорема 1 ([1])

Пусть R – кольцо Галуа характеристики p^n, состоящее из q^n элементов, и $f(x) \in R[X]$ – полином Галуа, $\deg f = m$. Тогда кольцо $S = R[X]/f(x)$ является кольцом Галуа с параметрами $char\ S = p^n$, $|S| = q^{mn}$.

В этом случае кольцо S называется расширением Галуа кольца R.

Также в дальнейшем понадобятся некоторые сведения из теории чисел.

Теорема 2 (Теорема Лукаса)

Пусть $n \geq 3$ – целое число. Тогда n простое в том и только в том случае, если $\exists a \in Z$ такое, что

1) $a^{n-1} \equiv 1 (mod\ n)$;

2) для любого простого делителя q числа $n-1$ выполнено: $a^{\frac{n-1}{q}} \equiv 1 (mod\, n)$.

Следствием данной теоремы является тест Лукаса для проверки простоты числа.

Основные результаты

В этом разделе сохраняются все обозначения предыдущих разделов.

Теорема (обобщённая теорема Лукаса)

Пусть $f(x) \in R[X]$, где R - кольцо Галуа характеристики p^n, $\overline{R} = F_q$ - соответствующее поле вычетов, $\overline{f}(x) \in F_q[X]$, $deg\ \overline{f}(x) = n$. Если существует полином $\overline{g}(x) \in F_q[X]$, такой, что

$$\overline{g}(x)^{q^n-1} \equiv 1 (mod\, \overline{f}(x)), \qquad (1)$$

но для любого простого s, делящего $q^n - 1$, выполнено:

$$\overline{g}(x)^{\frac{q^n-1}{s}}\ mod\ \overline{f}(x) \neq 1, \qquad (2)$$

то $f(x)$ - полином Галуа.

Доказательство:

Обозначим $\Phi_q(f)$ обобщённую функцию Эйлера в кольце $F_q[X]$. Как известно [2],

$$\Phi_q(f) = q^n \prod_{i=1}^{r} \left(1 - \frac{1}{q^{n_i}}\right), \qquad (3)$$

где $f = f_1^{\alpha_1} \ldots f_r^{\alpha_r}$, $deg\, f_i = n_i$, $i = \overline{1,r}$.

Обозначим

$$e = ordg(x) \text{ в } {F_q[X]}/{f(x)}.$$

Из (1) следует, что $e \mid q^n - 1$, а из (2) следует, что e не делит никакие делители числа $q^n - 1$. Следовательно, $e = q^n - 1$. Но, по обобщённой теореме Эйлера, $ord\ e \mid \Phi_q(f)$, значит, $q^n - 1 \mid \Phi_q(f)$. Это возможно только в том случае, когда в (3) выполнено $r = 1$ и $\Phi_q(f) = q^n - 1$, а это, в свою очередь, возможно только в том случае, если $f(x)$ неприводим.

Следствие

Тест Ферма-Лукаса распознавания полиномов Галуа

Вход: полином $f(x) \in R[X]$.

1. Вычислить соответствующий полином $\overline{f}(x) \in F_q[X]$ и его степень $n = deg\, f(x)$.

2. Вычислить $\overline{f}'(x)$ и $d_1 = (\overline{f}'(x)\, \overline{f}(x))$. Если $d_1 \neq 1$, то $f(x)$ не является полиномом Галуа. Иначе переходим к п.3.

3. Случайным образом сгенерировать полином

$$g(x) \in F_q[X], \quad deg\, g < n,\ g(x) \equiv 0,\ g(x) \equiv 1.$$

4. Вычислить $d_2 = (g(x), \overline{f}(x))$. Если $d_2 \neq 1$, то $f(x)$ не является полиномом Галуа. Иначе переходим к п.5.

5. Проверить выполнение условия

$$g(x)^{q^n-1} \equiv 1 (\mathrm{mod}\, \bar{f}(x)). \qquad (4)$$

Если условие не выполнено, то $f(x)$ не является полиномом Галуа. Иначе переходим к п.6.

6. Вычислить $s_1,\ldots,s_k$ - все (разные) простые делители числа q^n-1.
7. Проверить выполнение условий

$$g(x)^{\frac{q^n-1}{s_i}} \mod \bar{f}(x) \neq 1, \quad \forall i = \overline{1,k}.$$

Если все условия выполнены, то $f(x)$ является полиномом Галуа. В противном случае тест не принял никакого решения.

Замечания

Тест Лукаса является вероятностным Лас-Вегас алгоритмом распознавания полиномов Галуа, однако данный алгоритм также можно рассматривать как вероятностный алгоритм генерации полиномов Галуа.

Если $f(x)$ является полиномом Галуа, то вероятность неудачи данного теста (т.е. вероятность неопределённого ответа) равна $1-\frac{\varphi(q^n-1)}{q^n-1}$. В этом случае среднее количество шагов до успеха не превосходит $6\ln(n\ln q)$. На практике обычно достаточно сделать $12\ln(n\ln q)$ шагов.

Алгоритм использует порядка kn делений с остатком и является более выгодным, чем классический детерминированный алгоритм в случае, когда число q^n-1 легко разложить на множители и когда $k << n$. Если число q^n-1 простое (а для этого необходимо выполнение условий $q=2$ и n - простое), то п.п. 6 и 7 теста Лукаса являются лишними, а в п.5 в случае выполнения условия (3) делаем вывод о том, что полином является полиномом Галуа.

Частным случаем приведенного теста является хорошо известный алгоритм проверки примитивности полинома над конечным полем.

Как уже упоминалось, в [4] были введены понятия псевдонеприводимых полиномов Ферма, Эйлера и сильно псевдонеприводимых. Интересно заметить следующее. Многие свойства псевдонеприводимых полиномов являются аналогами свойств соответствующих псевдопростых чисел. Однако методы доказательства данных свойств для полиномов существенно отличаются от доказательств аналогичных свойств для чисел. Также, на наш взгляд, является интересным следующий вопрос: изучение свойств оснований, по которым полиномы являются псевдонеприводимыми, и сравнение этих свойств со свойствами оснований, по которым числа являются псевдопростыми.

Литература

1. Нечаев А. Код Кердока в циклической форме // Дискретная математика, т.1. – вып.4. – 1989. – с.123-139;
2. Lidl R., Niederrieter H. Finite fields. – London: Addison-Wesley Publishing Company, 1983.-819p;
3. Koblitz N. A Course of Number Theory and Cryptography.- Berlin: Springer, 1994.-231p;
4. Ковальчук Л. Псевдонеприводимые полиномы. Вероятностное тестирование неприводимости // Кибернетика и системный анализ, №4, 2004г., с. 168-176.

УДК 681.5.015:004.056.57

Айрапетян Р.А.

НОВЫЕ МЕТОДЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ НЕЛЕГАЛЬНОГО ИСПОЛЬЗОВАНИЯ

В статье проведен обзор и классификация существующих угроз и методов защиты программного обеспечения (ПО) от нелегального использования. На основе разработанных методов с использованием сетей Петри и теории графов создано программное средство защиты ПО для карманных персональных компьютеров (КПК).

Проблема защиты программного обеспечения от нелегального использования актуальна.

За последнее время доля пиратского ПО на рынке достигла астрономических масштабов. Так на Украине легально приобретенной является только каждая десятая копия программного продукта. Современные системы защиты ПО от нелегального использования позволяют сдерживать пиратский натиск, однако каких-либо значительных успехов в качестве защищенности не достигла ни одна из существующих методик защиты.

Сейчас широко используются следующие виды защит:

- использование недокументированных особенностей среды;
- использование отладочных регистров [1];
- навесные (аппаратные) защиты;
- использование криптографии;

и т.п.

Однако каждый из этих методов можно, так или иначе, обойти, все является лишь вопросом затраченного времени и материальных средств.

На рис. 1 приведена классификация угроз нелегального использования ПО, а также методы защиты от этих угроз.

Детализация методов защиты ПО приведена на рис. 2. Расшифруем некоторые блоки.

Методы привязки к носителю – это использование нестандартных параметров форматирования, специфических характеристик, информации о промежутках, о bad-секторах, физических дефектов на носителях, разноскоростных дорожек, нанесение физических меток, уникальной маркировки и т.п. [18].

Простые устройства шифрования/дешифровки – позволяют выполнять простые функции аутентификации наряду с шифрованием/дешифровкой данных.

Автономные, высокоинтеллектуальные устройства – smart-card, K-medulla. Позволяют хранить и выполнять алгоритмы разработчика.

SMC (самомодифицирующийся код) – код, который в процессе выполнения модифицирует сам себя.

Метаморфинг – необратимое преобразование кода рабочей программы посредством расширяющей замены оригинальных инструкций блоками других инструкций.

Exceptions – использование механизмов исключений, например SHE.

Использование отладочных регистров DR0…DR7 – запись в отладочные регистры «мусора».

Debug API – использование отладочных функций среды. В Windows – WaitForDebugEvent/ContinueDebugEvent. IsDebuggerPresent API – в среде ОС Windows позволяет определить наличие запущенного отладчика.

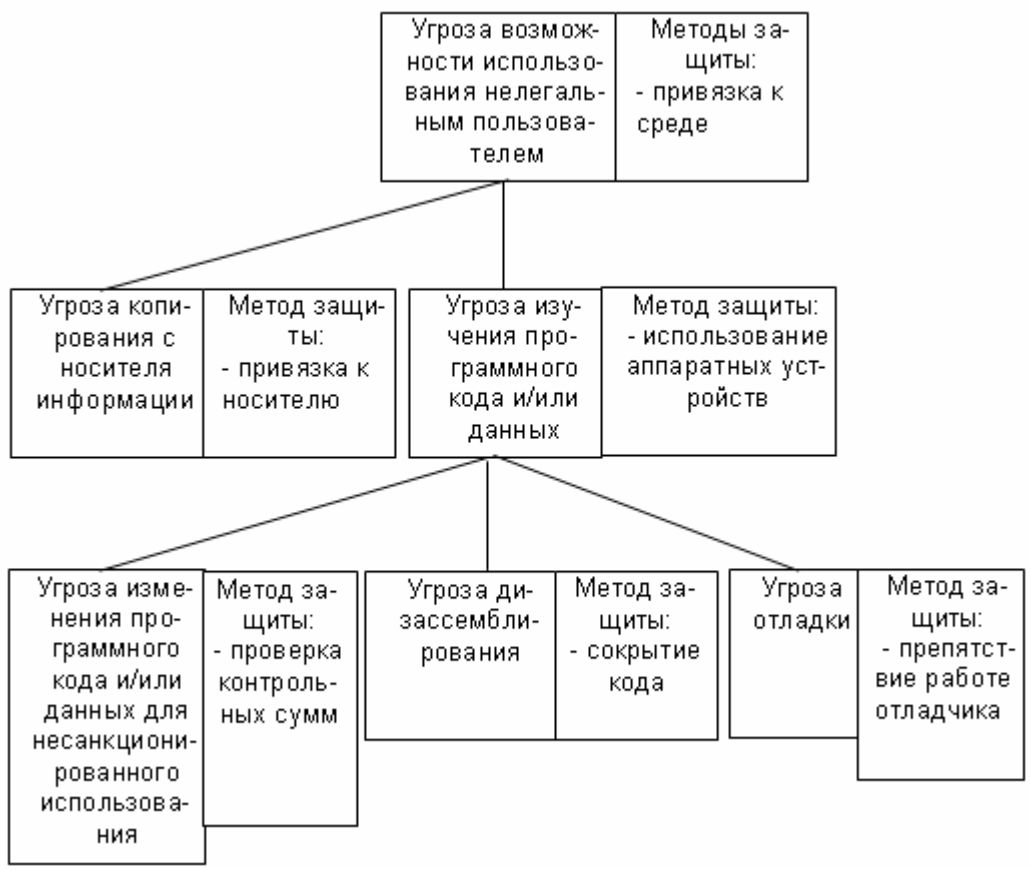


Рис. 1. Угрозы нелегального использования ПО и методы защиты.

Ранее нами был предложен метод защиты программного обеспечения с помощью сетей Петри [1]. Суть метода в том, что к защищаемой программе добавляется защитный фрагмент прогаммного кода, который реализует запуск специально разработанной сети Петри. Эта сеть содержит несколько позиций p, которые используются для задания начальной маркировки, - «начальных» позиций. В них перед запуском сети записывается введенный пользователем ключ (количество таких позиций равно количеству битов в ключе). В сети есть переход t, который сработает тогда и только тогда, когда введен правильный ключ, т.е. переход «решающий». При использовании сетей Петри достаточно легко построить сеть с нужными свойствами, а обратная задача решается трудно (фактически, полным перебором). Предложенный метод защиты программного обеспечения дополняет известные методы защиты программ от отладки и в то же время имеет некоторые преимущества, прежде всего, потому что при работе защитного механизма используется многопоточность, что значительно усложняет отладку. Каждый поток реализует один переход сети, и многопоточность для решения такой задачи, как выполнение сети Петри, естественна.

Также для построения системы защиты нами предложены методы, использующие алгоритмы на графах. Для них прямая задача решается относительно легко, а обратная задача является NP-полной, т.е. полиномиальный алгоритм не известен [2]. Например, защита, использующая задачу обхода Гамильтонова пути в ориентированном графе [3]. При этом каждая вершина графа представляется в виде фрагмента кода, а ребра – переходами между этими фрагментами. При вводе правильного ключа обход графа происходит по Гамильтонову пути из начальной вершины в конечную, после чего происходит переход на точку входа в защищаемую программу.

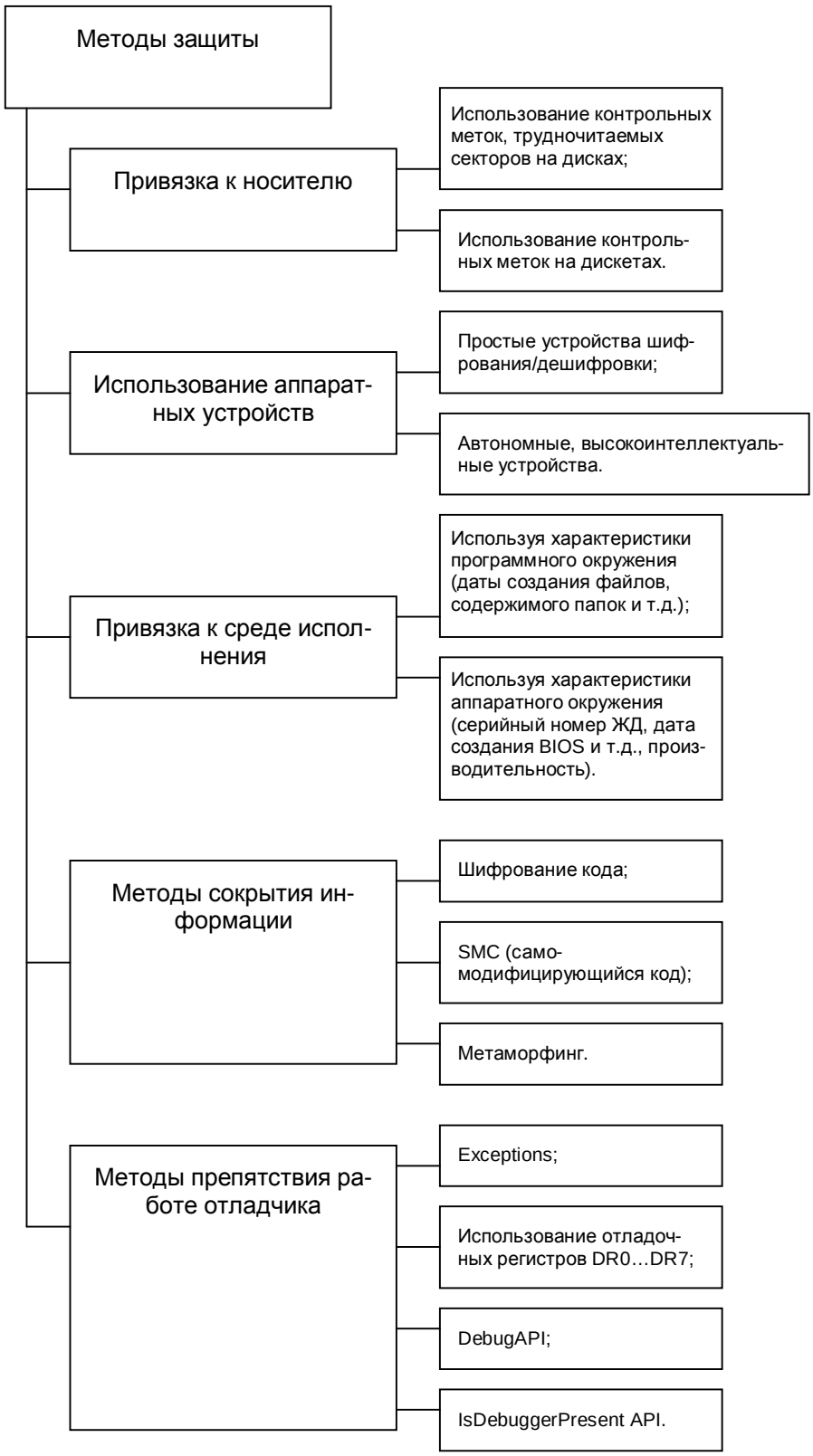


Рис. 2. Детализация существующих методов защиты ПО.

Разработанные методы были реализованы в программном продукте защиты ПО diProtector [4] для КПК. В настоящее время КПК приобретают все большую популярность у пользователей во всем мире.

Как и на рынке настольных компьютеров, проблема взлома и нелегального использования ПО существует и здесь. На фоне отсутствия каких-либо автоматических упаковщиков/протекторов бурно развивается распространение взломанных копий ПО. Представлены два продукта: diProtector (содержит все механизмы для обеспечения защиты от реверсной инженерии, упаковщик, генератор лицензий и т.п.), а также облегченный вариант – diPacker (содержит функциональность упаковщика с минимальными защитными функциями).

К защитным механизмам diProtector-а можно отнести:

- невозможность анализа дизассемблированного кода защищенного приложения;
- обнаружение и защита от отладчиков eVC, eVB и др. ;
- защита от трассировки под отладчиком;
- защита таблицы импорта приложения;
- защита точки входа в программу;
- защита от модификации кода (создания патчей);
- защищенная работа с реестром;
- компрессия ресурсов, данных и кода исполнимого файла;
- внешний модуль генератора ключей.

Вся система защиты реализована в виде нескольких модулей. Главный модуль запускается на настольном x86-совместимом ПК.

Первый шаг – выбор программы для защиты. Это должен быть оригинальный исполнимый файл той платформы, для которой осуществляется защита. Далее для защищаемого приложения можно задать уникальное имя программы (Product name), установить срок работы незарегистрированной копии (Trial Period), изменить текст напоминания о регистрации (Nag message), а также изменить сообщение об истекшем сроке использования (Expiration message), после чего осуществляется защита приложения.

В один исполнимый файл diProtector-а включены все необходимые для осуществления защиты ПО на различных платформах модули. В настоящее время разработан модуль защиты ПО для ARM-процессоров, работающих под управлением ОС Windows CE (как самого распространенного на сегодняшний день).

В ближайшее время планируется разработка модулей для защиты ПО на всех популярных процессорах (SH4, MIPS), а также под платформы Symbian, Palm, Blackberry и др. Также компания diProtector Software начала сотрудничество с пионерами рынка защиты ПО на настольных компьютерах – компанией Bitsum Technologies [5].

Литература

1. В.М.Рувинская, Р.А.Айрапетян, Е.Л.Беркович. Метод защиты программного обеспечения с помощью встроенных сетей Петри //Труды Одес. политехн. ун-та. —Одесса, 2005. —№ 1 (23). — с.62—67;
2. Э.Рейнгольд, Ю.Нивергельт, Н.Део. Комбинаторные алгоритмы. Теория и практика. Пер. с англ., «Мир», 1980;
3. Беркович Е.Л., Айрапетяна Р.А., Беркович Л.В. Метод защиты программного обеспечения на основе графов // Искуственный интеллект, 3’2005;
4. diProtector Software - http://www.diprotector.com;
5. Bitsum Technologies – http://www.bitsum.com.

УДК 681.3

Рыбальский О.В.

К ВОПРОСУ О ФРАКТАЛЬНОСТИ АНАЛОГОВЫХ СИГНАЛОВ, ПОДВЕРГНУТЫХ ЦИФРОВОЙ ОБРАБОТКЕ

В статье рассмотрены результаты анализа влияния расхождения частот дискретизации различных цифровых устройств, участвующих в процессе цифровой обработки, и операции стробирования фрагментов на нарушения фрактальности аналоговых сигналов, подвергнувшихся такой обработке

Введение

В течение последних пяти лет автором были разработаны основы теории выявления следов цифровой обработки цифровых и аналоговых сигналограмм [1–5]. Данная разработка относилась к системам защиты информации, в частности, к выявлению следов внешних вмешательств в информацию, содержащуюся в сигналограммах, произведенных путем несанкционированных внешних воздействий, произведенных с помощью цифровых технологий.

Называя разработку основами теории, автор подразумевал, что она (теория) должна развиваться. Как одно из направлений ее дальнейшего развития предполагалось исследование возможности гарантированного[1] выявления мест цифрового монтажа в обработанных в цифровой форме сигналограммах. Данная работа открывает новый аспект развития этой теории с целью создании методов и средств выявления конкретных мест монтажа сигналограмм, обработанных с использованием цифровых технологий.

Эта статья является постановочной, с той точки зрения, что в ней не рассмотрены задачи реализации предложенных идей.

В то же время она опирается на проведенные ранее разработки. В первую очередь это относится к концепции цифровой обработки (ЦО) сигналограмм, принятой в рамках данной теории, согласно которой для обработки любой сигналограммы необходимо использовать не менее двух различных цифровых устройств (например, цифрового диктофона и ПЭВМ) [3]. Кроме того, она опирается на принятый при разработке системный подход к процессу обработки сигналограмм и модели их обработки, рассмотренные ранее в рамках разработанной теории.

Основные положения

Как показано в [3], имеется весьма ограниченное количество способов обработки как аналоговой, так и цифровой сигналограммы в цифровой форме.

При этом автор, пользуясь системным подходом к процессу ЦО сигналограмм, расчленил этот процесс на различные операции. Отдельно была выделена и рассмотрена операция ввода/вывода сигналограммы, необходимая на этапе ввода сигналограммы в ПЭВМ для ее обработки и операция вывода обработанной сигналограммы при ее перезаписи из машины, с последующим воспроизведением переписанной обработанной сигналограммы.

Так же и операции, связанные непосредственно с обработкой сигналограмм, рассматривались отдельно [2,5]. Такой подход позволил выявить источники возникновения следов ЦО сигналограмм.

Однако, в методах и средствах выявления следов такой обработки, разработанных на основании проведенного теоретического осмысления процессов, происходящих при ЦО сигналограмм, имеется существенный пробел, – мы можем быстро и гарантированно установить наличие или отсутствие следов этой обработки, но оперативное выявление мест монтажа требует значительных временных затрат.

[1] Под гарантией выявления, как следов цифровой обработки, так и мест монтажа, автор подразумевает достаточность теоретического обоснования и достаточность разрешающей способности методов и средств их выявления.

Возможно, эту задачу можно решить путем выявления нарушения фрактальности аналоговых сигналов, подвергнувшихся ЦО. Но предварительно следует установить ряд фактов, на которые можно будет опираться в последующих рассуждениях.

Во-первых, следует понять, а являются ли преобразованные в цифровую форму (т.е. прошедшие через систему аналого-цифро-аналогового преобразования) аналоговые сигналы фрактальным образованием.

И, во-вторых, определить, а происходит ли нарушение их фрактальности при дополнительной ЦО. А эта обработка связана, во-первых, с прохождением сигналов через разные цифровые устройства, и, во-вторых, с использованием операции стробирования фрагментов, неизбежно применяемой в процессе цифрового монтажа [2]. Дополнительным источником таких нарушений может служить и операция преобразования форматов представления информации в цифровой форме в разных устройствах, используемых при ЦО [2,3].

Установлению этих фактов и посвящена данная работа. Как известно, аналоговый сигнал, прошедший систему аналого-цифро-аналогового преобразования (АЦАП) на выходе цифро-аналогового преобразователя (ЦАП) может быть представлен в виде:

$$s_2(t) = \sum_{n_1=-\infty}^{\infty} \mathrm{rect}\left(\frac{t-n_1T_1}{\Delta_1}\right) A_m \cos\omega_0(n_1T_1) = \sum_{n_1=-\infty}^{\infty} \mathrm{rect}\left(\frac{t-n_1T_1}{T_1}\right) A_m \cos\omega_0(n_1T_1), \quad (1)$$

где n_1 – номер отсчета (выборки) сигнала на выходе АЦАП;

T_1 – шаг дискретизации в АЦАП;

A_m – амплитуда аналогового сигнала;

Δ_1 – длительность импульса выборки в АЦАП [1].

Спектр этого сигнала представляется как

$$S_3(j\omega) == \frac{A_m\omega_{Д1}}{\omega} \sin\omega\frac{T_1}{2} \sum_{k_1=-\infty}^{\infty} \left[\delta(\omega-\omega_0-k_1\omega_{Д1}) + \delta(\omega+\omega_0-k_1\omega_{Д1})\right], \quad (2)$$

где $\omega_{Д1}$ – частота дискретизации в АЦАП, $\omega_{Д1} = \frac{2\pi}{T_1}$ [1].

Введем ограничение на максимальное верхнее значение частоты аналогового сигнала в соответствии с теоремой Котельникова, т.е. предположим, что частота аналогового сигнала может изменяться в пределах от 0 до $\omega Д/2$. Тогда выражение (1) в предельном случае $\omega_Д/2$ можно записать как

$$s_2(t) = \sum_{n_1=-\infty}^{\infty} \mathrm{rect}\left(\frac{t-n_1T_1}{T_1}\right) A_m \cos\frac{\omega_Д}{2}(n_1T_1) = \sum_{n_1=-\infty}^{\infty} \mathrm{rect}\left(\frac{t-n_1T_1}{T_1}\right) A_m \cos\frac{4\pi}{T_1}(n_1T_1), \quad (3)$$

где $\omega_0=\omega_Д/2$.

Из анализа выражения (3) видно, что в случае уменьшения частоты сигнал будет представлен в виде большего числа выборок, приходящихся на его период, но при этом длительность выборки сохраняется постоянной. Но это, в свою очередь, означает, что при уменьшении частоты сигнала снижается величина разности между уровнями двух соседних выборок при сохранении их длительности, т.е. имеется факт подобия, что говорит о фрактальной структуре такого сигнала.

Несложно предположить, что эталоном его фрактального представления будет прямоугольник, образованный длиной тактового интервала на выходе ЦАП, и величиной разности уровней сигналов, выбранных в двух соседних отсчетах, определяемой частотой исходного аналогового сигнала.

Таким образом, следует принять гипотезу о том, что аналоговый сигнал, прошедший через систему АЦАП, имеет на выходе ЦАП фрактальную структуру.

С учетом того, что в основах теории выявления следов цифровой обработки сигналограмм уже было принято шесть гипотез, доказанных затем аналитически и экспериментально [4], назовем эту гипотезу **гипотезой 7** и сформулируем ее следующим образом:

– аналоговый сигнал, прошедший через систему АЦАП, имеет на выходе ЦАП фрактальную структуру, а ее эталоном является прямоугольник, образованный длиной тактового интервала на выходе ЦАП, и величиной разности уровней сигналов, выбранных в двух соседних отсчетах, определяемой частотой исходного аналогового сигнала.

Как было доказано в основах теории, следы ЦО образуются в сигналограмме за счет расхождения истинных значений частот дискретизации различных устройств, принимающих участие в процессе цифровой обработки сигналов, и за счет расхождения размещения на статической характеристике (СХ) преобразования аналого-цифровых преобразователей (АЦП) и ЦАП уровней с дифференциальной нелинейностью и немонотонностью СХ (ДНСХ и НСХ соответственно) этих устройств [2]. Рассмотрим влияние различия частоты дискретизации устройств, участвующих в процессе ЦО, на изменение фрактальности обработанных сигналов.

Воспользуемся моделями ввода/вывода информации при ЦО, рассмотренными в [1]. Начнем с аналогового ввода/вывода. Упрощенная схема прохождения информации через цепочку АЦП и ЦАП устройств, участвующих в процессе обработки, показана на рис. 1. Полная схема ее прохождения приведена в [1]. При этом предполагалось, что первичная сигналограмма записывалась и переписывалась после обработки на одном и том же аппарате.

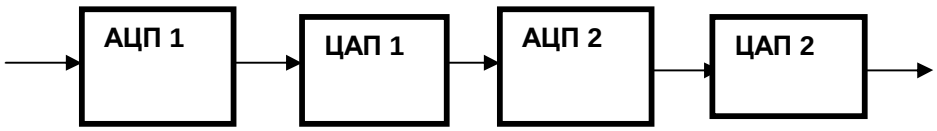


Рис. 1. Упрощенная схема прохождения информации через цепочку АЦП и ЦАП устройств, участвующих в процессе обработки.

Как показано в [1], сигнал на выходе АЦП второго устройства, в этом случае определяется выражением

$$s_3(t)=\sum_{n_1=-\infty}^{\infty}\sum_{n_2=-\infty}^{\infty}\mathrm{rect}\left(\frac{t-n_2T_2}{\Delta_2}\right)\mathrm{rect}\left(\frac{n_2T_2-n_1T_1}{T_1}\right)A_m\cos\omega_1(n_1T_1), \quad (4)$$

где

n_1 – номер отсчета (выборки) сигнала на выходе АЦАП первого устройства;

T_1 – шаг дискретизации в АЦАП первого устройства;

A_m – амплитуда аналогового сигнала;

Δ_2 – длительность импульса выборки в АЦП второго устройства;

n_2 – номер отсчета (выборки) сигнала на выходе АЦАП второго устройства;

T_2 – шаг дискретизации в АЦАП второго устройства;

А тогда сигнал на выходе ЦАП второго устройства определится как:

$$s_3(t)=\sum_{n_1=-\infty}^{\infty}\sum_{n_2=-\infty}^{\infty}\mathrm{rect}\left(\frac{t-n_2T_2}{T_2}\right)\mathrm{rect}\left(\frac{n_2T_2-n_1T_1}{T_1}\right)A_m\cos\omega_1(n_1T_1). \quad (5)$$

Как видно из (5), в этом случае нарушаются пропорции эталона фрактальности представления сигнала и возрастает порядок этого представления, иначе говоря, искажается форма сигнала. Разумеется, это сказывается и на спектре обработанного сигнала, что и

показано в [1], а так же использовано в разработанной теории, где была установлена закономерность возрастания количества спектральных компонент в обработанном сигнале.

Итак, при аналоговом вводе/выводе сигналов, используемом в процессе ЦО, изменяются пропорции эталона и возрастает порядок их фрактального представления.

Для случая ввода/вывода информации в цифровой форме упрощенная схема прохождения информации через цепочку АЦП и ЦАП устройств, участвующих в процессе обработки, показана на рис. 2. При этом предполагается, что процесс обработки представляется в виде синтезации в машине заданного текста по введенному в нее в цифровой форме образцу голоса (обозначена как АЦАП 2). Синтезированный текст в цифровой форме вводится в цифровой аппарат записи-воспроизведения информации. Предполагается, что для записи образца голоса и перезаписи синтезированного сообщения используется один и тот же аппарат (обозначается, как АЦП 1 и ЦАП 1). Более подробная схема прохождения информации представлена в [1].

Рис. 2. Упрощенная схема прохождения информации через цепочку АЦП и ЦАП устройств, участвующих в процессе обработки, при вводе/выводе информации в цифровой форме.

Как показано в [1], перезаписанный и воспроизведенный сигнал на выходе ЦАП аппарата записи-воспроизведения представляется как

$$s_{5d}(t) = \sum_{n_2=-\infty}^{\infty} \mathrm{rect}\left(\frac{t - n_2 T_1}{T_1}\right) A_m \cos\omega_1 (n_2 T_1), \qquad (6)$$

где

T_1 – тактовый интервал в ЦАП первого устройства,

A_m – амплитуда аналогового сигнала,

n_z – номер отсчета (выборки) сигнала второго устройства при его синтезации,

T_2 – тактовый интервал в АЦАП второго устройства.

Проанализируем формулу (6). Из нее вытекает, что сигнал с частотой ω_1 был синтезирован в компьютере со своим тактовым интервалом T_1 при числе выборок n_1. Это количество выборок было записано в цифровой форме в аппарате записи и воспроизведено на выходе его ЦАП. Но тактовый интервал T_2 этого аппарата отличается от тактового интервала машины. Он может быть больше или меньше того интервала, с которым синтезировался сигнал. А это, в свою очередь, означает, что пропорции эталона фрактального представления сигнала на выходе ЦАП аппарате записи-воспроизведения изменятся относительно эталона сигнала, не подвергавшегося ЦО.

Таким образом, в случае цифрового ввода/вывода информации для ее ЦО способом синтезации по заданному образцу голоса, изменяются пропорции эталона фрактального представления сигнала.

Рассмотрим влияние на фрактальность сигналов операции стробирования фрагментов, неизбежно используемую при монтаже сигналограммы. В [3,6] показано, что в результате выделения фрагмента цифровой сигналограммы для последующей компиляции в новом файле, выделенный и компилируемый сигнал можно записать в виде:

$$s_{11d}(t) = \mathrm{rect}\left(\frac{t}{\Delta_2}\right) \sum_{n_1=-\infty}^{\infty} \mathrm{rect}\left(\frac{t - n_1 T_1}{T_1}\right) A_m \cos\omega_0 (n_1 T_1), \qquad (7)$$

где Δ_2 – длительность вырезанного участка $(\Delta_2 > T_1)$.

Перепишем формулу (7), записав ее как

$$s_{11d}(t) = \sum_{n_1=-\infty}^{\infty} \mathrm{rect}\left(\frac{t}{\Delta_2}\right) \cdot \mathrm{rect}\left(\frac{t - n_1 T_1}{T_1}\right) A_m \cos\omega_0 (n_1 T_1), \qquad (8)$$

Из формулы (8) видно, что сигнал стробирования влияет на каждую выборку стробируемого сигнала. При этом на уровне младшего разряда оцифровки искажается его форма, что приводит, во-первых, к нарушению пропорциональности эталона и, во-вторых, к повышению порядка фрактального представления сигнала (происходит "дробление" поверхности ступеньки отсчета сигнала).

Это подтверждается появлением новых спектральных компонент в обработанном сигнале, что использовано при построении метода и средства выявления следов ЦО и показано в [3,6].

Выводы

1. Аналоговый сигнал, прошедший через систему АЦАП, имеет на выходе ЦАП фрактальную структуру, а ее эталоном является прямоугольник, образованный длиной тактового интервала на выходе ЦАП, и величиной разности уровней сигналов, выбранных в двух соседних отсчетах, определяемой частотой исходного аналогового сигнала.

2. При аналоговом вводе/выводе сигналов, используемом в процессе цифровой обработки, изменяются пропорции эталона и возрастает порядок их фрактального представления.

3. При цифровом вводе/выводе информации для ее цифровой обработки способом синтезации по заданному образцу голоса, изменяются пропорции эталона фрактального представления сигнала.

4. Использование операции стробирования для выделения и компиляции фрагментов приводит к нарушению пропорциональности эталона и к повышению порядка фрактального представления сигнала.

Литература

1. Рыбальский О.В., Жариков Ю.Ф. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе. – К.: НАВСУ, 2003. – 300 с;
2. Рибальський О.В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі. – К.: НАВСУ, 2004. – 167 с;
3. Рыбальский О.В. Анализ возможных цифровых и аналоговых способов подделки фонограмм и требований к анализаторам для выявления их следов // Захист інформації. – К.: КМУЦА, 2004. – Спеціальний випуск. – С. 44–48;
4. Рыбальский О.В. К экспериментальной проверке достоверности положений теории выявления следов цифровой обработки фонограмм // Реєстрація, зберігання та обробка даних. – К. – 2004. – Т.6, № 3. – С. 85–98;
5. Рыбальский О.В. Модели нестандартных способов обработки цифровых фонограмм // Реєстрація, зберігання і обробка даних. – К. – 2003 – Т. 5, № 4. – С. 25–32;
6. Рибальський О.В., Богданов О.М., Геранін В.О. Методологія розробки основ теорії виявлення слідів цифрової обробки фонограм та її деякі аспекти // Правове, нормативне, метрологічне забезпечення систем захисту інформації в Україні. – 2004. – Вип. 8. – С. 24–28.

Каток В.Б., Гордиенко С.Б.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЯХ СВЯЗИ

В последнее время одним из наиболее перспективных и развивающихся направлений построения сети связи в Украине и в мире являются волоконно-оптические линии связи (ВОЛС). В области систем передачи информации с большой информационной емкостью и высокой надежностью работы ВОЛС не имеют конкурентов. Это объясняется тем,

что они значительно превосходят проводные по таким показателям, как пропускная способность, длина регенерационного участка, а также помехозащищенность.

Считается, что ВОЛС, в силу особенностей распространения электромагнитной энергии в оптическом волокне (ОВ), обладают повышенной скрытностью. Это объясняется тем, что оптическое излучение, являющееся носителем информации, распространяется в ОВ согласно закону полного внутреннего отражения, а за ОВ электромагнитное излучение экспоненциально спадает. Участки, где возможна утечка электромагнитного излучения и несанкционированный съем информации (НСИ), относительно малочисленны, «классическими» радиотехническими методами (приемо-передающая аппаратура, регенерационные пункты) изучены и локализованы. По этой причине эти участки сравнительно легко могут быть поставлены под контроль.

Рассмотрим ВОЛС и ее основные параметры (рис. 1) [1, 2].

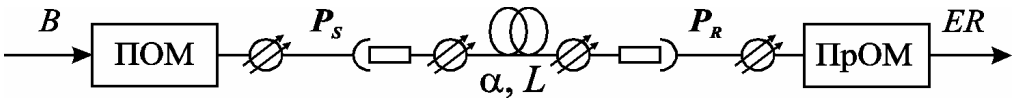


Рис. 1. Структурная схема ВОЛС.

В состав ВОЛС входит: передатчик оптической мощности (ПОМ) с выходной мощностью Ps, приемник оптической мощности (ПрОМ), обеспечивающий при входной оптической мощности Pr прием и преобразование оптического сигнала с заданным коэффициентом ошибок ER, и волоконно-оптический линейный тракт (ВОЛТ), имеющий длину L и затухание α. Приемо-передающая пара (ПОМ-ПрОМ) имеет энергетический потенциал Е, который зависит от мощности ПОМ, спектральной плотности шума, чувствительности ПрОМ и скорости передачи В. Заданный энергетический потенциал Е ограничивает длину волоконно-оптического тракта L, затухание которого (с учетом эксплуатационного запаса) не должно превосходить энергетический потенциал Е. Очевидно, что для того, чтобы осуществить НСИ, необходимо добраться до самого волокна ВОЛТ и каким-либо образом считать информацию, сняв часть оптической мощности P_{RX} через разветвитель оптический (РО) в точке с мощностью P_X , внеся потери α_X и не нарушая при этом функционирование канала связи (рис. 2).

Рассмотрим воздействие на параметры ВОЛТ съема информации при пассивном локальном не санкционированном доступе (НД) [1, 2]. Введем следующие обозначения: P_S , P_R , P_X , P_{RX} - мощности оптических сигналов, соответственно на выходе ПОМ (в начале ВОЛТ), на входе ПрОМ (в конце ВОЛТ), в месте съема информации и на входе ПрОМ НД, α [дБ/км] - затухание ВОЛТ, Е - энергетический потенциал приемопередатчиков ВОЛС.

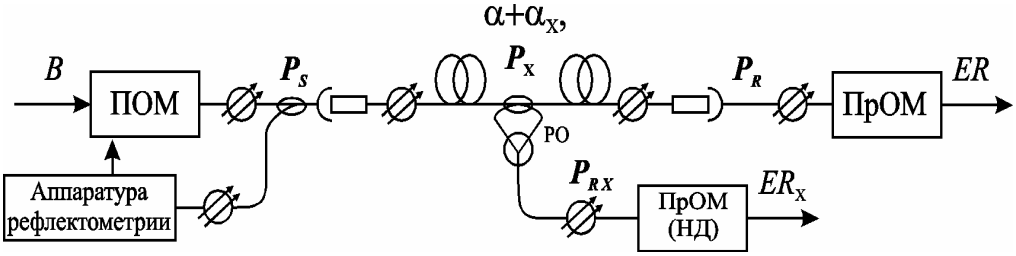


Рис. 2. ВОЛС с пассивным НД.

При НСИ в результате воздействия на ОВ возникает неоднородность, при этом из ОВ излучается оптический сигнал ΔPx, часть которого P_{RX} подается на ПрОМ НД, и в ВОЛТ вносится дополнительное затухание α_X.

Введем следующие коэффициенты: Кс = P_{RX}/P_X – коэффициент связи устройства НСИ; Кв = $P_{RX}/\Delta P_X$ – коэффициент отбора устройства НСИ; Кзч = P_{R0}/P_{RX0} – коэффициент

запаса чувствительности устройства НСИ, где P_{R0}, P_{RX0} – чувствительность соответственно фотоприемников ВОЛС и устройства НСИ.

Энергетический потенциал ВОЛС Е и координата х от начала ВОЛТ до места съема информации для устройства НД с заданным коэффициентом запаса чувствительности Кзч определяют коэффициент связи Кс устройства НСИ. В зависимости от конструктивных особенностей и технологии изготовления устройства вывода-ввода для НСИ обеспечивается некий уровень Кв, что вызывает дополнительное вносимое затухание ВОЛТ α_X.

Всегда существует принципиальная возможность съема информации с ОВ оптического кабеля. Несанкционированный доступ к ВОЛС, несмотря на сложность и дороговизну, все-таки возможен. Способы съема, которые могут быть использованы для перехвата информации с ВОЛС, можно условно разделить на несколько групп [3, 4]:

1. По способу подсоединения:

1.1. безразрывный;

1.2. разрывный;

1.3. локальный;

1.4. протяженный.

2. По способу регистрации и усиления:

2.1. пассивные – регистрация излучения с боковой поверхности ОВ;

2.2. активные – регистрация излучения, выводимого через боковую поверхность ОВ с помощью специальных средств, меняющих параметры сигнала в ВОЛТ;

2.3 компенсационные – регистрация излучения, выводимого через боковую поверхность ОВ с помощью специальных средств с последующим формированием и вводом в ОВ излучения, компенсирующего потери мощности при выводе излучения.

Основным и наиболее популярным способом безразрывного локального НД является способ линзовой фокусировки сингулярных (вытекающих) мод на изгибе волокна. Этот способ нашел применение в аппаратах для сварки ОВ (и юстировки) [3].

Устройства разрывного НД позволяют осуществлять более надежный съем информации. Однако разрывное подключение требует временного выключения линии, что может сигнализировать о наличии самого доступа. Вероятно, “для маскировки”, параллельно с подключением могут быть осуществлены и умышленные повреждения кабеля. Возможная схема организации разрывного НД приведена в [4].

Пассивные способы обладают высокой скрытностью, так как практически не меняют параметры распространяющегося по ОВ излучения, но имеют низкую чувствительность. Поэтому для перехвата информации используют участки, на которых уровень бокового излучения повышен. Даже после формирования стационарного распределения поля в волокне небольшая часть рассеянного излучения все же проникает за пределы оболочки и может быть каналом утечки передаваемой информации. Возможность существования побочных оптических излучений с боковой поверхности ОВ обусловлена рядом физических, конструктивных и технологических факторов (рис. 3):

- существование вытекающих мод на начальном участке волокна, обусловленное возбуждением его источником излучения с пространственным распределением, превышающим апертуру волокна;

- излучение вытекающих и излучательных мод на всем протяжении ОВ за счет рэлеевского рассеяния на структурных неоднородностях материала ОВ, характерные размеры которых существенно меньше длины волны излучения;

- преобразование направляемых мод в вытекающие за счет локальных изменений волноводного параметра на волноводных нерегулярностях волокна: микроизгибах (радиус изгиба сравним с диаметром ОВ) и макроизгибах (радиус изгиба намного больше диаметра ОВ);

- возникновение распределенных и локальных давлений на ОВ.

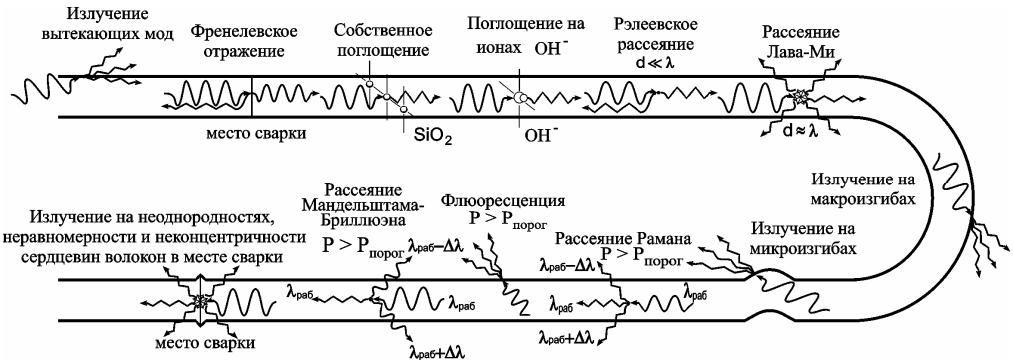


Рис. 3. Причины излучения и рассеивания в ОВ.

Использование вытекающих мод в местах стыковки ОВ представляет достаточную опасность с точки зрения защиты информации, т. к. имеется возможность организовать режим «прозрачности» НСИ, когда ВОЛС «не замечает» отбор достаточно большого оптического сигнала из ВОЛТ. В этом случае трудно фиксировать съем сигнала. Однако ввиду ограниченного и известного числа и расположения таких мест на трассе ВОЛТ обеспечение защиты информации относительно просто достигается организационно-техническими мероприятиями (охрана, наблюдение таких участков).

Активные способы позволяют вывести через боковую поверхность ОВ излучение значительно большей мощности. Однако при этом происходит изменение параметров распространяющегося по ОВ излучения (уровень мощности в канале, модовая структура излучения), что может быть легко обнаружено. К способам этой группы относятся: механический изгиб ОВ, вдавливание зондов в оболочку, бесконтактное соединение ОВ, шлифование и растворение оболочки, подключение к ОВ фотоприемника с помощью направленного ответвителя, термическое деформирование геометрических параметров ОВ и формирование неоднородностей в ОВ.

Компенсационные способы принципиально сочетают в себе преимущества первых двух групп – скрытность и эффективность, но сопряжены с техническими трудностями при их реализации. Вывод излучения, формирование и обратный ввод через боковую поверхность должны осуществляться с коэффициентом передачи, близким к единице. Однако статистический характер распределения параметров ОВ по длине (диаметров, показателей преломления сердцевины и оболочки и др.), спектральной полосы полупроводникового лазера и характеристик устройства съема приводит к тому, что разность между выведенным и введенным обратно уровнями мощности носит вероятностный характер. Поэтому коэффициент передачи может принимать различные значения. Практические устройства, реализующие компенсационные способы съема информации с боковой поверхности ОВ, в настоящее время неизвестны.

Следует отметить, что защитные оболочки и элементы конструкции кабеля существенно ослабляют боковое излучение. Поэтому перехват информации любым из вышеперечисленных способов возможен только при нарушении целостности внешней защитной оболочки кабеля и непосредственном доступе к оптическим волокнам.

Интересным является также протяженный безразрывный съем информации, который можно осуществить или на пологом изгибе волокна или на прямом волокне под воздействием низких температур. Дело в том, что при низких температурах происходит изменение коэффициентов преломления стекла, в результате чего в сердцевине может повыситься уровень рассеяния.

Конфиденциальность передаваемой по ВОЛС информации может быть обеспечена применением специальных методов и средств защиты линейного тракта от НД. К основным достоинствам применения защищенных ВОЛС относятся:

- независимость от структуры передаваемых цифровых сигналов;

- независимость от скорости передачи цифровых сигналов;
- относительно низкая стоимость;
- универсальность применения в локальных, абонентских или зоновых сетях связи.

В последние время проводятся интенсивные работы по созданию ВОЛС, обеспечивающих защиту передаваемой информации от НД. Можно выделить три основных направления этих работ:

- разработка технических средств защиты от НД к информационным сигналам, передаваемым по ОВ;
- разработка технических средств контроля НД к информационному сигналу, передаваемому по ОВ [1, 2];
- разработка технических средств защиты информации, передаваемой по ОВ, реализующих принципы маскировки [8,9], добавления помех, оптической и квантовой криптографии.

Первая группа работ связана с разработкой конструкционных, механических и электрических средств защиты от НД к оптическим кабелям (ОК), муфтам и ОВ. Одни из видов средств защиты этой группы построены так, чтобы затруднить механическую разделку кабеля и воспрепятствовать доступу к ОВ. Подобные средства защиты широко используются и в традиционных проводных сетях специальной связи. Также перспективным представляется использование пары продольных силовых элементов ОК, которые представляют собой две стальные проволоки, размещенные симметрично в полиэтиленовой оболочке, и используемые для дистанционного питания и контроля датчиков, установленных в муфтах, и контроля НД. Целесообразно также применение комплекта для защиты места сварки, который заполняет место сварки непрозрачным затвердевающим гелем. Одним из предложенных методов защиты является использование многослойного оптического волокна со специальной структурой отражающих и защитных оболочек [3]. Конструкция такого волокна представляет собой многослойную структуру с одномодовой сердцевиной. Подобранное соотношение коэффициентов преломления слоев позволяет передавать по кольцевому направляющему слою многомодовый контрольный шумовой оптический сигнал. Связь между контрольным и информационным оптическими сигналами в нормальном состоянии отсутствует. Кольцевая защита позволяет также снизить уровень излучения информационного оптического сигнала через боковую поверхность ОВ (посредством мод утечки, возникающих на изгибах волокна различных участков линии связи). Попытки приникнуть к сердцевине обнаруживаются по изменению уровня контрольного (шумового) сигнала или по смешению его с информационным сигналом. Место НД определяется с высокой точностью с помощью рефлектометра.

Вторая группа работ в этом направлении связана с мониторингом "горячих" волокон, и разработкой различных устройств контроля параметров оптических сигналов на выходе ОВ и отраженных оптических сигналов на входе ОВ.

Основой системы фиксации НД является система диагностики состояния (СДС) ВОЛТ. СДС можно построить с анализом либо прошедшего через ВОЛТ сигнала, либо отраженного сигнала (рефлектометрические СДС).

СДС с анализом прошедшего сигнала является наиболее простой диагностической системой. На приемной части ВОЛС анализируется прошедший сигнал. При НД происходит изменение сигнала, это изменение фиксируется и передается в блок управления ВОЛС.

При использовании анализатора коэффициента ошибок на приемном модуле ВОЛС (рис. 4) СДС реализуется при минимальных изменениях аппаратуры ВОЛС, т. к. практически все необходимые модули имеются в составе аппаратуры ВОЛС. Недостатком является относительно низкая чувствительность к изменениям сигнала.

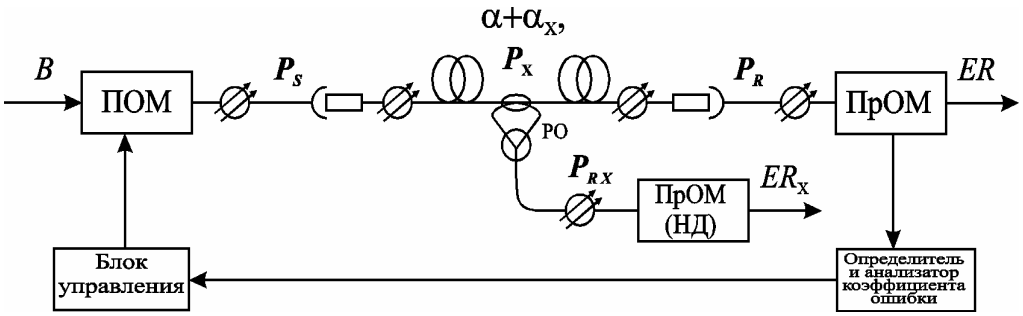


Рис. 4. ВОЛС с системой диагностики по анализу коэффициента ошибок.

Основным недостатком СДС с анализом прошедшего сигнала является отсутствие информации о координате появившейся неоднородности, что не позволяет проводить более тонкий анализ изменений режимов работы ВОЛС (для снятия ложных срабатываний системы фиксации НСИ).

СДС с анализом отраженного сигнала (рефлектометрические СДС) позволяют в наибольшей степени повысить надежность ВОЛС.

Для контроля величины мощности сигнала обратного рассеяния в ОВ в настоящее время используется метод импульсного зондирования, применяемый во всех образцах отечественных и зарубежных рефлектометров (рис. 5).

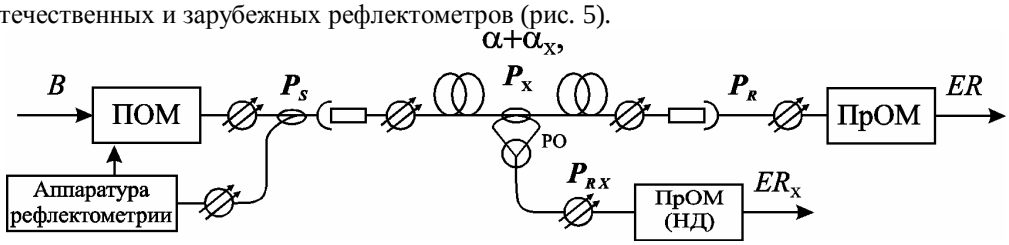


Рис. 5. ВОЛС с рефлектометрическими системами диагностики состояния ВОЛТ.

Суть его состоит в том, что в исследуемое ОВ вводится мощный короткий импульс, и затем на этом же конце регистрируется излучение, рассеянное в обратном направлении на различных неоднородностях, по интенсивности которого можно судить о потерях в ОВ, распределенных по его длине на расстоянии до 100 - 120 км. В качестве такого рефлектометра может быть использован оптический рефлектометр Минского института радиоэлектроники, выполненный на базе компьютера типа note-book (возможно использование и персонального компьютера семейства IBM) с соответствующим программным обеспечением. Начальные рефлектограммы линии фиксируются при разных динамических параметрах зондирующего сигнала в памяти компьютера и сравниваются с соответствующими текущими рефлектограммами. Локальное отклонение рефлектограммы более чем на 0,1 дБ свидетельствует о вероятности попытки несанкционированного доступа к ОВ.

Основными недостатками СДС с анализом отраженного сигнала на основе метода импульсной рефлектометрии являются следующие:

- при высоком разрешении по длине ВОЛТ (что имеет важное значение для обнаружения локальных неоднородностей при фиксации НД) значительно снижается динамический диапазон рефлектометров и уменьшается контролируемый участок ВОЛТ ;
- мощные зондирующие импульсы затрудняют проведение контроля ВОЛТ во время передачи информации, что снижает возможности СДС, либо усложняет и удорожает систему диагностики;
- источники мощных зондирующих импульсов имеют ресурс, недостаточный для длительного непрерывного контроля ВОЛС;

- специализированные источники зондирующего оптического излучения, широкополосная и быстродействующая аппаратура приемного блока рефлектометров значительно удорожает СДС.

Методы этой группы хорошо сочетаются со многими другими методами защиты.

Представляет интерес метод, основанный на использовании кодового зашумления передаваемых сигналов. При реализации этого метода применяются специально подобранные в соответствии с требуемой скоростью передачи коды, размножающие ошибки. Даже при небольшом понижении оптической мощности, вызванном подключением устройства съема информации к ОВ, в цифровом сигнале на выходе ВОЛС резко возрастает коэффициент ошибок, что достаточно просто зарегистрировать средствами контроля ВОЛС. Интересным также является метод, основанный на использовании пары разнознаковых компенсаторов дисперсии на ВОЛС. Первый компенсатор вводит в линию диспергированный сигнал, а на приемном конце второй компенсатор восстанавливает форму переданного сигнала.

При использовании маскировки информационного сигнала может применяться система, использующая спектральное разделение каналов [8, 9].

Для маскировки линейного кода в оптическом тракте при использовании кода типа RZ можно применить оптическую линию задержки (ОЛЗ), которая подключается на входе оптического тракта с помощью разветвителей оптических (РО) в соответствии с рис. 6 [8. 9]. Величина времени задержки зависит от типа RZ кода, и для RZ-25% составляет T/2, где T – длительность тактового интервала.

Для выделения сигнала на приемном конце можно использовать аналогичную ОЛЗ, соединенную с двумя РО. При этом на выходе ВОЛС получаем сигнал в коде типа NRZ, соответствующий информационному входному сигналу. Также перспективным является использование режима динамического (детерминированного) хаоса, который позволяет обеспечить передачу информации с псевдохаотически изменяющимися частотой и амплитудой несущей. В результате выходной сигнал внешне является шумоподобным, что затрудняет расшифровку.

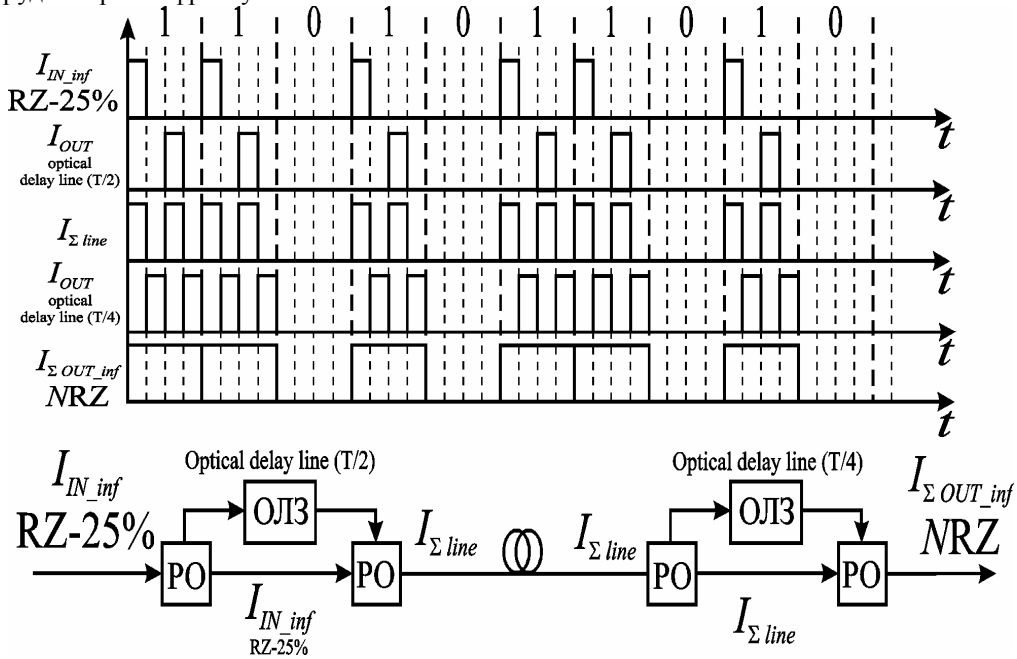


Рис. 6. Маскировка линейного кода.

С развитием науки и техники назрела необходимость и появилась возможность соединить достижения криптографической науки с квантовой механикой и квантовой стати-

стикой. Здесь может возникнуть естественная связь дискретной математики (криптографии) и дискретной (квантовой) механики физических процессов. На этом стыке возникло и интенсивно развивается новое перспективное направление – квантовая криптография.

Методы квантовой криптографии потенциально обеспечивают высокую степень защиты от перехвата информации на линии связи за счет передачи данных в виде отдельных фотонов, поскольку неразрушающее измерение их квантовых состояний в канале связи перехватчиком невозможно, а факт перехвата фотонов из канала может быть выявлен по изменению вероятностных характеристик последовательности фотонов.

Возможны различные варианты построения конкретных систем, отличающиеся степенью защиты и контроля НД к передаваемой по ВОЛС информации. Это делает необходимым проведение специальных исследований с целью экспертизы реализованных научно-технических решений и их соответствия требованиям обеспечения защиты информации.

Следует также отметить, что все перечисленные выше методы защиты и их комбинации могут обеспечивать безопасность информации лишь в рамках известных моделей НД. При этом эффективность систем защиты определяется как открытием новых, так и совершенствованием технологий НСИ, использующих уже известные физические явления. С течением времени противник может освоить новые методы перехвата, потребуется дополнять защиту, что не свойственно криптографическим методам защиты, которые рассчитываются на достаточно длительный срок.

В заключение следует отметить, что необходимость практического внедрения и эффективного использования защищенных ВОЛС в сетях связи является задачей сегодняшнего дня.

Литература

1. Свинцов А. А., Свинцов А. Г. “Численное моделирование систем диагностики состояния волоконно-оптического тракта ВОСП.” Науково-технічна конференція «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» Україна, Київ, 1998 р.
2. Свинцов А. Г. ”ВОСП и защита информации.” Науково-технічна конференція «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» Україна, Київ, 1998 р.
3. А. В. Корольков, И. А. Кращенко, В. Г. Матюхин, С. Г, Синев "Проблемы защиты информации, передаваемой по волоконно-оптическим линиям связи, от несанкционированного доступа" // Информационное Общество, 1997 г., № 1.
4. Ю. В. Аграфонов, Д. Б. Липов, А. Н. Малов. "Структура волноводных мод и несанкционированный доступ в волоконно-оптических линиях связи".

УДК 004.056

Герасин А.П., Петров А.С.

ПЭМИН – РИСК ПЕРЕХВАТА ИНФОРМАЦИИ

Статья посвящена проблеме утечки информации через побочные электромагнитные излучения и наводки (ПЭМИН).

Известно, что электронное оборудование генерирует электромагнитные поля, которые могут являться помеховыми для радио- и телевизионной аппаратуры. Причины лежащие в основе этого явления достаточно основательно изучались на протяжении многих лет. Результаты проведенных исследований нашли свое отражение в виде международных соглашений в области норм и методик измерения радиопомех, создаваемых различным электронным и электротехническим оборудованием.

Однако радиопомехи – не единственная проблема, которую создает электромагнитное излучение используемого оборудования. В некоторых случаях, принимая сигнал и декодируя его, возможно получить доступ к обрабатываемой техническим средством ин-

формации, которая содержится в сигналах, используемых внутри оборудования, особенно цифрового.

Побочные электромагнитные излучения (ПЭМИ) — это паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными.

Побочные электромагнитные излучения, генерируемые электронными устройствами, обусловлены протеканием токов в их электрических цепях. Спектр ПЭМИ цифрового электронного оборудования представляет собой совокупность гармонических составляющих в некотором диапазоне частот (учитывая достижения полупроводниковой электроники, в некоторых случаях имеет смысл говорить уже о диапазоне в несколько ГГц).

Употребляемый отечественный термин - ПЭМИН - в зарубежной литературе имеет синонимы TEMPEST и компрометирующие излучения (compromising emanations).

TEMPEST (сокращение от Transient Electromagnetic Pulse Emanation Standard) представляет собой стандарт на переходные электромагнитные импульсные излучения (работающей радиоэлектронной аппаратуры). В обиходе термин TEMPEST, употребляемый в Соединенных Штатах, используется, например, для обозначения процесса перехвата информации (TEMPEST-атаки) и т. п.

Европа и Канада в основном оперируют термином «компрометирующие излучения».

Исследования побочных излучений были начаты еще в начале 20-го века. Самыми первыми были работы Герберта Ядли, который разрабатывал способы выявления и перехвата скрытых радиопередач для армии США. При проведении исследований Ядли обратил внимание на присутствие побочных излучений и предположил, что они также могут нести полезную информацию.

Однако полномасштабные (но закрытые) исследования побочных «компрометирующих» электромагнитных излучений начались в конце 40-х - начале 50-х годов.

После окончания Второй мировой войны во время прослушивания телефонных переговоров советских представительств в Берлине американские спецслужбы обратили внимание на какой-то странный шум в виде слабых щелчков. Как выяснилось позже, это был сигнал, излучаемый электромагнитом печатающего устройства телетайпной машины, воспроизводящей открытый текст. Восстановив этот сигнал и подав его на телетайпную машину, сотрудникам ЦРУ удалось получить тот самый открытый текст.

Все исследования по TEMPEST и случаи перехвата, как правило, держались в секрете, а первое открытое описание TEMPEST-угрозы появилось в отчете шведа Кристиана Бекмана в начале 80-х. Однако большее внимание к проблеме привлекла статья голландского ученого Вима ван Эйка, опубликованная в 1985 году.

В этой статье («Электромагнитное излучение видеодисплейных модулей: риск перехвата информации?») автор показал, что содержимое экрана монитора может быть восстановлено дистанционно с помощью дешевого бытового оборудования - ТВ-приемника, в котором синхронизаторы были заменены генераторами, перестраиваемыми вручную.

В феврале 1985 года Ван Эйк совместно с Британской радиовещательной корпорацией провел эксперимент по «подслушиванию» с положительным результатом. Часть полученных результатов затем была показана в программе «Мир завтра» (Tomorrow's World).

Дело происходило в Лондоне на виду большого количества горожан, и экспериментаторов удивил тот факт, что никто не поинтересовался, что все-таки происходит.

Полученные Ван Эйком результаты были позднее подтверждены Мюллером, Бернстейном и Колбергом, которые занимались разработкой различных технических приемов экранирования оборудования.

Позднее, в 1987 году Смалдерс показал, что даже экранированные кабели RS-232 могут быть, в ряде случаев, прослушаны.

Середину 80-х можно назвать переломным рубежом, после которого количество открытых публикаций по этой теме стало неуклонно возрастать с каждым годом. Пробле-

ма утечки информации через ПЭМИН стала исследоваться не только в закрытых военных ведомствах, но и в гражданских организациях.

Не все составляющие спектра ПЭМИ являются опасными с точки зрения реальной утечки информации.

Условно весь спектр излучений можно разбить на потенциально информативные и неинформативные излучения.

Совокупность составляющих спектра ПЭМИ, порождаемая протеканием токов в цепях, по которым передаются содержащие конфиденциальную информацию сигналы, назовем **потенциально-информативными излучениями (потенциально-информативными ПЭМИ).**

Для персонального компьютера потенциально-информативными ПЭМИ являются излучения, формируемые следующими цепями:

- цепь, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате;
- цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора;
- цепи, формирующие шину данных системной шины компьютера;
- цепи, формирующие шину данных внутри микропроцессора, и т. д.

Практически в каждом цифровом устройстве существуют цепи, выполняющие вспомогательные функции, по которым никогда не будут передаваться сигналы, содержащие закрытую информацию. Излучения, порождаемые протеканием токов в таких цепях, являются безопасными в смысле утечки информации. Для таких излучений вполне подходит термин **«неинформативные излучения (неинформативные ПЭМИ)».** С точки зрения защиты информации неинформативные излучения могут сыграть положительную роль, выступая в случае совпадения диапазона частот в виде помехи приему информативных ПЭМИ (в литературе встречается термин «взаимная помеха»).

Для персонального компьютера неинформативными ПЭМИ являются излучения, формируемые следующими цепями:

- цепи формирования и передачи сигналов синхронизации;
- цепи, формирующие шину управления и шину адреса системной шины;
- цепи, передающие сигналы аппаратных прерываний;
- внутренние цепи блока питания компьютера и т. д.

На практике могут встретиться ситуации, когда восстановление информации при перехвате потенциально информативных излучений какой-либо электрической цепи (цепей) невозможно по причинам принципиального характера. Определение списка таких причин и их обоснование должно стать объектом отдельных исследований и публикаций. Однако один пример все-таки приведем: применение многоразрядного параллельного кода (для передачи каждого разряда используется своя электрическая цепь) в большинстве случаев (в зависимости от разрядности кода, формата представления информации) делает невозможным восстановление информации при перехвате ПЭМИ.

Потенциально информативные ПЭМИ, выделение полезной информации из которых невозможно при любом уровне этих излучений, назовем **безопасными информативными излучениями (безопасными информативными** ПЭМИ). Соответственно, потенциально информативные излучения, для которых не существует причин, однозначно исключающих возможность восстановления содержащейся в них информации, будем называть **принципиально-информативными излучениями (принципиально-информативными ПЭМИ).**

Так, например, к принципиально-информативным излучениям ПК можно отнести излучения, формируемые следующими цепями:

- цепь, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате;

- цепи, по которым «передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора.

Восстановление информации при перехвате излучений цепей, по которым передается видеосигнал, – это один из тех случаев, когда при использовании многоразрядного (как минимум три разряда для цветного монитора) параллельного кода формат представления информации позволяет восстанавливать большую ее часть (теряется цвет, но может быть восстановлено смысловое содержание), не восстанавливая при этом последовательности значений каждого разряда кода.

К безопасным информативным излучениям ПК можно отнести излучения цепей, формирующих шину данных системной шины и внутреннюю шину данных микропроцессора, а также излучения других цепей, служащих для передачи информации, представленной в виде многоразрядного параллельного кода.

При наличии в оборудовании нескольких электрических цепей, по которым может передаваться в разном виде одна и та же конфиденциальная информация, для перехвата, скорее всего, будут использованы принципиально-информативные излучения, формируемые какой-либо одной из этих цепей. Какие именно излучения будут использованы, определяется в каждом конкретном случае предполагаемой задачей перехвата и возможным способом ее решения.

В общем случае в отношении одного и того же оборудования может быть сформулировано несколько задач перехвата, каждая из которых, в свою очередь, может быть решена не одним способом. Выбор способа решения задачи перехвата зависит от трудности технической реализации, научно-технического потенциала и финансовых возможностей предполагаемого противника.

Часть принципиально-информативных ПЭМИ оборудования, которая не используется при решении конкретной задачи перехвата, может быть названа **условно-неинформативными излучениями (условно-неинформативными ПЭМИ**). Принципиально-информативные ПЭМИ, используемые для решения конкретной задачи перехвата, назовем ***информативными излучениями (информативными ПЭМИ).***

Предположим, например, что сформулирована следующая задача перехвата: восстановить информацию, обрабатываемую в текстовом редакторе с помощью персонального компьютера. Конфиденциальная информация в виде буквенно-цифрового текста вводится с клавиатуры, отображается на экране монитора, не сохраняется на жестком и гибком магнитных дисках, не распечатывается и не передается по сети. В данном случае принципиально-информативными ПЭМИ является совокупность составляющих спектра излучения ПК, обусловленная протеканием токов в следующих цепях:

- цепь, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате (источник № 1);
- цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора (источник №2).

Анализ технической документации показывает, что одна и та же информация передается по этим цепям в совершенно разном виде (временные и частотные характеристики сигналов, формат представления информации). Очевидно, что для решения задачи перехвата совместное использование излучений, формируемых этими цепями, невозможно. В этом случае при выборе источника информативных излучений противодействующая сторона будет учитывать следующие факторы:

– видеосигнал является периодическим сигналом, а сигнал, передаваемый от клавиатуры к системному блоку – апериодическим; для периодического сигнала возможно реализовать функцию его накопления в приемнике, что позволит повысить дальность перехвата и уменьшить вероятность ошибки при восстановлении информации;

– излучения источника № 1 базируются в низкочастотной части радиодиапазона;

– излучения источника № 2 занимают широкую полосу частот, расположенную частично в высокочастотной части радиодиапазона; в условиях большого города низкочастотная часть радиодиапазона перегружена индустриальными радиопомехами;

– с увеличением частоты сигнала увеличивается КПД антенны, в качестве которой выступает токовый контур для сигнала, и т. д.

Таким образом, наиболее вероятным представляется перехват ПЭМИ цепей, передающих видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора (информативные ПЭМИ). Излучения, обусловленные протеканием токов в цепи, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате, в этом случае будут условно-неинформативными ПЭМИ.

В условиях реальных объектов уровень информативных излучений цифрового оборудования на границе контролируемой зоны может быть различным. Информативные ПЭМИ, уровень которых на границе контролируемой зоны достаточен для восстановления содержащейся в них информации, предлагается называть ***объектово-опасными информативными излучениями (объектово-опасными информативными ПЭМИ).*** Информативные ПЭМИ, уровень которых на границе контролируемой зоны недостаточен для восстановления содержащейся в них информации, назовем ***объектово-безопасными информативными излучениями (объектово-безопасными информативными ПЭМИ).***

Подводя итоги, необходимо отметить, что наибольшую опасность с точки зрения утечки информации представляют побочные электромагнитные (паразитные) излучения технических средств, участвующих в процессе обработки, передачи и хранения информации. а в условиях информатизации общества и интенсивного развития информационных технологий защита информационных ресурсов является задачей государственной важности и обеспечивает приоритеты государства в политической, военной, экономической и научно-технической сферах деятельности.

Литература

1. Пятачков А. Г. Математическая модель защиты информации от утечки по техническим каналам Вопросы защиты информации. № 4, 1995;
2. Агеев А. С. Пятачков А. Г. и др. Организация и современные методы защиты информации. Концерн «Банковский Деловой Центр». 1998;
3. Сидельников В. В. Распространение синусоидальных электромагнитных волн высокой частоты по силовым кабелям с поясной изоляцией. Сб. Автоматика, телемеханика и приборостроение, Наука. 1964;
4. Соколов А. В., Степанюк О. М. «Защита от компьютерного терроризма» - СПб.: БХВ-Петербург; Арлит – 2002. – 496 с.: ил;
5. Генне В.И., К вопросу оценки уровня ПЕМИН цифрового электронного оборудования // Защита информации. Конфидент. №3, 1998;
6. «Безопасность информационных технологий. Методология создания систем защиты» Домарев В. В. – К.: ООО «ТИД «ДС», 2001. – 688 с;
7. Методы и средства защиты информации / Под ред. Ковтанюка Ю. С. – К.: Издательство Юниор, 2003,. – 504 с., ил.

УДК 681.3.06

Валуйский Е.А., Петров А.С.

ПРОГРАММНЫЙ ПАКЕТ NIST STATISTICAL TEST SUITE. СТРАТЕГИЯ ТЕСТИРОВАНИЯ И ИНТЕРПРЕТАЦИЯ РЕЗУЛЬТАТОВ

В статье исследована проблема тестирования качества генераторов псевдослучайных последовательностей с помощью программного пакета NIST Statistical Test Suite. Приводится описание интерпретации полученных результатов.

Введение

Потребность в случайных и псевдослучайных числах возникает во многих криптографических приложениях. Например, обычные криптосистемы используют ключи, которые должны быть сгенерированы случайным образом. В различных криптографических

протоколах, при создании цифровых подписей также требуется набор случайных или псевдослучайных данных в качестве вспомогательного материала.

Есть два основных типа генераторов, для производства случайных последовательностей: генераторы случайных чисел RNGs, и генераторы псевдослучайных чисел PRNGs. Для криптографических приложений, оба из этих типов генераторов производят поток нулей и единиц, которые могут быть разделены на подпотоки или блоки случайных чисел.

Первый тип генератора последовательности - генератор случайных чисел (RNG). RNG использует недетерминированный источник (то есть, источник энтропии), наряду с некоторой функцией обработки (то есть, процесс дистилляции энтропии), чтобы произвести случайность. Использование процесса дистилляции необходимо, чтобы избежать любую слабость в источнике энтропии, которая приводит к получению неслучайных чисел (например, возникновение длинных строк нулей или единиц). Источник энтропии типично состоит из некоторых физических величин, типа шума в электрической схеме, выбора времени, пользовательских процессов (например, нажатия клавиш или движения мыши), или квантовых эффектов в полупроводниках. Могут использоваться различные комбинации этих источников. Кроме того, генерация высококачественных случайных чисел может быть слишком трудоёмкой, делая эту процедуру нежелательной, когда необходимо большое количество случайных чисел. Чтобы производить большие количества случайных чисел, псевдослучайные генераторы могут быть предпочтительнее.

Второй тип генераторов - псевдослучайный генератор (PRNG). Для получения множества псевдослучайных чисел PRNG использует один или более входящих начальных значения.

В контексте, в котором непредсказуемость необходима, само начальное число должно быть случайно и непредсказуемо. Следовательно, по умолчанию, PRNG должен получить начальное число от выводов RNG; то есть, PRNG требует RNG как компаньон.

Как ни странно, псевдослучайные числа часто, кажутся, более случайными, чем случайные, полученные из физических источников. Если псевдослучайная последовательность должным образом сформирована, каждое значение в последовательности произведено от предыдущего значения через преобразования, которые вводят дополнительную случайность. Ряд таких преобразований может устранить статистическую автокорреляцию между начальным значением и полученным результатом. Таким образом, последовательности PRNG могут иметь лучшие статистические свойства и могут генерироваться быстрее, чем RNG.

Программный набор NIST - статистический пакет, состоящий из 16 тестов, которые были разработаны, чтобы проверить случайность двоичной последовательности произвольной длины. Последовательность генерируется аппаратными или программными средствами для применения в криптографических приложениях. Эти испытания основываются на разнообразии различных типов неслучайности, которые могут существовать в последовательности. В пакете реализованы частотный тест, тест последовательностей и серий, ранги двоичной матрицы, спектральный тест, «универсальный тест» Маурера и др.

Стратегия статистического анализа RNGs и PRNGs

На практике существует множество различных стратегий, используемых для статистического анализа генераторов случайных чисел. NIST принял стратегию тестирования генераторов случайных чисел, состоящую из пяти стадий.

Стадия 1: Выбор Генератора.

Выбирается аппаратно или программно реализованный генератор для оценивания. Генератор должен производить последовательность из нулей «0» и единиц «1» длиной n. Примеры псевдослучайных генераторов (PRNG), которые могут быть выбраны, включают PRNG на основе DES от ANSI X9.17, и два последующих метода, которые определены в FIPS 186 и основаны на безопасном хеш-алгоритме (SHA-1) и стандарте шифрования данных (DES).

Стадия 2: Генерация двоичной последовательности.

Для выбранной последовательности длиной n и генератора, создается набор m двоичных последовательностей и сохраняется в файл. Образцы случайных чисел могут быть получены также из других источников, например, сгенерированы программным комплексом Джорджа Марсальи Diehard.

Стадия 3: Выполнение набора тестов NIST.

Запускается набор тестов NIST, используя, в качестве параметров, полученный на второй стадии файл данных и желаемую длину последовательности. Выбираются статистические тесты и значения параметров (длина блока и т.д.)

Стадия 4: Исследование P-значений.

Выходной файл будет сгенерирован набором программ NIST с соответствующими промежуточными значениями, типа испытательной статистики, и P-значений для каждого статистического испытания. Заключение относительно качества последовательности может быть, сделано базируясь на этих P-значениях.

Стадия 5: Оценка: тест пройден \ или нет.

Для каждого статистического теста, произведен ряд P-значений (соответствующий набору последовательностей). Для фиксированного уровня значимости, определенный процент P-значений, как ожидается, укажет на отказ.

Например, если уровень значимости выбран, равным 0.01 (то есть, $\alpha = 0.01$), то приблизительно 1 % последовательностей, как ожидается, будет терпеть неудачу. Последовательность проходит статистический тест всякий раз, когда P-значение $\geq a$ и будет отвергнута в противном случае.

Интерпретация эмпирических результатов

Три сценария символизируют события, которые могут произойти в процессе эмпирического тестирования. Случай 1: анализ P-значений не указывает отклонение от случайности. Случай 2: анализ ясно указывает отклонение от случайности. Случай 3: анализ является неокончательным.

Интерпретация эмпирических результатов может быть проведена несколькими способами. Два подхода принятые NIST включают (1) проверка соотношения последовательностей прошедших испытание и (2) распределение P-значений, для проверки на равномерность.

Когда любой из этих подходов терпит неудачу (то есть, соответствующая нулевая гипотеза должна быть отклонена), дополнительные числовые эксперименты должны провестись на других образцах генераторов, чтобы определить, было ли явление статистической аномалией или ясным свидетельством неслучайности.

Соотношение последовательностей прошедших испытание

Учитывая эмпирические результаты для специфического статистического теста, вычисляется соотношение последовательностей прошедших тест.

Например, если 1000 двоичных последовательностей были проверены (то есть, m = 1000), $\alpha = 0.01$ (уровень значимости), и 996 двоичных последовательностей имели P-значения ≥ 0.01, то соотношение - 996/1000 = 0.9960.

Диапазон приемлемых соотношений при использование определенного доверительного интервала определен как $\hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}}$, где $\hat{p} = 1 - \alpha$, и m – размерность. Если соотношение выходит за пределы этого интервала, то это доказательство того, что данные неслучайны.

Следует обратить внимание, что другие значения среднеквадратичного отклонения могут также быть использованы. Для примера выше доверительный интервал $0.99 \pm 3\sqrt{\frac{0.99(0.01)}{1000}} = 0.99 \pm 0.0094392$, то есть, соотношение должно лечь выше 0.9805607. Это может быть иллюстрировано на рис 2. Доверительный интервал был расс-

читан, используя распределение как приближение к биноминальному распределению, которое является разумно точным для больших размерностей (например, m ≥ 1000).

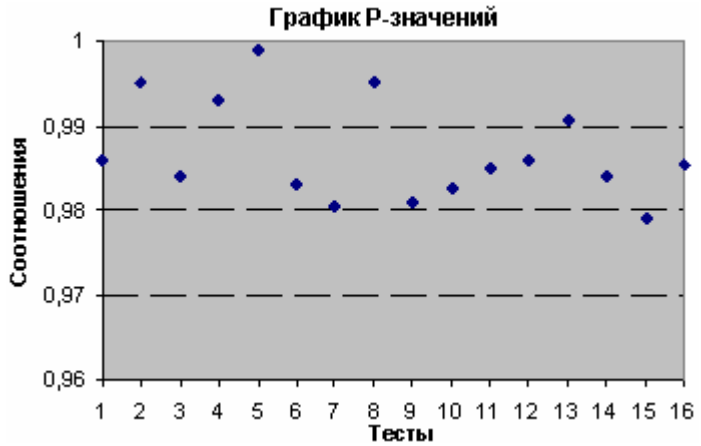


Рис. 1. График соотношений последовательностей прошедших тест.

Равномерность распределение P-значений

Распределение P-значений исследуется, чтобы гарантировать равномерность. Это может быть визуально иллюстрировано, используя гистограмму, в соответствие с которой интервал от 0 до 1 разделен на 10 подинтрвалов и P-значения, которые лежат в пределах каждого подинтервала, подсчитаны и отображены.

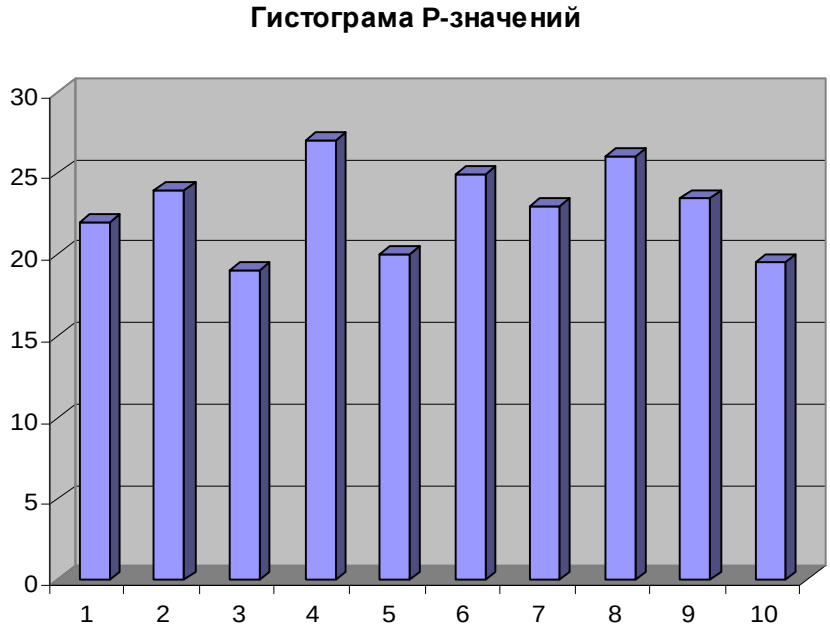


Рис. 2. График распределения P-значений.

Равномерность может также быть определена через χ^2 тест и P-значения соответствующих нормальному распределению, полученному для произвольных статистических тестов. Это достигнуто вычисляя, $\chi^2 = \sum_{i=1}^{10} \frac{(F_i - s/10)^2}{s/10}$, где F_i – номер P-значения в подинтервале i, а s – размерность. P-значение вычислены так, что P-значение$_T$ = igamc(9/2,

$\chi^2 / 2$). Если Р-значение$_T \geq 0.0001$, тогда можно полагать что последовательность равномерно распределена.

Литература

1. Кнут Д.Э. Искусство программирования, том 2, 3-е изд.:Пер. с англ..-М.:Издательский дом «Вильямс», 2000;
2. Иванов М.А., Чугунков И.В. Теория, применения и оценки качества генераторов псевдослучайных последовательностей.-М.: КУДИЦ-ОБРАЗ, 2003;
3. The Marsaglia Random number CDROM - available from http://www.stat.fsu.edu;
4. Rukhin A. et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications NIST special publication 800-22. - available from http://csrc.nist.gov.

УДК 681.5.015: 004.056.57

Маракова И.И., Потапов Н.В., Сыропятов А.А.

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ ЗАЩИТЫ КОМПЛЕКСНЫХ СИСТЕМ СВЯЗИ

Представлены методики оценки эффективности информационной защиты комплексных систем связи с точки зрения выбора механизмов защиты информации, и процессов распределения ресурсов, выделяемых на защиту информации.

Возросшие требования к оперативности информационных процессов в различных областях деятельности современного общества, а также расширение возможностей сетевого построения информационных систем и внедрения методов распределенной обработки данных за счет реализации беспроводного доступа к вычислительным средствам обусловили широкое распространение на практике комплексных (комбинированных) систем связи (КСС). При этом одной из основных проблем является обеспечение информационной защиты на участках беспроводных технологий связи.

Существует мнение, что беспроводные сети предназначены исключительно для передачи открытой информации. При этом, однако, теряется смысл построения комплексных систем связи. Таким образом, проблема обеспечения информационной безопасности комплексных систем связи, т.е. включающих в свой состав беспроводные инфраструктуры, является весьма актуальной, требующей разрешения, как на концептуальном уровне, так и на уровне конкретного технического решения.

Наиболее широкое применение КСС нашли в так называемых сферах критических приложений, к которым относится деятельность институтов государственной власти, финансовых структур, учебных заведениях и т.д. Не умаляя общности рассуждений, при исключительном многообразии основные составляющие структур КСС традиционны (рис.1).

Решение проблемы обеспечения безопасности информации в КСС должно осуществляться системно на основе оценки эффективности защиты информации, передаваемой по каналам связи, и не должно рассматриваться как чисто техническая задача, которая может быть решена попутно с разработкой элементов сети. При этом следует рассматривать различные аспекты эффективности. Во-первых, подсистема защиты информации должна эффективно противодействовать угрозам, которые могут нанести ущерб защищаемой информации (проблема эффективности механизмов защиты информации). Во-вторых, процесс защиты информации в КСС можно рассматривать как процесс распределения ресурсов, выделяемых на защиту информации (проблема экономической эффективности)[1].

Под угрозами подразумевают любые обстоятельства или события, которые могут быть причиной нарушения политики безопасности информации или нанесения ущерба системе на любом участке взаимосвязей КСС рис. 1. Задача формирования множества дестабилизирующих факторов является одной из ключевых задач в проблеме защиты информации, причем по понятным причинам абсолютным является требование полноты полу-

ченного перечня. Исходя из этого, к решению указанной задачи необходимо подойти в максимальной степени системно. Прежде всего, сформируем полный перечень возможных типов угроз и потенциальных источников их формирования.

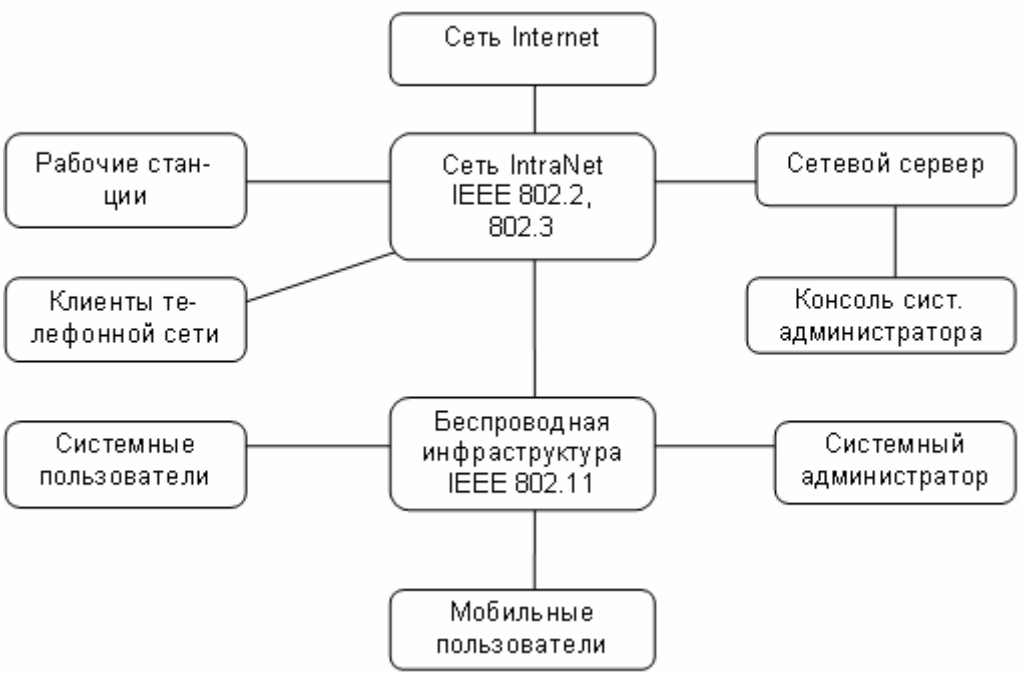


Рис. 1. Обобщенная структура комплексной системы связи.

На рис. 2 приведены типы угроз, которые являются характерными для современных КСС [2].

В общем виде полное множество угроз можно определить в виде:

$$U = \bigcup_{i=1}^{N} U_i , \qquad (1)$$

где: U – полное множество угроз информации КСС;

N – число участков функционирования системы;

U_i – полное множество угроз для i-го участка функционирования КСС.

В общем виде множество (1) для i-го участка функционирования системы может быть получено как объединение активных и пассивных угроз указанного участка функционирования КСС, при этом под активными угрозами будем понимать угрозы, вызванные действиями противника, а пассивные угрозы – это неблагоприятные обстоятельства и факторы, влияющие на работу участка функционирования КСС.

Множество пассивных угроз для i-го участка функционирования системы может быть получено по следующей формуле:

$$U_i = T \times R , \qquad (2)$$

где: T - множество типов угроз информации (рис. 2);

S - множество источников угроз информации.

Информационные потоки с точки зрения безопасности имеют такие важные свойства как: доступность информации, уровень конфиденциальности, сохранение целостности, что в свою очередь определяет и соответствующие угрозы (рис. 3) [3].

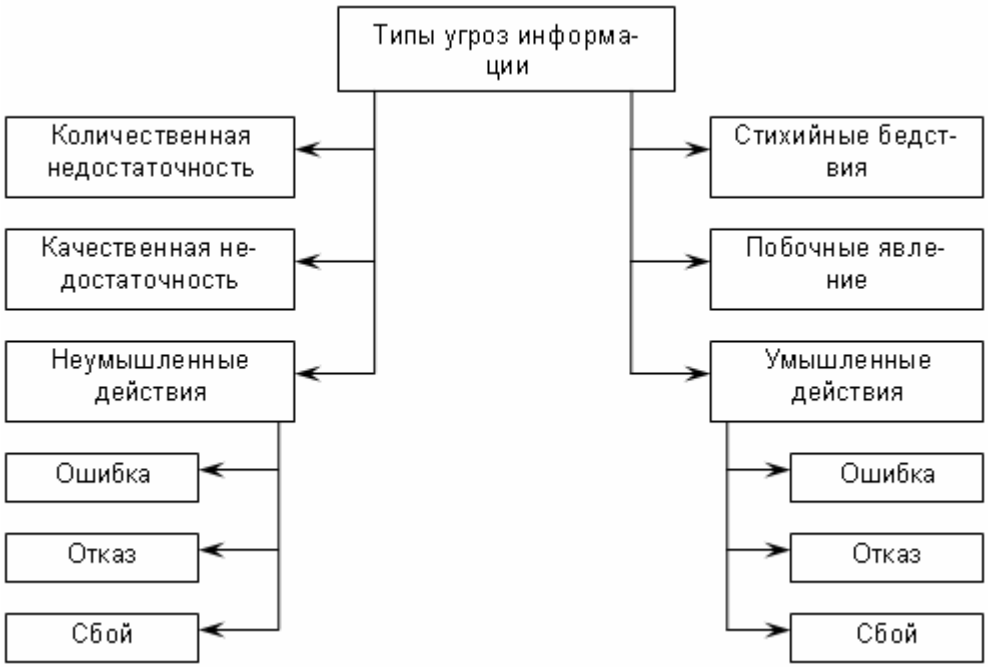


Рис. 2. Типы угроз информации.

Рис. 3. Виды угроз информации.

Для угроз доступности возможные потери могут быть рассчитаны следующим образом:

$$L = L_{ëò} + L_{â} + L_{ï} + L_{ïä}\ , \qquad (3)$$

где: $L_{ëò}$ - потери от несвоевременного оказания услуг по доступу к информации;

$L_В$ – потери, связанные с восстановлением работоспособности;

$L_П$ – потери, связанные с простоем узла КСС;

$L_{ПД}$ – потери, связанные с потерей дохода.

Для угроз целостности потери могут быть подсчитаны по следующей формуле:

$$L = L_{íì} + L_{â} + L_{ï} + L_{ïä}\ , \qquad (4)$$

где: $L_{íì}$ – потери от несанкционированной модификации информации. Размер потерь будет зависеть от значимости информации, целостность которой нарушена (указанные потери могут быть определены методами неформальных оценок.);

$L_В$ – потери, связанные с восстановлением работоспособности;

$L_П$ – потери, связанные с простоем узла КСС;

$L_{ПД}$ – потери, связанные с утратой возможного дохода.

Для угроз конфиденциальности сумма потерь определяется исключительно ценностью похищенной информации.

Потери, связанные с применением механизмов защиты зависят от двух обстоятельств. Во-первых, любое, даже самое совершенное средство защиты информации, как блок шифрования, средство разграничения доступа или средство сокрытия данных ограничены уровнем вычислительных, финансовых, временных ресурсов, применение которых оправдано для решения поставленных задач.

Во-вторых, следует учесть, что любое средство защиты информации должно отвечать ряду требований по эргономике. Данное требование связано с удобством эксплуатации указанного средства обслуживающим персоналом. В случае отсутствия документации на средство защиты информации в должном объеме, а также сложности его обслуживания, обслуживающий персонал будет расходовать свое рабочее время на выяснения вопросов, возникающих при эксплуатации средств защиты информации [4].

Исходя из изложенного выше, потери вызванные снижением производительности системы, связанные с использованием средств защиты данных, могут быть представлены следующим образом:

$$L_{çè} = D \cdot \sum_{i=1}^{N} \frac{t_{ñç_i} + t_{ñï_i}}{t_{ñç_i} + t_{ñï_i} + t_{îï_i}}; \qquad (5)$$

где: D – годовой доход от использования КСС;

N – количество узлов КСС;

$t_{ñç_i}$ - время, расходуемое средствами защиты информации для выполнения своих функций на i-ом узле системы;

$t_{ñï_i}$ - время, расходуемое персоналом i-го узла данной системы на выяснения вопросов, возникающих при эксплуатации средств защиты информации;

$t_{îï_i}$ - время, необходимое для обработки информации на i-ом узле системы (без учета времени, необходимого средствам защиты информации).

Для получения значений $t_{ñç_i}$ и $t_{ñï_i}$ необходимо внести выбранные средства защиты информации в модель функционирования КСС. Модель функционирования системы может быть формально представлена в виде функции:

$$F \rightarrow \{TS\}, \qquad (6)$$

где {TS}- формальное описание технологии функционирования КСС;

В качестве исходных данных функции будет выступать система обработки информации. Результатом указанной функции будет формальное описание технологии функционирования КСС. Указанные значения переменных могут быть получены как сумма потерь времени на участках технологических маршрутов системы. Потери времени могут быть рассчитаны по приведенным ниже зависимостям. Для линейного участка:

$$t_{ñç} = \sum_{i=1}^{N} t_{ñçè_i}; \qquad (7)$$

где: N – число средств защиты информации на участке;

$t_{ñçè_i}$ – время, расходуемое i-ым средством защиты информации на выполнение своих функций;

$$t_{ñï} = \sum_{i=1}^{N} t_{ñï_i}, \qquad (8)$$

где: $t_{ñï_i}$ – время, необходимое на выяснения вопросов, возникающих при эксплуатации средств защиты информации для пользователей, использующих *i*-ое средство защиты информации. Для циклического участка:

$$t_{ñç} = \sum_{j=1}^{K} \sum_{i=1}^{N} t_{ñçèi}\ , \qquad (9)$$

где: K – число циклов;

N – число средств защиты информации на участке;

$t_{ñçèi}$ – время, расходуемое i-ым средством защиты информации на выполнение своих функций;

$$t_{ñï} = \sum_{j=1}^{K} \sum_{i=1}^{N} t_{ñï\,i}\ , \qquad (10)$$

где $t_{ñï\,i}$ – время, необходимое на выяснения вопросов, возникающих при эксплуатации средств защиты информации для пользователей, использующих i-ое средство защиты информации.

Для участка ветвления значения $t_{ñç}$ и $t_{ñï\,i}$ могут быть получены как максимальные значения из числа возможных альтернатив.

Затраты, необходимые для использования механизмов защиты могут быть получены как сумма затрат на приобретение и использование механизмов защиты.

$$L = \sum_{j=1}^{M} C_j \times \gamma_j\ ; \qquad (11)$$

где: M - число существующих механизмов защиты;

C_j - цена использования j-го механизма защиты;

γ_j - признак использования j-го механизма защиты (γ_j равен 1 в случае использования j-го механизма защиты, в противном случае равен нулю).

Показатели эффективности средств защиты информации относятся к конкретному моменту времени либо небольшому отрезку времени. Поэтому, в общем виде, следует рассматривать использование системы защиты информации в течение заранее известного интервала времени (t_1, t_2). Указанный интервал будет продолжительной длины, - и будет представлять жизненный цикл КСС.

Подводя итоги следует сказать, что под оптимальностью использования средств защиты следует понимать достижение наивысших показателей защищенности при ограниченных затратах на использование средств защиты информации.

Литература

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ДиаСофт, 2002. – 688 с;
2. Герасименко В. А. Защита информации в автоматизированных средствах обработки данных. Книги 1,2. Москва: Энергоатомиздат, 1994. – 400с;
3. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
4. Скрипкин К.Г. Экономическая эффективность информационных систем – Москва:ДМК, 2002. – 252 с.

УДК 681.3

Капустян М.В., Хорошко В.А.

РАЗРАБОТКА ТРАФИКОВ ПЕРЕДАЧИ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ

В работе описывается алгоритм, который охватывает нейтральные детали, связанные с обратным ходом построения оптимального выходящего дерева для нахождения оптимальной конфигурации корпоративной сети.

При проектировании корпоративных сетей, разработке трафиков передачи информации постоянно приходится сталкиваться с задачами оптимизации. При этом особое внимание приходится уделять задачам определения в сети оптимальных конфигураций, имеющих структуру выходящих (растущих) лесов.

Во многих задачах синтеза сетей возникает следующая задача.

Задача 1. Задан орграф $G = (X, \theta)$, $|X| = n$, с корнем (источником) $x_0 \in X$, причем каждой дуге $u \in \theta$ приписана длина $l(u) > 0$. Требуется найти сграф $G' = (X, \theta'), \theta' \subset \theta$, в котором существует путь из вершины x_0 в любую другую вершину $x \in X \setminus \{x_0\}$ и сумма длин дуг которого минимальна.

Легко заметить, что сграф G' всегда будет иметь структуру выходящего дерева с корнем в вершине $x_0 \in X$. Для этого достаточно показать, что в каждую вершину $x \in X \setminus \{x_0\}$ сграфа G' заходит ровно одна дуга $u \in U$. В самом деле, если бы это было не так, то, взяв произвольную вершину $y \in X \setminus \{x_0\}$, в которую заходит более одной дуги, всегда можно выбрать такую заходящую дугу $u \in \theta$, которая принадлежит одному из простых путей $P(x_0, y)$ из x_0 в y. С удалением остальных заходящих в y дуг достижимость вершин $x \in X \setminus \{x_0\}$ из x_0 не нарушается. Таким образом, получается новый сграф, сумма длин дуг которого меньше чем у исходного.

Ясно, что задача 1 является некоторым обобщением задачи о построении минимального (по сумме длин ребер) связывающего дерева во взвешенном неориентированном графе [1], для решения которой существует довольно простой и эффективный алгоритм Прима-Краскала. Однако решение задачи 1 требует существенно иного подхода и алгоритма.

Эффективный алгоритм решения рассматриваемой задачи (в несколько иной формулировке) предложен Эдмондо [2]. В работах [3,4,5] появились иные модификации; наиболее интересной из них является модификация Фалкерсона [3] для проблемы оптимальной упаковки ориентированных корневых резервов. Этот алгоритм описан в [6], где отмечается, что трудная его часть есть обратный ход восстановления интересующего нас сграфа по его редукции. Поэтому, хотя сам алгоритм и не очень сложен, обратный его ход нужно четко определить и аккуратно реализовать.

Поэтому в работе приводится разработанный алгоритм, который охватывает нетривиальные детали, связанные с обратным ходом построения оптимального выходящего дерева и не приведенные в упомянутых выше работах. В действительности предлагаемым алгоритмом решается более общая задача.

Задача 2. Заданы орграф $G = (X, \theta), |X| = n$, каждой дуге $u = \theta$ которого приписана длина $l(u) > 0$, и некоторое подмножество вершин $X_0 \subset X, |X_0| = p (p < n)$, обладающие следующим свойством: для любого $y \in X \setminus X_0$ существует путь $P(x,y)$ из некоторой

$$x \in X_0 \text{ в } y. \qquad (1)$$

Требуется найти суграф $G' = (X, \theta'), \theta' \subset \theta$, удовлетворяющий условию (1) и обладающий минимальной суммой длин дуг.

Казалось бы, что рассмотрение этой задачи не дает ничего нового, так как добавлением к орграфу *G* новой вершины *z* (в качестве корня) и новых дуг V_i, *i=1,2,...,p* (исходящих из *z* и заходящих в соответствующие $x_i \in X_0$) с $l(V_i) = \varepsilon \left(< 0 \varepsilon < \min\limits_{u \in U} l(u) \right)$ сводится к задаче 1. На самом деле, ее изучение является существенным как для модификации вышеупомянутых алгоритмов, так и для исследования вопроса оптимального разбиения орграфа *G* на определенное количество подграфов с учетом построения минимальных (по сумме длин дуг) суграфа с корнями в соответствующих подграфах.

Кроме того, в отличие от Эдмонса и Фалкерсона, которые для обоснования предложенных ими алгоритмов использовали методы линейного программирования, будет дано наглядное обоснование, не выходящее за рамки теоретико-графовых рассуждений. Такой подход, как будет показано далее, полезен для решения и других оптимизационных задач, связанных с выбором не только оптимальной структуры искомого суграфа *G´*, но и соответствующего подмножества $X_0' \subset X$, в чем и заключается суть данной работы.

Для удобства дальнейшего изложения введем следующие определения и обозначения.

Определение 1. Орграф *T=(X,W)*, $|X| = n$, назовем выходящим лесом с базой $X_0 \subset X$, X, $|X_0| = p$, если он состоит из *p* компонент связности $T_i = (X_i, \theta_i), X_i \subset X, \theta_i \subset \theta$, *i=1,2,...,p*, где каждая компонента T_i представляет собой выходящее дерево с корнем $x_i \in X_0$ [7,8,9].

Легко заметить, что интересующий нас суграф *G´* в задаче 2 будет иметь всегда структуру выходящего леса с базой $X_0 \subset X$.

Для любого $Y \subset X$ обозначим через $\theta_G(Y)$ подмножество тех дуг $u \in q$, которые заходят в вершины *Y*; через L_G - сумму длин всего орграфа *G*.

Если в орграфе $G = (X, \theta)$ выделено подмножество $X_0 \subset X$, обладающее свойством (1), то можем записать $t(G) = X_0$.

Определение 2. Выходящий лес $T^* = (X, \theta^*)$ с базой $X_0 \subset X$ назовем минимальным выходящим лесом для орграфа G с $t(G) = X$, если $\theta^* \subset \theta$ и $L_{r*} = \min\limits_{W \subset \theta} L$, а выходящий лес $T^0 = (X, \theta^0)$ с базой $X_0 \subset X$ - максимальным выходящим лесом для орграфа G с $t(G) = X_0$, если $\theta^0 \subset \theta$ и $L_{r0} = \max\limits_{W \subset \theta} L$ и $t(T) = X_0$.

Определение 3. Пусть $Y \subset X$ - произвольное подмножество вершин. Сечением $\sigma_G(Y)$ орграфа G по Y назовем подмножество дуг $\theta' \subset \theta'$, имеющих начало в X\Y и конец в Y.

Определение 4. Приведением орграфа G по $\sigma_G(Y)$ назовем операцию уменьшения длин всех дуг $u \in \sigma_G(Y)$ на величину $t(u^*) = \min\limits_{u \in \sigma_G(Y)} t(u)$.

Дуга $u^* \in \sigma_G(Y)$ будет выделенной дугой по $s_G(Y)$, а величина $t(u^*)$ - константой приведения по множеству Y.

Алгоритм решения задачи 2 начинается с формирования простого программного счетчика CAL и массива MASS. В счетчике CAL накапливается значение L_{T^*} минимального выходящего леса, а в массиве MASS- соответствующие дуги, ему принадлежащие.

Предлагаемый алгоритм включает следующее:

1. Приводим орграф G по $\sigma_G(\{x\})$, $Vx \in X \setminus X_0$, и прибавляем сумму констант приведения к счетчику CAL (до начала работы алгоритма содержимое счетчика равно нулю).

2. Берем $i = I$.

3. Всем выделенным дугам $u \in U$ приписываем метки $\alpha(u) = i$.

4. Находим сураф $G^i = \left(X, \theta^i\right)$, где $\theta^i \subset \theta$ - множество всех выделенных дуг.

5. Проверяем, обладает ли сураф G^i свойством (1). Если да, то переходим к п.10, в противном случае- к п.6.

6. Находим сильно связные компоненты $G^i_j = \left(X^i_j, \theta^i_j\right)$, $j=1,2,\ldots,q_i$, в суграфе G^j, которые не содержат вершин $x \in X_0$.

7. Приводим орграф G по $\sigma_G(X^i_j)$, $j=1,2,\ldots,q_i$ и сумму констант приведения прибавляем к счетчику CAL.

8. Новым полученным выделенным дугам $u \in q$ приписываем метки $\alpha(u) = i+1$.

9. Заменяем *i* на *i+1* и переходим к п.4.

10. Берем множество $Z = X_0$.

11. В множестве всех выделенных дуг $\theta^* \subset \theta$, принадлежащих сечению $\sigma_G(X \setminus Z)$, выбираем одну из $u \in \theta^*$, имеющую наименьшую $a(u)$.

12. Находим величину $x \in X \setminus Z$, в которую заходит выбранная дуга $u \in \sigma_G(X \setminus Z)$.

13. Дуги *u* включаем в массив MASS, а множество Z заменяем на $ZU(x)$.

14. Проверим, имеет ли место $Z = X$. Если да, то переходим к следующему пункту, в противном случае - к п.11.

15. Выводим содержание CAL и MASS на дисплей или печать.

Замечание 1. В этом алгоритме можно выделить два этапа: прямой ход алгоритма- пункты 1-9 и обратный ход- пункты 10-15. В отличие от алгоритмов, изложенных в [2,3], здесь не требуется выполнения операции стягивания, а это облегчает реализацию обратного алгоритма.

Замечание 2. Метки $\alpha(u)$, применяемые в изложенном выше алгоритме,- целые числа от 1 до К, где к- число итераций прямого хода алгоритма (одна итерация определяется переходом к 5-му пункту алгоритма). В принципе, в качестве меток могут быть использованы произвольные элементы некоторого упорядоченного множества.

Особое внимание следует уделять 6-му пункту алгоритма. Для нахождения сильно связных компонент орграфа в [10] предложен эффективный алгоритм. Поскольку структура сильно связных компонент $G^i_j = \left(X^i_j, U^i_j\right)$, j=1,2,…,$q_i$ суграфа G^i_{j-1} такова, что каждая из сильно связных компонент $G^{i-1}_j = \left(X^{i-1}_j, U^{i-1}_j\right)$, j=1,2,…,$q_i$ суграфа G^{i-1}_j содержится в качестве подграфа в одной из G^i_j, то при использовании здесь этого алгоритма на каждой итерации нужно исходить из имеющегося первоначального разбиения множества

вершин на классы (результат применения упомянутого алгоритма на предыдущей итерации), а далее проводится ею без изменения.

Литература

1. Прим Р.К. Кратчайшие связывающие сети и некоторые обобщения.-/Кибернетический сборник, 1961, №2.-с.95-107;
2. Edmonda J. Optimum Branching.-J.res.Nat. bureau standards. Ser.B, 1967,718, №4.-p.233-240;
3. Fulkerson D.R. Packing rooted directed cuts in a weighted directed graf.-Math.Program., 1974,6, №1.p.1-13;
4. Karp R.M. A simple derivation of Edmonds' algorithm for optimum branching. –Network, 1971, 1, №3.p.265-272;
5. Dorfler, Willibald. Der lerbores zenzengraph eines gerichteten Grafen. –Math.Nachr., 1974, 59, №1-6.P.35-49;
6. Романовский И.В. Алгоритмы решения экстремальных задач. –М.: Наука, 1987. 284с;
7. Зыков А.А. Теория конечных графов. –Новосибирск: Наука, 1969ю -244 с;
8. Берж К. Теория графов и ее применение. –М.: ИЛ, 1962. -308 с;
9. Харари Ф. Теория графов. –М.: Мир, 1973. -342 с;
10. Фараджев И.А. Эффективные алгоритмы решения некоторых задач для ориентированных графов //Вычислительная математика и математическая физика, 1990, 10, №4. –с.1949-1954.

УДК 004.056

Браіловський М.М., Габович А.Г., Горобець А.Ю., Хорошко В.О.

КІЛЬКІСНО-ЯКІСНА ОЦІНКА РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті надана кількісно-якісна оцінка інформаційної безпеки життєво важливих інтересів особи, суспільства та держави від внутрішніх та зовнішніх загроз.

Існування і розвиток сучасних держав відбуваються в тісному зв'язку з геополітичними геостратегічними умовами і значною мірою залежить від відносин у суспільстві. При цьому все більшого значення надається забезпечення національної безпеки – стану захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз.

Серед багатьох факторів, що впливають на формування зовнішньої і внутрішньої політики держав, визначальна роль належить національній безпеці. Досвід України яскраво свідчить про те, що справжня державна незалежність існує тільки за умови надійного забезпечення національної безпеки та її составної частини інформаційної безпеки.

У зв'язку з цим розробка цілісної теорії інформаційної безпеки України залишається актуальною проблемою на шляху створення наукових засад формування і реалізації політики держави та суб'єктів діяльності в сфері інформаційної безпеки.

Інформаційна безпека України є об'єктивно існуюча реальність, що перебуває під впливом змін умов і чинників політичного, економічного, воєнного, науково-технічного і соціального характеру. Дуже важливо визначити зміст та взаємозв'язок характеристик інформаційної небезпеки, а також основні умови реалізації пріоритетів у інформаційній сфері.

Схема кількісно-якісної оцінки рівня інформаційної безпеки у суспільних відносинах відображена на рис.1. Кожний з етапів оцінки має конкретний, взаємопов'язаний з іншими етапами зміст, який у сукупності визначає порядок дій під час аналізу суспільної обстановки та визначення рівня інформаційної безпеки України.

І етап. Загальна оцінка стану відносин у суспільстві.

1. Вихідні дані:

- наявність, характер і кількісний вимір спонукального мотиву атаки (W);
- можливі втрати порушника у разі атаки (V);
- коефіцієнт експансії з боку потенційного порушника (Kn);
- величини потенціалів як порушника, так і сторони яка захищається;

– очікувані величини втрат сторін у разі атаки на інформацію;
– співвідношення сил сторін (G).

2. Можливі висновки:
– щодо рівня стабільності у суспільстві:
– баланс сил та інтересів ($Kn \approx 0, G \approx 1$);
– стабільність на основі балансу сил ($0<Kn<1$, $G \approx 1$);
– стабільність на основі балансу інтересів ($Kn \approx 0$, $0<G<\neq 1$);
– відносна стабільність на основі стримування ($Kn>1$, $G<1$);
– нестабільність на основі дисбалансу сил та інтересів ($Kn \geq 1{,}5$, $G \geq 1{,}5$);
– щодо наявності і характеру інформаційної небезпеки:
– відсутність вираженої інформаційної небезпеки;
– потенційна інформаційна небезпека;
– реальна інформаційна небезпека;
– інформаційна загроза, безпосередня інформаційна загроза;

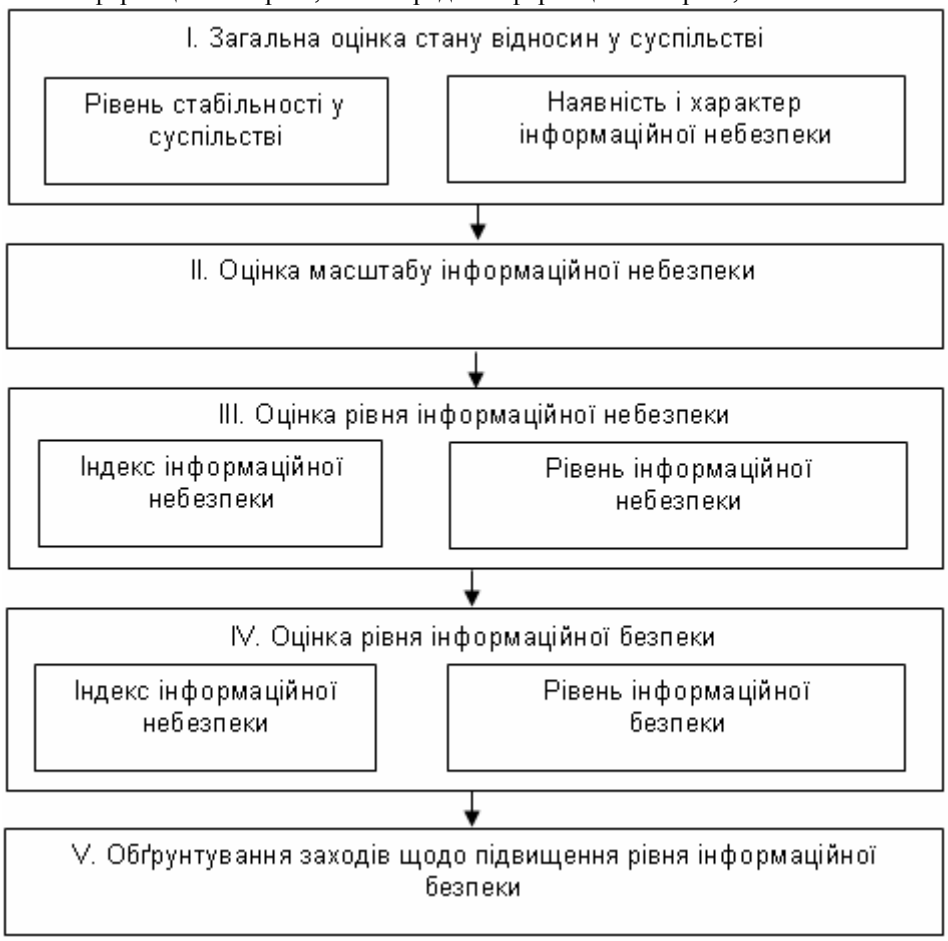


Рис. 1. Загальна схема оцінки рівня інформаційної безпеки.

3. Оцінка потенційного порушника:
– евентуальний порушник (відсутність вираженої інформаційної небезпеки);
– потенційний порушник (потенційна інформаційна небезпека);
– імовірний порушник (реальна інформаційна небезпека);
– конкретний порушник (інформаційна загроза, безпосередня інформаційна загроза).

ІІ етап. Оцінка масштабу інформаційної небезпеки.

1. Вихідні дані:

– висновки за етапом І;
– просторовий розмах можливої атаки (Sa).

2. Можливі висновки:

– щодо масштабу можливої зовнішньої атаки (Мза):
– локальний;
– регіональний;
– загальнонаціональний;
– глобальний;
– щодо масштабу інформаційної небезпеки:
– локальний (Мінб $\leq 1\%$);
– регіональний (1%<Мінб $\leq$ 10%);
– загальнонаціональний, глобальний (Мінб>10%).

ІІІ етап. Оцінка рівня інформаційної небезпеки.

1. Вихідні дані – висновки за етапами І, ІІ.
2. Можливі висновки:

– щодо імовірності розв'язання інформаційної атаки (Ррозв = 0,...,1,0);
– щодо імовірності невідбиття атаки (Рневід = 0...1,0);
– щодо чисельного значення індексу інформаційної небезпеки (Рінб = 0...1,0);
– щодо рівня інформаційної небезпеки:
– низький;
– підвищений;
– критичний.

IV етап. Оцінка рівня інформаційної безпеки.

1. Вихідні дані – висновки за етапами І-ІІІ.
2. Можливі висновки:

– щодо імовірності відвернення інформаційної атаки (Рвідв = 0...1,0);
– щодо імовірності відбиття атаки (Рвідб = 0...1,0);
– щодо чисельного значення індексу інформаційної безпеки (Ріб = 1-Рінб);
– щодо рівня інформацйної безпеки:
– задовільний;
– нестійкий;
– критичний.

V етап. Обгрунтування заходів щодо підвищення рівня інформаційної безпеки.

1. Вихідні дані – висновки за етапами І-IV.
2. Основні напрями:

– пасивне відвернення атаки;
– підвищення ефективності активного відвернення потенційної атаки зловмисника;
– підвищення можливості щодо відбиття атаки, яка перебачається.

Викладений підхід стосується відносин, коли розглядається лише один можливий напрям інформаційної небезпеки (один зловмисник).

Якщо інформаційна небезпека находить одночасно від декількох зловмисників, то залежно від конкретних обставин можуть бути використані такі способи визначення рівня інформаційної небезпеки.

Варіант1: інформаційна небезпека походить одночасно від двох або більше зловмисників, які утворюють злочинну групу.

Цей варіант припускає одночасну атаку декількох зловмисників. Така кооліція має розглядатися як єдиний зловмисник чи порушник з єдиними інтересами.Тому підхід до визначення всієї сукупності характеристик інформаційної небезпеки в цій ситуації відрізняється від підходу, що використовується для оцінки одного зловмисника, лише тим, що

інтереси і можливості злочинного угрупування необхідно належним чином узагальнювати та підсумовувати.

Варіант 2: інформаційна небезпека походить від двох або більше зловмисників, які не є спільниками. Якщо одночасна атака цих зловмисників виключена або малоімовірна, то слід оцінювати загальний рівень інформаційної небезпеки за найбільш небезпечним напрямом, якщо одночасна атака не виключається, то рівень інформаційної небезпеки слід оцінювати за варіантом 3.

Варіант 3: інформаційна небезпека походить від декількох зловмисників, інтереси і дії яких можуть збігатися за часом, тобто не виключена одночасна атака цих зловмисників.

За такої ситуації оцінка інформаційної небезпеки з боку кожного із зловмисників здійснюється з урахуванням можливості одночасної інформаційної атаки, внаслідок чого можна очікувати зменшення величин програшу та збільшення величини співвідношення сил за рахунок роздрібнення сил та засобів захисту інформацій – об'єкта атаки за декількома напрямами. Одержані в результаті такої оцінки значення індексів інформаційної небезпеки та масштабу інформаційної небезпеки узагальнюються таким чином:

– для двох напрямів інформаційної небезпеки (позначені цифрами 1 і 2) загальний індекс інформаційної небезпеки визначається за формулою:

$$Рінб_{\Sigma} = Рінб_1 + Рінб_2 - Рінб_1 \cdot Рінб_2, \qquad (1)$$

а загальний масштаб очікуваної атаки за формулою:

$$Mia_{\Sigma} = Mia_1 + Mia_2. \qquad (2)$$

– для трьох напрямів атаки

$$Ð^3íá_{\Sigma} = Ð^3íá_1 + Ð^3íá_2 + Ð^3íá_3 - Ð^3íá_1 \cdot Ð^3íá_2 - Ð^3íá_1 \cdot Ð^3íá_3 - Ð^3íá_2 \cdot Ð^3íá_3 + Ð^3íá_1 \cdot Ð^3íá_2 \cdot Ð^3íá_3 \qquad (3)$$

$$Ì^3à_{\Sigma} = Ì^3à_1 + Ì^3à_2 + Ì^3à_3. \qquad (4)$$

Очевидно, що величина Mia за своїм фізичним змістом не може перевищувати одиницю, тому, якщо одержане за формулами (2) або (4) значення Mia_{Σ} внаслідок похибок більше за одиницю, слід важати його таким, що дорівнює одиниці.

На основі розрахованих індексу і масштабу інформаційної небезпеки визначення рівня інформаційної безпеки в разі багатосторонніх відносин між зловмисниками за такою ж методикою, як і вразі одного зловмисника.

Вибір та обгрунтування заходів, спрямованих на підвищення рівня інформаційної безпеки, здійснюються з урахуванням накопиченого в світі досвіду відвернення атаки та припинення атак на інформацію як через власні зусилля – об'єкта атаки, так і за допомогою державних інститутів безпеки. Для цього також потрібні певні методичні підходи, які забезпечили б достатню ефективність таких заходів при раціональних витратах на їх здійснення.

Заходи, спрямовані на підвищення рівня інформаційної безпеки, як правило, мають комплексний характер, оскільки охоплюють одночасно політичну, економічну, воєнну та інші сфери діяльності держави. При цьому кожна конкретна ситуація потребує своїх пріоритетів у формуванні політики забезпечення інформаційної безпеки. Визначення цих пріоритетів є складним і відповідальним завданням державної політики, оскільки можливі помилки здатні призвести до без результативності зусиль, що докладаються, та (або) до нераціональності витрат, які при цьому здійснюються. Вихідні аксіоматичні положення, на основі яких доцільно вирішувати це завдання, можна сформулювати так:

– визначення основних напрямів забезпечення інформаційної безпеки має здійснюватися в інтересах найбільшої ефективності заходів, що вживаються, при мінімальних витратах часових, фінансових, матеріальних і людських ресурсів;

– головним стратегічним напрямком забезпечення інформаційної безпеки в будь-якій ситуації є запобігання ушкодження, знищення, отримання або модифікування інформації, яке в свою чергу, є найбільш ефективним шляхом відвернення або відбиття атаки;

– заходи, спрямовані на стримування можливої атаки та на підготовку до її відбиття є найбільш витратними і можуть у деяких випадках форсувати загострення відносин у суспільстві.

Магістральними шляхами забезпечення інформаційної безпеки є пасивне відвернення атаки, активне відвернення або відбиття можливої атаки. На кожному з цих шляхів відповідними зусиллями створюються необхідні передумови для того, щоб атака не відбулася або хоча б не потягла за собою тяжких наслідків. Ці передумови можуть характеризуватися відповідними кількісними показниками.

На рис. 2 і 3 наведені графіки залежності індексу інформаційної безпеки (Ріб) від імовірносте й пасивного відвернення атаки (Рпас) і відбиття інформаційної атаки (Рвід) відповідно до проведених авторами досліджень. Аналіз графіків дає змогу зробити такі висновки:

– переважний вплив на величину Ріб, особисто в області її малих та середніх значень, здійснює імовірність відбиття атаки Рвід;

– величина Рпас здійснює приблизно такий самий, як і величина Рвід або переважаючий вплив на індекс інформаційної безпеки лише в області його великих значень, і то за умови, коли величина Рвід не перевищує значення, що дорівнює 0,5.

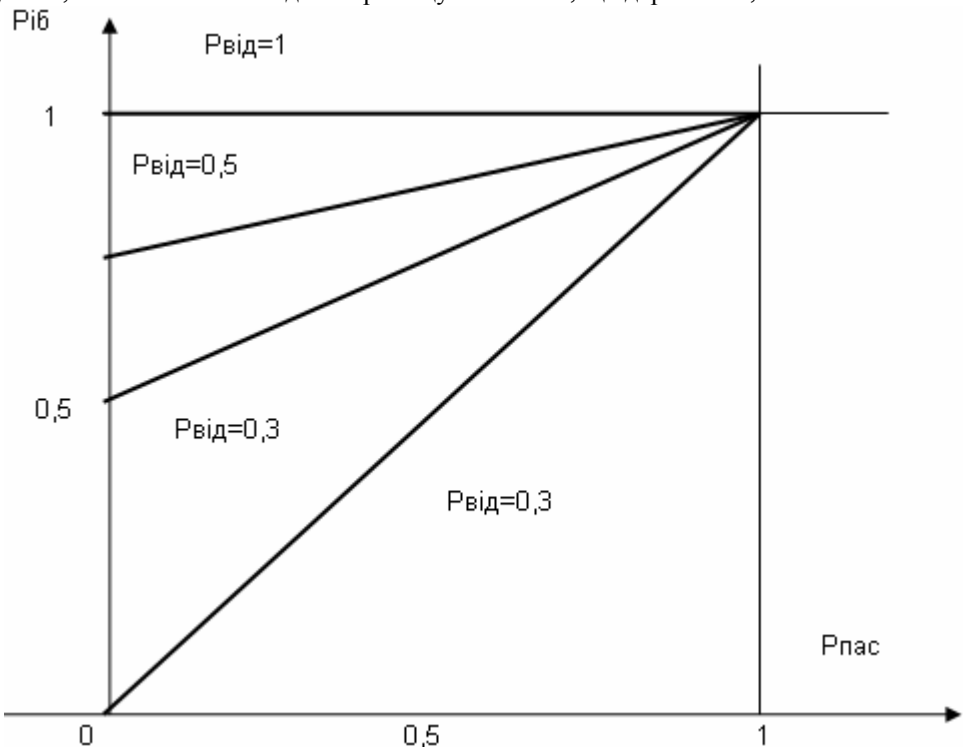


Рис. 2. Залежність індексу інформаційної безпеки від імовірності.

Зазначені особливості пояснюються тим, що, по-перше, величина Рвід здійснює на індекс інформаційної безпеки подвійний вплив, оскільки вона відображає як можливості щодо відбиття потенційної атаки, так і можливості щодо її активного відвернення, по-друге, якщо при складанні імовірносте й відповідно до формул (2), сумарний результат досягає значної величини за рахунок одного з доданків, то подальший відносний вплив цього доданка зменшується, проте зростає відносна значущість другого доданка, який до цього визначальної ролі не відігравав.

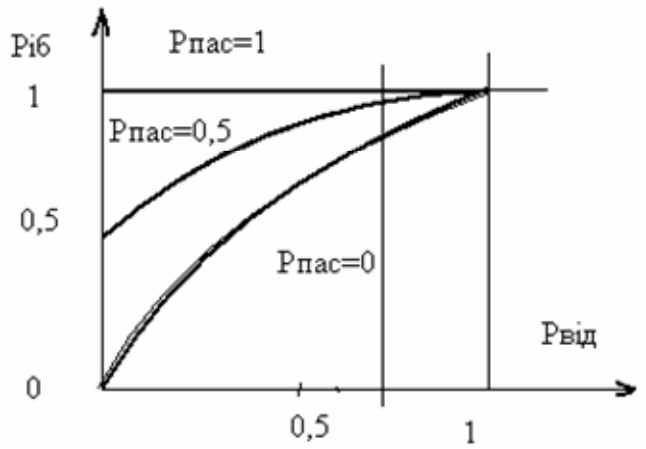


Рис. 3. Залежність індексу інформаційної безпеки від імовірності відбиття атаки.

УДК 681.3

Дудикевич В.Б., Гарасимчук О.І., Максимович В.М.

КІЛЬКІСНЕ ОЦІНЮВАННЯ ГЕНЕРАТОРА ПУАССОНІВСЬКОЇ ІМПУЛЬСНОЇ ПОСЛІДОВНОСТІ ПОБУДОВАНОГО НА ОСНОВІ ЛІНІЙНОГО КОНГРУЕНТНОГО ГЕНЕРАТОРА

В статті проведене дослідження базового генератора лінійного конгруентного методу та реалізованого на його основі генератора пуассонівського імпульсного потоку за допомогою групи графічних та оціночних тестів. Наведені результати цього тестування.

1. Постановка проблеми

Генератори пуассонівської імпульсної послідовності (ГПІП) – це важливий клас генераторів імпульсних послідовностей, які знайшли широке застосування в різних галузях техніки. Особливо широко такі генератори використовуються у вимірювальній, обчислювальній техніці та при моделюванні різноманітних процесів.

Для простого пуассонівського потоку імовірність появи рівно k імпульсів за час t підпорядковується закону Пуассона [1], [2]:

$$P_k(Z,t) = \frac{(Zt)^k}{k!} e^{-Zt}, \qquad (1)$$

де Z – середнє число імпульсів за одиницю часу (середня інтенсивність).

Пуассонівським законом розподілу описуються події, які трапляються дуже рідко. Також на основі простого потоку пуассонівських імпульсів можна отримати більш складні потоки, наприклад, потік Ерланга [2].

Актуальною задачею, на сьогоднішній день, є ґрунтовне дослідження алгоритмів побудови ГПІП і оцінка їх якості.

2. Аналіз останніх досліджень

Проблемі оцінки та дослідженню ГПІП на сьогоднішній день не надається належної уваги, хоча ця проблема є досить актуальною.

Відомим фактом є те, що для того щоб отримати псевдовипадкову послідовність з пуассонівським законом розподілу, необхідно спочатку отримати рівномірно розподілену псевдовипадкову послідовність чисел.

Питаннями отримання псевдовипадкових рівномірно розподілених чисел вчені займаються дуже давно і на сьогоднішній день існує велика кількість алгоритмів, за допомо-

гою яких можна отримати такі псевдовипадкові послідовності. Деякі з них наведені в роботах [1 – 7].

Для досліджень і оцінки якості генераторів псевдовипадкових послідовностей використовують, в основному, дві групи тестів:

– графічні тести – на основі яких користувач отримує певні графічні залежності та робить висновки про властивості псевдовипадкової послідовності, що тестується;

– оціночні тести – на основі певних оціночних критеріїв робиться висновок про степінь близькості статистичних властивостей псевдовипадкової послідовності, що тестується, до дійсно випадкової послідовності.

Більшість відомих тестів якраз і є присвячена дослідженню рівномірності розподілу псевдовипадкової послідовності. Але оцінювати кількісно чи якісно таку псевдовипадкову послідовність бажано не за допомогою одного тесту, а з використанням кількох тестів, оскільки тоді на основі загальної картини оцінки можна зробити більш точний висновок про якість послідовності, що досліджується. Окрім цього необхідно проводити оцінку якості кінцевого результату генерування – пуассонівської імпульсної послідовності.

3. Мета роботи

Метою даної роботи є кількісне та якісне оцінювання базового генератора рівномірно розподілених чисел, побудованого на основі лінійного конгруентного методу, а також оцінювання ГППП, реалізованого на основі цього генератора, з використанням групи тестів (графічних та оціночних).

4. Дослідження якості ГППП

Дослідження проводилось за допомогою імітаційного моделювання на алгоритмічній мові Turbo Pascal в два етапи:

– дослідження генератора псевдовипадкових рівномірно розподілених чисел;

– дослідження ГППП.

Оскільки, як було згадано вище, оцінювання небажано проводити за допомогою лише одного тесту, в даному дослідженні для оцінювання лінійного конгруентного генератора використаємо один графічний тест і сім оціночних, а для оцінювання ГППП використаємо один графічний та один оціночий тест. Таким чином ми отримаємо і кількісні, і якісні оцінки. Лінійний конгруентний метод описується формулою:

$$X_{n+1} = (a\,X_n + b) \bmod c \qquad (2)$$

Правила вибору параметрів a, b та c детально описані у багатьох авторів, зокрема в [3], [4], [6]. При правильно підібраних параметрах період псевдовипадкової послідовності повинен бути максимальним і дорівнювати c.

Для оцінювання лінійного конгруентного генератора використаємо наступні тести: розподіл на площині (графічний) та перевірка кореляції, тест дірок, частотний монобітний тест, монотонний тест, тест перестановок що перетинаються, тест перестановок, перевірка незціплених серій (оціночні тести).

Для оцінювання ГППП використаємо той факт, що кількість імпульсів пуассонівського імпульсного потоку, що зафіксована за час T_a:

а) з надійною ймовірністю p =0,68 знаходиться в межах [8]:

$$k_{ñåð} - \sqrt{k_{ñåð}} < k < k_{ñåð} + \sqrt{k_{ñåð}}\,, \qquad (3)$$

б) з надійною ймовірністю p =0,95 знаходиться в межах:

$$k_{ñåð} - 2\sqrt{k_{ñåð}} < k < k_{ñåð} + 2\sqrt{k_{ñåð}}\,, \qquad (4)$$

в) з надійною ймовірністю p =0,997 знаходиться в межах:

$$k_{ñåð} - 3\sqrt{k_{ñåð}} < k < k_{ñåð} + 3\sqrt{k_{ñåð}}\,, \qquad (5)$$

де $k_{ñåð}$ – середня кількість імпульсів за час T_a.

Також використаємо відомий оціночний тест – критерій χ^2, що використовується для оцінки псевдовипадкових послідовностей з довільним законом розподілу [2], [4], [9]:

$$\chi^2 = \sum \left(n_i - n_i^{'}\right)^2 / n_i^{'} \qquad (6)$$

де n_i – емпіричні частоти, $n_i^{'}$ – теоретичні частоти.

Отримання імпульсної послідовності з законом розподілу наближеним до пуассонівського базується на структурній схемі, в основі якої є генератор псевдовипадкових рівномірно розподілених чисел і схема порівняння [10]. При цьому імпульси вихідної послідовності формуються при умові, що ці числа є меншими від керуючого коду.

При дослідженні ГПІП, послідовність тактів, кожен з яких відповідає черговому значенню псевдовипадкового числа, буде розбита на n інтервалів по i_{max} тактів. Максимальну кількість інтервалів n позначимо n_{max}. Необхідно також дотримуватись виконання умови, що забезпечує повний період повторення псевдовипадкової послідовності чисел per:

$$i_{max} * n_{max} < per \qquad (7)$$

Для дослідження лінійного конгруентного генератора, згідно правил та попереднього пробного тестування на якість, були вибрані наступні параметри a=12345; b=12345, c=2^{30}.

При дослідженні було прийнято, що вхідна частота f_0=1 Мгц, вихідна частота $f_{âèõ}$ може приймати значення 100 чи 1000 Гц, час вимірювання, що відповідає одному інтервалу n, дорівнює $T_â = i_{max} / f_0$ = 0,01 с і 0,1 с. В результаті оцінювання генератора М-послідовності за допомогою тесту розподілу на площині були отримані результати тестування, які наведені на рис. 1. На даному рисунку x – поточне, а x_p – попереднє значення випадкового числа отриманого на виході генератора М-послідовності.

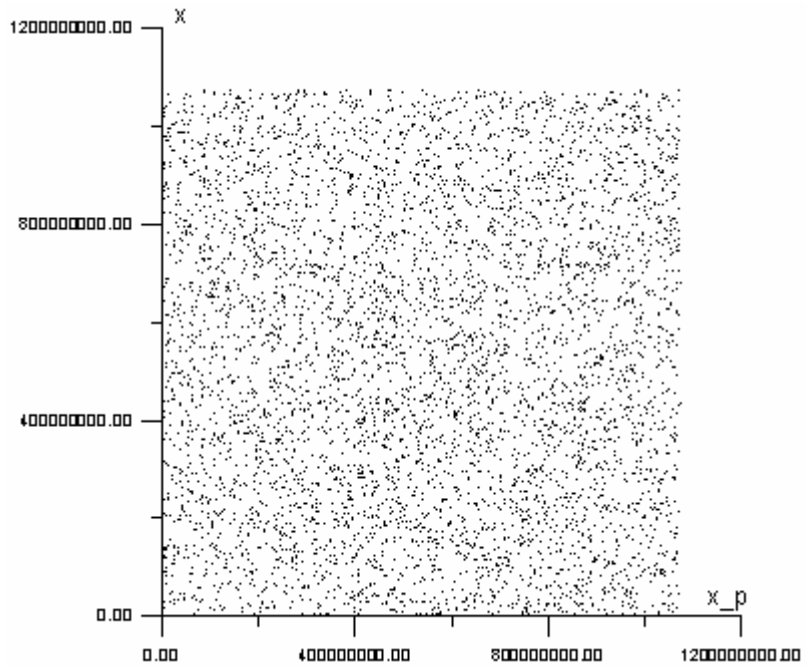


Рис. 1. Розподіл на площині лінійного конгруентного генератора.

Як видно з рисунку, площина повністю заповнена точками, що свідчить про рівномірність розподілу псевдовипадкових чисел.

При дослідженні лінійного конгруентного методу з даними параметрами за допомогою оціночних тестів, для різних значень добутку $i_{max} * n_{max}$ були отримані результати наведені в Таблиці 1. В даній таблиці "+" означає, що тест пройдено, а "–" означає, що тест не пройдено.

Таблиця 1.

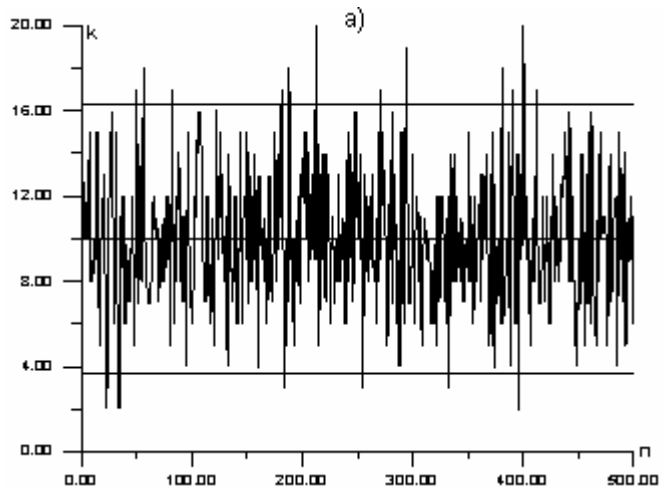
Результати оціночного тестування генератора М-послідовності.

Вид оціночного тесту	$i_{max} * n_{max}$	
	5000000	50000000
Перевірка кореляції	+	+
Перевірка перестановок, що пересікаються	+	+
Перевірка на монотонність	+	+
Перевірка перестановок	+	+
Тест дірок	+	+
Перевірка незціплених серій	+	+
Частотний монобітний тест	+	+

Отже, при правильному виборі параметрів лінійного конгруентного генератора, він проходить всі тести на випадковість і рівномірність розподілу, що свідчить про його високу якість.

Тепер потрібно провести графічне та оціночне тестування ГПІП побудованих на основі лінійного конгруентного генератора з різними параметрами.

Статичні характеристики ГПІП наведені на рис. 2. На даному рисунку k – це кількість імпульсів на виході ГПІП за час $T_â$, а n – це кількість інтервалів часу $T_â$. Межі вказані згідно формули (4), тобто для надійної ймовірності p =0,95.



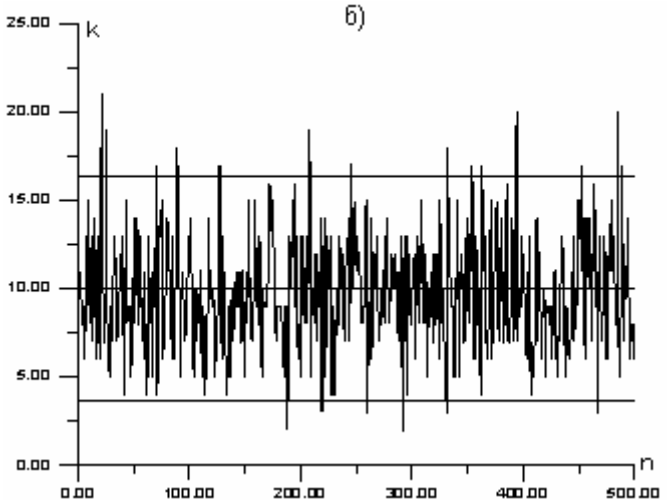


Рис. 2. Статичні характеристики ГПІП:
а) при $f_{âèõ}$ =1000 Гц і $T_â$ =0,01 с; б) при $f_{âèõ}$ =100 Гц і $T_â$ =0,1 с.

Кількісні оцінки при дослідженні згідно формул (3), (4), (5) наведені в Таблиці 2.

Як видно з Таблиці 2 псевдовипадкові послідовності на виході ГПІП володіють статистичними властивостями наближеними до теоретичних, що становлять для p =0,95 – 5, для p =0,68 – 32, для p =0,997 – 0,3.

Таблиця 2.

Значення $f_{âèõ}$ і $T_â$	Діапазон дослідження (значення n)	Кількість значень k, що виходить за межі згідно формул (3) – (5)		
		для p =0,95	для p =0,68	для p =0,997
$f_{âèõ}$ =1000 Гц і $T_â$ =0,01 с	0 – 100	5	26	0
	100 – 200	3	24	0
	200 – 300	4	28	1
	300 – 400	5	30	1
	400 – 500	1	26	0
$f_{âèõ}$ =100 Гц і $T_â$ =0,1 с	0 – 100	4	27	1
	100 – 200	2	26	0
	200 – 300	5	21	0
	300 – 400	5	27	1
	400 – 500	4	31	1

При оцінюванні послідовностей отриманих на виході ГПІП з допомогою статистичного критерію оцінки якості χ^2 були отримані кількісні результати, які наведені в Таблиці 3.

Таблиця 3.

Кількісна оцінка ГПІП на основі статистичного критерію χ^2

	при $f_{âèõ}$ =1000 Гц і $T_â$ =0,01 с;	при $f_{âèõ}$ =100 Гц і $T_â$ =0,1 с;
Результат тестування	тест пройдено	тест пройдено

Отже ще раз отримане підтвердження того що якість ГПІП, що досліджується, є високою.

5. Висновки

Проведені кількісні та якісні дослідження ГППП показують, що такі генератори мають статистичні характеристики максимально наближені до теоретичних, що підтверджено кількісним та якісним оцінюванням базового лінійного конгруентного генератора. Оскільки при оцінюванні рівномірності та випадковості базового лінійного конгруентного генератора вищенаведені тести були пройдені повністю, то доцільно при побудові ГППП на основі лінійних генераторів використовувати саме ці тести.

Література

1. Гарасимчук О.І., Максимович В.М., «Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості", "Захист інформації", м.Київ, 2002, 7 стор., 1 іл;
2. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ – ОБРАЗ, 2003 – 240 с. – (СКБ – специалисту по компьютерной безопасности);
3. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А., Защита информации в компьютерных системах – К.: "Корнейчук", 2000. – 152с.;
4. Кнут Д. Искусство программирования для ЭВМ: В 3-х т. Получисленные алгоритмы. Пер. с англ. – М.: Мир, 1977. – Т.2. – 724 с;
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. И доп. – М.: Радио и связь, 2001. – 376 с.;
6. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ – ОБРАЗ, 2001 – 368 с;
7. Гарасимчук О.І., Максимович В.М., "Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей", Вісник Національного університету "Львівська політехніка" "Комп'ютерна інженерія та інформаційні технології";
8. Моисеев А.А., Иванов В.И. Справочник по дозиметрии и радиационной гигиене. 4-е изд., перераб. и доп. – М.: Энергоиздат, 1990. – 251 с;
9. Гурман В.Е. Теория вероятностей и математическая статистика. Учеб. пособие для втузов. Изд. 5-е, перераб. и доп. М., "Высшая школа", 1977;
10. Гарасимчук О.І., Дудикевич В.Б., Максимович В.М., Смук Р.Т. "Генератори тестових імпульсних послідовностей для дозиметричних пристроїв", Вісник Національного університету "Львівська політехніка" "Теплоенергетика. Інженерія довкілля. Автоматизація", 2004, с.187 - 193, 4 іл.

УДК 681.03

Дудикевич В.Б., Ломницький І.Б., Опірський І.Р.

АНАЛІЗ ЗАСОБІВ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ ПОВІДОМЛЕНЬ В ЦИФРОВИХ ЗОБРАЖЕННЯХ

Виявлення прихованих повідомлень в середовищі цифрових зображень, тобто стеганоаналіз зображень, є новим та перспективним напрямом у сфері інформаційної безпеки. Механізми стеганоаналізу розвинуті ще досить слабо і потребують дослідження та вдосконалення. Відомі на сьогодні засоби стеганоаналізу умовно можна поділити на дві головні категорії:

– засоби, які враховують відомі алгоритми вбудовування;
– засоби „сліпого" стеганоаналізу.

Для підвищення ефективності стеганоаналізу зображень можна використати комплексний підхід, який поетапно використовує різні механізми стеганоаналізу, починаючи з найпростіших. На основі сумарної оцінки робиться висновок, чи присутнє в зображені приховане повідомлення, чи ні.

Вступ

Важливим напрямком в галузі інформаційної безпеки, поява якого пов'язана із вимогами сьогодення, є стеганоаналіз. Стеганоаналіз, як вітка в стеганографії, виник подібно як і криптоаналіз в криптографії. Головним завданням стеганоаналізу є виявлення самого факту присутності прихованих повідомлень в стеганоконтейнері, який зазвичай є файлом,

котрий візуально не викликає підозр на присутність вбудованої інформації. Якщо ця мета досягнута, то можна вважати, що система практично зламана. Проте, маючи справу з ключовою стегосистемою, немає гарантій того, що зламавши систему перший раз ми це зможемо зробити знову в наступному сеансі зв'язку, при зміненому стегоключі. Якщо ж ми можемо визначити й стеганоключ, за допомогою якого таємне повідомлення вбудовується у чистий контейнер, то тоді ми можемо вважати, що система зламана повністю. Далі, у залежності від мети, яку переслідує несанкціонований учасник процесу передачі конфіденційних повідомлень, приховане повідомлення, при можливості, може бути прочитаним, модифікованим або знищеним.

Подібно криптоаналізу, стеганоаналіз покликаний досліджувати стійкість стеганографічних алгоритмів вбудовування інформації до певних видів атак. При успішному стеганоаналізі, розробники атакованого стегоалгоритму мають можливість вдосконалити його або взагалі відмовитись від використання цього алгоритму.

Велике значення алгоритми стеганоаналізу можуть мати і в боротьбі з терористичними організаціями. Адже, згідно інформації спецслужб багатьох країн світу, терористичні організації широко використовують світові інформаційні ресурси, зокрема ресурси мережі Інтернет (звук, графіку, відео), для передачі прихованих повідомлень, які мають загрозливий зміст і становлять потенційну небезпеку для цивільного населення.

На сьогодні існує досить багато підходів при аналізі зображень, ефективність яких може бути різною при використанні того чи іншого алгоритму вбудовування інформації.

Для підвищення ефективності алгоритмів стеганоаналізу ми пропонуємо використовувати комплексний підхід, в якому аналіз зображення здійснюється поетапно, використовуючи засоби стеганоаналізу, які враховують специфіку певних алгоритмів вбудовування та засоби „сліпого" стеганоаналізу.

Далі ми коротко зупинимось на деяких механізмах для стеганоаналізу зображень.

Узагальнена класифікація атак на стегосистеми

Виходячи із мети, яку переслідує порушник, та вихідних даних, якими він володіє на початковому етапі, згідно [1,2], можна виділити наступні види атак на систему таємної передачі даних.

1 *Атака з відомою стеганограмою.* У цьому випадку при аналізі відома одна або кілька стеганограм. На основі цих даних аналітик намагається визначити, чи містять стеганограми приховані дані, чи ні.

2 *Атака з відомим контейнером.* Аналітику відомий один або декілька чистих контейнерів та відповідних їм стеганограм. Фактично, даний тип атаки лежить в основі більшості засобів для адаптивного практичного стеганоаналізу.

3 *Атака з вибраним контейнером.* Зловмисник здатний нав'язати для використання в системі таємної передачі даних зручний для себе стегоконтейнер, якому притаманні деякі риси, які б допомогли згодом полегшити процес виявлення прихованих повідомлень.

4 *Атака з вибраною стеганограмою.* В даному випадку з допомогою певних стегосистем (алгоритмів вбудовування) створюються стеганограми для відповідного обраного повідомлення. Далі здійснюється аналіз, які взірці із створеної сукупності можуть ідентифікувати використання того чи іншого стеганографічного засобу в системі прихованої передачі інформації.

5 *Атака з відомим повідомленням.* Зловмиснику відомий зміст одного чи кількох таємних повідомлень, тому він намагатиметься встановити факт їх передачі та знайти стегоключ, який використовується при цій передачі.

6 *Атака з вибраним повідомленням.* В даному випадку порушник намагатиметься нав'язати для передачі по таємному каналу конкретне повідомлення і потім встановити факт таємної передачі цього повідомлення та ключ вбудовування.

7 *Атака з повною інформацією.* Зловмисник володіє повною інформацією про стегосистему: алгоритм вбудовування, контейнери і відповідні їм стеганограми. Основною метою аналітика є обчислення стеганографічного ключа.

Крім цього можливі різноманітні поєднання цих атак. Але на практиці, в більшості випадків, окрім файлу, підозрілого на вміст деякої таємної інформації, нам більше нічого невідомо про використовувану стегосистему, тобто ми маємо справу з першим видом стеганографічної атаки.

Пошук та аналіз засобів для практичного стеганоаналізу зображень

Перераховані вище види атак є в значній мірі ідеалізовані, тому більшість із вище перерахованих методів стеганоаналізу практично не використовуються для виявлення прихованих повідомлень в цифрових зображеннях. В практичному житті, як вже згадувалось вище, ми в більшості випадків оперуємо лише з підозрілим на стеганограмму об'єктом.

В практичному стеганоаналізі цифрових зображень, можна виділити два основні види атак на стегосистему:

1. *Виявлення з відомою схемою вбудовування*. Використання засобів аналізу зображень, які враховують специфіку певних алгоритмів вбудовування. В цьому випадку стеганоаналіз побудований на припущенні, що нам відома техніка (алгоритм) вбудовування таємного повідомлення або алгоритм, який використовувався для вбудовування, належить до певної сукупності механізмів вбудовування, принцип роботи яких нам заздалегідь відомий.

2. *Виявлення без інформації про схему вбудовування*, тобто використання засобів „сліпого" стеганоаналізу. Механізми виявлення цієї категорії є більш загальними і засновані на аналізі спільних, для всіх зображень певного формату, властивостей. Виявлення прихованих повідомлень здійснюється із припущення, що нам заздалегідь не відомий алгоритм вбудовування повідомлення. Для стеганоаналізу використовуються усі можливі властивості зображень, значення яких з певною закономірністю можуть змінюватись під час вбудовування інформації. В більшості випадків аналізуються зміни енергетичних характеристик та статистичні значення певних параметрів зображення.

Однак, немає чіткої межі між засобами аналізу орієнтованих на певні алгоритми і засобами „сліпого" стеганоаналізу. Як і засоби „сліпого" аналізу, механізми, в яких враховано основні принципи існуючих алгоритмів вбудовування, також можуть відзначатися своєю універсальністю при збереженні високих показників ефективності.

Як засоби для „сліпого" стеганоаналізу так і засоби для виявлення прихованих повідомлень, які враховують відомі механізми вбудовування, можна розділити на такі категорії:

1. Засоби для візуальних атак, які використовують механізм накладання на зображення спеціальних фільтрів з наступною візуалізацією результатів фільтрації;

Статистичні оцінки зображень, результат роботи яких відображається в числовій або графічній формі.

Перед тим як детальніше розглянути деякі із алгоритмів стеганоаналізу, коротко ознайомимось з формами представлення цифрових зображень та класифікацію ділянок зображень, які можуть використовуватись як стеганоконтейнер.

Форми представлення цифрових зображень для стеганоаналізу

Існує декілька моделей для представлення зображень [4], найпростішою із них є представлення зображення у вигляді матриці пікселів, з визначеними для кожного пікселя значеннями інтенсивності кольорів або відтінків чорного кольору (для чорно-білих зображень).

При такій формі представлення, чорно-біле зображення розміром $n \times n$ можна розглядати як елемент n^2 – мірного простору, де і – та координата позначає значення інтенсивності і – го пікселя (кольоровий RGB – малюнок представляється як елемент $3n^2$ – мірного простору). У випадку такої форми представлення аналізується гістограма значень інтенсивності відтінків.

Але слід відзначити, що піксельне представлення є неефективним навіть для виділення на фоні зображення досить сильної шумової складової.

Інша поширена форма представлення заснована на декомпозиції зображення з допомогою перетворення Фур'є. В цьому випадку зображення представлене як сума синусних та косинусних складових, значення яких змінюються по частоті та орієнтації в просторі.

$$F(\omega_x, \omega_y) = \sum_x \sum_y I(x,y) e^{-j(\omega_x x + \omega_y y)} \qquad (1)$$

де $I(x,y)$ – представлення чорно-білого зображення; $F(\omega_x, \omega_y)$ – результат перетворення Фур'є.

Щодо кольорового зображення, то кожен його канал представляється подібно формулі (1).

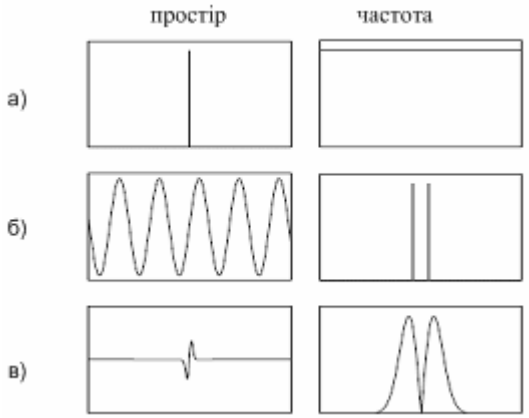


Рис.1. Зображення пікселя: а) функції Фур'є б) та вейвлет – функції; в) в просторі (1D – просторі) та в частотній області.

Представлення зображення у вигляді базисних функцій, які локалізовані в просторовій та частотній області (вейвлетів), в певній мірі є компромісом між попередніми двома представленнями, рис.1.

Загалом, така форма представлення зображень краща представлення у вигляді матриці пікселів чи представлення на основі перетворення Фур'є, при дослідженні структури зображення на певній локальній ділянці.

Огляд засобів стеганоаналізу орієнтованих на певні алгоритми вбудовування

До засобів даної категорії можна віднести як дуже прості ідеї та рішення, так і більш загальні, в яких враховані деякі поширені принципи вбудовування, такі як вбудовування в найменші значущі біти (НЗБ).

Перевагою таких методів є те, що вони ефективно з високим ступенем правдоподібності виявляють факт приховування повідомлення певними алгоритмами, механізм роботи яких заздалегідь відомі. Натомість, виявити факт присутності прихованого повідомлення вбудованого певним невідомим алгоритмом в невідомі заздалегідь ділянки контейнера, в багатьох випадках вони не зможуть.

На сьогодні існує велика кількість механізмів вбудовування повідомлень в зображення та відповідних їм програмних реалізацій. Багато із них здійснюють вбудовування в практично всі відомі на сьогодні формати представлення зображень, найбільш популярним серед яких є JPEG – формат. Цей формат підтримує більшість із існуючих програм для перегляду та редагування зображень.

Для вбудовування повідомлень в зображення JPEG – формату можна використати такі програми як EzStego, J-steg, JP Hide&Seek, F5, OutGuess та багато інших програм.

В усіх перерахованих вище програмах, окрім EzStego, біти таємного повідомлення вбудовуються шляхом модифікації та зміни порядку ДКП – коефіцієнтів (коефіцієнтів дискретного косинусного перетворення).

В J – Steg та OutGuess біти повідомлень вбудовуються в НЗБ значень ДКП – коефіцієнтів.

В багатьох системах, як наприклад EzStego, Steganos, таємне повідомлення вбудовується в НЗБ елементів зображення. В системі EzStego молодший біт колірного компонента кожного пікселя, починаючи від початку зображення, послідовно замінюється відповідним бітом таємного повідомлення. В інших стегосистемах біти повідомлення, яке необхідно вбудувати, заміщають молодші біти компоненти яскравості для кожного пікселя зображення. Раніше вважалося, що НЗБ компонент яскравості або кольору пікселів зображення не пов'язані між собою, а також незалежні від інших складових елементів зображення. Однак, насправді це не так, молодші біти не є цілком випадковими. Між молодшими бітами сусідніх пікселів природних зображень є істотні кореляційні зв'язки. Також виявлені залежності між НЗБ й бітами інших параметрів природних зображень.

Візуальні атаки на зображення.

При вбудовуванні у кожен НЗБ компонентів кольору пікселів прихованого повідомлення, послідовно біт за бітом, розходження між пустим контейнером і стеганограмою візуально не проявляється. Але якщо зображення сформувати тільки із НЗБ пікселів стеганограми, то можна досить легко побачити сліди процесу вкладення. Ще простіше виявити приховане повідомлення, яке до вбудовування зашифровувалось, тому, що ймовірність появи кожного біта зашифрованого повідомлення практично однакова, і крім цього, вони перестають бути взаємокорельованими, що дозволяє легко візуально виявити факт вбудовування повідомлення, відповідно зіставивши зображення утвореного з молодших бітів стеганограми і зображення порожніх природних контейнерів. Компресія повідомлення перед вбудовуванням також спрощує завдання виявлення прихованого повідомлення.

Слід відзначити, що відправник повідомлення може підібрати контейнер, закон розподілу якого збігається із законом розподілу конкретного повідомлення, яке вбудовується. У цьому випадку як візуальна атака так і статистичні атаки, побудовані на статистиці першого порядку, є неефективними. Але складність, пов'язана з підбором необхідного контейнера, може зробити таку стегосистему непрактичною.

У програмі Steganos [5] вбудовування повідомлення будь-якої довжини здійснюється в усі НЗБ пікселів контейнера, тому приховане повідомлення також виявляється візуальною атакою.

В деяких стеганографічних системах елементи таємного повідомлення вкладаються в молодші біти коефіцієнтів дискретного перетворення Фур'є (ДКП – коефіцієнти) зображення – контейнера. Проти таких методів приховування візуальна атака малоефективна, тому що зміна будь-якого коефіцієнта перетворення Фур'є приводить до зміни багатьох пікселів зображення. Наприклад, у програмі Jsteg перетворення виконується над матрицею 16×16 пікселів контейнера. Вкладення таємного повідомлення в молодші біти ДКП - коефіцієнтів призведе до порівняно невеликих змін кожного з 256 пікселів, що візуально малопомітно. Тому для виявлення прихованих повідомлень у цьому випадку використовують статистичні методи аналізу. Засоби статистичного аналізу відносяться до універсальних механізмів для стеганоаналізу, після незначної „адаптації" їх можна використовувати для виявлення прихованих повідомлень, вбудованих з допомогою багатьох стегоалгоритмів (EzStego, F5, OutGuess та інших).

Огляд засобів для „сліпого" стеганоаналізу зображень

Найбільш перспективнішим напрямком в стеганоаналізі є використання засобів, для яких врахування відомих існуючих алгоритмів вбудовування не є обов'язковим. Вони відзначаються своєю універсальністю і гнучкістю, не вимагають адаптації у випадку зміни алгоритму вбудовування.

„Сліпий" стеганоаналіз може бути здійснений, використовуючи:

1. енергетичну оцінку параметрів зображення;
2. статистичну оцінку параметрів зображення;

3. засоби для виявлення прихованого повідомлення, присутнього у вигляді адитивного шуму.

Статистичні тести зображень призначені для виявлення факту порушення статистичних закономірностей природних зображень – контейнерів внаслідок вбудовування таємної інформації. У даному випадку аналізуються статистичні характеристики потенційної стеганограми і визначається, чи вони схожі на характеристики „чистих" зображень, чи вони схожі на характеристики стеганограм.

Статистичні методи стегоаноаналізу використовують множину статистичних характеристик, таких як оцінка ентропії, коефіцієнтів кореляції, імовірності появи та залежності між елементами послідовностей значень параметрів зображень, порівняння розподілів за критерієм χ^2 (хі-квадрат) та багато інших характеристик. Найпростіші тести оцінюють кореляційні залежності між елементами зображення, у які можуть вбудовуватись таємні повідомлення.

Статистична оцінка може бути здійснена за допомогою аналізу статистичної вибірки значень параметрів зображення властивих для форм представлення зображення, які вже наводились вище. Тобто, можна аналізувати матрицю пікселів, параметри дискретного косинусного перетворення (ДКП) та параметри дискретного вейвлет – перетворення.

Для дослідження параметрів пікселів зображення можна використати такі статистичні механізми як аналіз гістограми яскравості, аналіз статистичних вибірок за критерієм χ^2 (хі-квадрат), кореляційні залежності та інші статистичні тести.

Оскільки результат процедури вбудовування зазвичай локалізований в певній ділянці зображення, то аналіз доцільно проводити розбиваючи його на сегменти з однорідною структурою, тобто елементи яких не є різко відмінними між собою, а близькі за значенням.

При статистичному аналізі даних отриманих внаслідок вейвлет – декопозиції використовуються статистики першого та вищого порядків.

Комплексний підхід у стеганоаналізі зображень

Для підвищення ефективності стеганоаналізу можна використати комплексний підхід. У цьому випадку процес виявлення повідомлень буде складатись із двох основних етапів:

1. Аналіз зображення з виявленням факту вбудовування повідомлення одним із відомих алгоритмів.
2. Аналіз зображення використовуючи засоби „сліпого" стеганоаналізу.

При цьому, якщо перший етап показав позитивний результат, то наступний етап можна пропустити.

Алгоритм роботи стеганоаналізатора цифрового зображення можна подати як послідовність наступних кроків:

1. Представляємо зображення у вигляді матриці пікселів.
2. Для $i=(1;n)$ послідовно здійснюємо візуальні атаки з врахуванням певного алгоритму вбудовування під індексом i із сукупності алгоритмів – n.
3. Далі здійснюємо статистичні атаки, аналізуючи параметри пікселів зображення.
4. Якщо два попередні етапи атаки дали позитивний результат, то можна завершити процес стеганоаналізу. Якщо отримані показники ймовірності присутності вбудованого повідомлення не високі, то необхідно продовжити процес аналізу.
5. Здійснюємо декомпозицію зображення з використанням перетворення Фур'є. Аналізуємо параметри дискретного косинусного перетворення.
6. Здійснюємо вейвлет – декомпозицію. Аналізуємо параметри, отримані у результаті вейвлет – декомпозиції.

Жодний із засобів стеганоаналізу не гарантує присутність прихованих даних на сто відсотків, комплексний підхід при цьому забезпечує найвищу достовірність результату стеганоаналізу.

Висновки

Стеганоаналіз є новим та перспективним напрямом у науці. Поява цього напряму завдячує вимогам сьогодення. Оскільки він є ще досить молодим, його методи та засоби мало розвинуті. Із вдосконаленням методів приховування інформації, необхідно розвивати і методи виявлення прихованих повідомлень. Для ефективного стеганоаналізу ми вважаємо за доцільне використовувати комплексний підхід, згідно якого необхідно поєднувати засоби аналізу, які враховують інформацію про принципи роботи алгоритмів вбудовування і засоби „сліпого" стеганоаналізу.

Механізми стеганоаналізу розвинуті ще дуже слабо, тому важливим завданням, яке стоїть перед нами сьогодні, є пошук нових ефективних засобів стеганоаналізу.

Література

1. В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Я. Яремчук. Основи комп'ютерної стеганографії. Вінниця. ВДТУ .2003 р;
2. В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. Цифровая стеганография. Москва. Солон-Прес. 2002 г;
3. Вентцель Е. С. Овчаров Л. А. Теория вероятностей и ее инженерные приложения. Москва. Наука. Гл. ред. физ.-мат. лит. 1988. – 480 с;
4. S. Lyu and H. Farid, "Detecting hidden messages using higher-order statistics and support vector machines," in 5th International Workshop on Information Hiding, Noordwijkerhout, The Netherlands, 2002;
5. N. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," Lecture notes in Computer Science, vol. 1525, pp. 273–289, 1998.

УДК 004.522

Темников В.А., Пономаренко Л.В.

СИСТЕМА РАСПОЗНАВАНИЯ ЛИЧНОСТИ КАК ОСНОВА ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

В статье представлена комплексная система распознавания личности по совокупности ее идентифицируемых признаков, что является основой увеличения эффективности систем контроля и управления доступом на объекты с различной степенью секретности.

Одним из важнейших направлений повышения безопасности информации, обрабатываемой и хранящейся на объектах информационной деятельности, является разработка эффективных автоматизированных систем контроля и управления доступом (СКУД) на эти объекты [1,2]. Существенно повысить эффективность указанных систем можно на основе усовершенствования автоматизированных биометрических систем распознавания личности как элемента искусственного интеллекта.

Под „биометрической системой распознавания личности" авторы предлагают понимать систему, обеспечивающую распознавание человека (личности) на основе аутентификации и анализа психофизического состояния (ПФС) личности, что особенно актуально при решении задачи контроля и управления доступом на объекты информационной деятельности с высокой степенью секретности. В качестве объекта информационной деятельности могут выступать как физические объекты (помещение, здание, территория), так и автоматизированные (информационно-телекоммуникационные) системы различного функционального назначения.

Система распознавания личности производит анализ предъявленных идентифицируемой личностью биометрических, поведенческих и медицинских информативных признаков и полученных на их основе статических и динамических образов; описание параметров, характеризующих предъявленные признаки (образы); поиск информативных параметров, достаточных для правильного распознавания; описание образов в пространстве преобразованных информативных параметров, а также сравнение выбранных информати-

вных параметров с хранящимися в базе данных и принятие решения по отнесению личности к определенному классу (с некоторой погрешностью, ошибками первого и второго рода). Основным заданием системы распознавания личности является решение задачи классификации.

На рис. 1 представлена разработанная комплексная система распознавания личности на основе аутентификации и анализа ПФС личности, которая позволяет анализировать несколько индивидуальных признаков (образов) личности и осуществлять принятие решения о возможности доступа и перечне разрешаемых действий на основании комплексного анализа совокупности образов идентифицируемой личности, в том числе, ее ПФС.

Сложность такой системы распознавания личности зависит от степени секретности, которую необходимо обеспечить для доступа на конкретный объект информационной деятельности.

Определение ПФС личности производится на основе анализа образов, характеризующих медицинские, биометрические и поведенческие информативные признаки человека (электрокардиограмма, электроэнцефалограмма, голос, радужная оболочка глаза и др.).

Предлагаемая система распознавания личности включает в себя основные структурные элементы классической теории распознавания образов и решает задачи определения принадлежности данного субъекта к одному из заранее выделенных классов.

Ниже в качестве примера предложена система распознавания личности, в которой аутентификация производится на основе распознавания по голосу (признак 1) и радужной оболочке глаза (признак 2) [3], а вывод о ПФС делается на основе электрокардиограммы (ЭКГ) человека (признак 3).

Алгоритм системы распознавания личности состоит из следующих этапов.

Сканирование

Учет биометрических, поведенческих и медицинских признаков производится на основе анализа образов, формируемых путем их сканирования. В качестве анализируемого образа выступает либо временная зависимость (в случае обработки речевого сигнала или ЭКГ), либо изображение, которое получается в результате сканирования радужной оболочки глаза.

В дальнейшем анализируемый образ подвергается предварительной обработке, которая может, например, заключаться в выделении локальных участков информативных признаков, шумоочистке и представлении анализируемого образа в наиболее пригодном для дальнейшей обработки виде.

Шумоочистка

Для решения задачи шумоочистки авторами выбран математический аппарат вейвлет-преобразования, поскольку он позволяет решать данную задачу эффективно и применительно к двум видам анализируемых образов. При применении вейвлетного разложения для подавления шумов шумовые компоненты и случайные выбросы значений сигналов рассматриваются в виде множеств локальных особенностей сигналов [4]. Путем задания определенного порога для их уровня и срезания по нему детализирующих коэффициентов достигается уменьшение уровня шумов и устанавливаются пороговые ограничения на нескольких уровнях разложения с учетом конкретных характеристик шумов и сигналов для различных типов вейвлетов. Это позволяет создавать адаптивные системы очистки сигналов от шумов в зависимости от их особенностей.

На рис. 2 представлено рабочее окно Wavelet Toolbox − пакета расширения MatLab, используемого для выполнения этапа подавления шумов.

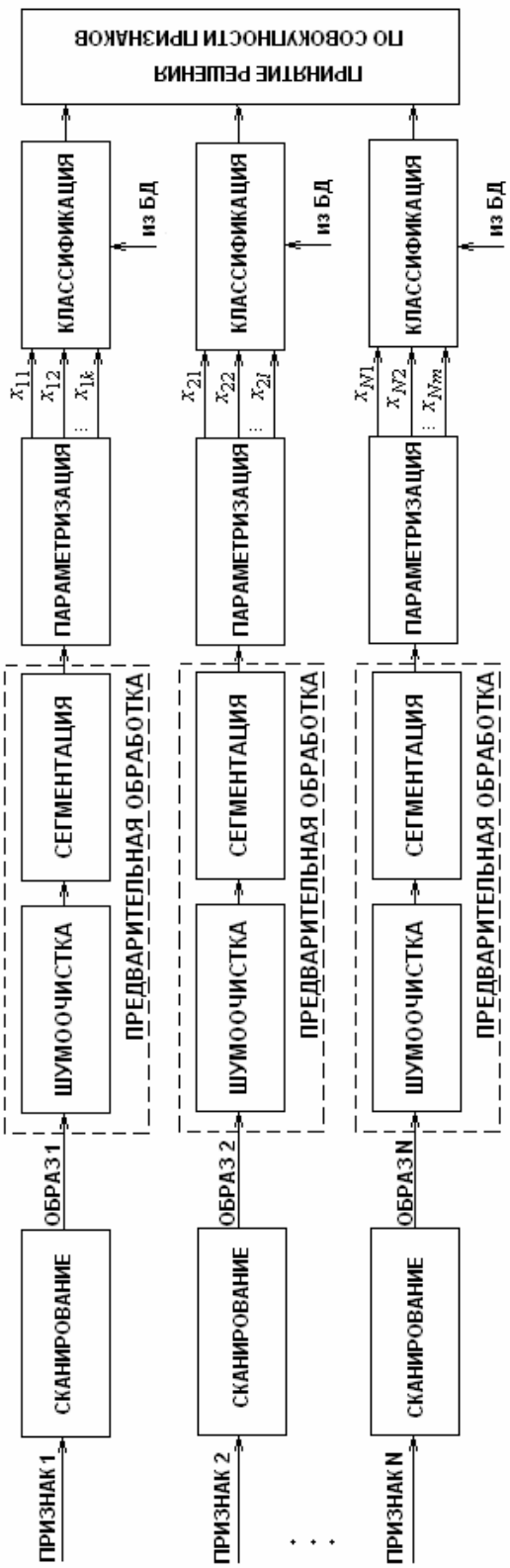


Рис. 1 Комплексная система распознавания личности по совокупности ее идентифицируемых признаков

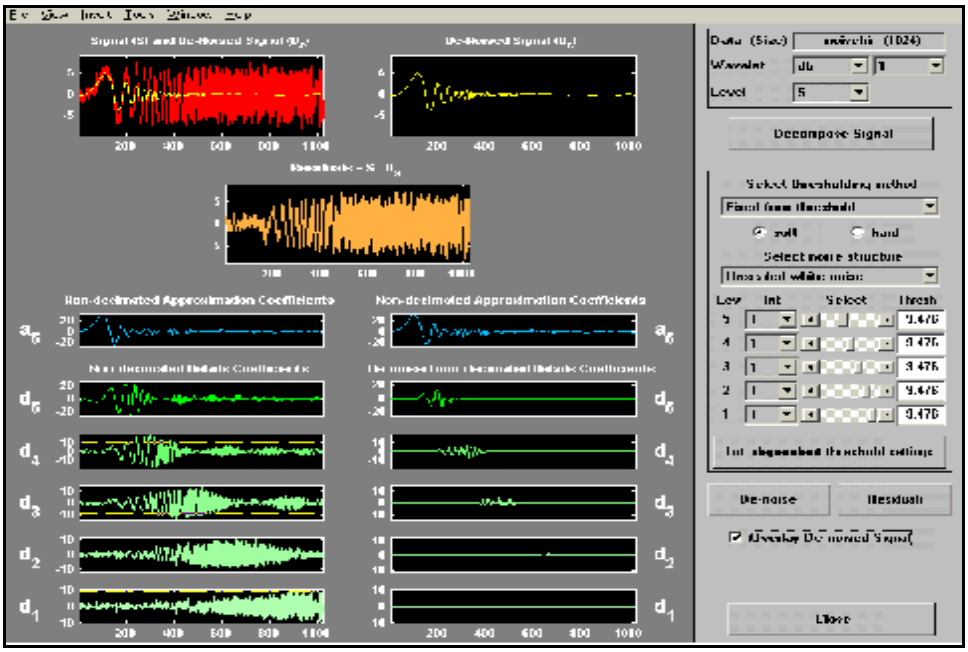


Рис. 2. Иллюстрация рабочего окна Wavelet Toolbox.

Сегментация

Вопрос сегментации актуален для всех видов признаков, поскольку подобная обработка выделяет наиболее информативные участки образа.

При аутентификации личности по голосу задача сегментации решается с применением вейвлетов путем обнаружения межфонемных переходов, на которых сигнал претерпевает значительные изменения одновременно на многих масштабах исследования и, соответственно, характеризуется возрастанием вейвлет-коэффициентов для многих уровней детализации, в то время как на стационарных участках фонем вейвлет-коэффициенты оказываются сгруппированными вблизи определенных масштабов. Отыскание межфонемных границ сводится к отысканию моментов увеличения вейвлет-коэффициентов на значительном количестве уровней масштабирования. Для решения задачи сегментации речевого сигнала предлагается использовать алгоритмы с применением быстрого вейвлет-преобразования, представленные в [5]. При этом существенным является выбор вейвлетного базиса, который должен позволять описывать стационарный речевой сигнал со сравнительно малым числом ненулевых коэффициентов. На рис. 3 представлена сегментация фрагмента речевого сигнала.

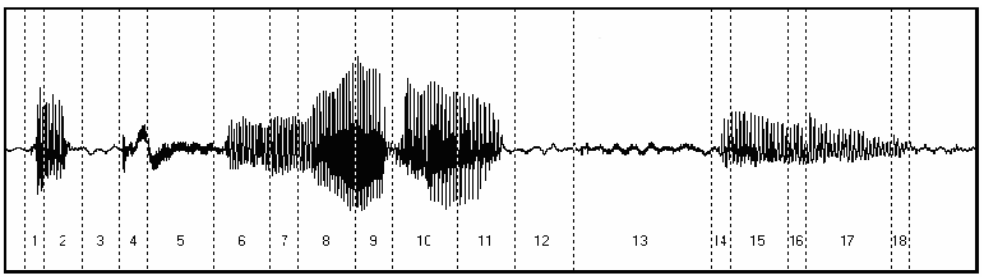


Рис. 3 Сегментация фрагмента речевого сигнала.

Аналогично производится процесс сегментации в случае обработки сигнала ЭКГ.

Процесс сегментации при аутентификации по радужной оболочке глаза выполняется с целью выбора из полного изображения наиболее информативных участков, что по-

зволяет значительно увеличить скорость обработки анализируемого образа. Подробно этот вопрос рассмотрен в [3].

Параметризация

На этапе параметризации решается несколько сложных задач.

1. Задача выбора информативных параметров. Сложность решения задачи обусловливается тем, что исходный набор характеристик часто бывает очень большим, и, в то же время, приемлемое решающее правило должно быть основано на использовании небольшого числа параметров, наиболее важных для точного распознавания образа. Правильный выбор информативных параметров в значительной мере определяет эффективность решения задачи распознавания личности.

2. Задача выбора способа параметризации образа, т.е. поиска и выбора математического аппарата, способного максимально точно и эффективно описать анализируемый образ.

В рамках рассматриваемой комплексной системы распознавания личности по совокупности ее идентифицирующих признаков авторы решают задачу выбора способа параметризации путем применения кратномасштабного анализа и вейвлет–преобразования. Выбранные базисные функции обладают свойствами частотно-временной локализации и позволяют производить эффективную обработку сложных сигналов без потери информации о временных характеристиках сигнала. Кроме того, указанный вид преобразования оптимально подходит как для обработки одномерного сигнала, так и для работы с изображениями.

В качестве информативных параметров $X = \{x_i\}$ в случае использования предложенного способа параметризации выступают коэффициенты детализации ортогонального вейвлет-преобразования каждого сегмента. Подобное представление образа удобно для дальнейшей его оценки, обработки, сравнения. Более того, вейвлет-преобразование при использовании разных масштабов времени и разрешения сигнала позволяет получить дополнительную информацию об особенностях образа (временной зависимости или изображения), и тем самым, повысить точность распознавания личности.

Классификация

Производится после обучения системы на основании выбранного решающего правила и сравнения информативных параметров с хранящимися в базе данных (БД) (см. рис. 1). Процедура формирования БД (обучающей выборки) основана на вейвлет-преобразовании анализируемого образа. Как результат, в БД хранятся значения вейвлет-коэффициентов, с которыми в дальнейшем сравниваются параметры идентифицируемого образа (контрольной выборки).

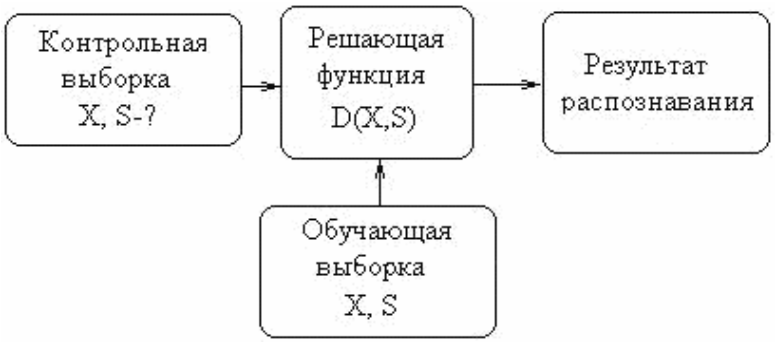


Рис. 4. Схема проведения классификации.

Одна из основных задач распознавания личности − выбор правила (решающей функции) D (рис. 4), в соответствии с которым по значению контрольной выборки X устанав-

ливается её принадлежность к одному из классов. Помимо совокупности информативных параметров $X = \{x_i\}$, анализируемый образ характеризуется дополнительной характеристикой S, указывающей на принадлежность образа к некоторому классу. Таким образом, при распознавании указываются „наиболее правдоподобные" значения характеристики S для данного массива X.

Выбор решающей функции D требуется произвести так, чтобы стоимость распознающего устройства, его эксплуатации и потерь, связанных с ошибками распознавания, была минимальной.

Принятие решения

Принятие решения по совокупности признаков производится на основании статистических оценок уровней ошибок разрабатываемой биометрической системы, полученных на этапе классификации личности по каждому из идентифицирующих признаков. Значения ошибок, в свою очередь, зависят от того, насколько эффективно в системе распознавания реализованы основные структурные этапы, а именно: качественная предварительная обработка, оптимальное соотношение количества анализируемых параметров и их информативности, приемлемое решающее правило.

Таким образом, в статье предложена реализация основных этапов алгоритма системы распознавания личности, основанной на аутентификации человека и анализе его психофизического состояния.

Литература

1. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації / За ред. проф. В.О. Хорошка – К.: НАУ. – 2002. – 208с;
2. Темников В.А., Пономаренко Л.В. Повышение эффективности систем контроля и управления доступом, построенных на основе автоматизированного распознавания личности // Сборник научных трудов „Защита информации". – Вып. 13. – К.: НАУ. – 2006. – С. 19-23;
3. Темников В.А., Пономаренко Л.В., Голембиевская Ю.Г. Алгоритмы распознавания личности по биометрическим и поведенческим признакам // Сб. трудов VI Международной научной конференции „Интеллектуальный анализ информации" (ИАИ-2006). – К.: Просвіта. – С. 288-297;
4. Donoho D.L. De-Noising by soft-thresholding // IEEE Trans. on Inform. Theory. – Vol.41. – №3. – 1995. – P.613-627;
5. Ермоленко Т., Шевчук В. Алгоритмы сегментации с применением быстрого вейвлет-преобразования // Труды Международной конференции «Диалог 2003». – М., 2003. – С.132-139.

УДК 621.391:519.7:510.5

Алексейчук А. Н., Конюшок С. Н., Скрыпник Л. В.

БЕЗУСЛОВНО СТОЙКИЕ СХЕМЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ПОСТРОЕННЫЕ ПО КОНГРУЭНЦИЯМ УНИВЕРСАЛЬНЫХ АЛГЕБР

Предложена комбинаторная модель схемы предварительного распределения ключей, с использованием которой получено описание таких схем в терминах определенных систем отношений эквивалентности на конечном множестве. Предложен метод построения схем предварительного распределения ключей по системам конгруэнций конечных универсальных алгебр, обобщающий известный способ их синтеза на основе линейных отображений конечных векторных пространств.

Одним из перспективных направлений современной криптографии, активно развивающихся на протяжении последних 15 – 20 лет, является построение криптографически стойких протоколов (схем) распределения ключей в системах защищенной многоадресной связи. Характерная особенность таких систем заключается в наличии большого числа авторизованных абонентов, образующих наделенные различными правами группы (коалиции), состав которых может динамически изменяться [1, 2].

Говоря неформально, схема распределения ключей (СРК) представляет собой криптографический протокол, с ипользованием которого доверенная сторона (центр распределения ключей (ЦРК) или дилер) передает абонентам сети связи некоторую вспомогательную секретную информацию так, что со временем абоненты, входящие в определенную привилегированную коалицию, могут вычислить общий (групповой) ключ. Схема распределения ключей называется безусловно стойкой, если каждая запрещенная (для данной привилегированной) коалиция абонентов не может получить никакой информации об этом ключе даже при наличии неограниченных вычислительных ресурсов [3, 4].

Подробные сведения об известных методах построения, анализа и различных аспектах практического применения СРК можно найти в обзорных работах [3, 5, 6].

Настоящая статья посвящена изучению специального класса безусловно стойких СРК, а именно, схем предварительного распределения ключей (СПРК). Центральной задачей исследования таких схем является разработка конструктивных методов синтеза СПРК, имеющих оптимальные или близкие к оптимальным характеристики эффективности (так называемые информационную скорость и полную информационную скорость) [3 – 7].

В настоящее время конструкции оптимальных СПРК известны лишь для отдельных типов структур спецификаций (совокупностей пар привилегированных и запрещенных коалиций участников схемы) [3, 7]. При этом, несмотря на разнообразие конкретных видов СПРК, общая теория построения и анализа схем предварительного распределения ключей для произвольных структур спецификаций находится в состоянии становления. Отметим статью [7], в которой предложена конструкция так называемых линейных СПРК, включающих в себя большинство известных видов схем предварительного распределения ключей.

В настоящей статье предложена комбинаторная модель СПРК, позволяющая, по мнению авторов, более наглядно и, практически, без потери общности выразить существенные свойства произвольной схемы предварительного распределения ключей. С использованием данной модели получено формальное описание СПРК в терминах определенных систем отношений эквивалентности (ОЭ) на конечном множестве. Предложен метод построения СПРК по системам конгруэнций конечных универсальных алгебр, обобщающий конструкцию линейных схем предварительного распределения ключей [7]. Отметим, что решения аналогичных задач для другого класса протоколов распределения ключей (так называемых совершенных схем разделения секрета) получены ранее в [8].

Далее в статье свободно используются понятия универсальной алгебры, определения которых можно найти в [9, 10]. Более подробная информация о схемах предварительного распределения ключей приведена в [3 – 5, 7].

Перейдем к изложению основных результатов статьи.

Пусть $V = \{1,2,..,v\}$ – множество абонентов сети связи, $\Gamma \subseteq 2^V \times 2^V$ – структура спецификации на множестве V [7]. Обозначим $\Re(\Gamma) = \{P \subseteq V \mid \exists C \subseteq V : (P,C) \in \Gamma\}$ совокупность Γ-привилегированных коалиций абонентов. Для любого $P \in \Re(\Gamma)$ обозначим $\Im_\Gamma(P) = \{C \subseteq V \mid (P,C) \in \Gamma\}$ множество всех P-запрещенных коалиций абонентов. Отметим, что $\Im_\Gamma(P)$ является монотонно невозрастающим классом множеств, каждое из которых не пересекается с P.

Опишем предлагаемую комбинаторную модель схемы предварительного распределения ключей со структурой спецификации Γ (Γ-СПРК).

Пусть $U, U_1, \ldots, U_V$ – конечные множества, где $U \subseteq U_1 \times \ldots \times U_V$. Пусть, далее, для любого $P \in \Re(\Gamma)$ задано конечное множество K_P такое, что $|K_P| \geq 2$, и сюръективное отображение $\varphi_P : U \to K_P$. Будем говорить, что набор $D = (U, (U_i)_{i \in V}, (K_P, \varphi_P)_{P \in \Re(\Gamma)})$ задает Γ-СПРК на множестве V, если выполняются следующие условия:

$$\forall P \in \Re(\Gamma)\ \forall i \in P\ \forall u = (u_1,\ldots,u_V),\ \tilde{u} = (\tilde{u}_1,\ldots,\tilde{u}_V) \in U : (u_i = \tilde{u}_i) \Rightarrow (\varphi_P(u) = \varphi_P(\tilde{u})), \quad (1)$$

$$\forall (P,C) \in \Gamma : \ |\{(u_C, \ _P(u)) : u \in U\}| = |\{u_C : u \in U\}| \cdot |\{ \ _P(u) : u \in U\}|, \quad (2)$$

где u_C обозначает подвектор вектора u с координатами, номера которых принадлежат множеству C.

Для любых $i \in V$, $P \in \Re(\Gamma)$ множества U_i и K_P называются соответственно множеством вспомогательных секретных данных i-го абонента и множеством групповых ключей коалиции P.

Протокол распределения ключей абонентам из множества V с использованием заданной СПРК D описывается следующим образом. На первом этапе в ЦРК случайно и равновероятно выбирают элемент $u = (u_1,...,u_V) \in U$ и передают каждому абоненту $i \in V$ значение u_i по защищенному каналу связи. На втором этапе, согласно условию (1), каждый участник произвольной привилегированной коалиции P может однозначно вычислить групповой ключ $k_P = \ _P(u)$. При этом на основании равенства (2) участники произвольной P-запрещенной коалиции $C \in \Im_\Gamma(P)$ не получат никакой (апостериорной) информации об этом ключе.

Стандартными показателями эффективности СПРК D являются ее информационная скорость ρ и полная информационная скорость ρ_T [3, 4, 7], которые, в рассматриваемом случае, определяются по формулам:

$$\rho = min\{\frac{log \mid K_P \mid}{log \mid U_i \mid} : i \in P, P \in \Re(\Gamma)\}, \quad (3)$$

$$\rho_T = min\{\frac{log \mid K_P \mid}{log \mid U \mid} : P \in \Re(\Gamma)\}. \quad (4)$$

Отметим, что данное выше формальное определение является переложением на комбинаторный язык (без существенной потери общности) общепринятого вероятностного определения схемы предварительного распределения ключей (см., например, [3, 4, 7]).

Покажем, что произвольная Γ-СПРК может быть, по существу, однозначно задана определенной системой отношений эквивалентности на конечном множестве.

Обозначим $\vartheta(U)$ решетку отношений эквивалентности на множестве U. Символы $\bullet$, $\vee$ и $\wedge$ обозначают соответственно произведение, точную верхнюю грань и точную нижнюю грань (пересечение) ОЭ на множестве U [9]. Каждое ОЭ $\pi \in (U)$ отождествляется с фактормножеством (разбиением) U/π, число элементов (блоков) которого обозначается $n(\pi)$. Символ 1_U обозначает наибольший элемент решетки $\vartheta(U)$, равный U^2.

Справедливо следующее утверждение.

Утверждение 1. Тогда и только тогда существует Γ-СПРК на множестве V, имеющая информационную скорость (3) и полную информационную скорость (4), когда существуют конечное множество U и система ОЭ π_i, $\theta_P \in \vartheta(U)$, $i \in V$, $P \in \Re(\Gamma)$, которые удовлетворяют следующим соотношениям:

$$\bigvee_{i \in P} \pi_i \subseteq \theta_P \neq 1_U \ , \ P \in \Re(\Gamma), \quad (5)$$

$$(\bigwedge_{j \in C} \pi_j) \bullet \theta_P = 1_U \ , \ (P,C) \in \Gamma, \quad (6)$$

$$\rho = min\{\frac{log\, n(\theta_P)}{log\, n(\pi_i)} : i \in P, P \in \Re(\Gamma)\}, \quad (7)$$

$$\rho_T = min\{\frac{log\, n(\theta_P)}{log\, |U|} : P \in \Re(\Gamma)\}. \quad (8)$$

Сформулированное утверждение доказывается аналогично утверждению 1 в статье [8]. Отметим, что для заданной Γ-СПРК $D = (U, (U_i)_{i \in V}, (K_P, \varphi_P)_{P \in \Re(\Gamma)})$ ОЭ π_i, θ_P можно определить по формулам $\pi_i = \mathrm{Ker}(pr_i)$, $i \in V$, $\theta_P = \mathrm{Ker}(\ _P)$, $P \in \Re(\Gamma)$, где $pr_i : U \to U_i$ – проекция множества U на множество U_i, $\mathrm{Ker}(f)$ – ядро произвольного отображения f (см. [9]). При этом соотношение (5) равносильно условию (1) и неравенству $|K_P| \geq 2$, $P \in \Re(\Gamma)$, а соотношения (6), (7) и (8) равносильны соотношениям (2), (3) и (4) соответственно.

Полученное утверждение позволяет предложить общий метод построения СПРК, исходя из определенных наборов конгруэнций конечных универсальных алгебр. Сущность метода раскрывается в формулировках следующих результатов.

Пусть Γ – произвольная структура спецификации на множестве V. Обозначим $\Im_{max}(P)$ множество всех максимальных элементов класса $\Im_\Gamma(P)$. Будем говорить, что система ОЭ $\pi_1, ..., \pi_V \in \vartheta(U)$ порождает Γ-СПРК на множестве V, если существуют отношения $\theta_P \in (U)$, $P \in \Re(\Gamma)$, удовлетворяющие условиям (5), (6).

Утверждение 2. Система ОЭ $\pi_1, ..., \pi_V \in (U)$ порождает некоторую Γ-СПРК на множестве V в том и только в том случае, когда существует подрешетка ϑ решетки $\vartheta(U)$, содержащая отношения $\pi_1, ..., \pi_V$, и для любого $P \in \Re(\Gamma)$ существует максимальный элемент μ_P решетки ϑ такой, что

$$\bigvee_{i \in P} \pi_i \subseteq \mu_P, \ \bigwedge_{j \in C} \pi_j \not\subset \mu_P, \ (\bigwedge_{j \in C} \pi_j) \bullet \theta_P = \theta_P \bullet (\bigwedge_{j \in C} \pi_j), \ C \in \Im_{\max}(P). \quad (9)$$

Справедливость утверждения 2 вытекает из предыдущего утверждения и известного критерия перестановочности отношений эквивалентности на множестве U (см. [9], стр. 104).

Рассмотрим теперь конечную универсальную алгебру A с носителем U. Обозначим $\vartheta_A(U)$ подрешетку решетки $\vartheta(U)$, состоящую из всех конгруэнций алгебры A [9, 10]. Напомним, что A называется конгруэнц-перестановочной алгеброй, если для любых $\pi_1, \pi_2 \in {}_A(U)$ выполняется равенство $\pi_1 \bullet \pi_2 = \pi_2 \bullet \pi_1$.

Непосредственно из утверждения 2 вытекает следующий результат.

Утверждение 3. Пусть $\pi_1, ..., \pi_V \in \vartheta_A(U)$ – различные конгруэнции конечной конгруэнц-перестановочной алгебры A. Пусть, далее, Γ – структура спецификации на множестве V такая, что для любого $P \in \Re(\Gamma)$ существует максимальная конгруэнция алгебры A, содержащая конгруэнцию $\bigvee_{i \in P} \pi_i$ и не содержащая конгруэнцию $\bigwedge_{j \in C} \pi_j$ для любого $C \in \Im_{max}(P)$. Тогда ОЭ $\pi_1, ..., \pi_V$ порождают Γ-СПРК на множестве V, информационная скорость ρ и полная информационная скорость ρ_T которой удовлетворяют неравенствам

$$\rho \geq (max\{log\ n(\pi_i) : i \in V\})^{-1}, \ \rho_T \geq (log\, |U|)^{-1}. \quad (10)$$

В качестве одного из возможных применений утверждения 3, рассмотрим следующую конструкцию СПРК, основанную на подпространствах n-мерного векторного пространства U над полем из q элементов.

Пусть $V_1,...,V_v$ – все k-мерные подпространства векторного пространства U, $2 \le k \le n-2$, $n \ge 4$. Обозначим $M_1,...,M_m$ и $L_1,...,L_m$ соответственно все максимальные и все минимальные подпространства пространства U. Справедливы равенства [11]

$$v = \frac{(q^n-1)\cdots(q^{n-k+1}-1)}{(q^k-1)\cdots(q-1)},\ m = \frac{q^n-1}{q-1}.$$

Построим СПРК $D_{n,k}$ на множестве участников $V = \{V_1,...,V_v\}$ со структурой спецификации Γ следующего вида:

$$\Re(\Gamma) = \{P_1,...,P_m\},\ \Im_{max}(P_i) = \{C_i(L_s) \mid L_s \cap M_i = 0,\ s \in \overline{1,m}\},\ i \in \overline{1,m},$$

где

$$P_i = \{V_l \mid V_l \subseteq M_i,\ l \in \overline{1,v}\},\ C_i(L_s) = \{V_l \mid V_l \supseteq L_s,\ l \in \overline{1,v}\},\ i \in \overline{1,m}.$$

Другими словами, для любой пары подпространств (M_i, L_s) таких, что $L_s \cap M_i = 0$, определим привилегированную коалицию P_i как множество всех k-мерных подпространств V_l, $l \in \overline{1,v}$, сумма которых равна M_i, и максимальную P_i-запрещенную коалицию $C_i(L_s)$ как множество всех k-мерных подпространств V_l, $l \in \overline{1,v}$, пересечение которых равно L_s, $i,s \in \overline{1,m}$.

Ясно, что все привилегированные и максимальные запрещенные коалиции СПРК $D_{n,k}$ имеют одинаковую мощность

$$v\left(\frac{q^k-1}{q^n-1}\right) = \frac{(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^{k-1}-1)\cdots(q-1)}. \qquad (11)$$

При этом для любой привилегированной коалиции $P_i \in \Re(\Gamma)$ существует ровно q^{n-1} максимальных запрещенных коалиций.

Информационная скорость ρ и полная информационная скорость ρ_T СПРК $D_{n,k}$ определяются по формулам $\rho = (n-k)^{-1}$, $\rho_T = n^{-1}$. По существу это означает, что на первом этапе протокола распределения ключей достаточно сгенерировать и передать абонентам сети связи ровно n секретных значений (элементов поля $GF(q)$). При этом каждый абонент будет хранить $n-k$ указанных значений. На втором этапе абоненты произвольной привилегированной коалиции P_i, $i \in \overline{1,m}$, могут вычислить общий ключ, секретный для любой из q^{n-1} максимальных P_i-запрещенных коалиций абонентов, каждая из которых имеет мощность (11).

В целом, полученные результаты позволяют строить разнообразные схемы предварительного распределения ключей, исходя из определенных систем ОЭ на конечных множествах, в частности, систем конгруэнций конечных конгруэнц-перестановочных алгебр (луп, ассоциативных колец, модулей над кольцом с единицей, векторных пространств над полем и др. [10]). В частном случае, когда алгебра A является векторным пространством,

схемы распределения ключей, описанные в формулировке утверждения 3, совпадают с линейными СПРК, предложенными ранее в [7]. Разнообразие и особенности строения конкретных классов конечных универсальных алгебр свидетельствуют о возможности синтеза новых видов схем предварительного распределения ключей, имеющих практически удовлетворительные характеристики эффективности.

Литература

1. Canetti R., Malkin T., Nissim K. Effcient communication-storage tradeoffs for multicast encryption // Advances in Cryptology – EUROCRYPT'99, Lecture Notes in Computer Science. – 1999. – P. 459 – 474;
2. Canetti R., Garay J., Itkis G., Micciancio D., Naor M., Pinkas B. Issue in multicast security: a taxonomy and efficient constructions // INFOCOM'99. – 1999. – P. 708 – 716;
3. Stinson D.R. On some methods for unconditionally secure key distribution and broadcast encryption // Designs, Codes and Cryptography. – 1997. – Vol. 12. – P. 215 – 243;
4. Stinson D.R., van Trung T. Some new results on key distribution patterns and broadcast encryption // Designs, Codes and Cryptography. – 1998. – Vol. 15. – P. 261 – 279;
5. Конюшок С.М., Олексійчук А.М. Безумовно стійки схеми розподілу ключів в інформаційних та телекомунікаційних системах з великою кількістю абонентів: I. Схеми попереднього розподілу й узгодження ключів // Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 83 – 93;
6. Конюшок С.М., Олексійчук А.М. Безумовно стійки схеми розподілу ключів в інформаційних та телекомунікаційних системах з великою кількістю абонентів: II. Схеми багатоадресного розподілу ключів // Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 94 – 104;
7. Padro C., Gracio I., Martin S., Morillo P. Linear key predistribution schemes // Designs, Codes and Cryptography. – 2002. – Vol. 25. – P. 281 – 298;
8. Алексейчук А.Н. Схемы разделения секрета и конечные универсальные алгебры // Реєстрація, зберігання і обробка даних, 2005. – Т. 7. – № 2. – С. 55 – 65;
9. Кон П. Универсальная алгебра / Пер. с англ. – М.: Мир, 1968. – 351 с;
10. Биркгоф Г. Теория решеток / Пер. с англ. – М.: Наука, 1984. – 568 с;
11. Сачков В.Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.

УДК 004.056.5: 518: 512.624.3

Кобозева А.А.

ПРИМЕНЕНИЕ СИНГУЛЯРНОГО И СПЕКТРАЛЬНОГО РАЗЛОЖЕНИЯ МАТРИЦ В СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМАХ

В работе теоретически обоснованы свойства сингулярного и спектрального разложения матриц, дающие математическую основу для использования этих разложений в стеганографических алгоритмах; предлагается алгоритм, в основе которого лежит спектральное разложение симметричной матрицы, применимый для произвольного основного сообщения.

1. Введение

Одной из старейших и нерешенных на сегодняшний день проблем является задача защиты авторских прав, прав интеллектуальной собственности, а также конфиденциальных данных, имеющих цифровой формат, от несанкционированного доступа. Это приводит к чрезвычайной актуальности вопроса защиты информации, представленной в цифровом виде. Одним из направлений в решении этого вопроса является разработка методов сокрытия информации, в частности, цифровой стеганографии [1,2].

Общей чертой всех стеганографических методов является то, что скрываемое сообщение, или дополнительная информация (ДИ), встраивается в некоторый объект, или основное сообщение (ОС), не привлекающий внимания, который затем открыто пересылается адресату по каналу связи. Эффективность любого стеганографического метода оценивается, исходя из совокупности требований, среди которых основное место занимают надежность восприятия после погружения скрываемого сообщения, эффе-

ктивность декодирования ДИ при заданных помехах, устойчивость декодирования к возмущающим воздействиям в канале связи, пропускная способность.

В качестве ОС может использоваться изображение, аудио-, видеосигнал и т.д. Не ограничивая общности рассуждений, для простоты изложения далее везде в качестве ОС (контейнера) будем рассматривать изображение в градациях серого, математической моделью которого выступает матрица.

Многие известные стеганографические алгоритмы производят погружение информации с использованием различных трансформаций контейнера, например, дискретного преобразования Фурье, вейвлет-преобразования и т.д. Не осталось без внимания и преобразование ОС за счет сингулярного разложения его матрицы, хотя количество работ, посвященных этому вопросу, чрезвычайно ограничено. Кроме того, теоретическое математическое обоснование получаемых практических результатов применения такого разложения, их причин и следствий, как правило, является недостаточным, что, очевидно, не защищает предлагаемые стеганографические алгоритмы от ситуаций, когда результат их работы окажется непредсказуемо неудовлетворительным в соответствии с каким-либо критерием. Так в [3] используется сингулярное разложение в области цифровых водяных знаков. В [4] предлагается алгоритм встраивания секретной информации в изображение-контейнер, основанный на нормальном сингулярном разложении матрицы, чрезвычайно заинтересовавший автора настоящей работы множеством оставленных без ответов вопросов. Автор настоящей статьи постарался математически обосновать некоторые свойства сингулярного и спектрального разложений матриц, важные с точки зрения возможности применения этих разложений для целей компьютерной стеганографии, что никогда не делалось ранее в таком контексте, позволившие ему не только объяснить особенности алгоритма, предложенного в [4], указав их истинные причины, а также пойти дальше по пути использования SVD- и спектрального разложений матрицы в области стеганографии. Так в настоящей работе предлагается алгоритм, основанный на спектральном разложении симметричной матрицы (которое не использовалось ранее в рассматриваемой области, поскольку матрица изображения, как правило, не обладает таким свойством), имеющий ряд преимуществ по сравнению с [4] и применимый для любого изображения, рассматриваемого в качестве ОС.

2. Сингулярное и спектральное разложения матриц. Свойства и особенности

Пусть A – произвольная $n \times n$ матрица, элементы которой $a_{ij} \in R,\ i,j = \overline{1,n}$. Для A справедливо представление [5,6], называемое сингулярным разложением матрицы (SVD):

$$A = U\Sigma V^T , \qquad (1)$$

где $U, V - n \times n$ -ортогональные матрицы, $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$. Столбцы $u_1,...,u_n$ матрицы U и столбцы $v_1,...,v_n$ матрицы V называют соответственно левыми и правыми сингулярными векторами матрицы A, величины $\sigma_1,...,\sigma_n$ сингулярными числами. Разложение (1) матрицы A, очевидно, может быть представлено в эквивалентном виде:

$$A = \sum_{i=1}^{n} \sigma_i u_i v_i^T . \qquad (2)$$

Если матрица A является симметричной с собственными значениями $\lambda_i \in R$, $i = \overline{1,n}$, и ортонормированными собственными векторами u_i, $i = \overline{1,n}$, т.е.

$$A = U\Lambda U^T \qquad (3)$$

-спектральное разложение (СР) матрицы A [7] (здесь $\Lambda = diag(\lambda_1,...,\lambda_n)$, $U = [u_1,...,u_n]$), тогда в SVD для матрицы A имеем [5]: левые сингулярные вектора сов-

падают с собственными векторами, $\sigma_i = |\lambda_i|$, $v_i = sign(\lambda_i)u_i$, $i = \overline{1,n}$, причем $sign(0) = 1$. Если же в дополнение ко всем вышеперечисленным свойствам матрицы A добавить еще положительную определенность, то в этом случае спектральное и сингулярное разложения A просто совпадают.

В соответствии с [4], будем называть вектор u лексикографически положительным, если его первая ненулевая компонента положительна, а сингулярное разложение (1) нормальным, если столбцы матрицы U лексикографически положительны. Известно [4], что невырожденная матрица имеет единственное нормальное сингулярное разложение, если ее сингулярные числа попарно различны. Далее будем считать, что все рассматриваемые матрицы обладают таким свойством.

Обоснуем некоторые свойства матричных множителей разложений (1), (3), которые будут полезны в дальнейшем.

1. Пусть s_i - произвольное сингулярное значение A, δ - некоторое возмущение, полученное σ_i, которое привело к соответствующему возмущению dA матрицы A. Очевидно,

$$\delta A = U\,diag\,(\sigma_1,...,\sigma_{i-1},\sigma_i+\delta,\sigma_{i+1},...,\sigma_n)\,V^T - U\,diag(\sigma_1,...,\sigma_n)\,V^T = \delta u_i v_i^T,$$
$$\|\delta A\|_2 = |\delta|, \qquad (4)$$

где $\|\bullet\|_2$ -матричная норма, согласованная с векторной 2-нормой [8]. Непосредственным вычислением можно установить, что не только 2-норма матрицы dA, но и ее евклидова норма также будет равна $|\delta|$ независимо от местоположения δ. Таким образом, одинаковые возмущения различных сингулярных значений приводят к одинаковым возмущениям исходной матрицы. Аналогичное утверждение имеет место для собственных значений симметричной матрицы.

2. Иначе обстоит дело с возмущением сингулярных векторов. Пусть для матрицы A получено SVD- разложение (1), u_k - левый сингулярный вектор A, отвечающий сингулярному значению σ_k, Δ- вектор возмущений u_k размерности n. Обозначим $\overline{A} = [u_1,...,u_{k-1},u_k+\Delta,u_{k+1},...,u_n]\Sigma V^T$. Такое представление для $\overline{A}$ очевидно не является сингулярным разложением, однако по аналогии с (2) может быть записано:

$$\overline{A} = \sum_{i=1,i\neq k}^{n}\sigma_i u_i v_i^T + \sigma_k(u_k+\Delta)v_k^T = \sum_{i=1}^{n}\sigma_i u_i v_i^T + \sigma_k \Delta v_k^T = A + \sigma_k \Delta v_k^T. \quad (5)$$

$\left\|\overline{A} - A\right\|_2$ -возмущение исходной матрицы A, вызванное возмущением Δ сингулярного вектора. Поскольку для рассматриваемой нами матричной нормы имеет место неравенство: $\|BC\|_2 \le \|B\|_2\|C\|_2$ для любых матриц B, C [5], из (5) получаем:

$$\left\|\overline{A} - A\right\|_2 = \left\|\sigma_k \Delta v_k^T\right\|_2 \le \sigma_k \|\Delta\|_2 \left\|v_k^T\right\|_2 = \sigma_k \|\Delta\|_2. \qquad (6)$$

Из (6) вытекает, что чем меньше σ_k, тем меньше $\left\|\overline{A} - A\right\|_2$, т.е. меньшие возмущения матрицы будут, как правило, порождаться возмущением сингулярных векторов, отвечающих меньшим сингулярным значениям. Однако заметим, что (6) – это лишь верхняя оценка для возмущения исходной матрицы. Для симметричной матрицы аналогичное утверждение можно сформулировать в терминах модулей собственных значений и собственных векторов. Отсюда вытекает важный в дальнейшем вывод: если возмущение исходной матрицы происходит вследствие погружения ДИ в столбцы матрицы ее левых сингулярных (собственных для симметричной матрицы) векторов, то для обеспечения наде-

жности восприятия стегосообщения, мерой которой здесь выступает норма матрицы возмущения ОС после погружения ДИ, целесообразно встраивать ДИ в сингулярные (собственные) вектора, соответствующие меньшим сингулярным (меньшим по модулю собственным) значениям.

3. Легко показать, что собственные значения симметричной $n \times n$-матрицы AA^T - числа σ_i^2, а левые сингулярные векторы u_i, $i = \overline{1,n}$, матрицы A - ортонормированные собственные векторы AA^T. Поскольку AA^T является симметричной, то ее можно привести к трехдиагональной симметричной матрице T посредством конечного числа элементарных ортогональных подобных преобразований, в частности, при помощи отражений, не меняющих спектра матрицы и известным образом меняющих собственные вектора [7]. Используя этот факт, а также то, что если T - неразложимая симметричная матрица, то ее матрица собственных векторов не имеет нулевых элементов в первой и последней строках [7], можем сделать вывод, что если (1) отвечает нормальному SVD-разложению матрицы A, то первая строка матрицы U содержит только положительные элементы.

4. Пусть матрица A является симметричной со спектральным разложением (3), $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$ - собственные значения A. Число $gap(i, A) = \min\limits_{i \neq j} \left| \lambda_j - \lambda_i \right|$ называется отделенностью собственного значения λ_i. Пусть $A + E$ - возмущенная исходная матрица, соответствующая возмущению A только за счет возмущения U (например, $A + E$ - результат погружении ДИ в собственные вектора A в разложении (3)), тогда она симметрична, и ее СР можно представить в виде: $A + E = \overline{U} \Lambda \overline{U}^T$. Пусть $u_i, \overline{u_i}$ - нормированные исходный и возмущенный собственные векторы, а θ_i - острый угол между ними. Тогда имеет место соотношение [5]:

$$\sin \theta_i \leq \frac{2\|E\|_2}{gap(i, A)}, \qquad (7)$$

при условии, что $gap(i, A) \neq 0$. Аналогичный результат можно доказать для сингулярного разложения и сингулярных векторов. Из соотношения (7) вытекает, что чувствительность собственного (сингулярного) вектора зависит не от величины соответствующего собственного (сингулярного) значения, а от его отделенности: собственный (сингулярный) вектор тем более чувствителен, чем меньше отделенность соответствующего собственного (сингулярного) значения. Отсюда следует вывод: если погружение ДИ осуществляется непосредственно в собственные (левые сингулярные) вектора A, то для обеспечения нечувствительности получаемого стегосообщения и, как следствие, увеличения устойчивости декодирования, очевидно, предпочтение следует отдать собственным (сингулярным) векторам, соответствующие собственные (сингулярные) значения которых не будут иметь малое значение отделенности. Именно отделенность, а не величина собственного (сингулярного) значения, как предполагалось в [4], является мерой чувствительности соответствующих собственных (сингулярных) векторов и играет основную роль в обеспечении устойчивости стегосообщения. Подтверждением этому является следующее свойство спектрального разложения.

5. Поскольку неравенство (7) имеет место для каждого собственного значения матрицы A, то из него получаем:

$$\max_{1 \leq i \leq n} \left(\frac{1}{2} \sin \theta_i \; gap(i, A) \right) \leq \|E\|_2 . \qquad (8)$$

Формула (8) означает, что если при возмущении исходной матрицы A ее собственные значения не меняются, то даже сравнительно большие возмущения собственных векторов, отвечающих плохо отделенным собственным значениям, будет визуально не

очень заметны. Мы опять пришли к тому, что определяющим свойством для устойчивости как процесса декодирования, так и визуальной является отделенность собственных значений, отвечающих собственным векторам, в которые производится погружение ДИ, а не величины этих собственных значений. Аналогичное утверждение имеет место для сингулярных векторов при разложении (1).

3. Стеганографический алгоритм, основанный на SVD-разложении матрицы ОС

Используя свойства 1-5, становится возможным ответить на вопросы, поставленные [4] и послужившие толчком для написания настоящей работы.

Пусть F - произвольная прямоугольная матрица, отвечающая монохромному изображению, являющемуся ОС, элементы которой $f_{ij} \in \{0,1,...,255\}$. Секретное сообщение, подлежащее погружению в ОС, – последовательность $p_1, p_2, ...,$ где $p_i \in \{-1,1\}$. F разбивается на блоки одинаковой размерности $n \times n$, в каждый из которых происходит погружение части ДИ. Далее будем считать, что $n = 8$. Пусть A один из таких блоков. Для матрицы A строится нормальное сингулярное разложение вида (1), затем в выделенную на рис.1 треугольную область матрицы U погружаются биты ДИ в соответствии с формулой:

$$u'_{ij} = p_k \left| u_{ij} \right|, \quad j = \overline{3,8}, \quad i = \overline{2,9-j}, \tag{9}$$

где u'_{ij} - элементы матрицы U' новых возмущенных сингулярных векторов. Таким образом, без изменения остаются сингулярные векторы, отвечающие максимальным сингулярным значениям (это позволяет обеспечить малые визуальные изменения заполненного контейнера по сравнению с первоначальным изображением в соответствии со свойством 2), и первая строка матрицы (для обеспечения единственности нормального сингулярного разложения, что вытекает из свойства 3). Обеспечение ортогональности столбцов U' после погружения ДИ происходит за счет модификации элементов, содержащихся в выделенной на рис.1 трапецевидной области U, путем решения неоднородных систем линейных алгебраических уравнений [4]. Заметим, что целесообразность выбора области для возмущения сингулярных векторов частично вытекает из свойства 2, но не может быть полностью объяснено только ним, т.к. оценка (6) гарантирует малость $\left\| \overline{A} - A \right\|_2$ только в том случае, когда $\|\Delta\|_2$ достаточно мала. Возмущение сингулярных векторов в соответствии с (9) может привести за счет изменения знаков их компонент к немалому углу θ_i, определенному в свойстве 4, т.е. к ситуации, когда $\|\Delta\|_2$ не будет достаточно малой. В этом случае визуальная устойчивость может иметь место, в соответствии со свойством 5, только, если сингулярные векторы, в которые происходит погружение ДИ, отвечают сингулярным числам с малой отделенностью, что никак не учтено в [4]. Заметим, однако, что, как показывает вычислительный эксперимент, величина сингулярного значения и его отделенность в матрицах реальных изображений, как правило, находятся в прямой зависимости, т.о., чем правее столбец в матрице U, тем меньше отделенность соответствующего ему сингулярного числа.

После погружения ДИ в блок A, вычисляется $A' = U' \Sigma V^T$, элементы которой, вообще говоря, могут и не быть целыми числами, принадлежащими множеству $\{0,1,...,255\}$. Из A' получаем матрицу $\overline{\overline{A}}$ той же размерности следующим образом: если $a'_{ij} < 0$, то $\overline{\overline{a}}_{ij} = 0$; если $a'_{ij} > 255$, то $\overline{\overline{a}}_{ij} = 255$; если $0 \le a'_{ij} \le 255$, но не является целым числом, то $\overline{\overline{a}}_{ij}$ является результатом округления a'_{ij} до ближайшего целого. Процесс получения $\overline{\overline{A}}$

из A' ниже будем называть «округлением». $\overline{\overline{A}}$ является блоком сформированного стего-сообщения. Для декодирования ДИ вычисляется SVD-разложение $\overline{\overline{A}} = \overline{\overline{U}}\,\overline{\overline{\Sigma}}\,\overline{\overline{V}}^T$, используя которое, элементы последовательности ДИ восстанавливаются в соответствии с формулой:

$$p_k = \overline{\overline{u}}_{ij} / \left|\overline{\overline{u}}_{ij}\right|, \; j = \overline{3,8}, \; i = \overline{2, 9-j}\,. \qquad (10)$$

Заметим, что увеличение количества сингулярных векторов, оставляемых без изменения при погружении ДИ, являющихся самыми левыми по своему расположению в матрице U, очевидно, приведет к увеличению визуальной устойчивости стегосообщения, однако, как было экспериментально установлено в [4], к ухудшению устойчивости процесса декодирования. Объяснение этого непосредственно вытекает из свойства 4. Очевидно, что наибольшее количество ошибок при декодировании получается в тех элементах последовательности, которые были погружены в наиболее правые вектора, т.к. эти сингулярные вектора, как уже отмечалось выше, соответствуют сингулярным числам, отделенность которых сравнительно малая, а, значит, являются наиболее чувствительными. При увеличении количества левых оставляемых без изменения сингулярных векторов уменьшается общий объем погружаемой информации, а, значит, увеличивается относительное количество ошибок по сравнению с общим количеством встроенных p_i. Поскольку, как уже отмечалось выше, для оценки эффективности стеганографического метода важным является как требование надежности восприятия после погружения скрываемого сообщения, так и требование устойчивости процесса декодирования ДИ, мы приходим к выводу о том, что местоположение для погружения скрытой информации необходимо определять путем компромисса: для обеспечения первого требования наиболее предпочтительными будут сингулярные вектора, отвечающие сингулярным числам с малой отделенностью, а для обеспечения второго требования отделенность должна быть как можно больше. Ответ на это противоречивое требование может дать только непосредственный вычислительный эксперимент.

Увеличение устойчивости процесса декодирования можно провести за счет уменьшения чувствительности сингулярных векторов путем искусственного «выравнивания» отделенности соответствующих сингулярных значений, состоящего в следующем. Как мы уже упоминали, малые по величине сингулярные значения матрицы изображения, как правило, являются и наименее отделенными. Пусть таковыми будут $\sigma_{k+1},\ldots,\sigma_n$. Заменим их на $\sigma_k - h,\ldots,\sigma_k - (n-k)h, \quad h = (\sigma_k - \sigma_n)/(n-k)$. Ниже такую операцию будем называть разделением сингулярных значений (РСЗ). В силу свойства 1, поскольку h невелико, РСЗ не приведет к заметному возмущению исходной матрицы. Аналогичную операцию с той же целью можно провести для собственных значений в СР симметричной матрицы, что будет использовано ниже.

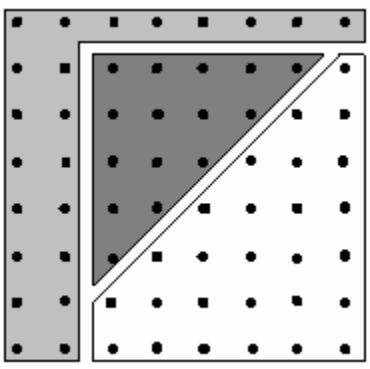


Рис. 1. Матрица U.

4. Новый стегоалгоритм, основанный на спектральном разложении симметричной матрицы

Блоку A исходного изображения (см. п.3) поставим в соответствие две матрицы B, C той же размерности в соответствии со следующим правилом:

$$A = \begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots a_{18} \\ a_{21}\, a_{22}\, a_{23} \ldots a_{28} \\ a_{31}\, a_{32}\, a_{33} \ldots a_{38} \\ \mathbf{L\ L\ L\ L\ L\ L} \\ a_{81}\, a_{82}\, a_{83} \ldots a_{88} \end{pmatrix} \rightarrow B = \begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots a_{18} \\ a_{12}\, a_{22}\, a_{23} \ldots a_{28} \\ a_{13}\, a_{23}\, a_{33} \ldots a_{38} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{18}\, a_{28}\, a_{38} \ldots a_{88} \end{pmatrix}, \quad C = \begin{pmatrix} a_{11}\, a_{21}\, a_{31} \ldots a_{81} \\ a_{21}\, a_{22}\, a_{32} \ldots a_{82} \\ a_{31}\, a_{32}\, a_{33} \ldots a_{83} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{81}\, a_{82}\, a_{83} \ldots a_{88} \end{pmatrix},$$

Матрицы B, C являются симметричными. Пусть их спектральные разложения – это $B = U_B \Lambda_B U_B^T$, $C = U_C \Lambda_C U_C^T$. Заметим,что для матриц одной размерности и одного уровня заполненности, одна из которых симметрична, а другая общего вида, построение СР для первой является более предпочтительным по сравнению с сингулярным для второй как по количеству арифметических операций, так и по запросам к памяти для хранения множителей матричного разложения [5, 7]. В соответствии со свойствами 1-5 для погружения ДИ выбираем столбцы и одноименные строки U_B, U_B^T и U_C, U_C^T матриц B, C соответственно, которые не только отвечают малым по модулю собственным значениям B, C, но, что не менее важно, отделенность которых не является малой. Такая тактика, как подтверждает вычислительный эксперимент, результаты которого в настоящий момент готовятся автором к печати, является предпочтительной по сравнению с [4] с точки зрения устойчивости процесса декодирования. Кроме того, встраивание ДИ в B, C, результатом чего являются B', C', получение которых аналогично получению A' в п.3, увеличивает объем погружаемой информации, или пропускную способность, в 2 раза по сравнению с встраиванием только в A. «Округление» для получения $\overline{\overline{B}}, \overline{\overline{C}}$ из B', C' произведем только в верхнем треугольнике B' и нижнем треугольнике C', исключая главную диагональ. Блок $\overline{\overline{A}}$ пересылаемого стегосообщения будет иметь вид:

$$\overline{\overline{A}} = \begin{pmatrix} a_{11} & \overline{\overline{b}}_{12} & \overline{\overline{b}}_{13} & \ldots & \overline{\overline{b}}_{17} & \overline{\overline{b}}_{18} \\ \overline{\overline{c}}_{21} & a_{22} & \overline{\overline{b}}_{23} & \ldots & \overline{\overline{b}}_{27} & \overline{\overline{b}}_{28} \\ \overline{\overline{c}}_{31} & \overline{\overline{c}}_{32} & a_{33} & \ldots & \overline{\overline{b}}_{37} & \overline{\overline{b}}_{38} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \overline{\overline{c}}_{81} & \overline{\overline{c}}_{82} & \overline{\overline{c}}_{83} & \ldots & \overline{\overline{c}}_{87} & a_{88} \end{pmatrix},$$

где $\overline{\overline{b}}_{ij}, \overline{\overline{c}}_{ij}$ - элементы матриц $\overline{\overline{B}}, \overline{\overline{C}}$ соответственно. Для декодирования ДИ по матрице $\overline{\overline{A}}$ получаем соответствующим образом $\overline{\overline{\overline{B}}}, \overline{\overline{\overline{C}}}$:

$$\overline{\overline{B}} = \begin{pmatrix} a_{11} & \overline{b}_{12} & \overline{b}_{13} \ldots & \overline{b}_{17} & \overline{b}_{18} \\ \overline{b}_{12} & a_{22} & \overline{b}_{23} \ldots & \overline{b}_{27} & \overline{b}_{28} \\ \overline{b}_{13} & \overline{b}_{23} & a_{33} \ldots & \overline{b}_{37} & \overline{b}_{38} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & \\ \overline{b}_{18} & \overline{b}_{28} & \overline{b}_{38} \ldots & \overline{b}_{78} & a_{88} \end{pmatrix}, \qquad \overline{\overline{C}} = \begin{pmatrix} a_{11} & \overline{c}_{21} & \overline{c}_{31} \ldots & \overline{c}_{71} & \overline{c}_{81} \\ \overline{c}_{21} & a_{22} & \overline{c}_{32} \ldots & \overline{c}_{72} & \overline{c}_{82} \\ \overline{c}_{31} & \overline{c}_{32} & a_{33} \ldots & \overline{c}_{73} & \overline{c}_{83} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & \\ \overline{c}_{81} & \overline{c}_{82} & \overline{c}_{83} \ldots & \overline{c}_{87} & a_{88} \end{pmatrix},$$

Декодирование элементов ДИ происходит после СР матриц $\overline{\overline{B}}, \overline{\overline{C}}$ аналогично (10). Для уменьшения ошибки декодирования, что подтверждается проведенным вычислительным экспериментом, здесь возможно использование итерационного процесса, являющегося многократным погружением одного и того же секретного сообщения. Обоснуем его сходимость. Для определенности рассмотрим только матрицу B.

Первую итерацию процесса погружения ДИ в блок B, используя и операцию РСЗ (разделение собственных значений), схематически можно изобразить следующим образом:

$$B \xrightarrow{\text{ïîñòðîåíèå}\quad \text{ÑÐ}} U_B \Lambda_B U_B^T \xrightarrow{\text{ÐÑÇ}} B_1 \xrightarrow{\text{ïîãðóæåíèå}\ \text{ÄÈ}} B_1' \xrightarrow{\text{"îêðóãëåíèå"}} \overline{\overline{B}}_1$$

Для визуальной устойчивости $\left\| B - \overline{\overline{B}}_1 \right\|_2$ должна быть малой. Очевидно, имеет место оценка:

$$\left\| B - \overline{\overline{B}}_1 \right\|_2 = \left\| B \pm B_1 \pm B_1' - \overline{\overline{B}}_1 \right\|_2 \le \left\| B - B_1 \right\|_2 + \left\| B_1 - B_1' \right\|_2 + \left\| B_1' - \overline{\overline{B}}_1 \right\|_2 . \quad (11)$$

Первое и второе слагаемые в правой части (11) малы. Действительно, первое слагаемое в соответствии с (4) сравнимо с h (см. п.3), построенным для соответствующих собственных значений, а малое значение второго вытекает из свойств 2,5 в применении их к предлагаемому алгоритму погружения. $\left\| B_1' - \overline{\overline{B}}_1 \right\|_2$ отвечает возмущению B_1' только за счет «округления», поэтому очевидно, удовлетворяет соотношению:

$$\left\| B_1' - \overline{\overline{B}}_1 \right\|_2 \le \left\| B_1' - B \right\|_2 = \left\| B_1' \pm B_1 - B \right\|_2 \le \left\| B - B_1 \right\|_2 + \left\| B_1 - B_1' \right\|_2 . \quad (12)$$

Значит, третье слагаемое в (11) также имеет малое значение. Собственные значения в B_1' отделены также, как в B_1, значит, очень чувствительных собственных векторов здесь нет, переход к $\overline{\overline{B}}_1$ при малом возмущении, конечно, изменит собственные значения и собственные вектора в $\overline{\overline{B}}_1$ по сравнению с B_1', но не на много. Действительно, по теореме Бауэра-Файка [5], собственные значения $\overline{\overline{B}}_1$ находятся в кругах с центрами в собственных значениях B_1', и радиусами $8\left\| B_1' - \overline{\overline{B}}_1 \right\|_2$, которые, как отмечено выше, достаточно малы. Т.о., хотя отделенность собственных значений в $\overline{\overline{B}}_1$ может быть и ухудшена, но это ухудшение невелико: отделенность собственных значений в $\overline{\overline{B}}_1$ лучше, чем в первоначальной матрице В.

Для второго итерационного шага в качестве контейнера используется $\overline{\overline{B}}_1$, ДИ не меняется, а сам итерационный шаг в точности соответствует приведенной выше схеме ($B_2, B_2', \overline{\overline{B}}_2$ соответствуют $B_1, B_1', \overline{\overline{B}}_1$ на первой итерации). Нетрудно обосновать следующие оценки:

а) $\left\| B_2 - \overline{\overline{B}}_1 \right\|_2 \le \left\| B - B_1 \right\|_2$, т.к. собственные значения в исходном для второй итерации контейнере $\overline{\overline{B}}_1$ отделены больше, чем в B;

б) $\left\| B_2' - B_2 \right\|_2 \le \left\| B_1' - B_1 \right\|_2$,т.к. при погружении ДИ аналогично (9) в соответствующие столбцы матрицы собственных векторов в СР $\overline{\overline{B}}_1$, являющейся исходным контейнером для второго итерационного шага, изменение знаков здесь произойдет в меньшем количестве элементов, чем на предыдущем шаге. Заметим, погружение ДИ в первоначальный контейнер B могло привести к повсеместной замене знаков в элементах матрицы U , используемых для этой цели. Спектральное же разложение матрицы $\overline{\overline{B}}_1$, как показывает проведенный вычислительный эксперимент, дает возможность правильного декодирования в среднем 75% элементов, а, значит, повторное погружение той же ДИ вызовет, как правило, изменение знаков в меньшем количестве элементов матрицы собственных векторов.

в) $\left\| \overline{\overline{B}}_2 - B_2' \right\|_2 \le \left\| B_1' - \overline{\overline{B}}_1 \right\|_2$. Это непосредственно вытекает из (12) с учетом а), б).

Последняя оценка крайне важна, т.к. она позволяет утверждать, что при «округлении», проводимом на второй итерации, отделенность собственных значений нарушится меньше, чем при аналогичном процессе на первой итерации, что приведет к меньшему в сравнении с первым шагом увеличению чувствительности собственных векторов, а, значит, к уменьшению количества ошибок при декодировании. Действительно, уменьшение погрешности при округлении приведет к гарантированно меньшему возмущению собственных значений по сравнению с первой итерацией, т.к. собственные значения являются непрерывными функциями коэффициентов матрицы [6], кроме того $\max_{1 \le j \le 8} \left| \lambda_j \left(\overline{\overline{B}}_2 \right) - \lambda_j \left(B_2' \right) \right| \le \left\| \overline{\overline{B}}_2 - B_2' \right\|_2$ [7].

Все вышесказанное будет иметь место не только на втором, но и на последующих шагах итерационного процесса. Наибольшее относительное увеличение устойчивости процесса декодирования, очевидно, соответствует второму шагу, т.к. худшая отделенность собственных значений отвечает исходной матрице, а по мере проведения итерационного процесса наименьшие значения отделенностей возрастают и становятся сравнимыми друг с другом. Поэтому достаточно провести 2-3 итерации описанного процесса, т.к. при дальнейшем увеличении их числа качественная картина декодирования, очевидно, существенно улучшаться не будет.

5. Выводы

В работе проведено математическое обоснование свойств сингулярного и спектрального разложения матриц, представляющих интерес с точки зрения использования этих разложений в стеганографических алгоритмах. Данное исследование дает возможность не только объяснить и оценить эффективность работы существующих стеганометодов, использующих рассмотренные разложения матриц, но и открывает перспективу создания новых стегоалгоритмов, учитывающих математические особенности SVD-разложения и СР матрицы, что является в настоящее время приоритетной областью исследований автора статьи.

В работе предлагается алгоритм, основанный на спектральном разложении симметричной матрицы, применимый для любого изображения, рассматриваемого в качестве ОС, что никогда не делалось ранее в стеганографических методах, дающий возможность вдвое увеличить пропускную способность и улучшить результат декодирования по сравнению с [4]. Для практического подтверждения приведенных теоретических выкладок был проведен вычислительный эксперимент, подробное описание которого вместе с результатами в настоящий момент готовятся к печати. Здесь же будут затронуты и вопросы, касающиеся устойчивости стеганосистемы, построенной с использованием SVD-разложения и СР матрицы, к возмущающим воздействиям.

Литература

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003. - 501 с;
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК – Пресс, 2006.- 288 с;
3. R.Liu and T.Tan, “An SVD-based watermarking scheme for protecting rightful ownership,” IEEE Trans. Multimedia 4(1), pp. 121-128, 2002;
4. C.Bergman, J.Davidson. Unitary embedding for data hiding with the SVD. – Security, steganography, and watermarking of multimedia contents VII, SPIE Vol.5681, 2005;
5. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. - 430 с;
6. Каханер Д., Моулер К., Нэш С. Численные методы и программное обеспечение. – М.: Мир, 2001. – 575 с;
7. Парлетт Б. Симметричная проблема собственных значений. Численные методы.- М.: Мир, 1983. 384 с;
8. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы.- М.: БИНОМ. Лаборатория знаний, 2006 г.-636 с.

УДК 347.78:004.627;004.056.52

Лигун А.О., Шумейко О.О., Тимошенко Д.В.

ALLDOCUMENT- ТЕХНОЛОГІЯ НОВОГО ПОКОЛІННЯ ДЛЯ ЗБЕРЕЖЕННЯ, ПЕРЕДАЧІ ТА ВІДОБРАЖЕННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

В статті представлено аналіз існуючих методів стиску та передачі електронних документів, наведено особливості розробленої технології збереження, передачі та відображення електронних документів - ALLDOCUMENT та сфери її використання.

У сучасному світі з'явився ще один критерій розділення країн на багаті і бідні – по доступності до глобальних інформаційних ресурсів. У країнах "Великої сімки" послугами Інтернет користується більше половини жителів, а на території України цей показник складає близько 5% [1]. У Європі по кількості користувачів щодо чисельності населення Україна займає 46 місце з 50. На нинішній час Інтернет став загальновизнаним, а для багатьох користувачів ПК – основним джерелом поширення різноманітної інформації. Електронні газети і журнали більш оперативні, чим традиційні паперові видання, більш того, багато видань виходять в електронному вигляді раніш, ніж на папері. Широке поширення електронних версій різних видань зобов'язано електронній верстці.

"Де факто" стандартом для електронних видань є використання формату PDF фірми Adobe (www.adobe.com). Однак існують причини, що стримують поширення цього формату. Насамперед, це той факт, що документи у форматі PDF мають досить великий обсяг, що ускладнює широке використання цього формату в Інтернеті, особливо за умови використання модемного зв'язку.

Іншою причиною є обмеження на використання електронних версій поліграфічної продукції, що пов'язано з законодавчими актами про охорону авторських прав. Але навіть при відсутності авторських претензій до використання електронних версій, видавництва

протестують проти публікації відсканованих і перетворених у текстовий формат книг. У той же час методи копіювання, що не дозволяють безпосередньо використовувати фрагменти документа, такі як ксерокопіювання або мікрофільмування, протидії не викликають. У зв'язку з цим, формати, що дозволяють копіювати і надалі використовувати фрагменти документа, часто є неприйнятними для електронних бібліотек.

Першою спробою рішення цієї проблеми було створення відомою фірмою AT&T графічного формату DJVU (вимовляється Дежавю) (www.djvu.com). Не поглиблюючи особливо цієї розробки, відзначимо, що цей формат дозволив зберігати документи з досить пристойною якістю при істотно менших обсягах, чим той же PDF. Крім того, цей формат, будучи графічним, а не текстовим, не дозволяє виділяти і копіювати фрагменти документа. Аналогічний формат LuraDocument LDF був розроблений німецькою фірмою LuraTech. Зовсім недавно з'явився ще один формат стиску документів JPEG2000/Part 6 або JPM (http://www.luratech.com/).

Використання даних форматів для потреб електронних бібліотек стримує той факт, що всі перелічені формати, як PDF, так і DJVU, LuraDocument, JPEG2000/Part 6 при їх використанні on-line зберігають документ на клієнтській машині, що дозволяє несанкціоноване копіювання та тиражування документу, що є суттєвим порушенням авторських прав на документ.

В рамках проекту створення електронної бібліотеки ALLIBRARY нами розроблена технологія векторизації, стиску, збереження, передачі та відображення документів ALLDOCUMENT.

Для реалізації ALLDOCUMENT розроблено альтернативний метод стиску документів, який засновано на принципах інших, ніж DJVU, LuraDocument та JPEG2000/Part 6. Якщо основою методів DJVU, JPEG2000/Part 6 і LuraDocument є ідея поділу документа на шари кольорів, то в основі ALLDOCUMENT лежить виділення символів і локалізація елементів, що не є символами, тобто таблиць, малюнків і т. ін. Усе, що не ввійшло в цей перелік, є тіло документа. Запропонований підхід разом з розробленим методом стиску зображень на основі сплесків, дозволив одержати формат, що надає змогу по багатьом параметрам випередити існуючі аналоги.

Іншою родзинкою ALLDOCUMENT є спосіб уявлення і передачі документів, який надає видаленому клієнту можливість ознайомлення з електронними ресурсами без порушення авторських прав на даний документ. Документ поставляється клієнту у вигляді, що не допускає копіювання, як фрагментів, так і всього документа в цілому. З метою прискорення доставки документа в мережі Інтернет, він передається читачеві в стислому вигляді по одній сторінці, яка одразу відображається в відео-буфер і витискується наступною. Для роботи з документом в режимі on-line використовується plugin для Internet Explorer. В разі використання клієнтом іншого браузера, підготовлено JAVA-додаток. ALLDOCUMENT забезпечує читача елементами навігації і пошуку по ключовим словам. Окрім того, для корпоративних клієнтів, при використанні ALLDOCUMENT має додаткові можливості – замітки на полях, формування колекції, створення елементів навігації, пошук по ключовим словам в рамках колекції, чи конкретного документу. Підготовлена версія цього формату для кишенькових комп'ютерів PocketPC.

Наскільки нам відомо, повних аналогів ALLDOCUMENT не існує. На даний час деяку подібну послугу надає GoogleLibrary, але при наданні цієї послуги кожна сторінка передається в графічному форматі gif чи jpeg і може бути легко збережена, наприклад, з використанням браузера Opera. Цей факт привів до цілої низки судових справ між компанією Google та авторами документів, які використовуються GoogleLibrary.

Схематично структура файлу ALLDOCUMENT виглядає наступним чином.

Технологія ALLDOCUMENT інтегрована як складова частина електронної бібліотеки ALLIBRARY, але може використовуватися і автономно.

На даний час технологія ALLDOCUMENT упроваджена в Дніпродзержинському державному технічному університеті, електронній бібліотеці ТОВ «Техноінжинірінг», а також використовується в науково-технічній бібліотеці Криворіжсталі.

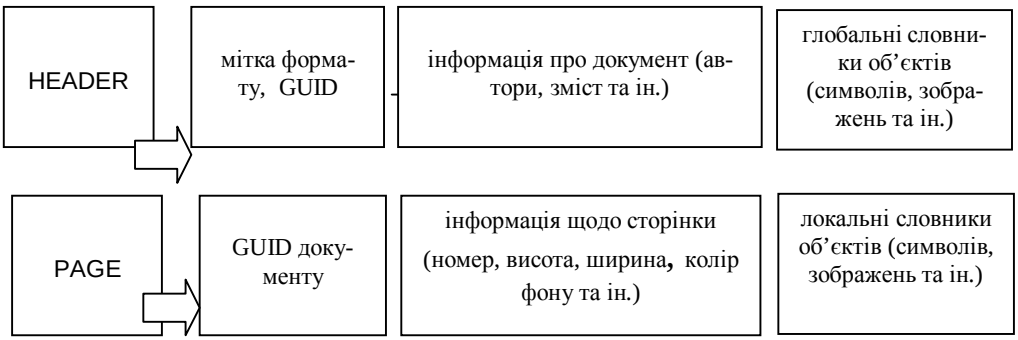


Рис. 1. Структура файлу ALLDOCUMENT.

Висновки

Використання технології ALLDOCUMENT для електронного документообігу в умовах необхідності збереження авторських прав на документи, дозволяє підвищити інформативність та ефективність електронних бібліотек та хранилищ знань.

Література

1. Ядрова Г.В. Региональные информационные центры как форма ликвидации информационного неравенства –Науч. и техн.б-ки, 2005, №11 с. 14-17.

УДК 681.03

Дудикевич В.Б., Горпенюк А.Я.

ІНКРЕМЕНТНИЙ ОБЧИСЛЮВАЧ ВАЖКООБОРОТНОЇ ФУНКЦІЇ РАБІНА

В статті подано результати синтезу та аналізу структури інкрементного обчислювача важкооборотної функції Рабіна, застосування якої дозволяє покращити швидкодію обчислювачів функції Рабіна за рахунок обробки послідовності аргументів функції за приростами.

Постановка проблеми

Як відомо [1], причиною низької швидкодії асиметричних криптосистем (стосовно шифрування великих об'ємів інформації) є великі затрати часу на обчислення важкооборотних функцій для великої кількості багаторозрядних значень аргументу. Слід сказати, що сьогодні при обчисленні значень важкооборотних функцій застосовують виключно алгоритмічні методи обчислень. Тобто, незалежно від алгоритму обчислення важкооборотної функції і ступеня розпаралелення процесу обчислення, кожне нове значення важкооборотної функції обчислюють виходячи з нового повнорозрядного значення аргументу. В роботах [2,3] пропонується там, де це вигідно з точки зору швидкодії, використовувати також аналітичні методи обчислень, тобто за допомогою моделі функціонального перетворювача визначати нове значення функції, спираючись на її попереднє (початкове) значення і на приріст цієї функції, розкладений в послідовність елементарних приростів. Причому як модель функціонального перетворювача пропонується використовувати цифрову інтегруючу структуру, синтезовану за відомою [4] модифікованою методикою побудови цифрового функціонального перетворювача на основі модифікованої системи породжуючих диференціальних рівнянь Шеннона. Такі цифрові інтегруючі структури зручно застосовувати для брутальної атаки з вибраним відкритим текстом. Що стосується власне шифрування, то такі структури не дають істотного ефекту через те, що основна частина приростів між блоками є великими числами, і їх розклад в послідовність одиничних приростів породжує надто довгу послідовність імпульсів, яка підлягає обробці інтегруючою структурою. В таких випадках [2,3] одним з методів покращання швидкодії є перехід від

обробки одиничних приростів до обробки великих приростів, і зокрема, приростів, кратних цілій степені двійки. Схеми, здатні обробляти такі прирости, називають інкрементними. Розроблення інкрементної структури для обчислення важкооборотної функції Рабіна дозволить покращити швидкодію обчислювачів функції Рабіна при їх застосуванні для шифрування інформації.

Мета роботи

Метою роботи є покращання швидкодії інтегруючого функціонального обчислювача функції Рабіна шляхом забезпечення можливості обробки великих приростів.

Теоретичний синтез інкрементного обчислювача функції Рабіна

Як відомо [2,3], одним з шляхів покращання швидкодії різницевих обчислювачів функції Рабіна є перехід від оброблення одиничних приростів аргументу до оброблення приростів, кратних цілій степені двійки. Такі перетворювачі називають вже не числоімпульсними, а інкрементними. Розробка інкрементного відтворювача функції Рабіна, зважаючи на величину блоків (а значить і різниць), що обробляються в процесі шифрування методом Рабіна, дозволить кардинально покращити швидкість обробки великих приростів різницевими структурами. За певних характеристик інкрементної структури стане можливим її пряме застосування для обробки цілого (повнорозрядного) блоку інформації, що підлягає шифруванню.

Переходячи до теоретичного синтезу структури інкрементного відтворювача функції Рабіна, будемо виходити з припущення, що нам необхідно обчислити функцію Рабіна, нарощуючи (прирощуючи) її аргумент «цифра за цифрою» від 0 до X.

Нехай нам необхідно обчислити функцію Рабіна y_i від аргументу x_i:

$$y_i = x_i^2 \bmod k \qquad (1)$$

Розкладемо n - розрядний аргумент x_i за степенями двійки:

$$x_i = a_{0i} \cdot 2^0 + a_{1i} \cdot 2^1 + a_{2i} \cdot 2^2 + \cdots + a_{(n-1)i} \cdot 2^{n-1} \qquad (2)$$

де a_{ji} ($j = \overline{0,n-1}$) - значення двійкових розрядів x_i. Позначимо x_{ji} ($j = \overline{0,n-1}$) двійкове число, складене з молодших розрядів числа x_i аж до розряду з вагою 2^j. Таким чином:

$$x_{(n-1)i} = x_i \qquad (3)$$

Позначимо y_{ji} - функцію Рабіна від аргументу x_{ji}. Обчислимо за (1) y_{0i} - функцію Рабіна від аргументу x_{0i}:

$$y_{0i} = x_{0i}^2 \bmod k = \left(a_{0i} \cdot 2^0\right)^2 \bmod k = a_{0i} \bmod k = a_{0i}, \qquad (4)$$

оскільки a_{0i} (0 або 1) - завжди менше за k.

Далі визначимо y_{1i} за (1) з врахуванням (4):

$$\begin{aligned} y_{1i} &= x_{1i}^2 \bmod k = \left(a_{0i} \cdot 2^0 + a_{1i} \cdot 2^1\right)^2 \bmod k = \\ &= \left[\left(a_{0i} \cdot 2^0\right)^2 \bmod k + 2 \cdot a_{0i} \cdot a_{1i} \cdot 2^1 \bmod k + a_{1i} \cdot 2^2 \bmod k\right] \bmod k = \\ &= \left(y_{0i} + a_{0i} \cdot a_{1i} \cdot 2^2 \bmod k + a_{1i} \cdot 2^2 \bmod k\right) \bmod k \end{aligned} \qquad (5)$$

Аналогічно визначаємо y_{2i}:

$$\begin{aligned} y_{2i} &= x_{2i}^2 \bmod k = \left(a_{0i} \cdot 2^0 + a_{1i} \cdot 2^1 + a_{2i} \cdot 2^2\right)^2 \bmod k = \\ &\left[\left(a_{0i} \cdot 2^0 + a_{1i} \cdot 2^1\right)^2 \bmod k + 2 \cdot \left(a_{0i} \cdot 2^0 + a_{1i} \cdot 2^1\right) \cdot a_{2i} \cdot 2^2 \bmod k + a_{2i} \cdot 2^4 \bmod k\right] \bmod k = \\ &= \left(y_{1i} + 2^3\left(a_{0i} \cdot 2^0 + a_{1i} \cdot 2^1\right) \cdot a_{2i} \cdot \bmod k + a_{2i} \cdot 2^4 \bmod k\right) \bmod k \end{aligned} \qquad (6)$$

Нарешті для y_{ji} отримаємо:

$$y_{ji} = \left(y_{(j-1)i} + 2^{j+1} x_{(j-1)i} \cdot a_{ji} \cdot \bmod k + a_{ji} \cdot 2^{2j} \bmod k\right) \bmod k \qquad (7)$$

Розглянемо інший підхід до теоретичного синтезу інкрементного відтворювача функції Рабіна. Нехай аргументу x_i відповідає значення функції y_i (1). Далі аргумент x_i приростає на величину $\Delta x_i = 2^j$. Визначимо нове значення функції Рабіна y_{i+1}:

$$y_{i+1} = (x_{i+1})^2 mod k = \left(x_i + 2^j\right)^2 mod k = \left(x_i{}^2 \, mod k + 2^{j+1} x_i \, mod k + 2^{2j} \, mod k\right) mod k = \\ = \left(y_i + 2^{j+1} x_i \, mod k + 2^{2j} \, mod k\right) mod k \quad (8)$$

Аналізуючи вирази (7), (8), запропонуємо наступний алгоритм обчислення функції Рабіна при нарощенні її аргументу «цифра за цифрою».

1. Зчитати двійковий розряд a_{ji} аргумента x_i, який має вагу 2^j. Якщо $a_{ji} = 0$, встановити $y_{ji} = y_{(j-1)i}$ і перейти до зчитування наступного розряду аргументу (до пункту 1 алгоритму). Якщо $a_{ji} = 1$, перейти до пункту 2 алгоритму.

2. Виконати операцію $\alpha = \left(2^{j+1} x_{(j-1)i} + 2^{2j}\right) mod\, k$ і перейти до пункту 3 алгоритму.

3. Виконати операцію $y_j = \left(y_{j-1} + \alpha\right) mod\, k$ і перейти до зчитування наступного розряду аргументу (до пункту 1 алгоритму).

Аналізуючи пункт 2 алгоритму зауважимо, що тут здійснюється швидка операція зсуву і додавання одиниці в старший розряд (що не викликає більше одного переносу). Разом з тим для спрощення аналізу структур будемо вважати ці дві операції еквівалентними одному додаванню. Крім того в цьому пункті здійснюється операція модульної редукції.

Аналізуючи пункт 3 алгоритму і пам'ятаючи, що обидва доданки в дужках є меншими за k , робимо висновок, що операція зведення за модулем k в цьому пункті еквівалентна одному додаванню (а саме додаванню числа $\left(2^n - k\right)$).

Взявши до уваги розглянуті особливості пунктів 2,3 алгоритму, робимо висновок, що коригування результату обчислення функції Рабіна при зростанні її аргументу на 2^j вимагає максимум трьох додавань n - розрядних чисел і одної операції модульної редукції.

Розроблення структури інкрементного обчислювача функції Рабіна

Розглянемо алгоритм обчислення функції Рабіна при нарощенні її аргументу «цифра за цифрою», запропонований в попередньому пункті статті. Зокрема, пункт 2 цього алгоритму. Очевидно, що максимальне число, за яким необхідно здійснювати модульну редукцію - число $\left(2^{j+1} x_{(j-1)i} + 2^{2j}\right)$ - може досягати значення 2^{2n}. Тобто воно може мати в два рази більшу розрядність, ніж модуль k. Тому операція модульної редукції може бути трудоємкою і повільною. Разом з тим, аналізуючи згаданий алгоритм, можна зробити висновок про можливість формування доданків:

$$\left(2^{j+1} x_{(j-1)i} + 2^{2j}\right) mod\, k \quad (9)$$

для всіх розрядів паралельно. Наприклад, для старшого розряду ($j = n-1$):

$$\left(2^n x_{(n-2)i} + 2^{2n-2}\right) mod\, k = 2^n \left(x_{(n-2)i} + 2^{n-2}\right) mod\, k . \quad (10)$$

Такий доданок можна сформувати за допомогою нагромаджуючого суматора з регістром зсуву (рис.1). В структурній схемі на рис.1 регістр зсуву РгЗ має два керуючі входи - вхід Т на зсув інформації в бік старших розрядів, і вхід С на запис паралельного коду з суматора СМ. На вхід Т подається n імпульсів, які зсувають початковий код $\left(x_{(n-2)i} + 2^{n-2}\right)$ на n розрядів. Після кожного зсуву, якщо на виході РгЗ або СМ з'являється імпульс переповнення, здійснюється модульна редукція - в регістр перезаписується сума попереднього його вмісту (який більший за k) і числа $\left(2^n - k\right)$. Імпульс пе-

реповнення при цьому ігнорується, що рівносильно відніманню від попереднього вмісту регістра модуля k.

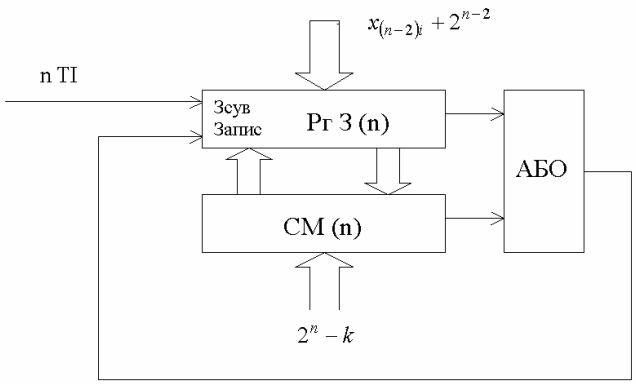


Рис. 1. Допоміжний нагромаджуючий суматор для формування доданка (10).

Для $j = n-2$ допоміжна структура буде виглядати подібним чином. Однак в РгЗ такої структури на початку роботи записується число меншої розрядності, ніж в схемі на Рис.1 - в старшому розряді завжди 0. Менше подається також тактових імпульсів для зсуву інформації. В наступних допоміжних схемах початкові коди і число тактових імпульсів будуть ще меншими відповідно до (9) (адже j зменшується).

Загалом n/2 допоміжних нагромаджуючих суматорів для обробки приростів 2^j, де $\overline{j = n/2-1, n-1}$ будуть подібними до схеми на рис.1. Що стосується інших n/2 допоміжних структур - то це регістри зсуву без суматорів. Це пов'язано з тим, що початковий код в таких регістрах менший $2^{n/2}$. І зсувається цей код не більше, ніж на n/2 розрядів. Тому переповнення не виникає і потреби в модульній редукції немає. Приклад допоміжного регістра зсуву - для приросту 2^j, де $j = n/2-1$ - на рис.2.

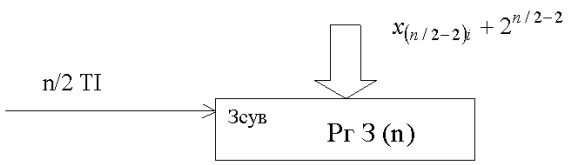


Рис. 2. Допоміжний регістр зсуву.

Для подальшої розробки структури введемо спільне умовне позначення для допоміжних нагромаджуючих суматорів і регістрів зсуву, незалежно від їх типу. Таке умовне позначення подане на рис. 3.

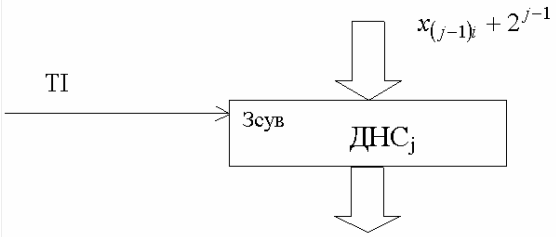


Рис. 3. Умовне позначення допоміжних суматорів та регістрів зсуву.

Загалом в структурі інкрементного обчислювача функції Рабіна, яка розробляється, необхідно передбачити (n-1) допоміжних нагромаджуючих суматорів. Взагалі кажучи, мінімальна необхідна кількість допоміжних нагромаджуючих суматорів дорівнює кількості розрядів аргументу функції Рабіна, які не дорівнюють нулю. Але для покращання ре-

гулярності структури доцільно передбачити саме (n-1) допоміжних суматорів - для всіх розрядів крім молодшого. Відбір потрібних ДНС можна здійснювати за допомогою цифрових ключів.

Крім ДНС в структурі інкрементного обчислювача функції Рабіна необхідно передбачити головний нагромаджуючий суматор, який буде здійснювати підсумовування допоміжних доданків, сформованих за допомогою ДНС, і постійну модульну редукцію результатів підсумовування. Таким чином, головний нагромаджуючий суматор має складатися з двох: перший підсумовує черговий допоміжний доданок, другий - за необхідності здійснює модульну редукцію.

Крім головного і допоміжних нагромаджуючих суматорів в структурі необхідно передбачити мультиплексор для підключення до головного нагромаджуючого суматора потрібних допоміжних доданків, генератор тактових імпульсів та інші допоміжні елементи. Розроблену відповідно до цього опису структуру інкрементного обчислювача функції Рабіна подано на Рис.4.

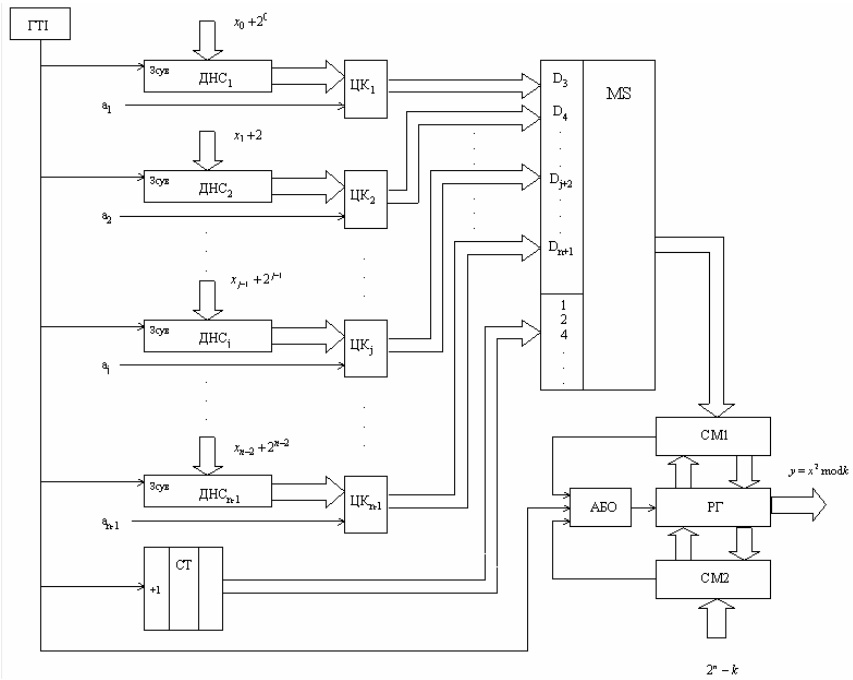


Рис. 4. Структурна схема інкрементного обчислювача функції Рабіна.

Структура містить (n-1) допоміжних нагромаджуючих суматорів ДНС1-ДНСn-1, в які перед початком роботи структури записується число $\left(x_{j-1}+2^{j-1}\right)$; (n-1) цифрових ключів $ЦК_1$ – $ЦК_{n-1}$, які при одиничному значенні відповідного розряду аргументу a_j подають на мультиплексор MS відповідний допоміжний доданок (якщо $a_j = 0$, на вхід MS подається нульовий код); генератор тактових імпульсів ГТІ; лічильник тактів СТ; мультиплексорMS і головний нагромаджуючий суматор в складі двох комбінаційних суматорів СМ1, СМ2 і регістра РГ з елементом АБО на вході.

На вхід РГ подаються тактові імпульси починаючи з третього (саме тому на входи D0, D1, D2 мультиплексора подається нульовий код). За командою тактових імпульсів до результату перетворення y (початкове значення результату дорівнює a_0 відповідно до (4)) по черзі додаються допоміжні доданки, сформовані допоміжними нагромаджуючими суматорами. При необхідності (при переповненні СМ1 або СМ2) здійснюється модульна редукція результату. Тобто робота структури на Рис.4 відповідає запропонованому алго-

ритму обчислення функції Рабіна при нарощенні аргументу “цифра за цифрою”. Перейдемо тепер до аналізу розробленої структури.

Оцінка точності, швидкодії та діапазону перетворення інкрементної структури обчислювача функції Рабіна

Оцінюючи точність розробленої структури, необхідно звернути увагу на те, що ми маємо справу з модулярною арифметикою. Тому будь-яка найменша похибка в обчисленні проміжної функції x^2 призводить до великої похибки результату перетворення. Це означає, що нас задовольняє тільки абсолютна точність – структура повинна працювати без похибки.

Як відомо [4], сьогодні не існує аналітичної методики оцінки точності числоімпульсних інтегруючих структур. Тому доводиться вдаватися до імітаційного моделювання. Такий підхід застосовано для оцінки точності розробленої структури.

З метою дослідження розробленої структури було розроблено імітаційні моделі її структурних блоків – допоміжних і головного нагромаджуючих суматорів – а також імітаційну модель структури в цілому. За допомогою розробленої імітаційної моделі досліджувалась розроблена структура. Результати моделювання доводять той факт, що розроблена структура відтворює згадану функцію без похибки.

Переходячи до аналізу діапазону перетворення розробленої структури, звернемося до співвідношення (10) та Рис.1. Співвідношення (10) визначає допоміжний доданок відповідно до (7) для максимального вхідного приросту 2^{n-1}. А на Рис.1 подано структуру допоміжного нагромаджуючого суматора, який формує такий доданок. Крім того розроблена структура (Рис.4) формує допоміжні доданки для всіх приростів меншої ваги (2^{n-2}, 2^{n-3}, … 2^0). Тобто максимальне значення аргументу, яке може обробити розроблена структура інкрементного обчислювача функції Рабіна – це n – розрядне двійкове число з одиницями у всіх розрядах. Значення такого числа – 2^n-1. Отже, діапазон зміни аргументу для розробленої структури визначається нерівністю:

$$0 \le x < 2^n \qquad (11)$$

Перейдемо до аналізу швидкодії розробленої структури. Під швидкодією будемо розуміти максимальний час обчислення функції Рабіна від n – розрядного значення аргументу. Вимірювати швидкодію домовимося в умовних одиницях – в кількості часових інтервалів, необхідних для додавання двох n- розрядних чисел.

Аналізуючи роботу $ДНС_{n-1}$ в структурі на Рис.4 відзначаємо, що для її роботи необхідно n тактів (Рис.1). На кожному такті здійснюється операція зсуву і (при необхідності) операція модульної редукції – одне додавання двох n- розрядних чисел.

Тобто для $ДНС_{n-1}$ мінімальна необхідна тривалість такту:

$$T_{ДНС(n-1)} = t_{СМ} + t_З \qquad (12)$$

де $t_{СМ}$ – тривалість операції додавання, $t_З$ – тривалість операції зсуву.

Для роботи $ДНС_{n-2}$ необхідно (n-1) тактів. Мінімальна тривалість такту також визначається (12). Для половини ДНС – для ДНС молодших розрядів, які будуються за схемою Рис.2, мінімальна тривалість такту визначається виразом:

$$T_{ДНС1} = t_З \qquad (13)$$

оскільки в цих ДНС не виникає необхідності в модульній редукції.

Всі ДНС працюють паралельно, формуючи допоміжні доданки за час від 2Т (для $ДНС_1$) до nТ (для $ДНС_{n-1}$). По мірі формування ці допоміжні доданки підсумовуються до результату перетворення в РГ головного нагромаджуючого суматора (Рис.4). Однак крім власне підсумовування, головному нагромаджуючому суматору на кожному такті необхідний ще час на здійснення модульної редукції за допомогою СМ2. Тобто для головного нагромаджуючого суматора мінімальна тривалість такту визначається так:

$$T_{ДНС(n-1)} = 2t_{СМ} \qquad (14)$$

Очевидно, що з оцінок тривалості такту – (12), (13), (14), - максимальна (14). Її приймаємо за мінімально-необхідну тривалість такту роботи структури на Рис.4.

Перейдемо до оцінки кількості тактів, необхідних розробленій структурі для обробки n – розрядного аргументу. Найдовше формується старший допоміжний доданок за до-

помогою $ДНС_{n-1}$ (див. Рис.4, Рис.1) – протягом n тактів. Цей доданок попадає на вхід головного нагромаджуючого суматора в кінці n-го такту, тобто на початку n+1 – го такту. Протягом цього n+1 такту здійснюється підсумовування цього доданку до результату перетворення і модульна редукція за допомогою головного нагромаджуючого суматора (СМ1, РГ, СМ2 на Рис.4). На кінець n+1 – го такту ми маємо результат перетворення на виході регістра РГ розробленої структури. Тобто в цілому структурі інкрементного обчислювача функції Рабіна, для обробки n – розрядного аргументу, необхідно n+1 такт роботи. Враховуючи тривалість такту (14), час обробки n – розрядного аргументу, який визначає швидкодію структури, дорівнює:

$$t_{IC} = (n+1)T_{ГНС} = (n+1)2t_{СМ} = (2n+2)t_{СМ} \qquad (15)$$

Таким виразом оцінюється також швидкодія алгоритмічних методів обчислення важкооборотної функції Рабіна [5]. Однак, розроблена структура здатна обробляти не тільки повнорозрядні значення аргументів, але й прирости аргументу. Причому в цьому випадку при оцінці швидкодії за виразом (15) n буде розрядністю приросту, яка, як правило, менша за розрядність аргументу. А алгоритмічні методи завжди обробляють повне значення аргументу (n_{max}). Саме тому розроблена структура характеризується вищою швидкодією.

Висновки

Асиметричні криптосистеми грунтуються на важкооборотних функціях. Одною з популярних є важкооборотна функція Рабіна. Основною проблемою асиметричних криптосистем є їх низька швидкодія. Для обчислення важкооборотних функцій, як правило, застосовують алгоритмічні методи, швидкодія яких є недостатньою. Відомі число-імпульсні відтворювачі функції Рабіна, які працюють за аналітичним принципом обчислень, дають виграш в швидкодії тільки при невеликих приростах аргументу. Перспективним способом подальшого покращання швидкодії є перехід від обробки одиничних приростів аргументу до обробки великих приростів. Зокрема, перехід до обробки приростів, кратних цілій степені двійки.

Розроблена структура інкрементного обчислювача функції Рабіна дозволяє обробляти прирости аргументу функції Рабіна, кратні цілій степені двійки, без похибки. Діапазон перетворення та швидкодія розробленої структури при обробці повнорозрядного значення аргументу, відповідає кращим алгоритмічним методам обчислення. При обробці запропонованою структурою приростів, розрядність яких менша за розрядність аргументу, швидкодія інкрементного відтворювача є значно вищою за швидкодію алгоритмічних методів обчислення.

Література

1. Перспективы развития и использования асимметричных алгоритмов в криптографии/ Лунин А.В., Сальников А.А.; Конфидент, 1999. №10;
2. Обгрунтування перспективності застосування різницевих методів при обчисленнях важкооборотних функцій/ Горпенюк А.Я.; Науково-технічний журнал "Захист інформації", Київ, 2001. №3(8);
3. Fast algorithms and computing means of cryptological functions/Andriy Horpenyuk.; Computing, 2005, Vol. 4, Issue 2, pp. 69-76;
4. Число-імпульсні функціональні перетворювачі/ Дудикевич В.Б.; Автореф. дис. д-ра техн. наук. - Львів, 1991;
5. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. 2-е издание /Брюс Шнайер.; "Триумф" - Москва, 2002.

УДК.681.5

Однороманенко С.Г.

СИСТЕМНИЙ ПІДХІД ДО ПРОЕКТУВАННЯ ВІДОМЧИХ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

В статті розглянуто реалізацію системного підходу, що пропонується як узагальнюючий інструмент при розв'язанні науково-технічної задачі по системному проектуванню відомчих цифрових телекомунікаційних мереж. Наведені основні висновки до застосування результатів.

Вступ

Світовий процес переходу від індустріального до інформаційного суспільства, а також соціально-економічні зміни, що відбуваються в Україні, вимагають суттєвих змін у багатьох сферах діяльності держави. В першу чергу це стосується галузі зв'язку. У відповідності до постанов КМ України "Про концепцію розвитку зв'язку України до 2010 року" від 09.12.99 року №2238 та "Про комплексну програму створення єдиної національної системи зв'язку" від 23.09.93 року №790, крім завдання переоснащення підприємств та відомств країни сучасними засобами зв'язку, постає й науково-технічна задача по проектуванню відомчих цифрових телекомунікаційних мереж (ВЦТМ), як складових єдиної національної системи зв'язку.

Підходи до проектування, що застосовувалися раніше, застаріли, оскільки з'явилися нові концепції організації цифрових мереж зв'язку і технології їх використання.

Розробка методології раціонального проектування складних технічних систем одержала назву системного проектування або системотехніки [1-2].

Системний підхід до проектування - один з молодих напрямків науки і виділений в самостійну дисципліну зі своєю аксіоматикою, теоретичним апаратом і областями додатків.

Повніше усього системний підхід розвитий стосовно до проектування систем керування, які характеризуються складністю розв'язуваних задач і необхідністю розгляду проблеми в цілому.

СИСТЕМНЕ ПРОЕКТУВАННЯ ВЦТМ - це методологія рішення складних проблем, яка засновується на концепції системи. Система є те, що вирішує проблему. Визначаючи "рішення проблеми" як "цілеспрямовану систему", системний підхід тим самим дозволяє уявити процес рішення проблеми як процес створення і використання системи відповідно до етапів її життєвого циклу [2].

При цьому ефективність рішення проблем залежить у першу чергу від методів, які застосовуються для виконання функцій рішення складових проблеми.

У будь-якій системі існує два основних і різноманітних по ролі підпроцеса:

- основний процес;
- зворотній зв'язок (а також вхід, вихід і обмеження).

Поняття "процесу" є центральним поняттям системного підходу в рішенні проблеми, що являє собою різницю між існуючою і бажаною ситуацією.

Основний зміст системного підходу полягає не стільки у формальному математичному апараті, що описує "системи", "рішення проблеми", і не в спеціальних математичних методах, а в його концептуальному, тобто понятійному апараті, у його ідеях, підході й установках. У загальному випадку, виходячи з концепцій системного проектування, рішення проблеми традиційно включає наступні етапи:

- ідентифікація (виявлення) проблеми;
- оцінка актуальності проблеми;
- визначення мети (установлення критеріїв і обмежень);
- виявлення (розкриття) структури системи ВЦТМ і її дефектних елементів;
- визначення структури системи ВЦТМ для побудови набору варіантів;
- знаходження, оцінка і вибір варіанта (альтернативи);

– підготовка рішення (визначення процесу реалізації);
– узгодження знайденого рішення (визнання рішення колективом виконавців і керівників);
– запуск процесу реалізації рішень (реалізація рішення);
– керування процесом реалізації рішення;
– оцінка реалізації і її наслідків (ефективності).

Нижче викладаються основні концепції системного проектування стосовно до складних систем, як керованих систем логіко-динамічного класу. Під керованою системою тут розуміється система, яка має такі характерні ознаки, як:
– підсистеми, кожна з яких має власну ціль функціонування;
– підпорядковану загальній цілі системи в цілому;
– велике число зв'язків між підсистемами;
– розгалужену інформаційну мережу й ін [5].

Це призводить до необхідності підходити до проектування керованої системи як складної системи.

ПРОЦЕС СИСТЕМНОГО ПРОЕКТУВАННЯ керованої системи як складної (в тому числі і ВЦТМ) містить у собі два основних етапи: етап зовнішнього (макропроектування) й етап внутрішнього проектування (мікропроектування).

Перший етап включає вибір функцій, структури системи і її складу, а також визначення системних характеристик і принципів функціонування підсистем, причому, основними питаннями першого етапу є:
- розробка системи критеріїв (якості функціонування й оцінки варіантів системи);
- побудова архітектури (складу) системи;
- дослідження реалізованих алгоритмів керування для прийнятої системи критеріїв;
- формалізація процесів функціонування системи;
- розробка математичної моделі системи і її підсистем;
- синтез і дослідження оптимальних режимів функціонування системи та ін.

Основна задача другого етапу полягає в розробці проектних рішень, пов'язаних із технічною реалізацією системи, оптимізацією характеристик, параметрів системи і її підсистем, на основі прийнятої математичної моделі, що задовольняє критеріям якості.

Системний аналіз дозволяє сформулювати основні задачі, вирішення яких і складає основу системного підходу до проектування керованої системи.

Таким чином, вирішення проблеми системного проектування ВЦТМ повинно містити, принаймні, три основних положення:
- чітке визначення цілей створення ВЦТМ і сукупності розв'язуваних нею задач;
- перелік і характеристики діючих на ВЦТМ факторів, які підлягають обов'язковому врахуванню при розробці системи і її моделі;
- вибір показників ефективності процесів та якості результатів.

Для розробки методики розрахунку показників ефективності, а також для дослідження різноманітних властивостей системи необхідна її математична модель [1]. Відомості про систему, що отримані в результаті моделювання й експерименту, дають можливість обґрунтувати оптимальну структуру ВЦТМ, визначити оптимальні значення її параметрів і переконатися в тому, що обраний варіант ВЦТМ відповідає цілі її розробки і має достатню ефективність.

Як підсумок вищесказаному, наведемо визначення проектування з використанням системного підходу (системне проектування), а саме: системне проектування – це процес побудови проектів складних об'єктів, як цілеорієнтованих систем в категоріях системних властивостей (будови, функціонування, розвитку), системних ресурсів (час, кошти, людиновитрати) та структури життєвих циклів (наукових досліджень, проектування, виготовлення, використання та утилізація) [3].

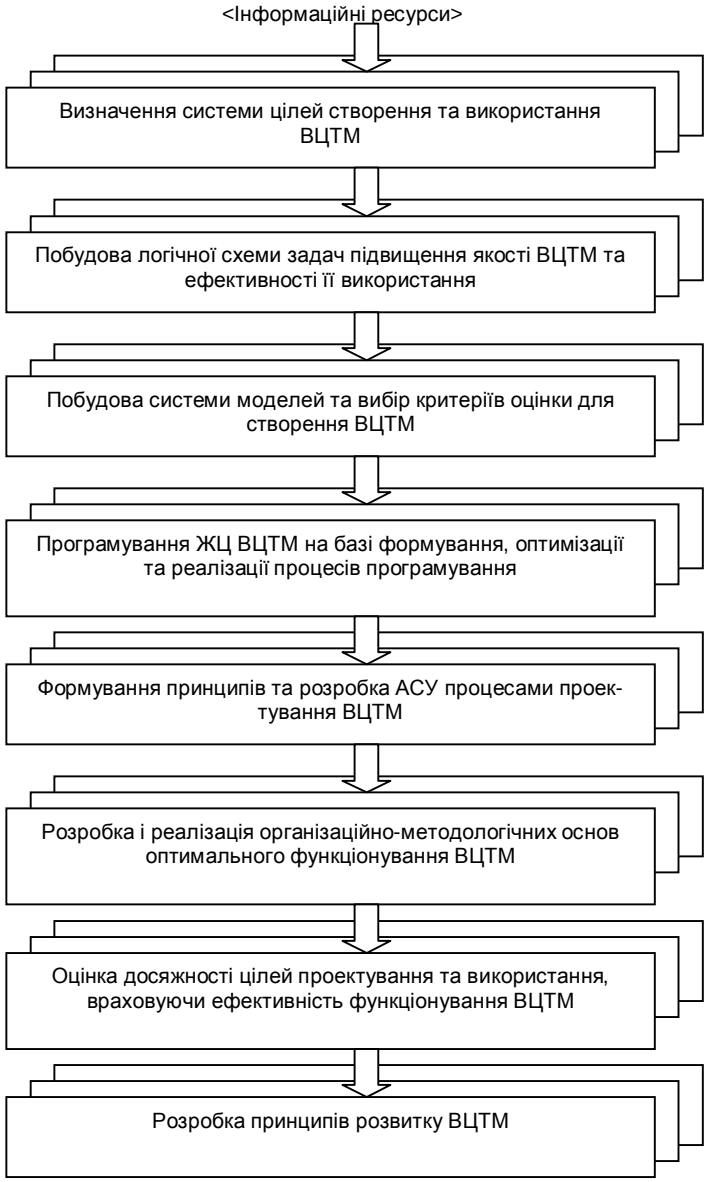


Рис. 1. Блок-схема алгоритму автоматизації процесу проектування ВЦТМ.

При проектуванні ВЦТМ часто здійснюється вибір одного з декількох можливих варіантів. Критерієм для такого вибору служить, у першу чергу, значення показника ефективності ВЦТМ як об’єкту проектування, причому перевагу з еквівалентних показників ефективності одержує менш складний із них.

Тоді, як окремий випадок, можна розглянути спрощення:

$$S = \sum_{i=1}^{n} S_i \cdot K_i \left(1 + v \cdot \alpha\right),$$

де S_i – складності окремих елементів (i=1,2,...n);

K_i – число елементів і-го типу, що входять у систему;

v – коефіцієнт, що враховує складність зв'язків у порівнянні зі складністю елементів системи;

$\alpha = \dfrac{M^*}{N \cdot (N-1)}$ - відносне число реалізованих зв'язків;

M^* – фактичне число зв'язків, реалізованих у системі;

$N \cdot (N-1)$ – максимальне число зв'язків між елементами;

$N = \sum_{i=1}^{n} K_i$ - число елементів системи.

Таким чином, даний показник складності може використовуватися при оцінці ВЦТМ як складних систем керування. Системний підхід, що є методологією рішення складних проблем, реалізується в три великих етапи:

- Систематизація (цілей, задач, моделей, методів і т.д.) на базі проведення класифікації та упорядкування (декомпозиції);
- Використання формалізованого поняття «система» (<вхід>- <перетворення> - <вихід>) і проведення математичних і комп'ютерних експериментів;
- Застосування методології цілеорієнтування системи (<цілі>↔<засоби>), що деталізується в більш конкретну структуру:

(<цілі> ↔ <задачі, моделі> ↔ <методи, алгоритми> ↔ <завдання, технічні засоби>) [4].

Для опису системи повинні бути точно визначені категорії і поняття, що дозволяють уявити її формальними засобами. З одного боку, система являє собою відособлену частину середовища, що може бути розглянута як окремий об'єкт, що виконує визначені функції. З іншого боку, система є сукупністю елементів і зв'язків між ними. При створенні системи необхідно використовувати поняття "цілеорієнтованість", що розуміє проходження визначеної цілі протягом усього процесу створення або дослідження.

Висновки

Як конструктивний підхід до розв'язання вище сформульованої проблеми підвищення ефективності і якості системного проектування ВЦТМ запропоновано системні принципи її декомпозиції на логічну сукупність цілей і задач, що забезпечують вирішуваність останніх в класі сучасних ефективних методів моделювання і оптимізації.

Наведено основні підходи до побудови і дослідження моделей процесів і об'єктів автоматизації, що складають математичну основу визначення шляхів підвищення ефективності створення сучасних телекомунікаційних мереж.

Побудована і описана таким чином системна модель вже створених систем дозволяє досліджувати процеси досягнення цілей (функціонування) і отримувати значення показників ефективності на основі вивчення характеру процесів.

Для відображення питань якості проектованого виробу можна сформувати системну модель, нижнім рівнем якої є організаційна структура діяльності. Наступний рівень - алгоритмічний - відображає процеси формування показників якості по всій сукупності властивостей, що вивчаються. Рівень задач визначає загальну структуру технологічного процесу в категоріях якості.

Логічні змінні характеризують досягнення заданих рівнів якості. Варіант технології створення виробу представляє собою деякий шлях на впорядкованій множині станів процесу проектування. Цільовий рівень представляє собою модель, що інтерпретує множину варіантів технологій.

Оптимальне рішення полягає у відшуканні оптимального маршруту на множині технологічних варіантів.

Література

1. Жук К.Д., Тимченко А.А., Доленко Т.И. Исследование структур и моделирование логико-динамических систем.-К.: Наукова думка, 1975.- 199 с;
2. Кестенбаум Р. Что такое системный поход? // Электроника, 1969, т.42.№9.-С.2-11;

3. Жук К.Д., Тимченко А.А., Родионов А.А. и др. Построение современных систем автоматизированного проектирования.- К.: Наукова думка, 1983. -420 с;
4. Тимченко А.А. Основи системного проектування та системного аналізу складних об'єктів: Підручник: Книга 1. Основи САПР та системного проектування складних об'єктів/ За ред. В. І. Бикова. – К.: Либідь, 2000. - 272 с;
5. Тимченко А.А. Основи системного проектування та системного аналізу складних об'єктів: Основи системного підходу та системного аналізу об'єктів нової техніки: Навч. Посібник/ За ред. Ю.Г.Леги.- К.: Либідь, 2004.- 288 с.

УДК 621.317.799.297+681.849

Рыбальский О.В., Тимко Е.В.

К РАЗРАБОТКЕ НОВЫХ МЕТОДОВ И СРЕДСТВ ЭКСПЕРТНЫХ ИССЛЕДОВАНИЙ АУТЕНТИЧНОСТИ МАТЕРИАЛОВ ВИДЕОЗАПИСИ

В статье рассматриваются постановочные вопросы создания методов и средств экспертизы аутентичности материалов видеозаписи, адекватных уровню угроз нарушения целостности и модификации содержащейся в них информации.

В современной правоохранительной деятельности в качестве доказательной базы широко используются материалы видеозаписи. Они применяются при расследовании большинства дел, связанных со взятками, коррупцией, вымогательством и т.д.

Для процессуального введения таких материалов в рассматриваемое дело они должны пройти экспертизу, подтверждающую (или отрицающую) их аутентичность.

В настоящее время основными методами проверки аутентичности видеозаписей (далее – сигналограмм) являются органолептический (просмотр видеозаписи экспертом и оценка синхронности изображения и звука, отсутствия прерываний и т.п.) и магнитооптический (проверяется непрерывность импульсов управления, записанных по отдельной дорожке). Основными средствами такой проверки являются видеомагнитофон и магнитооптический визуализатор [1].

Появление мощных персональных компьютеров и доступных эффективных программных продуктов для обработки изображения привели к повышению уровня угрозы невыявления нарушений целостности информации, содержащейся в проверяемых сигналограммах. Это поясняется неадекватностью разрешающей способности методов и средств выявления следов обработки сигналограмм, применяемых экспертизой, разрешающей способности способов и средств, используемых атакующей стороной.

Авторов такое состояние развития экспертной техники проверки аутентичности видеозаписей не устраивает, поскольку несложно догадаться, что его сохранение приведет к потере доверия к результатам экспертизы. Это, в свою очередь, вызовет неизбежный отказ от признания материалов видеозаписи в качестве доказательств, что уже никак не может устроить и правоохранительные органы.

Поэтому разработка новых методов и средств проверки аутентичности материалов видеозаписи, применяемых для проведения экспертизы, является актуальной задачей.

Но, приступая к ее решению, следует, по нашему мнению, четко сформулировать саму задачу и представлять пути и методы ее реализации. Именно это и является целью данной статьи.

Саму задачу, по нашему мнению, следует сформулировать так: разработать современные методы и средства проведения экспертизы аутентичности материалов видеозаписи, отвечающие уровню угроз нарушения целостности или модификации содержащейся в них информации.

Для ее решения в первую очередь следует провести исследования процессов, происходящих при записи, воспроизведении и обработке информации, содержащейся в материалах видеозаписи.

Следовательно, объектом исследования будут процессы, происходящие при записи, воспроизведении и обработке информации, содержащейся в материалах видеозаписи.

Предметом таких исследований будет проявление в материалах видеозаписи следов внешних вмешательств в информацию, содержащуюся в этих материалах.

Результат исследований позволит выявить возможные пути создания необходимых методов и средств экспертизы и разработать эти методы и средства.

Мы полагаем, что для этого необходимо рассмотреть конструктивные особенности аппаратуры видеозаписи в ее различных модификациях, и выявить те из них, которые фиксируются в сигналограммах в виде индивидуальных признаков, характеризующих каждый конкретный аппарат.

Эти признаки должны быть, во-первых, устойчивыми и повторяемыми для данного конкретного аппарата и, во-вторых, изменяться в процессе обработки информации, содержащейся в сигналограмме.

При этом обязательно следует рассмотреть структуру и особенности сигналов, записываемых на видеоаппаратуре. Это позволить, во-первых, определить наиболее перспективные информационные признаки проявления следов внешних вмешательств в информацию, передаваемую в такой аппаратуре. И, во-вторых, определить те из них, выявление которых обеспечивается реализуемой на современном этапе развития техники разрешающей способностью аппаратуры контроля.

При этом следует учесть, что в настоящее время широко используется как аналоговая, так и цифровая аппаратура видеозаписи.

Разумеется, что после этого следует разработать необходимые методы и средства проведения экспертизы и провести экспериментальную проверку их эффективности.

Таким образом, решение задачи разработки методов и средств проверки аутентичности материалов видеозаписи требует серьезных теоретических и экспериментальных исследований.

Литература

1. Рыбальский О.В., Жариков Ю.Ф. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе. – К.: НАВСУ, 2003. – 300 с.

УДК 681

Журавель В.В., Рибальський О.В.

ПІДГОТОВКА, ЗБЕРІГАННЯ ТА ПОРЯДОК НАДАННЯ МАТЕРІАЛІВ ТА ЗАСОБІВ ВІДЕОЗВУКОЗАПИСУ НА ЕКСПЕРТИЗУ

Розглянуто вимоги, які висуваються до підготовки проведення експертизи відеозвукозапису, в тому числі вимоги до їх зберігання та транспортування.

Матеріали відеозвукозапису складають суттєву частину доказової бази при розслідуванні та розгляді у суді справ, пов’язаних з корупцією, хабарництвом, здирництвом, рекетом, викраданнями людей тощо.

Експертизу матеріалів відеозвукозапису історично називають фоноскопічною (інколи судово-акустичною). Вона є комплексною, оскільки при її проведенні залучаються фахівці з різних галузей технічних та гуманітарних знань [1].

З цієї позиції й витікає класифікація судового експерта-фоноскопіста, адже право проведення судових експертиз присвоюється з чотирьох спеціальностей, а саме:

- спеціальність 7.1 – дослідження матеріалів та засобів відеозвукозапису;
- спеціальність 7.2 – дослідження диктора за параметрами усного мовлення;
- спеціальність 7.3 – дослідження акустичних сигналів та середовищ;
- спеціальність 7.4 – лінгвістичні дослідження диктора.

І якщо спеціальності 7.1 – 7.3 вимагають від експертів наявності вищої технічної (електроакустика, звукотехніка, радіотехніка, електроніка, програмування, математика,

тощо) освіти, то спеціальність 7.4 вимагає від експерта наявності вищої гуманітарної (філологічної та лінгвістичної) освіти.

З переліку спеціальностей також витікає, які види досліджень проводить фоноскопічна експертиза.

Ці види поділяються на дослідження мовлення людини та дослідження самих сигналограм та апаратури, на якій вони були записані.

Крім того кожен з цих видів поділяється на два великих класи: ідентифікаційні та діагностичні дослідження [2]. Ці обидва класи наявні як у дослідженнях мовлення, так і у дослідженнях сигналограм та апаратури.

Так, наприклад, зрозуміло, що ідентифікація людини за параметрами її мовлення та за лінгвістичними ознаками є ідентифікаційними дослідженнями. Але при дослідженні мовлення людини можна проводити і діагностичні дослідження, наприклад: дослідження емоційного стану людини, а лінгвістичні дослідження дозволяють, з'ясування рівня її інтелектуального розвитку, рівня освіти, діалектичних особливостей, тощо.

Або якщо, наприклад, необхідно ідентифікувати апарат запису інформації, на якому зроблено сигналограму, то це є ідентифікаційне дослідження, а виявлення ознак монтажу у сигналограмі – діагностичне. Але діагностичні дослідження щодо виявлення ознак монтажу можуть проводитися шляхом ідентифікаційних, тобто через ототожнення апаратури запису. При цьому об'єктом, що ідентифікується, є апарат запису, а об'єктом, що ідентифікує є зразкова (експериментальна) сигналограма, записана на наданому на експертизу апараті, та спірна (досліджувана) сигналограма, що надана на експертизу [3]. Ідентифікуючими ознаками при цьому є ті параметри апаратури запису, які відображаються на записаній сигналограмі та є індивідуальними для даного апарату запису. При цьому обов'язково перевіряється й оригінальність спірної сигналограми. Отже такі дослідження проводяться шляхом порівняння певних ідентифікаційних ознак, виділених зі спірної та експериментальної сигналограм. Саме цим пояснюється вимога, що для проведення експертизи необхідно надавати на дослідження апаратуру, на якій була записана спірна фонограма.

На експертизу можуть надаватися будь-які сигналограми, отримані законним шляхом. Це можуть бути матеріали відеозвукозапису, отримані при проведенні оперативно-розшукових заходів, або вилучені у встановленому законом порядку у потерпілих, свідків чи звинувачуваних при проведенні слідчих дій.

До поняття "сигналограма" входять фонограми (тобто, сигналограми з записом розмов), та сигналограми, що містять запис розмов та зображень, тобто сигналограми з відеозвукозаписом. Також це можуть бути записи інших сигналів, наприклад, телеметричні сигнали, що характеризують стан окремих систем літака, корабля, тощо.

Сигналограми можуть бути аналоговими та цифровими, тобто такими, що записані або на аналоговій, або на цифровій апаратурі запису.

Вченими та фахівцями МВС України розроблені методи, обладнання та методики проведення експертиз автентичності як аналогових, так і цифрових сигналограм [4, 5].

Як правило, на експертизу потрібно надавати оригінали сигналограм, але в окремих випадках експертизу цифрових сигналограм можна провести по копіях сигналограм за спеціальними методиками, розробленими у МВС України. Але в цьому разі слід пам'ятати, що проведення експертизи за копіями вимагає надання експерту можливості запису експериментальної сигналограми на тій апаратурі, на який робився запис оригіналу, та її копіювання з витримкою всіх технологічних параметрів перезапису на тій самій апаратурі, на якій робилася копія спірної сигналограми. Крім того, надання копії сигналограми значно підвищує обсяг робіт з перевірки її автентичності, отже вимагає більшого часу проведення експертизи та підвищує її вартість.

В залежності від типу апаратури та технології, що використовується для запису (аналогова чи цифрова), до сигналограм висуваються певні вимоги, виконання яких з боку оперативних працівників та осіб, які проводять досудове слідство, направлене на максимально швидке та якісне експертне дослідження матеріалів відеозвукозапису.

Так, у випадку аналогового запису на експертизу потрібно надавати лише оригінали сигналограм. Ця вимога пояснюється в першу чергу значним погіршенням точності передавання сигналів при перезапису аналогових сигналограм, тобто втратою якості.

Не можна копіювати на аналогову апаратуру цифрові записи, та видавати їх за оригінальні аналогові сигналограми, оскільки при перевірці автентичності (тобто оригінальності та відсутності ознак монтажу) такої сигналограми в ній будуть виявлені сліди цифрової обробки, що одразу призведе до висновків експертизи щодо надання на експертизу копії та наявності у наданій сигналограмі ознак цифрового монтажу [6].

Для забезпечення необхідної якості запису необхідно користуватися виносними мікрофонами.

Під час проведення оперативного запису необхідно зробити відмітку у відповідному журналі, де вказати номер апарату та номер виносного мікрофону, за допомогою яких робився запис. Ця вимога пов'язана з тим, що в подальшому експертові необхідно здійснити запис експериментальної сигналограми.

Аналогова апаратура магнітного запису, на якій записана спірна сигналограма, повинна забезпечувати верхнє значення діапазону частот, що записуються, не нижче 3,4 кГц. Тому не слід користуватися під час запису малою швидкістю транспортування магнітної стрічки. Тобто, якщо апарат має дві швидкості протягування магнітної стрічки, то слід використовувати більшу. Це стосується у першу чергу малогабаритних аналогових диктофонів. Використання швидкості 1,2 см/сек робить, за правило, запис непридатним для ідентифікації голосу людини за фізичними ознаками її мовлення.

Певні вимоги висуваються і до записів, які здійснюються за допомогою цифрової апаратури. Цифрові фонограми не слід записувати при частоті дискретизації 8 (або нижче) кГц, оскільки при такій частоті дискретизації неможливо забезпечити верхнє значення частот, що записуються, вище 3,4 кГц, а це, у свою чергу, унеможливлює ідентифікацію особи за фізичними параметрами сигналів її усного мовлення [7].

Не слід користуватися апаратурою, яка проводить запис на змінний носій, оскільки застосування такої апаратури викличе ускладнення умов проведення експертизи, що, у свою чергу, призведе до подовження термінів її проведення та підвищить вартість виконання експертизи.

Цифрова апаратура, на якій робиться запис, повинна мати аналоговий вихід звукових сигналів. Якщо використовується малогабаритні цифрові диктофони, що не мають такого виходу (наприклад, "MINI EDIC"), і запис для прослуховування має вводитися у комп'ютер, необхідно надати експерту змогу зробити експериментальну фонограму на цьому апараті з розкриттям запису у тому ж комп'ютері. Зрозуміло, що комп'ютер із записом не може надаватися в суд, як доказ. Отже цей запис необхідно скопіювати на оптичний диск. Тому краще одразу переписувати оригінальний запис у комп'ютер, який пристосований для запису оптичних дисків.

З цього випливає вимога щодо обов'язкового фіксування у відповідному журналі номерів та типів всього технологічного ланцюга апаратури (включаючи комплекти передавальної та приймальної апаратури), умов та параметрів проведення запису та перезапису, що забезпечить експерту можливість правильно записати експериментальну сигналограму, а це, у свою чергу, надасть змогу підтвердити автентичність наданої сигналограми [8].

При застосуванні спеціальної техніки з вбудованими функціями фіксації дати та часу запису слід користуватися цими функціями.

Значну роль для збереження сигналограми в первинному стані відіграють умови правильного зберігання, упакування та транспортування носіїв запису. Вимоги до умов зберігання та транспортування матеріалів відеозвукозапису обумовлюються в першу чергу типом запису, а саме: аналоговим чи цифровим.

Зберігання і транспортування досліджуваних фонограм і експериментальних зразків усного мовлення, записаних на магнітну стрічку, вимагає певних умов. Магнітна стрічка (на касеті чи котушці) повинна бути упакована у стандартний пластмасовий чи паперовий футляр. Бажано футляр розмістити у металевій коробці з магнітом'якого матеріалу

(тобто, заліза, сталі, пермалою, але не з алюмінію або інших кольорових металів) для запобігання випадкового впливу магнітного чи електричного полів на магнітну стрічку та ушкодження зафіксованих на ній записів. Зберігати магнітну стрічку необхідно при температурі 10–25^0 С і відносній вологості 45–75%. Не можна зберігати магнітну стрічку біля нагрівальних приладів, джерел сильних магнітних (електричних) полів (трансформатори, джерела безперебійного живлення комп'ютерів, тощо) чи під безпосередньою дією прямих сонячних променів [9].

На відміну від магнітного запису, носії оптичного запису не піддаються впливу електромагнітного (електричного) поля, тому основними факторами, які впливають на збереження таких матеріалів, є відсутність механічних ушкоджень та впливу прямих сонячних променів.

Перед упакуванням матеріалів відеозвукозапису рекомендується виконати певні умови збереження фонограм чи сигналограм від стирання шляхом необачного чи навмисного стирання. Так, для магнітного запису на носіях (мікро-, компакт- чи відеокасета) доречно видаляти захисні упори карманів захисту запису, що виключає можливість ненавмисного стирання інформації. Для цифрового запису на дискету використовуються перемикачі захисту запису (для 3,5" дискет), а для запису на оптичні диски (CD та DVD) слід надавати перевагу використанню носіїв із можливістю однократного запису (носії типу CD-R та DVD-R).

Матеріали чи засоби відеозвукозапису, які мають надходити на дослідження, повинні бути належним чином упаковані та опечатані. Носії запису зі спірними сигналограмами повинні бути опечатані печаткою відповідного підрозділу та скріплені підписами посадової особи та понятих. Для матеріалів із записами досліджуваних зразків – досить опечатування та підпису посадової особи.

Зберігати матеріали та засоби відеозвукозапису необхідно в приміщеннях, сейфах, тощо, які мають необхідну сигналізацію, надійно опечатуються, обмежують доступ сторонніх осіб та відповідають умовам зберігання носіїв, що зазначені вище.

Транспортувати матеріали відеозвукозапису необхідно в жорсткій упаковці. При цьому найкращий спосіб надання матеріалів в розпорядження експертів – це доставка нарочним. Адже доставка звичайною поштою не виключає шкідливих впливів та можливих механічних пошкоджень.

Одним з головних чинників швидкого та якісного експертного дослідження матеріалів відеозвукозапису є виконання з боку особи, яка проводить досудове слідство чи дізнання, конкретних вимог щодо відбору матеріалу, по якому належить провести експертизу, правильної його підготовки, тощо.

При проведенні оперативно-технічних заходів в переважній більшості записується велика кількість інформації, що не має ніякого доказового значення. Як свідчить практика проведення досліджень під час документування оперативно-технічними підрозділами фактів злочинних дій чи правопорушень, інформація, яка дійсно є суттєвою для розслідування, становить 25-30%. Тому, після отримання матеріалів відеозвукозапису слідчому потрібно визначити, які саме записані епізоди становлять інтерес для слідства. При цьому необхідно скласти протокол прослуховування записів, який мають підписати особи, що були присутні при прослуховуванні.

Для дослідження фонограми, на якій зафіксована мовленнєва інформація, чітко визначаються об'єкти дослідження: слідчому (або особі, яка провадить дізнання) необхідно прослухати фонограму з метою встановлення місця розташування розмови на магнітному (сторона касети, початок і кінець розмови у хвилинах та секундах відносно початку магнітної стрічки, зазначивши початкові та кінцеві слова розмови) чи оптичному носії (назва файлу із записом розмови; початок та кінець у хвилинах та секундах, початкові та кінцеві слова у випадку виділення фрагменту розмови). При цьому бажано залучити спеціаліста із звукозапису з метою уникнення некваліфікованого поводження з фонограмою – порушення її цілісності.

У постанові на проведення експертизи необхідно зазначити, які саме місця на кожному з носіїв, на яких записані спірні сигналограми, підлягають експертизі. Для цього

можна скористатися або відмітками дати і часу запису (якщо вони є на сигналограмах), або наводити межі початку та кінця сигналограм, тобто позначати, наприклад, таким чином: який дослівний зміст розмов, що записні на касеті № 3, сторона А, починаючи зі слів "…" та закінчуючи словами "…".

Для зменшення часу проведення експертизи експертам слід обов'язково надавати протокол прослуховування. При цьому слід пам'ятати, що протокол прослуховування не є експертним висновком, і що експерт, прослухавши розмови, може надати зовсім інший текст (бо він спеціаліст, що має відповідні спеціальні знання та фахову підготовку).

При складанні постанови на експертизу не варто ставити перед експертами зайвих завдань, які не мають відношення до сутності справи. Запитання до експертів повинні бути конкретними та відповідати завданням слідства.

Нижче надається орієнтовний перелік питань, які слід ставити перед експертами при проведенні експертиз в справах, де необхідно ідентифікувати особу за параметрами її голосу та мовлення, та перевірити автентичність записів.

При цьому ідентифікувати потерпілих або свідків, що брали участь у розмові, якщо вони не заперечують факт та зміст розмови, і якщо цього не вимагає тактика побудови звинувачення, немає сенсу.

Орієнтовний перелік тих питань, які є основними (що підтверджується практикою досліджень), для проведення експертиз матеріалів відеозвукозапису:

1. Чи є у наданій(их) сигналограмі(ах) голос громадянина (вказати прізвище, ім'я по батькові)? Якщо є, то які фрази, що записані на сигналограмі(ах), записаної на касеті № … (чи іншому носії), на стороні …, що починається словами "…" та закінчується словами "…", належать громадянину (громадянці)…?

2. Який дослівний зміст розмови, записаної на касеті № … (чи іншому носії), на стороні …, що починається словами "…" та закінчується словами "…"?

3. Оригіналом чи копією є надана на експертизу сигналограма?

Питання виноситься в разі запису сигналограми на аналоговій апаратурі відеозвукозапису.

4. Чи є у сигналограмі, що записана на касеті № … (чи іншому носії), на стороні …, що починається словами "…" та закінчується словами "…", сліди механічного, електроакустичного або цифрового (електронного) монтажу?

Питання ставиться в разі запису сигналограми на аналоговій апаратурі відеозвукозапису.

5. Чи одночасно у наданій сигналограмі проводився запис звукового супроводження та зображення?

Питання ставиться в разі надання на експертизу сигналограми з відеозвукозаписом.

6. Чи є автентичною цифрова сигналограма № …, що записана на диску "…" цифрового диктофону марки "…", зав. №…?

Питання ставиться в разі запису сигналограми на цифровому диктофоні за умови надання на експертизу оригіналу сигналограми.

7. Чи містяться на сигналограмі, яка записана у файлі "…" та надана на оптичному диску марки "…", ознаки цифрового, чи якогось іншого монтажу?

Питання ставиться в разі запису сигналограми на цифровій апаратурі та надання на експертизу копії сигналограми.

Якісно записана спірна фонограма є лише частиною успішного експертного підтвердження наявності на ній голосів та мовлення конкретних осіб. Для ідентифікації особи за її голосом на експертизу необхідно надати зразки голосу та мовлення людини, голос якої необхідно ідентифікувати. Зразок повинен являти собою запис вільного спонтанного мовлення людини. Тривалість зразкової розмови особи, яку треба ідентифікувати, повинна становити не менш, ніж 5 хв. Читання тексту чи заздалегідь підготовлений текст не підходить для ідентифікації особи за її голосом і мовленням.

При проведенні ідентифікаційних досліджень традиційними спектральними методами не має значення, яка апаратура використовувалася для запису зразка голосу й мовлення особи. Для експерта важливо, щоб запис відповідав вимогам якості, які були надані

вище. У випадку використання під час ідентифікаційних досліджень особи за голосом і мовленням методики "ДИАЛЕКТ" (Російська Федерація), відповідність тракту запису спірної сигналограми та експериментальних зразків відіграє значну роль [10], так само як і для ідентифікації лінгвістичними методами.

Можна використати як зразок голосу та мовлення, відеозвукозапис певних слідчих дій, наприклад, запис слідчого експерименту та т. інше, тобто записи, де особа того, хто розмовляє, встановлена документально.

Як свідчить практика проведення ідентифікаційних досліджень, оптимальним для запису зразку голосу та мовлення є слідча дія у вигляді допиту [11]. При цьому особа, яка її проводить, повинна заздалегідь продумати тактику її проведення та перелік питань з метою отримання від особи, яку допитують, максимально розгорнутих відповідей. Можливе використання для процедури відібрання зразків проведення очної ставки, але із дотриманням чергування реплік учасників дії (учасник–слідчий–учасник).

Не слід відбирати зразки голосу у приміщеннях, де існує лункість (явище реверберації), наприклад, у великих напівпустих кімнатах з бетонними стінами.

Інколи є сенс залучення експерта для відбирання зразків голосу та мовлення.

Як підсумок всіх розглянутих вище вимог щодо підготовки, запису, зберігання та транспортування матеріалів відеозвукозапису наводиться перелік матеріалів, які в загальному випадку обов'язково надаються на експертизу:

1. Супровідний лист (із зазначення номера кримінальної справи та переліком матеріалів, що надаються на експертизу).
2. Постанова слідчого (уповноваженої особи) на проведення експертизи.
3. Носії запису з оригіналами спірних сигналограм.
4. Протокол прослуховування сигналограм.
5. Записи зразків голосів та мовлення.
6. Апаратуру запису, на якій проводився запис спірних сигналограм.
7. Увесь комплект апаратури, яка використовувалася для запису спірних сигналограм.

Зрозуміло, що апаратура запису та негласного зняття інформації, яка використовується оперативними підрозділами МВС України (чи інших відомств) є, по-перше, таємною, та, по-друге, не може довго затримуватися для проведення експертних досліджень. Але ж експерту для проведення експертизи необхідно зняти зразковий запис. Тому є прямий сенс в разі застосування апаратури, що має відповідний гриф, залучати до експертизи експертів, які мають відповідний допуск.

Крім того, ця апаратура може бути надана експерту у присутності оперативного працівника, що несе за цю апаратуру відповідальність, для запису зразкової сигналограми, та введення зразкової та спірних сигналограм у комп'ютер для подальшої експертизи, оскільки такі операції не вимагають багато часу.

А ось в разі вилучення апаратури слідчим у потерпілого, свідка чи підозрюваного, експертні дослідження та запис зразків вимагають набагато більше часу (необхідно з'ясувати та відтворити всі обставини запису спірної сигналограми, бо в разі порушення цих умов експерт може схибить у своєму висновку). Тому в цьому випадку необхідно надавати максимально повний комплект апаратури на весь час проведення експертизи.

Висновки

Дотримання вимог експертизи щодо порядку підготовки матеріалів відеозвукозапису до її проведення є однією з необхідних умов отримання позитивних відповідей на питання, поставлені перед експертами, та дозволяє суттєво підвищити достовірність експертиз й зменшити терміни та вартість їх проведення.

Література

1. Вертузаев М.С., Жариков Ю.Ф. Судебная акустика: теоретические основы и экспертная практика: Научно-практическое пособие. – К.: РИО МВД Украины, 1992. – 112 с;

2. Салтевський М.В. Криміналістика (у сучасному викладі): Підручник. – Кондор, 2005. – 588 с., 32 іл;
3. Рамишвили Г.С., Чикоидзе Г.Б. Криминалистическое исследование фонограмм речи и идентификация личности говорящего. – Тбилиси, 1991;
4. За заг. ред. Лєвого С.В. Криміналістичні дослідження матеріалів і засобів звуко- та відеозапису. Методичні рекомендації. – К.: РИО МВД Украины, 1998. – 439 с;
5. Рибальський О.В., Жаріков Ю.Ф., Орлов Ю.Ю. Спосіб перевірки оригінальності та автентичності магнітних фонограм. Патент України на винахід № 27206 кл. МКВ G 11 b 27/00, 27/36;
6. Рибальський О.В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі: Монографія. – К.: НАВСУ, 2004. – 168 с., іл;
7. Рекомендации по эффективному использованию возможностей АРМЭФ SIS при выполнении криминалистических фоноэкспертиз. - ЦРТ. г. Санкт-Петербург, 1995 (документация к программно-аппаратному комплексу SIS);
8. Рыбальский О.В., Жариков Ю.Ф. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе. Монография. – К.: НАВДУ, 2003. – 302 с;
9. Магера В. Н. Подготовка материалов и вещественных доказательств для криминалистического исследования сигналограмм: Метод. рекомендации. – К.: РИО МВД Украины, 1997. – 48 с;
10. Ред. Фесенко А.В., Попов Н.Ф., Линьков А.Н., Кураченкова Н.В., Байчаров Н.В. Идентификация лиц по фонограммам русской речи на автоматизированной системе “Диалект”. В/ч 34435, 1996. – 102 с;
11. Магера В.Н. Применение звукозаписи и видеозаписи в следственных действиях. К.: РИО МВД Украины, 1987.

УДК 621.317.799 297 + 681.849

Журавель В.В., Рыбальский О.В., Струк И.А., Тимко Е.В.

К ЭКСПЕРИМЕНТАЛЬНЫМ ИССЛЕДОВАНИЯМ ВЗАИМОСВЯЗИ МЕЖДУ ОПЕРАЦИЯМИ, ИСПОЛЬЗУЕМЫМИ ПРИ ЦИФРОВОЙ ОБРАБОТКЕ СИГНАЛОГРАММ, И ПРОЯВЛЕНИЯМИ ИХ ИНФОРМАТИВНЫХ ПРИЗНАКОВ

В статье рассмотрена идеология организации и построения экспериментальных исследований взаимосвязи операций цифровой обработки и их проявлениям при экспертизе аутентичности сигналограмм.

Введение

Для внедрения методов и средств экспертной проверки цифровых сигналограмм, разработанных в Киевском национальном университете внутренних дел (КНУВД), в широкую экспертную практику необходимо создать методику их применения, доступную уровню квалификации среднего эксперта.

Это позволит, учитывая простоту метода и используемого оборудования, создать сеть лабораторий фоноскопии в ряде экспертных подразделений МВД Украины, что, в свою очередь, значительно разгрузит центральные экспертные подразделения, как МВД, так и Минюста, и значительно сократит время ожидания проведения таких экспертиз следственными органами.

Для этого решением секции фоноскопических экспертных исследований Министерства Юстиции Украины программа "Академия", разработанная в КНУВД, передана на апробацию в основные экспертные подразделения страны, проводящие такие экспертизы. В процессе апробации необходимо провести ряд экспериментальных исследований, цель которых – выявление информативных групповых и индивидуальных признаков проявления следов цифровой обработки сигналограмм и усовершенствование на этой основе методики проверки их аутентичности.

Организационно проведение исследований обеспечивается взаимосогласованными планом и методикой их проведения, где расписаны сроки, исполнители, методы и схемы проведения каждого конкретного эксперимента. В работе участвуют Киевский и Львовс-

кий научно-исследовательские институты судебной экспертизы, Государственный научно-исследовательский экспертно-криминалистический центр МВД Украины и КНУВД.

Основной подход к таким исследованиям состоит в проведении серии сравнительных экспериментов на обработанных синусоидальных сигналах и стационарных фрагментах с одной превалирующей частотой, выделяемых из речевой информации. Авторы полагают, что, во-первых, таким образом можно определить, имеются ли групповые идентификационные признаки информативных проявлений следов внешних вмешательств для каждого из конкретных видов цифровой обработки (ЦО), из числа используемых при подделке сигналограмм, и, во-вторых, есть ли различия в таких проявлениях для различных видов цифровой аппаратуры записи аналоговых сигналов (ЦАЗАС). Если предположения авторов подтвердятся, то открывается возможность для классификации таких признаков, что существенно упростит процесс подготовки экспертов и позволит решить задачу расширения сети фоноскопических лабораторий в экспертных подразделениях МВД Украины.

Основная часть

Исходя из основ теории выявления следов ЦО сигналограмм, разработанной одним из авторов [1,2], вниманию коллег предлагается подход к организации и проведения экспериментов. Ее рассмотрение и является целью настоящей работы.

Теоретически установлено и экспериментально проверено, что, во-первых, для проведения цифровой (как, впрочем, и любой другой), обработки сигналограммы необходимо использовать не менее двух различных цифровых устройств (например, ЦАЗАС и ПЭВМ) [1,2]. Во-вторых, имеются следующие источники возникновения следов ЦО сигналограмм:

– несовпадение размещения на статической характеристике квантователей уровня аналого-цифровых и цифро-аналоговых преобразователей (АЦП и ЦАП соответственно) разных устройств, участвующих в процессе обработки, уровней квантования с технологическими дефектами;

– расхождение истинных значений частот тактовых генераторов устройств, участвующих в процессе обработки;

– использование операции стробирования для вырезания фрагментов фонограммы при монтаже методом компиляции нового целого из вырезанных фрагментов ("сшивки") в ПЭВМ;

– возникновение информационных потерь при преобразовании форматов представления информации, используемых при обработке сигналов в ПЭВМ и их записи на ЦАЗАС [1,2].

Поэтому, исходя из поставленных задач, планируется провести эксперименты так, чтобы охватить все известные экспертам возможные способы ЦО сигналограмм (аналитически промоделированные ранее [3–6]), классифицируемые как несанкционированные внешние вмешательства в информацию, содержащуюся в сигналограммах, т.е. монтаж.

Для обеспечения удобства последующей обработки и обобщения результатов эксперимента (как и при разработке теории) предложен системный подход к процессу монтажа сигналограммы с использованием метода декомпозиции по отдельным операциям, что позволит выявить проявление признаков следов применения конкретных операций, используемых при монтаже. При этом они рассматриваются в различных вариантах применения, а сами варианты охватывают все известные способы монтажа. Среди них есть и те, что синтезированы самими экспертами в процессе разработки теории выявления следов цифровой обработки сигналограмм [5–7].

Доказано, что в соответствии с разработанной теорией, проявление следов ЦО будет представлено в виде появления дополнительных спектральных компонент на эквивалентах спектрограмм, полученных из вейвлет-портретов обработанных сигналов, относительно таких же спектрограмм сигналов, не подвергавшихся обработке [1,2]. Данные проявления исследованы одним из авторов теоретически и экспериментально. Но до настоящего времени не установлено, имеет ли место связь между применением конкретной опе-

рации обработки и появлением этих компонент в определенном частотном диапазоне. Если такое явление существует, то его выявление позволит классифицировать операции, применяемые при монтаже.

Чтобы определиться в этом вопросе, предполагается проводить эксперименты в два этапа:

– на первом этапе провести исследования на синусоидальных сигналах, что позволит установить наличие или отсутствие такой взаимосвязи;

– на втором этапе провести исследования на речевых сигналах, что позволит установить различие в проявлении информативных признаков между синусоидальными и стационарными отрезками квазигармонических сигналов, применяемых в такой экспертизе.

При планировании экспериментов учтено и то, что в случае записи первичных сигналограмм на ЦАЗАС для их последующей обработки и перезаписи полученной в результате ЦО обработанной версии на аналоговую аппаратуру магнитной записи (ААМЗ), проявление признаков следов такой обработки в аналоговой записи могут отличаться от следов, проявляющихся в цифровой сигналограмме. Поэтому эксперименты спланированы отдельно для случаев перезаписи полученной обработанной версии сигналограммы на ЦАЗАС и ААМЗ.

Эксперименты проводятся с применением программы "Академия" [8,9], предназначенной для выявления следов ЦО аналоговых и цифровых сигналограмм. Минимальные требования к звуковой карте, с которой работает программа "Академия":

– частота дискретизации не менее 48 кГц;

– оцифровка на одну выборку не менее 16 разрядов.

Приняты общие требования к порядку проведения экспериментов:

1. Эксперименты проводятся методом сравнения образцовой сигналограммы, не подвергавшейся обработке, и обработанной сигналограммы.

2. На ЦАЗАС записываются все первичные сигналограммы.

3. Эти сигналограммы вводятся (как образцовые) через аналоговый вход/выход в экспертную ПЭВМ (с программой "Академия") и сохраняются под своим именем на жестком (или оптическом) диске. Для ввода сигналограмм применяется программа Cool pro или аналогичная. Ввод и сохранение сигналограмм производится в формате wav.

4. Эти же сигналограммы вводятся в соответствии с требованиями каждого конкретного эксперимента через аналоговый или цифровой вход в другую ПЭВМ для последующей обработки и сохраняются на жестком (или оптическом) диске под своим именем. В случае аналогового ввода применяется программа Cool pro или аналогичная. Ввод и сохранение сигналограмм производится в формате wav.

5. Сигналограмма подвергается ЦО и переписывается из ПЭВМ на аппарат звукозаписи в соответствии с методикой конкретного эксперимента.

6. С выхода этого аппарата воспроизведенная обработанная сигналограмма через аналоговый вход/выход вводится в экспертную ПЭВМ, где сохраняется под своим именем.

7. Сигналограммы в ПЭВМ с программой "Академия" вводятся через аналоговый вход звуковой карты с частотой дискретизации максимально возможной для данной карты (но не ниже 48 кГц). В качестве входных и выходных фильтров нижних частот используются фильтры аппаратуры звукозаписи и ПЭВМ, на которой проводятся эксперименты.

Установлены следующие общие требования к обработке сигналограмм при проведении экспериментов:

1. Экспериментальная обработка сигналограмм и их последующая проверка должны проводиться на разных ПЭВМ.

2. Для записи первичных сигналограмм необходимо использовать ЦАЗАС. При этом для выполнения экспериментов по любому из пунктов плана необходимо использовать не менее чем 5 типов и по 3 разных экземпляра каждого из типов такой аппаратуры.

3. Если ввод сигналограмм в ПЭВМ для обработки производится через аналоговый вход, то он должен производиться в двух вариантах:

– на номинальной частоте дискретизации того аппарата, на котором была записанная первичная сигналограмма;

– на большей номинальной частоте дискретизации относительно частоты дискретизации того аппарата, на котором была записанная первичная сигналограмма.

4. При вводе первичной сигналограммы частота дискретизации должна быть меньше частоты дискретизации, на которой будет вводиться сигналограмма в ПЭВМ с программой "Академия" для последующей проверки.

5. Для перезаписи обработанных сигналограмм необходимо использовать как цифровую, так и аналоговую аппаратуру звукозаписи (в зависимости от вида эксперимента). При этом для выполнения экспериментов по любому из пунктов плана необходимо использовать не менее чем 5 типов и по 3 разных экземпляра каждого из типов такой аппаратуры.

6. Обработка сигналограмм должна производиться на тактовой частоте, равной частоте дискретизации, на которой сигналограмма вводилась в ПЭВМ для обработки.

Документирование результатов эксперимента должно производиться с помощью функции "Создание отчета" программы "Академия". Отчет необходимо составлять для каждого конкретного эксперимента. При этом:

1. В заголовке отчета необходимо указать тип, марку и зав. № аппарата, на котором проводилась запись первичной сигналограммы, его частоту дискретизации и разрядность, при которых была записанная сигналограмма, способ ее ввода в ПЭВМ и частоту дискретизации ввода (если он проводился в аналоговой форме) для обработки, способ обработки, способ и параметры вывода обработанной сигналограммы при перезаписи, тип, марку и зав. № аппарата, на которую переписывалась обработанная сигналограмма, и параметры перезаписи.

2. В отчете также должны помещаться графики участков исследуемых сигналов, длительность сигналов (в количестве выборок), частота дискретизации и графики спектрограмм сигналов, выделенных из образцовой и обработанной сигналограмм, полученных из их вейвлет-портретов. Вейвлет-портреты необходимо снимать при следующих параметрах вейвлет преобразования:

– минимальный масштаб параметра a = 0,1;

– шаг параметра a = 0,015;

– максимальный масштаб параметра a = 15.

Вычисление спектрограмм необходимо проводить при тех же значениях параметра a.

3. В отчете следует предоставлять графики для всего диапазона параметра a (всей зоны исследования) и зон выявленных расхождений (растянутые участки графиков).

Запланировано проведение экспериментов для следующих вариантов обработки цифровых сигналограмм:

1. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, первично записанных и переписанных после обработки на одной аппаратуре, введенных в ПЭВМ для обработки в цифровой форме с раскрытием информации в звуковом редакторе.

2. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, первично записанных на одной аппаратуре, введенных в ПЭВМ для обработки в аналоговой форме с раскрытием информации в звуковом редакторе.

3. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, первично записанных на одной аппаратуре и введенных в ПЭВМ для обработки в цифровой форме без раскрытия информации в звуковом редакторе.

4. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, первично записанных на разной аппаратуре и введенных в ПЭВМ для обработки в цифровой форме с раскрытием информации в звуковом редакторе.

5. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, первично записанных на разной аппаратуре и введенных в ПЭВМ для обработки в аналоговой форме с раскрытием информации в звуковом редакторе.

6. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, первично записанных на разной аппаратуре и введенных в ПЭВМ для обработки в цифровой и в аналоговой форме с раскрытием информации в звуковом редакторе и преобразованием формата представления обработанной информации в формат аппаратуры, на которую произведена перезапись, при перезаписи в цифровой форме.

7. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, записанных на разной аппаратуре и введенных в ПЭВМ для обработки в цифровой форме без раскрытия информации в звуковом редакторе.

8. Исследование особенностей проявления признаков ЦО в случае копирования сигналограмм через ПЭВМ, записанных и скопированных на одной аппаратуре и введенных в ПЭВМ для копирования в цифровой форме с раскрытием информации в звуковом редакторе.

9. Исследование особенностей проявления признаков ЦО в случае копирования сигналограмм через ПЭВМ, записанных и скопированных на одной аппаратуре и введенных в ПЭВМ для копирования в аналоговой форме с раскрытием информации в звуковом редакторе.

10. Исследование особенностей проявления признаков ЦО в случае копирования сигналограмм через ПЭВМ, записанных и скопированных на разной аппаратуре и введенных в ПЭВМ для копирования в цифровой форме с раскрытием информации в звуковом редакторе.

11. Исследование особенностей проявления признаков ЦО в случае копирования сигналограмм через ПЭВМ, записанных и скопированных на разной аппаратуре и введенных в ПЭВМ для копирования в аналоговой форме с раскрытием информации в звуковом редакторе.

12. Исследование особенностей проявления признаков ЦО в случае копирования сигналограмм через ПЭВМ, записанных на одной аппаратуре и введенных в ПЭВМ для копирования в аналоговой форме с перезаписью сигналограммы на другую аппаратуру в цифровой форме с преобразованием формата представления информации в ПЭВМ в формат аппаратуры, на которую она переписывается, без раскрытия информации в ПЭВМ в звуковом редакторе.

Для обработанных версий сигналограмм, переписанных после ЦО на ААМЗ, предполагается провести следующие эксперименты:

1. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, записанных на цифровой аппаратуре и введенных в ПЭВМ для обработки в цифровой форме с раскрытием информации в звуковом редакторе для обработки и перезаписи на аналоговую аппаратуру.

2. Исследование особенностей проявления признаков ЦО с применением стробирования и компиляции фрагментов сигналограмм, записанных на цифровой аппаратуре и введенных в ПЭВМ для обработки в аналоговой форме с раскрытием информации в звуковом редакторе для следующей компиляции и перезаписи на аналоговую аппаратуру.

3. Исследование особенностей проявления признаков ЦО в случае перезаписи сигналограмм, записанных на цифровой аппаратуре непосредственно с цифровой на аналоговую аппаратуру с раскрытием информации в звуковом формате, при условии записи первичных сигналограмм для следующей перезаписи на разной цифровой аппаратуре.

Таким образом, экспериментами охвачены все возможные комбинации операций, используемых для ЦО аналоговых и цифровых сигналограмм.

Выводы

Предложенный подход организации и построения экспериментальных исследований позволяет, по мнению авторов, выявить новые взаимосвязи между видом используемых операций, применяемых при цифровой обработке сигналограмм, и информационными проявлениями следов такой обработки.

Литература

1. Рыбальский О.В. Основные положения теории выявления следов цифровой обработки фонограмм и особенности ее программной и методической реализации. Ч. 1. // Захист інформації. – К. – 2006, № 1. – С. 71–76;
2. Рыбальский О.В. Основные положения теории выявления следов цифровой обработки фонограмм и особенности ее программной и методической реализации. Ч. 2. // Захист інформації. – К. – 2006, № 2. – С. 75–78;
3. Рыбальский О.В., Жариков Ю.Ф. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе. – К.: НАВСУ, 2003. – 300 с;
4. Рибальський О.В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі. – К.: НАВСУ, 2004. – 167 с;
5. Рыбальский О.В. Модели нестандартных способов обработки цифровых фонограмм // Реєстрація, зберігання і обробка даних. – К. – 2003. – Т. 5, № 4. – С. 25–32;
6. Рыбальский О.В., Тимко Е.В., Усков К.Ю. Выявление следов цифровой обработки цифровых фонограмм, проведенной с перекодировкой форматов // Реєстрація, зберігання і обробка даних. – К.. – 2004. – Т. 6, № 1. – С. 99–109;
7. Рыбальский О.В. К экспериментальной проверке достоверности положений теории выявления следов цифровой обработки фонограмм // Реєстрація, зберігання та обробка даних. – К. – 2004. – Т.6, № 3. – С. 85–98;
8. Свідоцтво № 11088 про реєстрацію авторського права на твір. Комп'ютерна програма "Академія". Рибальський О.В., Волкович С.Л. (Україна); Рибальський О.В. № 10986; Заявл. 26.07.2004; Опуб. 17.09.2004;
9. Пат. 73631 України, МКВ G 11 b 27/00, 27/36. Спосіб виявлення слідів цифрової обробки аналогових і цифрових сигналограм: Пат. 73631 України, МКВ G 11 b 27/00, 27/36 Рибальський О.В., Геранін В.О., Жаріков Ю.Ф., Орлов Ю.Ю., Волкович С.Л., Струк І.О. (Україна); НАВСУ. – № 2003076921; Заявл. 22.07.03; Опубл. 15.08.05, Бюл. № 8.

УДК 681.3.07

Кийко А. В.

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

В статье рассмотрен нейросетевой подход к задаче идентификации пользователя по клавиатурному почерку. Перечислены основные параметры, характеризующие индивидуальные особенности ввода текстовой информации. Представлена структура соответствующей нейронной сети и описан алгоритм ее настройки.

Анализ состояния вопроса

Почерк уникален, это знают все. Но немногие догадываются, что в общении с компьютером также проявляется индивидуальность пользователя, т.е. каждый человек по-своему вводит текстовую информацию. Современные исследования показывают, что клавиатурный почерк пользователя обладает некоторой стабильностью. Такие характеристики как скорость ввода слов, использование основной или дополнительной части клавиатуры, относительное время нажатия клавиш различных полей клавиатуры, характер "сдвоенных" и "строенных" нажатий клавиш, излюбленные приемы управления компьютером, позволяют с довольно высокой точностью выделить конкретного человека среди всех работавших на данной машине. Для этого применяются статистические методы обработки исходных данных и формирования выходного вектора, являющегося идентификатором данного пользователя. В качестве исходных данных используются временные интервалы между нажатием клавиш на клавиатуре и время их удержания. При этом временные инте-

рвалы между нажатием клавиш характеризуют темп работы, а время удержания клавиш характеризует стиль работы с клавиатурой − резкий удар или плавное нажатие.

Достоинства подобных систем очевидны. Во-первых, не нужно никакое дополнительное оборудование. Во-вторых, идентификация очень удобна для пользователя: вроде бы он вводит обычный пароль, а на самом деле система точно определяет, имеет ли право сидящий за компьютером на доступ к информации. Главный недостаток использования клавиатурного почерка для идентификации личности − это кратковременное изменение почерка у пользователей под влиянием стрессовых ситуаций, что может привести к отказу в доступе человеку, имеющему на это право.

Традиционно ограничение доступа к информации осуществляется по паролям. При их достаточной длине (20–40 символов) появляется возможность наблюдать при вводе пароля характерный для пользователя клавиатурный почерк. При вводе парольной фразы биометрическая система фиксирует время нажатия t_1, t_2, t_3, ..., t_N каждой клавиши и интервал времени τ_1, τ_2, τ_3, ..., τ_{N-1} между отпусканием предыдущей клавиши и нажатием очередной клавиши. Времена нажатий клавиш различны, поэтому значения этих параметров могут быть использованы для выявления характерных особенностей индивидуального клавиатурного почерка пользователя. Контролируемые параметры $t_к$ и $\tau_к$ существенно зависят от того, сколько пальцев использует при наборе пользователь, от характерных для пользователя сочетаний движений различных пальцев руки и от характерных движений рук при наборе. В частности, если заставить пользователей работать одним пальцем одной руки, то клавиатурный почерк практически полностью теряет свою индивидуальность. В этом случае стираются различия между временами нажатия клавиш для разных людей. Интервалы между нажатиями становятся пропорциональны расстоянию между клавишами, а перекрытие нажатий соседних клавиш становится невозможным (параметр $\tau_к$ всегда оказывается больше нуля). С другой стороны по мере увеличения навыков работы с клавиатурой и по мере переходу к слепому набору всеми пальцами обоих рук, существенно растет индивидуальность клавиатурного почерка любого из пользователей.

Обработка первичных данных

В задаче идентификации пользователя по клавиатурному почерку важным этапом является обработка первичных данных, в результате которой входной поток данных разделяется на ряд признаков, характеризующих те или иные качества идентифицируемой личности.

Начальный этап обработки данных – фильтрация. На этом этапе из потока данных удаляется информация о служебных клавишах (клавишах управления курсором, функциональных клавишах и т. п.).

Затем выделяется информация, относящаяся к следующим характеристикам пользователя:

- количество ошибок при наборе;
- интервалы между нажатиями клавиш;
- время удержания клавиш;
- число перекрытий между клавишами;
- степень аритмичности при наборе;
- скорость набора.

Постановка задачи

Идентификация пользователя по клавиатурному почерку возможна следующими способами:

- по набору ключевой фразы;
- по набору произвольного текста.

Принципиальное отличие этих двух способов заключается в том, что в первом случае используется ключевая фраза, задаваемая пользователем в момент регистрации его в системе (пароль), а во втором случае используются ключевые фразы, генерируемые сис-

темой каждый раз в момент идентификации пользователя. Оба способа подразумевают два режима работы:

- обучение;
- идентификация.

На этапе обучения пользователь вводит некоторое число раз предлагаемые ему тестовые фразы. При этом рассчитываются и запоминаются эталонные характеристики данного пользователя. При наборе ключевой фразы компьютер позволяет зафиксировать много различных параметров, но для идентификации наиболее удобно использовать время, затраченное на ввод отдельных букв. Биометрический эталон ввода парольной фразы получают путем вычисления математических ожиданий и дисперсий контролируемых параметров, предварительно исключив из обучающей выборки аномальные выбросы.

Выбор текста, на котором выполняется обучение системы, − важный этап для нормального функционирования системы. Предлагаемые пользователю фразы необходимо подбирать таким образом, чтобы используемые в них символы полностью и равномерно покрывали рабочее поле клавиатуры. Более того, если в процессе обучения системы видно, что статистические характеристики отдельных клавиш имеют существенный разброс, необходимо формировать очередную тестовую фразу таким образом, чтобы уменьшить эту неопределенность. Возможна организация "неявного" процесса обучения системы, когда программа перехватывает весь ввод с клавиатуры и соответственно рассчитывает эталонные характеристики пользователя. Данная процедура достаточно легко организуется практически в любой операционной системе. В DOS для этого используется перехват прерываний от клавиатуры, в Windows − стандартный механизм ловушек (hooks).

На этапе идентификации рассчитанные оценки сравниваются с эталонными, на основании чего делается вывод о совпадении или несовпадении параметров клавиатурного почерка. При идентификации по «свободному тексту» получаемый ряд значений сильно отличается от эталона (любой символ "ключа" даже если и встретится, то окажется не на "своем" месте). Поэтому при составлении множеств в качестве базисных используются величины, которые можно подобрать и в ключевой, и в случайной фразах, например, время между нажатием двух клавиш в одинаковых сочетаниях. Если эталоном является слово "Внимание", то в свободном тексте ищем "Вн", "ни", "им" и т.д. и определяем размер паузы, прошедшей с момента нажатия "В" до нажатия "н", считая, что пользователь будет переносить руку от одной клавиши к другой одинаково в обоих случаях (при настройке и идентификации).

Однако существует ряд ограничений по применению данного способа на практике. Применение способа идентификации по клавиатурному почерку целесообразно только по отношению к пользователям с достаточно длительным опытом работы с компьютером и сформировавшимся почерком работы на клавиатуре, т. е. к программистам, секретарям и т. д. В противном случае вероятность неправильного опознания легального пользователя существенно возрастает и делает непригодным данный способ идентификации на практике. Исходя из теории машинописи и делопроизводства, время становления почерка работы с клавиатурой, при котором достигается необходимая вероятность идентификации пользователя, составляет примерно 6 месяцев.

Эталонные характеристики пользователя, полученные на этапе обучения системы, позволяют сделать выводы о степени стабильности клавиатурного почерка пользователя и определить доверительный интервал разброса параметров для последующей идентификации пользователя. Во избежание дискредитации работы системы можно отсеивать пользователей, клавиатурный почерк которых не обладает необходимой стабильностью. Для этого можно пользоваться следующей таблицей.

Однако при использовании стандартных методов статистической обработки входного потока данных возникает ряд серьезных проблем. Применение этих методов базируется на утверждении, что входные величины подчинены нормальному закону распределения, хотя в ряде случаев оно неверно. Например, проведенные исследования показывают, что время удержания клавиш при малом шаге дискретизации описывается пересечением

двух нормальных распределений, что приводит к большим погрешностям при расчете эталонных характеристик пользователя.

Таблица 1.

Оценка стабильности клавиатурного почерка пользователя

Ошибки, %	Аритмичность, %	Скорость, зн./мин	Характеристика перекрытий		Оценка
			Число перекрытий, %	Используемое число пальцев	
менее 2	менее 10	более 200	более 50	все	отлично
менее 4	менее 15	более 150	более 30	большинство	хорошо
менее 8	менее 20	более 100	более 10	несколько	удовл.
более 8	более 20	менее 100	менее 10	по одному	неуд.

Применение нейросетевого подхода к задаче идентификации пользователя по клавиатурному почерку позволяет решить эти проблемы. Кроме того, нейронная сеть обладает свойством фильтрации случайных помех, присутствующих во входных данных, что позволяет отказаться от алгоритмов сглаживания экспериментальных зависимостей, необходимых при статистической обработке данных.

Нейросетевой подход к задаче идентификации

Нейронные сети – это обобщенное название нескольких групп алгоритмов, обладающих одним ценным свойством: они умеют обучаться на примерах, извлекая скрытые закономерности из потока данных. Если между входными и выходными данными существует какая-то связь, пусть даже не обнаруживаемая традиционными корреляционными методами, нейронная сеть способна автоматически настроиться на нее с заданной степенью точности.

Наиболее перспективным методом решения задачи идентификации пользователя по клавиатурному почерку является использование трехслойного перцептрона Розенблатта [1-4] следующей конфигурации (рис. 1):

- первичный слой – входной, состоит из m формальных нейронов с линейной активаторной функцией $\varphi(s) = ks + b$, где m – размерность входного вектора, содержащего параметры клавиатурного почерка пользователя;
- второй слой – скрытый, состоит из m формальных нейронов с сигмоид- ной активаторной функцией $\varphi(s) = (1 + e^{-k(s-a)})^{-1}$;
- третий слой – выходной, состоит из n формальных нейронов с сигмоидной активаторной функцией, где n - число зарегистрированных пользователей.

Обучение этой нейронной сети выполняется с помощью алгоритма обратного распространения ошибки, состоящего из двух проходов по всем слоям сети: прямого и обратного. При прямом проходе входной вектор подается на сенсорные узлы сети, после чего распространяется по сети от слоя к слою. В результате генерируется набор выходных сигналов, который и является фактической реакцией сети на данный входной вектор. Во время прямого прохода все синаптические веса сети фиксированы, а функциональные сигналы вычисляются последовательно, от нейрона к нейрону. Функциональный сигнал на выходе нейрона j на итерации r вычисляется по формуле:

$$y_j(r) = \varphi(v_j(r)) = \varphi\left(\sum_{i=0}^{m_j} w_{ji}(r) y_i(r)\right),$$

где $v_j(r)$ – индуцированное локальное поле нейрона j; m_j – общее число входов нейрона j; $w_{ji}(r)$ – синаптический вес, соединяющий нейроны i и j; $y_i(r)$ – входной сигнал нейрона j или выходной сигнал нейрона i.

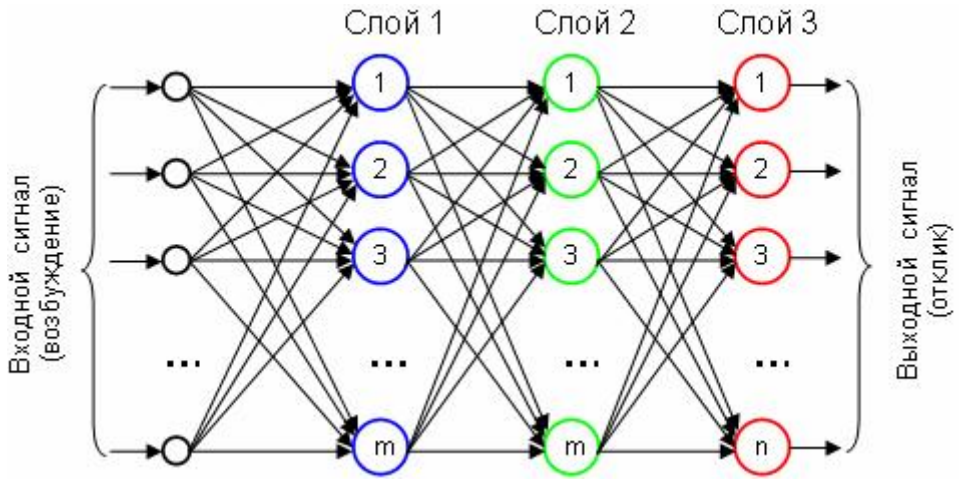


Рис. 1. Архитектурный граф трехслойного перцептрона.

Если нейрон j расположен в первом слое сети, то $m_j = m$, а индекс i относится к i-му входу сети, для которого можно записать:

$$y_i(r) = x_i(r),$$

где $x_i(r)$ – i-й элемент входного вектора.

С другой стороны, если нейрон j расположен в выходном слое сети, то $m_j = n$, а индекс j означает j-й выход сети, для которого можно записать:

$$y_j(r) = o_j(r),$$

где $o_j(r)$ – j-й элемент выходного вектора. Выходной сигнал сравнивается с желаемым откликом $d_j(r)$, в результате чего вычисляется сигнал ошибки $e_j(r)$ для j-го выходного нейрона.

Обратный проход начинается с выходного слоя предъявлением ему сигнала ошибки, который передается справа налево от слоя к слою с параллельным вычислением локального градиента для каждого нейрона. Этот рекурсивный процесс предполагает изменение синаптических весов в соответствии с дельта-правилом:

$$\begin{pmatrix}\text{Коррекция}\\ \text{веса}\\ \Delta w_{ji}(r)\end{pmatrix} = \begin{pmatrix}\text{Параметр ско-}\\ \text{рости обучения}\\ \eta\end{pmatrix} \cdot \begin{pmatrix}\text{Локальный}\\ \text{градиент}\\ \delta_j(r)\end{pmatrix} \cdot \begin{pmatrix}\text{Входной сиг-}\\ \text{нал нейрона j}\\ y_i(r)\end{pmatrix}. \quad (1)$$

Для нейрона, расположенного в выходном слое, локальный градиент равен соответствующему сигналу ошибки, умноженному на первую производную нелинейной функции активации. Затем соотношение (1) используется для вычисления изменений весов, связанных с выходным слоем нейронов. Зная локальные градиенты для всех нейронов выходного слоя, вычисляем локальные градиенты всех нейронов предыдущего слоя по формуле:

$$\delta_j(r) = \varphi'_j(v_j(r)) \sum_k \delta_k(r) w_{kj}(r).$$

По формуле (1) определяем величины коррекций весов связей с выходным слоем нейронов. Такие вычисления проводятся для всех слоев в обратном направлении.

Практическая реализация

В качестве элементов входного вектора были выбраны параметры наиболее часто встречающихся при наборе русскоязычного текста сдвоенных нажатий клавиш, таких как ен, ер, ет, ве, ем, во, ат, ан, ва, ес, го, вы, де, за, ав, же, ач, ед, ал, ей, ел, ак, дн, да, гр, жн, ам, ад, ае, зн, аз и т.д., всего 160. Каждое сдвоенное нажатие характеризуется тремя параметрами: временем удержания клавиши с первым символом, интервалом времени между отпусканием первой клавиши и нажатием клавиши со вторым символом, временем удержания второй клавиши. Нейронная сеть была обучена на данных, полученных от пяти пользователей. Проверка работы нейронной сети в режиме идентификации пользователя показала ее высокую точность.

Выводы

Предлагаемый подход к задаче идентификации пользователя по клавиатурному почерку позволяет увеличить размерность вектора, содержащего эталонные характеристики пользователя. Применение нейронных сетей упрощает математический аппарат обработки данных и уменьшает вероятность возникновения ошибок второго рода – положительного результата идентификации для незарегистрированных пользователей. В результате возможно существенное повышение надежности и устойчивости работы систем идентификации пользователя по клавиатурному почерку.

Литература

1. Хайкин, Саймон. Нейронные сети: полный курс, 2-е издание: Пер. с англ. – М.: Издательский дом "Вильямс", 2006. – 1104 с., ил;
2. Калан, Роберт. Основные концепции нейронных сетей: Пер. с англ. – М.: Издательский дом "Вильямс", 2003. – 288 с., ил;
3. Барский А. Б. Нейронные сети: распознавание, управление, принятие решений. – М.: Финансы и статистика, 2004. – 176 с., ил;
4. Комашинский В. И., Смирнов Д. А. Нейронные сети и их применение в системах управления и связи. – М.: Горячая линия–Телеком, 2003. – 94 с.

УДК 004.056

Петров А.С., Талыкин О.А.

ПОСТРОЕНИЕ ОБОБЩЕННОЙ МОДЕЛИ ФУНКЦИОНИРОВАНИЯ WEB-СИСТЕМЫ

В статье проанализированы существующие компллексы средств защиты информации, требования к ним и предложена обобщенная модель функционирования Web-системы, способной обеспечить высокий уровень безопасности обрабатываемой информации.

Web-технологии являются одним из современных направлений развития информационных систем. Вопросам обеспечения безопасности систем, использующих Web-технологии для предоставления информации пользователям сети Интернет, уделяется в последнее время все больше внимания. Существует множество направлений исследований в этой области, среди которых можно назвать следующие: построение методов и способов безопасного и конфиденциального обмена данными, криптография, аутентификация, интеграция с автоматизированными банковскими системами и др.

В то же время отдельного внимания заслуживает вопрос построения комплексной системы защиты информации (КСЗИ) автоматизированной системы (АС) как совокупности всех компонентов, участвующих в обработке информации. Среди работ в данной области необходимо выделить НД ТЗИ [1], в которой предоставляется нормативно-методологическая база для разработки комплекса средств защиты (КСЗ) от несанкциони-

рованного доступа к информации Web-страницы при построении КСЗИ. Установленные данным документом требования являются обязательными для исполнения при обработке информации, являющейся собственностью государства.

В то же время для создания КСЗИ необходимо разработать совокупность моделей позволяющих оценить систему со стороны осуществления угрозы безопасности.

К таким моделям следует отнести: модель функционирования системы, модель нарушителя и модель угроз.

Предложенная в НД ТЗИ [1] общая функционально-логическая структура вычислительной системы АС, включающая в себя подсистему обработки информации, подсистему взаимодействия с пользователями АС и подсистему обмена данными, не в полной мере соответствует архитектуре построения Web-систем и носит сильно упрощенный характер. К ее основным недостаткам следует отнести:

а) невозможность выделить отдельно взятую подсистему и рассмотреть ее без взаимодействия с другими подсистемами. Так, к подсистеме обработки информации относятся средства обработки информации (Web-сервер и рабочие станции), системное и прикладное ПО. В то же время, если рассматривать подсистему взаимодействия с пользователями АС, то в его состав входит сетевая подсистема Web-сервера и интерфейс пользователя, которые, по сути, являются теми же компонентами АС;

б) одноуровневая структура, не позволяющая отделить логику функционирования Web-системы от вычислительной системы.

Целью работы является построение на основе анализа множества существующих Web-систем и их архитектурных особенностей обобщенной модели функционирования Web-системы, способной обеспечить высокий уровень безопасности обрабатываемой информации от несанкционированного доступа.

Основными компонентами любой АС являются: информация, технология обработки, вычислительная система, физическая среда и пользователи системы.

Информация Web-системы делится на две большие категории:

- общедоступная;
- технологическая.

Для сохранения совместимости с НД ТЗИ [1] все возможные дополнительные категории информации рассматриваются в качестве общедоступной, т.к. в соответствии с НД ТЗИ [1] технологическая информация предназначена для использования только уполномоченными пользователями из числа сотрудников службы защиты информации.

В зависимости от сложности реализуемых функций системой и владельца информации в системе, может существовать конфиденциальная информация, требующая дополнительных условий обеспечения безопасности доступа к ней. В частности, в качестве таковой можно рассматривать почтовые ящики пользователей сети Интернет, расположенные на общедоступных серверах.

Безопасность информации обеспечивается сохранением ее свойств, в связи с чем основными требованиями к КСЗИ являются:

- сохранение целостности и доступности размещаемой в Web-системе общедоступной информации;
- сохранение конфиденциальности и целостности технологической информации;
- сохранение целостности и наблюдаемости всей Web-системы в целом.

Основными требованиями к технологии обработки информации являются следующие:

- соответствие политике безопасности;
- обеспечение реализации контролированного и санкционированного доступа к информации;
- выявление попыток несанкционированного доступа к информации;
- блокирование пользователей в случае нарушения политики безопасности или правил распределения доступа;
- реализация резервного копирования;

- реализация возможности использования пользователями и процессами вычислительных ресурсов АС и обеспечение управления ресурсами.

Предлагаемая архитектура вычислительной системы изображенная на рис. 1, имеет иерархическую структуру и состоит из следующих компонентов:

1 уровень. Вычислительная система

Подсистема управления ВС

Позволяет пользователям, исполняющим роль системного администратора ВС, или администратора безопасности ВС производить изменение конфигурации сервера, отслеживать соблюдение политики безопасности и др. Доступ к данной подсистеме может осуществляться двумя способами посредством сетевого протокола управления, таких как ssh, rdp или с консоли сервера. В первом случае выдвигаются дополнительные требования к обеспечению безопасности рабочей станции администратора.

Подсистема обмена данными

Необходима для взаимодействия ВС с другими системами, а также для обновления системного и функционального ПО.

Комплексная система защиты информации ВС. Отслеживает взаимодействие всех компонентов системы и обеспечивает соблюдение правил политики безопасности, целостность КСЗИ Web-системы.

2 уровень. Web-система

Подсистема управления Web-системой

Позволяет управлять Web-системой, разграничивать полномочия доступа субъектов к объектам, отслеживать состояния и соблюдение политики безопасности Web-системы. Реализуется в виде отдельного функционального ПО или дополнительного модуля к ПО, реализующего подсистему обработки информации. Данное ПО должно функционировать с привилегиями пользователя, не имеющего возможности влиять на функционирования ВС.

Подсистема обработки информации

Представляет собой совокупность средств обработки информации, включает в себя: ПО, реализующее механизмы обработки информации, рабочие станции, другие Web-системы.

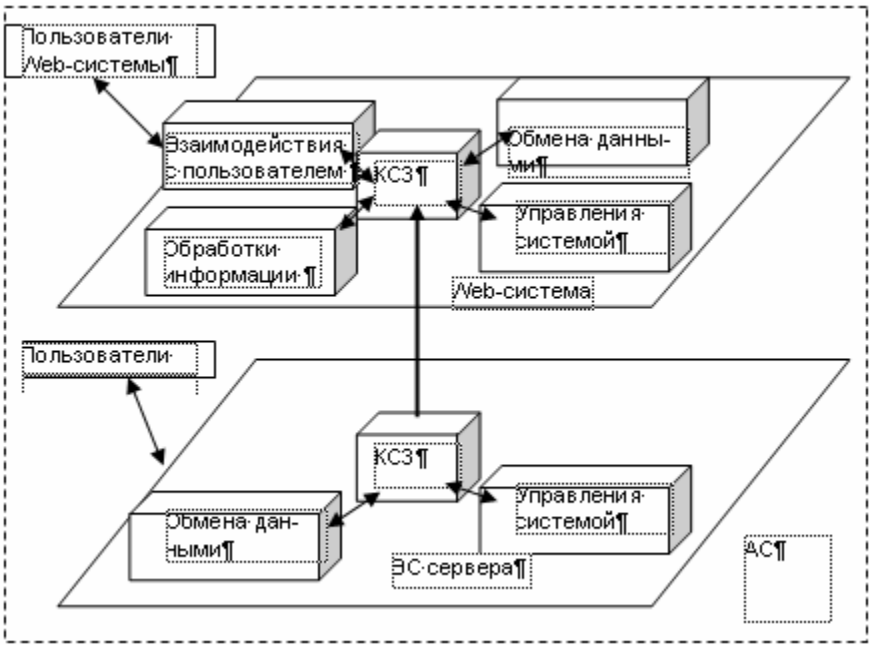


Рис. 1. Архитектура вычислительной системы.

Подсистема взаимодействия с пользователями

Обеспечивает доступ пользователей АС к общедоступной информации посредством предоставления соответствующего интерфейса. Реализовывается функциональным ПО, имеющим минимальные привилегии в ВС.

Подсистема обмена данными

Обеспечивает непосредственный обмен общедоступной информацией Web-системы пользователями, имеющими полномочия на обработку информации, а также используется Web-системой для доступа к информационным хранилищам (базам данным).

Комплексная система защиты информации Web-системы

Отслеживает взаимодействие всех компонентов системы и обеспечивает соблюдение правил политики безопасности на уровне Web-системы. Контроль целостности и корректности функционирования КСЗ 2 уровня возлагается на КСЗ 1 уровня.

Подобный подход позволяет отделить логику функционирования ВС от Web-системы, обеспечивая более гибкое разделение функций и полномочий между возможными пользователями системы. Локализация функций Web-системы на отдельном уровне позволяет ВС обеспечивать функционирование множества Web-систем на соответствующем уровне безопасности.

Особые требования выдвигаются к КСЗ 2 уровня. Она должна тесно интегрироваться со всеми компонентами Web-системы, участвовать во всех существующих процессах обработки информации и обеспечивать минимальный необходимый функциональный профиль: КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1,ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НВ-1 [3]. Выполнение данных условий возможно только при совместной разработке компонентов КСЗ с функциональным ПО и их полной интеграции.

При подходе, когда каждая подсистема комплектуется отдельными средствами защиты информации (в соответствии с существующей политикой безопасности), в полной мере не обеспечивает должного уровня безопасности, так как разрозненные средства защиты не имеют возможности отслеживать внутренние механизмы и потоки информации в системе.

Однако требование соответствия технических средств защиты информации, входящих в состав КСЗ, по наличию соответствующих сертификатов не гарантирует обеспечения должного уровня безопасности, что может быть связано с уязвимостями, найденными в данной версии. В то же время отсутствие необходимых документов препятствует немедленному обновлению программного продукта. При развертывании Web-систем в локальных сетях, где потенциальными нарушителями являются узкий круг лиц (из числа сотрудников или обслуживающего персонала), подобные изъяны могут быть устранены внедрением дополнительных организационных мер. Совсем иначе выглядит ситуация в глобальных сетях, где наличие уязвимости требует немедленного ее устранения.

Анализ программного обеспечения, имеющего сертификаты, свидетельствующие о возможности использования их в составе КСЗ, показал отсутствие сертифицированных серверных операционных систем и приложений, реализующих функции Web-сервера, что затрудняет развертывание Web-систем, соответствующих нормативным документам защиты информации.

Пользователи АС по уровню полномочий и характеру работ, ими выполняемых в процессе функционирования АС, делятся на такие категории [1]:

А) пользователи, которым дано право доступа только к общедоступной информации;

Б) пользователи, наделенные полномочиями по сопровождению КСЗИ и обеспечению управления АС (в эту категорию входит весь персонал, обслуживающий Web-систему, в том числе дизайнеры и вебмастеры);

В) технический обслуживающий персонал, обеспечивающий надлежащие условия функционирования АС (электрики, персонал по обслуживанию помещений, линий связи и т.д.);

Г) разработчики ПО, осуществляющие разработку и внедрение новых функциональных процессов, а также сопровождение функционирующего ПО;

Д) поставщики оборудования и технических средств и специалисты, осуществляющие его монтаж, гарантийное и послегарантийное обслуживание.

Для обеспечения более гибкого управления полномочиями в соответствии с предложенной моделью функционирования системы необходимо категорию «Б» разделить на несколько дополнительных:

Б1) системные администраторы и администраторы безопасности ВС (обеспечение доступа ко всему уровню 1);

Б2) системные администраторы и администраторы безопасности Web-системы (обеспечение доступа ко всему уровню 2);

Б3) пользователи Web-системы участвующие в обработке общедоступной информации (обеспечение доступа к подсистеме обработки информации и обмена данными, уровня 2);

Среди требований, предъявляемых к пользователям АС нормативным документом [1], следует отметить следующие:

Обязательная регистрация в АС пользователей категории Б.

Пользователи категории В-Д могут иметь доступ к программным и аппаратным средствам АС только во время проведения работ по тестированию и инсталляции ПО, установления или регламентированного обслуживания оборудования и т.д. с условием ограничения их доступа к технической информации УСЗИ.

Доступ ко всем помещениям, где расположены компоненты АС, разрешается без ограничений пользователям с категориями Б и В, Г и Д только при необходимости.

Последнее требование не обеспечивает должного уровня обеспечения безопасности, так как физический доступ злоумышленника к консоли сервера неминуемо приводит к обходу существующих средств защиты и нарушению политики безопасности. В связи с чем, доступ к помещению, где располагается сервер, должен быть разрешен только пользователям категории Б1, а всем другим только при необходимости и под контролем.

Заключение

Предложенная в данной работе обобщенная модель функционирования Web-системы способна обеспечить высокий уровень безопасности обрабатываемой информации от несанкционированного доступа. Она не противоречит требованиям нормативных документов в области технической защиты информации, действующих в Украине и может использоваться как разработчиками Web-систем, так и провайдерами сети Интернет для развертывания Web-систем, имеющих более высокие требования по безопасности.

Литература

1. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації Web-сторінки від несанкціонованого доступу;
2. НД ТЗІ 1.1-004-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
3. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
4. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу;
5. НД ТЗІ 2.5-005 -99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

УДК 681.3

Петров А.С., Петров А.А.

ТЕХНОЛОГИЯ ЗАЩИТЫ ПРОГРАММНОГО КОДА ПОСРЕДСТВОМ ПРИМЕНЕНИЯ ВИРТУАЛЬНОЙ МАШИНЫ

Целью статьи является нахождение оптимального способа противодействия анализу исполняемого кода.

Не секрет, что идеальной защиты в области программного обеспечения до сих пор не создано, хотя уже десятилетия идет война создателей защит и хакеров. Неизменно победителями выходят последние, лишь иногда оставляя пальму первенства создателям защит. Под защитой я понимаю такой блок исполняемого кода, который противодействует (успешно или нет) нелегальному использованию программы. Это может быть защита от копирования с носителя информации, ввод серийного регистрационного номера программы, средство, ограничивающее максимальное количество лицензий в сети и так далее.

В нашей статье мы не будет углубляться в детали реализации каждой из этих технологий, поскольку все они имеют свои, специфические, и только им присущие черты. Разговор пойдет о компоненте, который присутствует в любой программной защите. Это компонент называется *исполняемый код*. То есть машинный, двоичный код, который непосредственно выполняет центральный процессор. Собственно, это материал, из которого состоит программа вообще и защита в частности.

Основной проблемой, с которой сталкиваются программисты, создающие *защищающий код* (тот участок кода, который принимает решение, открыть или закрыть доступ к основному коду, иными словами, выполняет функции идентификации, аутентификации и авторизации), является проблема потенциальной возможности анализа и исправления данного двоичного кода.

На сегодняшний день широко известно уже не одно решение криптозащиты кода приложения, позволяющее обезопасить его от дизассемблирования, и привязать к аппаратному ключу, например, Guardant.

Возьмем наиболее популярный метод криптозащиты. Закодируем важные участки кода так, чтобы правильно декодировать их можно было только с помощью законно полученного ключа. Без ключа приложение перестает быть работоспособным, или работает в режиме оценочной версии. Алгоритм кодирования будет являться тестом законного использования. Условный переход IF «декодировано_правильно» THEN ... – это всего лишь формальность, которая исключит ошибку нарушения доступа при выполнении неверно декодированного участка. Приложение с криптозащитой остается уязвимым по отношению к атаке, когда взломщик покупает лицензированную копию и, запустив ее, снимает из дампа памяти декодированную версию. Следовательно, сразу после исполнения декодированного участка приложения необходимо его вновь закодировать, или переносить обратно заранее сохраненный закодированный участок. У взломщика останется единственная возможность поймать момент, когда в памяти исполняется декодированный участок, сохранить рабочий код приложения и действовать таким образом далее, в конечном итоге собирая приложение в единое целое по кускам, но это ручная кропотливая работа, тем более если предусмотреть большое количество маленьких участков кода, с их последовательной расшифровкой. Борьба с атаками такого рода заключается в как можно большем количестве закодированных участков, их замене в каждой новой версии системы.

Однако, оказывается, такая казалось бы сложная защита легко обходится посредством анализа кода защиты по частям и последующего «вырезания» из приложения.

За истекшее десятилетие наработана масса приемов противодействию вскрытию. В различных защитах используются разные подходы, реализованные с разными степенями надежности. Если писать об основных приемах написания защит, то можно выделить следующие:

- Защита пишется целиком на ассемблере;
- Присутствуют механизмы расчета контрольных сумм;
- Используются отладочные прерывания в собственных целях (и иные антитрассировочные способы);
- Шифруются фрагменты кода;
- Используются механизмы многопоточности;
- Вбрасывают "мусор" в тело защиты, для запутывания хакера;

И так далее… Перечислять все способы нет смысла, поскольку они хорошо известны и описаны в прессе и Интернете.

К сожалению, практика показывает, что такие защиты держат оборону недолго. Программный продукт можно найти в Интернете раньше, чем его начнут продавать в розничной торговле. Причем это полная версия, работающая либо с виртуального образа, либо с уже готовым генератором серийных номеров.

Каким бы сложным ни был алгоритм защиты, «узким горлышком» все равно остается машинный код, который практически всегда можно дизассемблировать и/или проанализировать в работающем состоянии. Тем не менее, существует технология, которая позволяет обезопасить критичные участки кода, или значительно затруднить их анализ.

Итак, эффективность защиты в значительной степени определяется сложностью ее анализа и если защиту в принципе невозможно проанализировать в заданные сроки, соответственно, принципиально можно говорить о ее стойкости.

Основная идея состоит в использовании псевдокомпилируемых языков со стековой структурой и или подобных им, преобразующих сходный код программы в последовательность инструкций собственной виртуальной машины. В отличие от машинного кода, который всем хорошо известен, архитектура виртуальных машин, как правило, вообще не документирована и подвержена катастрофическим изменениям при переходе с одной версии среды разработки к другой.

Тем не менее, для подавляющего большинства существующих языков, хакеры и специалисты по информационной безопасности разработали автоматические декомпиляторы, если не восстанавливающие исходный текст, то, по крайней мере значительно упрощающие его анализ.

Сделаем небольшое отступление, позволяющее разобраться с оставшейся частью статьи. Законы кибернетики гласят: чтобы построить процессор, достаточно всего лишь одного логического элемента — **Стрелки Пирса** или **Штриха Шеффера.** Такой прибор может соорудить даже начинающий радиолюбитель из пары микросхем ИЛИ-НЕ. Этого будет достаточно для того, чтобы решить любую мыслимую задачу — вычислить квадратный корень или синус угла, возвести число в степень, даже распознать речь!

Программировать на нем будет очень просто — достаточно выучить всего лишь одну машинную инструкцию... но и весь аппарат булевой, дискретной алгебры, тригонометрию и... еще множество других наук! В частности, для того чтобы сравнить два числа, потребуется вспомнить формулу эквивалентности:

```
NOT  == NOT  (PIRS  A, A);
OR    == OR (PIRS(PIRS(A,B), PIRS(A,B));
AND  == NOT[( OR(NOT(A), NOT (B))];
CMP  ==OR   [AND   (A,B),   NOT(OR(A,NOT(C)))];
```

Но кто мешает создателям защиты придумать *собственную* виртуальную машину? При этом, архитектура последней может быть сколь угодно запутанной и нетривиальной, а потому и сложной для анализа. Вообще же говоря, трудозатраты на создание и анализ виртуальных машин несопоставимы, — виртуальную машину, разработанную начинающим программистом за несколько дней, даже "матерые" специалисты могут "раскручивать" не одну неделю!

Сложность анализа обусловлена чрезвычайной "элементарностью" Стрелки Пирса, реализуемой двумя следующими инструкциями, представленными в листинге 1.

Листинг 1. Пример реализации Стрелки Пирса.

```
OR      A,   B
NOT     A
```

Этого вполне достаточно для решения любой задачи (конечно, при условии, что задача вообще имеет решение), но даже простейшие операции, такие, например, как *сравнение* или *условный переход*, требуют для своей реализации десятков Стрелок Пирса, а организация цикла может составить сотню или около того операций! Таким образом, даже

простейшая программа будет состоять из тысяч, а то и *миллионов* (!) однотипных команд, "физический" смысл которых установить будет не так-то просто, ведь каждая из них совершает *абсолютно* бессмысленную операцию и только все вместе они что-нибудь да значат. Анализ такого кода потребует совершенно немыслимых затрат времени и труда.

Правда, если код самой виртуальной машины (листинг 2) будет постоянным, то грубое опознание можно осуществить по наличию соответствующей виртуальной машины. Поскольку в "реальных" приложениях данная последовательность инструкций не встречается, — это решение кажется не лишено смысла.

Листинг 2. Пример реализации виртуальной машины Стрелки Пирса.

```
Repeat:
        MOV   SI, [0152]                ; Указатель команд
        LODSW                           ; Читаем 1st операнд
        XCHG  DI, AX        ; DI := [1st]
        MOV   DI, [DI]      ; л
        LODSW                           ; Читаем 2st операнд
        XCHG  BX, AX         ; BX := &2st
        OR    DI, [BX]                  ; tO := [1st] | [2st]
        LODSW                           ; Читаем 3st операнд
        XCHG  DI, AX        ; AX := tO; DI = 3st
        NOT   AX                        ; AX := NOT tO
        MOV   [0152], SI                ; Update emIP
        STOSW                  ; mov [3st],NOT(OR [1st],[2st])
        JMP   Repeat; — цикл выборки команд
```

Пусть, например, команда виртуальной машины вируса состоит из кода команды и указателя на следующую обрабатываемую команду (при этом, сам код команды может быть "поксорен" текущим и/или следующим указателем, или зашифрован каким-либо иным образом):

Листинг 3. Пример команды виртуальной машины, перемешивающий свой код.

```
struct command
{
    CODE code;
struct command* next_command;
}
```

Грубо говоря, память виртуальной машины будет представлять собой связанный список, что позволит: а) легко, элегантно и безболезненно "перемешивать" код вируса; б) эффективно добавлять и удалять "мусорные" команды; в) полностью "рассеивать" тело вируса по "пустотам" заражаемого файла, г) запутает многих разработчиков наконец...

В общем, мы получим чрезвычайно простой, но весьма "хитрый" полиморфный код, для анализа которого разработкам антивируса придется написать специальный обработчик. А если реализовать память виртуальной машины в виде двоичного дерева, выполнение инструкций организовать в виде дека (двухсторонней очереди), а аргументы передавать через списки?

Словом, вирус, написанный на "виртуальной машине", требует уймы времени для анализа. Если появится тенденция в написании таких, то сомневаюсь, что антивирусная индустрия сможет справиться с подобным объемом работы — потребуются дополнительные высококвалифицированные сотрудники и вклады. А где их взять? Специа-

листы обычно не сидят без дела, в ожидании предложений, а уже имеют любимую работу, переманить с который их будет ой как не просто!

Вместе предложенной технологией хорошо сочетается *динамическая шифровка*, позволящая свести на нет какой-либо анализ кода. В этом случае ни в какой момент код не расшифровывается целиком. По мере надобности расшифровываются лишь небольшие фрагменты (функции или даже отдельные машинные команды), которые после отработки зашифровываются вновь. Понятно, чем меньше длина декодируемого блока, тем сложнее справиться с таким вирусом, ибо последовательность несколько десятков байт уже достаточна для надежного отождествления вируса. В доведенной до абсурда идее можно сократить размер "окна" расшифровщика до одного-единственного бита (вообще-то можно и *меньше*, но подобные алгоритмы выходят за рамки данной статьи), впрочем, на практике вполне достаточно ограничиться шифровкой одной машинной команды, поскольку надежной сигнатурой она служить никак не может.

Создатели защиты (читай виртуальной машины) и взломщики находятся далеко не в равноправных условиях. Действительно, виртуальные машины в принципе возможно генерировать и автоматически, но до сих пор не создана (да и вряд ли когда-нибудь будет создана) программа автоматической "декомпиляции" виртуальных процессоров в какой бы то ни было "читабельный" язык. Более того, даже нет дизассемблера, легко настраиваемого на различные архитектуры. (IDA Pro для этой цели все же недостаточно гибка, хотя это единственный выбор.) Выходит, каждой ВМ — по персональному дизассемблеру?! Это огромные трудозатраты.

Впрочем, виртуальные машины рано или поздно усложнятся до той степени, когда "ручным" анализом нескольких специалистов их будет уже не "взять". Для этого ВМ достаточно научиться генерировать виртуальные процессоры, обрабатывающие Р-код по произвольному алгоритму. А если еще к этому подключить и машинную "эволюцию", то потенциал таких ВМ многократно усилится.

Интенсивные и небезуспешные исследования в этом направлении ведутся уже не один десяток лет. В качестве наглядного примера рассмотрим следующий эволюционный алгоритм, основанный на случайных изменениях тела вируса, — т. е. *мутациях*. Разумеется, эти изменения не должны нарушать работоспособности вируса. В рамках машинного языка процессоров Intel 80x86 это сделать довольно затруднительно, поэтому лучше прибегнуть к виртуальной машине, устойчивой к изменениям кода. Как и любая другая виртуальная машина, она будет состоять из двух функциональных частей — *выборщика* инструкций и их *исполнителя*. Исполнитель может разбивать сложные инструкции на последовательность простейших микроопераций. В частности, инструкция LOOP xxx на самом деле распадается на две: DEC CX и JZ xxx.

Теперь рассмотрим еще более интересный вариант — *виртуальные машины с произвольно генерируемым набором инструкций*. В самом деле, можно уничтожить инструкцию LOOP, *автоматически* заменяя ее исходной последовательностью команд DEC\JZ. Аналогично, любую устойчивую комбинацию наподобие CALL xxx\OR AX,AX\JZ xxx можно заменить одной "суперинструкцией" (это кстати еще и минимизирует объем исполняемого кода). Если пойти дальше, то можно наугад взять несколько инструкций, даже не обязательно соседних, и заменить их одной новой, продолжая так до тех пор, пока "не надоест" или код окажется до неузнаваемости измененным.

Во втором поколении окажется большой выбор инструкций для "дробления". При условии, что такое дробление будет осуществляться по случайному закону, полученные инструкции, вероятнее всего, не совпадут с исходными, в результате чего второе поколение станет практически неузнаваемо!

При этом проанализировать логику такой виртуальной машины невероятно трудно. Дело в том, что "физический" смыл команд, сгенерированных произвольным образом в подавляющем большинстве случаев, совершенно непостижим. Что, впрочем, неудивительно, т. к. число связей между отдельными командами стремится к n!, где n — количество исходных команд. Поскольку виртуальная машина может оперировать сотнями и даже тысячами команд, ни проанализировать, ни декомпилировать код невозможно.

Хакеры и специалисты по информационной безопасности уже давно экспериментируют с виртуальными машинами, манипулирующими *сотнями тысяч* инструкций. Чтобы понять логику работы такой виртуальной машины требуется с особой тщательностью проанализировать реализации всех команд, поскольку результат выполнения одной инструкции зачастую зависит от всех остальных.

Выводы

Безусловно, статья имеет обзорный, общий характер, не предлагает свою конкретную реализацию. Однако авторы попытались показать высокую перспективность данного направления, которое пока не заслуженно обходится стороной. Потенциал технологии виртуальных машин в области защиты информации очень высок. Внедрять сложную аппаратную защиту не всегда целесообразно исходя из затрат времени, средств и сложности внедрения. Программная же реализация обладает чрезвычайной гибкостью и простотой, ограничиваясь лишь средствами математики, языков программирования и, конечно, талантом разработчиков!

Литература

1. Крис Касперски. Эвристический анализ – что стоит за ним?
2. Компиляторы: принципы, технологии и инструменты.: Пер. с англ. - М.: Издательский дом «Вильямс», 2001. – 768 с.: ил;
3. Дискретна математика: Підручник / Ю.М. Бардачов, Н.А. Соколова, В. Е. Ходаков; За ред. В. Е. Ходакова. – К.:Вища шк., 2002. – 287 с.: іл.

УДК 004.056

Чаплинский Д.А., Белозеров Е.В.

ПОЛНОТЕКСТОВЫЙ ПОИСК ИНФОРМАЦИИ С УЧЁТОМ МОРФОЛОГИИ РУССКОГО И УКРАИНСКОГО ЯЗЫКА

Описана реализация алгоритма полнотекстового поиска информации, основывающегося на анализе особенностей морфологии русского и украинского языка.

Постановка проблемы

На текущий момент объём доступной информации увеличивается лавинообразно. Переводятся и оцифровываются старые библиотеки, постоянно появляются новые.

Такое увеличение объёмов информации закономерно приводит к проблемам поиска, доступа, категоризации и каталогизации статей и публикаций.

Несмотря на то, что алгоритмами поиска занимаются уже довольно продолжительное время, большинство из них ещё не совершенно. Так, среди представленных на рынке решений немногие позволяют проводить поиск с учётом синонимов и полисемии, а также, что не менее важно, с учётом морфологических особенностей славянских языков.

Анализ основных исследований и публикаций

В данный момент известно несколько основных методик поиска, а также множество их вариаций [1]. Наиболее перспективным на данный момент считается алгоритм латентно-семантического построения индекса LSI/LSA [2]. Он довольно эффективно решает проблему полисемии и синонимов причём независимо от языка. Также существуют модификации этого метода, как например вероятностное латентное семантическое индексирование [1], и алгоритмы кластеризации и автоматической классификации документов в коллекции.

Формулировка цели статьи (постановка задачи). Целью данной работы является проектирование и разработка системы полнотекстового поиска, базирующейся на алгоритме индексирования LSI/LSA, а также подбор и разработка алгоритмов предварительной обработки текста с учётом морфологии кириллических языков.

Основная часть

Построение индекса и последующий поиск в нём выполняется по следующему алгоритму:

- Удаляется форматирование, текст приводится к единной кодировке и единному формату. Особенности форматирования (заголовки, полужирное начертание, ссылки) также могут учитываться при построении индекса;
- Определяется язык текста;
- С учётом языка текста выполняется фильтрация стоп-слов;
- С учётом языка текста выполняется операция стемминга [3], в ходе которой для каждого слова находится его основа;
- Полученные после стемминга основы-термы заносятся в словарь. Ведётся одновременно несколько словарей – общий для всей коллекции и отдельный для каждого документа в ней;
- По полученным словарям производится расчёт взвешенной частоты для каждого слова в коллекции;
- Вычисленные частоты заносятся в матрицу термы/документ;
- Для матрицы производится разложение на сингулярные значения с последующим понижением ранга. Вычисленное сингулярное разложение и будет LSI индексом для заданной коллекции;

Остановимся подробнее на основных моментах описанного выше алгоритма.

Для определения текста используется алгоритм N-Gramm, описанный в работе [4]. Метод основывается на подсчете частот N-грамм (подстрок длины не более N) и предположении, что примерно 300 самых частоиспользуемых N-грамм сильно зависят от языка. Алгоритм метода заключается в нахождении частот N-грамм для всех тестовых документов, для которых известен язык, а также для каждого документа, язык которого пытаемся определить. После этого среди всех тестовых документов находим тот, для которого расстояние от его N-граммной статистики до статистики тестируемого документа минимально. После этого языком теституемого документа считается язык найденного тестового документа.

Расстояние между статистиками подсчитывается следующим образом: все N-граммы сортируются в порядке убывания частоты их появления, затем для кадой N-граммы вычисляется разница её позиций в отсортированном списке N-грамм тестового и тестируемого документов. Расстояние между статистиками определяется как сумма разниц позиций каждой N-граммы.

Значение N предлагается использовать равным 5.

Возможна также фильтрация N-грамм для больших текстов с учётом законов Зипфа, чтобы избежать лексического «мусора».

Также, можно использовать иной способ вычисления расстояния между списками N-грамм. В качестве расстояния между статистиками используется следующая функция определения количества информации:

$$\sum_{i=1}^{M} \log^2\left(\frac{P_i}{Q_i}\right), \qquad (1)$$

где Q_i - частота N-граммы тестируемого документа, а P_i - частота этой же N-граммы в очередном эталонном документе.

Определив таким образом язык текста необходимо выполнить его стемминг. Это позволит заменить все однокоренные слова в тексте корнем и при поиске не различать, например, слова задача и задачи. Для английского языка имеется простая и широко используемая процедура, которая называется алгоритмом Портера (Porter) [5], которая выделяет основы слов с некоторыми погрешностями. Например, слова animal и animation алгоритм Портера преобразует в anim, в результате чего смысл может быть полностью искажен. Однако статистический подход всегда предполагает возможность ошибок при сопоставлении запроса пользователя с документами и предлагает различные меры к их нейтрализации.

В свою очередь, существуют аналогичные операции и для многих других языков, в частности, для русского и украинского языка был предложен алгоритм Стемка [6].

Идея алгоритма в том, что для представления автоматических правил усечения слов была выбрана модель хранения возможного окончания с двумя предшествующими буквами неизменяемой части слова. Так, например, словоформа словарями порождает правило, разрешающее отщепление окончания -ями при условии, что ему предшествует последовательность -ар-. Аналогично, встретив словоформу морями, мы породим правило о возможном отщеплении того же окончания (-ями) при условии, что оно встретилось после фрагмента -ор-.

По результатам тестирования описываемый стеммер показал наиболее корректные в лингвистическом отношении результаты при максимальной полноте и минимальном шуме, то есть количестве неверно выделенных основ.

Теперь построим матрицу частот, необходимую нам для последующего сингулярного разложения. Для этого вычислим для каждого терма каждого документа tf-idf частоту [1].

Значение tf-idf пропорционально частоте появления этого терма в данном документе и обратно пропорционально частоте вхождения терма в коллекцию, из чего следует, что редкие термы имеют большее значение tf-idf, которое отражает их важность.

Исходная матрица частот даёт представление об отношении между термами и документами. Метод Латентного Семантического Анализа преобразовывает их в отношение между термами и концептами(образами) и отношениями между документами и этими же концептами. Таким образом, после применения метода термы и документы становятся выраженными через концепты.

Полученные матрицы концептов дают возможность:

– сравнивать документы в пространстве концептов (кластеризация данных, классификация документов);

– находить отношение между термами (синонимы и полисемия);

– преобразовать поисковый запрос в набор термов, перевести его в пространство концептов и найти релевантные документы (непосредственно поиск).

Как видно из написанного выше, подобное преобразование позволяет до определённой меры решить многие серьёзные задачи (среди которых фундаментальные задачи обработки естественного языка: синонимы и полисемия).

После составления матрицы вхождений LSA понижает ранг матрицы таким образом аппроксимируя её. Можно назвать несколько причин понижения ранга:

- Оригинальная матрица чересчур большая для непосредственных вычислений. С этой точки зрения, аппроксимация матрицы рассматривается как приближение (“необходимое зло”);
- Оригинальная матрица зашумлена. К примеру, в неё включены откровенно бессмысленные документы. С этой точки зрения, аппроксимация матрицы рассматривается как очистка матрицы (лучшая матрица, чем оригинальная);
- Оригинальная матрица чересчур разрежена по сравнению с “настоящей” матрицей документ-терм. Это возможно потому как оригинальная матрица учитывает только слова входящие в каждый документ, в то время, как более интересным была бы матрица, учитывающая все слова, близкие к данному документу (в общем случае, гораздо большее множество ввиду присутствия синонимов).

Таким образом, понижение ранга матрицы приводит к тому, что некоторые её значения «слепливаются»:

$$\{(\text{машина}), (\text{грузовик}), (\text{цветок})\} \rightarrow \{(1.3136*\text{машина} + 0.2783*\text{грузовик}), (\text{цветок})\} \quad (2)$$

Это уменьшает проблему синонимов, так как понижение ранга приводит к тому, что родственные по смыслу термы «слепливаются». Это также помогает решить проблему

с полисемией, так как части слов полисемии «растекаются» в нужных направлениях и объединяются со словами, которые близки им по смыслу.

Как уже было указано выше, для построения такого индекса необходимо выполнить сингулярное разложение матрицы (SVD).

$$\begin{array}{ccccc} & X & & U & \Sigma & V^T \\ & (\mathbf{d}_j) & & & & (\hat{\mathbf{d}}_j) \\ & \downarrow & & & & \downarrow \\ (\mathbf{t}_i^T) \rightarrow & \begin{bmatrix} x_{1,1} & \dots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{m,1} & \dots & x_{m,n} \end{bmatrix} & = & (\hat{\mathbf{t}}_i^T) \rightarrow \begin{bmatrix} \begin{bmatrix} \\ \mathbf{u}_1 \\ \\ \end{bmatrix} & \dots & \begin{bmatrix} \\ \mathbf{u}_l \\ \\ \end{bmatrix} \end{bmatrix} & \cdot \begin{bmatrix} \sigma_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sigma_l \end{bmatrix} & \cdot \begin{bmatrix} [& \mathbf{v}_1 &] \\ & \vdots & \\ [& \mathbf{v}_l &] \end{bmatrix} \end{array} \quad (3)$$

Это разложение имеет следующий вид:

Значения $\sigma_1,\dots,\sigma_l$ называются сингулярными значениями, значения $u_1,\dots,u_l$ и $v_1,\dots,v_l$ называются левыми и правыми сингулярными векторами. Обратите внимание, что часть матрицы U (i-ая строка) относится к t_i. Аналогично и для строк. Это не собственный вектор, но он зависит от всех собственных векторов.

Теперь выберем k наибольших сингулярных значений, и соответствующие им сингулярные векторы из матриц U и V. В результате мы получим апроксимацию ранга k для X, причём с наименьшей ошибкой. Главным свойством этой аппроксимации является не только то, что она даёт наименьшую ошибку, но и то, что она переводит терм-векторы и документ-векторы в пространство концептов. Вектор t_i, состоящий из k значений даёт нам значение терма i для каждого из k концептов. Аналогично, вектор d_j даёт нам отношение документа j для каждого концепта.

Это даёт нам следующие возможности:

- Вычислить, насколько близки документы j и q в пространстве концептов простым сравнением векторов d_i и d_k. Таким образом мы можем кластеризовать документы.
- Аналогично кластеризовать термы в пространстве концептов.
- Рассматривать поисковый запрос как мини-документ, преобразовать его в пространство концептов и найти наиболее релевантные ему документы.

Для выполнения последнего нам нужно преобразовать запрос в пространство концептов аналогично тому, как мы сделали с документами. Рассчитывая угол между вектором концептов запроса и векторами концептов документов можно определить релевантность документа запросу.

На основании полученных результатов и описанных алгоритмов разработана компьютерная программа, позволяющая проводить полнотекстовый поиск в коллекциях документов с учётом особенностей славянских языков.

Выводы

Усовершенствование технологий полнотекстового поиска за счёт применения специальных алгоритмов обработки кириллических текстов позволяет расширить возможности поиска и эффективно решить проблему поиска в больших коллекциях документов.

Литература

1. Foltz, P. W. (1996) Latent Semantic Analysis for text-based research. Behavior Research Methods//Instruments and Computers-1996-№28-p.197-202;
2. Foltz, P. W., Britt, M. A., & Perfetti, C. A. (1996) Reasoning from multiple texts: An automatic analysis of readers' situation models. In G. Cottrell (Ed.) Proceedings of the 18th Annual Cognitive Science Conference. Hillsdale, NJ: Lawrence Erlbaum Associates;

3. Laham, D. Latent Semantic Analysis Approaches to Categorization. In M. G. Shafto & P. Langley (Eds.), Proceedings of the 19th Annual Conference of the Cognitive Science Society. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc. – 1996 – p.979;
4. Foltz, P. W. & Dumais, S. T. (1992). Personalized information delivery: An analysis of information filtering methods.//Communications of the ACM-1992- №35, p.51-60;
5. S. Ortmanns, H. Ney, F. Seide, I. Lindam: A Comparison of Time Conditioned and Word Conditioned Search Techniques for Large Vocabulary Speech Recognition, in International Conference on Spoken Language Processing, Philadelphia, 1996, S. 2091-2094;
6. Mason, O. "Programming for Corpus Linguistics." Edinburgh University Press, 2000. – 568p;
7. ДСТУ 2395-94 Інформація та документація. Обстеження документа, встановлення його предмета та відбір термінів індексування. Загальні вимоги.

УДК 004.77+004.415

Могильный Г.А., Шкандыбин Ю.А.

РАЗРАБОТКА ДОПОЛНИТЕЛЬНОГО КОМПОНЕНТА ДЛЯ АУТЕНТИФИКАЦИИ

В работе описан процесс создания вспомогательного приложения, которое может быть использовано на любых ОС для аутентификации пользователей через SSL соединение.

Современные темпы развития информационных технологий приводят к широкой интеграции различного программного обеспечения на основе интрасетей и Интернет. Это выдвигает дополнительные требования к обеспечению доступа большого числа пользователей к базам данных, документам и различным приложениям интрасети, при обеспечении условий минимизации затрат и угрозы безопасности.

Ограничение доступа обычно выполняется на основе списка пользователей (служб каталогов). В крупных смешанных сетях с различными операционными системами это приводит к появлению нескольких служб каталога, децентрализует управление сетью, вызывает дополнительные затраты на администрирование и обеспечение системы безопасности.

Опыт показывает, что в крупных организациях, имеющих несколько баз пользователей для отдельной авторизации на том или ином приложении неудобно выполнять настройки доступа, поэтому администраторы стараются унифицировать формат хранения соответствующих данных и сделать их доступными для различных сервисов и приложений. В перспективе такое решение может быть использовано как «первый шаг» на пути к организации единого хранилища. Данное решение, не является однократной регистрацией (Single Sign-On, SSO) в полном смысле, так как SSO подразумевает однократное введение пользовательских данных, после чего доступ к ресурсам осуществляется автоматически. Но этот вариант весьма интересен с точки зрения унификации данных при минимальных начальных инвестициях.

Таким образом, целью данной работы является анализ условий создания и разработка дополнительного компонента позволяющего проводить аутентификацию пользователей в гетерогенной сетевой среде на основе единой службы каталогов.

В настоящий момент на рынке сетевых технологий предложено несколько служб, обеспечивающих хранение списков и свойств пользователей. К наиболее распространенным относятся службы каталога AD фирмы Microsoft и eDirectory фирмы Novell [1]. Все эти службы каталогов созданы с одной целью, обеспечить единое место хранения информации о сетевых ресурсах, списках пользователей их свойствах и т.д. Все данные службы поддерживают несколько протоколов и способов аутентификации, однако наиболее широким спектром обладает служба eDirectory. Поэтому при разработке дополнительного компонента учитывались особенности именно этой службы.

Кроме того, предварительный анализ показал, что служба каталога eDirectory может функционировать практически на любой операционной системе, что значительно ра-

сширяет возможности ее использования, служба AD в настоящий момент поддерживается только на операционных системах линейки Windows Server 2000/2003.

В процессе анализа основных структурных элементов дополнительного компонента для авторизации пользователей было выяснено, что все службы каталогов поддерживают протокол LDAP предложенный CCITT (Consultative Committee for International Telegraphy and Telephony).

CCITT разработал серию рекомендаций для создания так называемого сервиса директории или каталога. Каталог, в этом случае, является сервером или распределенным набором серверов, которые поддерживают распределенную базу данных, содержащую информации о различных субъектах, таких как пользователи, устройства и т.п. Эта распределенная база данных называется информационной базой каталога (Directory Information Base – DIB). Информация включает имя субъекта, а также различные атрибуты, характеризующие этот субъект. Данные рекомендации носят название стандарта X.500. Первоначально LDAP начал развиваться как программный продукт переднего плана (front end) для каталога X.500.

LDAP предоставляет большинство возможностей X.500 при существенно меньшей стоимости реализации. Например, удалены избыточные и редко используемые операции. LDAP, в отличие от X.500, использует стек TCP, а не OSI.

Следует заметить, что базовые операции протокола могут выполнять большинство операций сервисов каталога X.500. Однако не существует полного соответствия один-к-одному между операциями протокола LDAP и операциями протокола DAP (Directory Access Protocol) стандарта X.500.

Первая реализация LDAP написана в Мичиганском университете. Общая модель данного протокола состоит в том, что клиент выполняет операции протокола на серверах и передает запрос, описывающий операцию, которая должна быть выполнена сервером. Сервер выполняет необходимые операции в каталоге. После завершения операции (операций) сервер возвращает клиенту ответ, содержащий результаты или ошибки.

Основные причины роста популярности LDAP связаны с тем, что он позволяет быстро отыскивать необходимые данные, поскольку ориентирован в большей степени на чтение и поиск информации, чем на модификацию. Кроме того, LDAP не обязательно должен быть ограничен конкретным сервером, есть возможность организовывать распределенные системы из нескольких серверов. В LDAP предусмотрена возможность создавать ссылки между различными серверами LDAP, что обеспечивает возможность поиска сразу на нескольких серверах LDAP.

Вполне логично, в качестве базового протокола доступа к информации о пользователях использовать протокол LDAP. Однако сам протокол и служба каталогов не предоставляют никаких сервисных услуг по обработке информации и поэтому требуют разработки дополнительных компонентов. Кроме того, более точный анализ показал, что в процессе передачи по сети используются нешифрованные сообщения, что не допустимо с точки зрения системы безопасности. А использование его в открытых сетях (например, Интернет) вообще не целесообразно. Однако данный недостаток может быть сведен к минимуму за счет использования дополнительной поддержки SSL.

В настоящий момент существует несколько вариантов библиотек и программных средств, в которые интегрирована поддержка LDAP поэтому разработку можно выполнять на любом языке программирования. Однако наиболее эффективным и универсальным языком, позволяющим разрабатывать приложения, которые не зависят от операционной системы, является JAVA. Именно данный язык предлагается использовать для создания дополнительного компонента для аутентификации пользователей.

Поскольку использование данного языка позволяет создать компонент, работающий на любой операционной системе, то с позиции его расположения возможны три варианта:

- размещение на отдельном сетевом ресурсе с доступом по сети через протокол TC/IP (рис. 1а);

- размещение на сетевом ресурсе (месте со службой Каталога) с доступом по сети через протокол TC/IP (рис. 1б);

- размещение на каждом вычислительном ресурсе с доступом через консоль или по сети через протокол TC/IP на адрес 127.0.0.1 с ограничением на использование других адресов (рис. 1в).

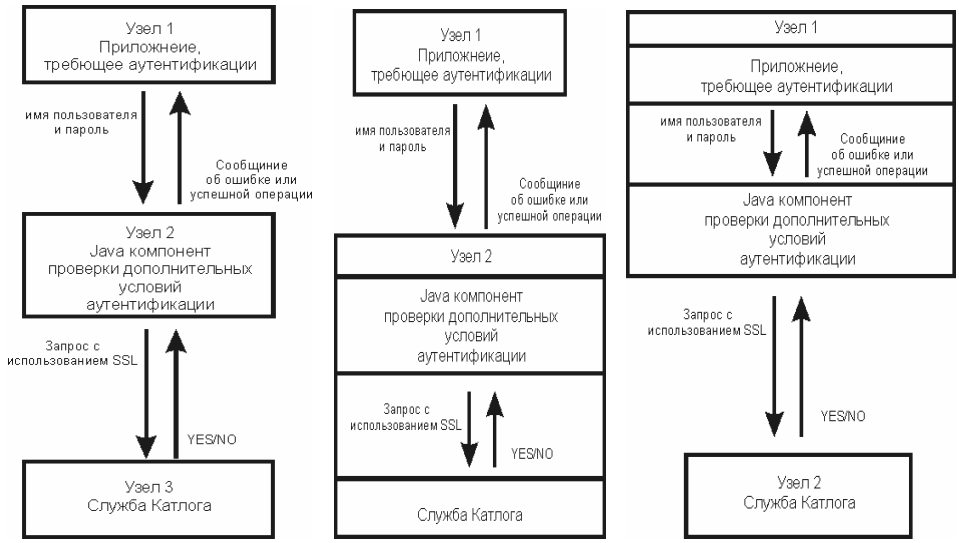


Рис. 1. Схемы размещения приложения.

С целью обеспечения более высокой степени безопасности был выбран третий вариант (рис. 1в).

Однако данный вариант имеет высокую степень децентрализации управления, что снижает его эффективность при использовании однотипных приложений. Этот недостаток устраняется за счет загрузки по сети с использованием SSL файла свойств (property файла). Тогда общая схема работы приложения примет вид, изображенный на рис. 2.

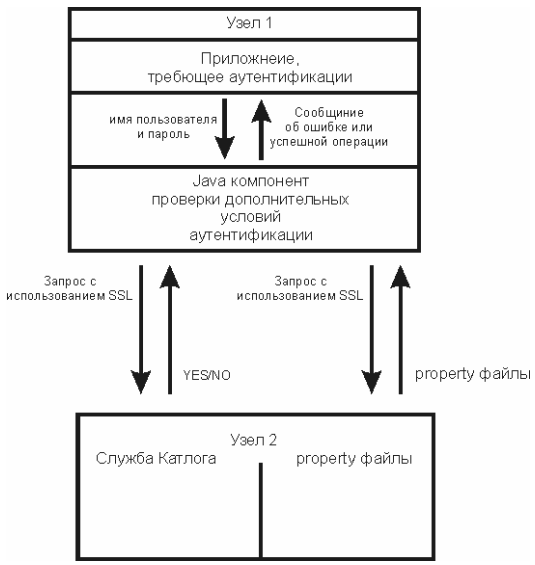


Рис. 2. Принятая схема размещения приложения.

В процессе разработки данного приложения было выяснено, что для использования SSL необходима поддержка специального сертификата. В системе Novell NetWare данный сертификат размещен в каталоге sys:\public и имеет имя RootCert.der. Однако для его использования надо предварительно создать файл «ключа» приложения.

Для этого необходимо воспользоваться специальной утилитой keytool.exe – программой управления ключами и сертификатами, которая входит в состав SDK 1.4. При этом нужно ввести следующую командную строку:

```
keytool.exe  -import -file %1  -keystore sslkey.keystore -alias "type = r.name = sslkey"
```

где %1 - имя файла сертификата сервера (например, RootCert.der)

В процессе выполнения данной команды будет запрос на ввод пароля администратора хранилища «ключа». В результате будет создан файл sslkey.keystore. Именно данный файл необходимо подключать при использовании SSL [5]. Для этого необходимо сначала назначить свойство в значение пути к файлу.

```
System.setProperty("javax.net.ssl.trustStore", st.path);
```

Установить систему безопасности [4].

```
Security.addProvider(new com.sun.net.ssl.internal.ssl.Provider());
LDAPSocketFactory ssf = new LDAPJSSESecureSocketFactory();
LDAPConnection.setSocketFactory(ssf);
```

Создать объект для LDAP соединения, произвести подключение к узлу (st.ldapHost), на котором работает служба каталога, используя порт SSL соединения (st.ldapPort_ssl, обычно 636) и проверить имя пользователя (this.name) и пароль.

```
LDAPConnection lc = new LDAPConnection();
lc.connect(st.ldapHost, st.ldapPort_ssl);
lc.bind(3, this.name, new String(bbp).getBytes("UTF8"));
```

Если пользователя с заданным именем и паролем не существует, то вырабатывается исключительная ситуация LDAPException.

Для проверки других свойств данного пользователя необходимо воспользоваться методами lc.search класса LDAPConnection, а также классом LDAPAttribute для получения значения конкретного атрибута.

Таким образом, используя предложенную схему можно не только проверить имя пользователя и его пароль, но любые другие дополнительные параметры.

Используя данный механизм, было разработано отдельное приложение на языке JAVA. Данное многопоточное приложение принимает запросы от других программных средств с локального узла, проверяет пароль и другие дополнительные свойства данного пользователя (например, принадлежность какой-то группе) и возвращает результат об успехе или неудаче данной проверки.

Дополнительные параметры работы приложения и условия проверки свойств пользователей настраиваются с помощью дополнительного файл свойств (property файла).

В результате проделанной работы были установлены особенности использования программных средств в гетерогенной сетевой среде, проведен анализ различных способов разработки дополнительного приложения аутентификации, предложены варианты его реализации и размещения на основе протокола LDAP с поддержкой SSL. Одна из версий данного приложения используется в Луганском национальном педагогическом университете для интеграции прокси-сервера SQUID [3] и eDirectory фирмы Novell.

Литература

1. Хьюз Джефри Ф., Томас Блейер В. Руководство от Novell. Сети NetWares -М. - Изд. дом "Вильямс", 1999. - 958с;
2. Гаскин Дж. Е. Администрирование Novell NetWare6.0/6.5: Пер. с англ. - СПб.: БХВ - Петербург, 2003 - 1056с;
3. www.squid-cache.org – сайт прокси-сервера SQUID;
4. www.sun.com – сайт разработчиков JAVA;
5. www.osp.ru/lan - В. Шабата «Каталоги LDAP и их применение», LAN #03/2003.

УДК 004.7.056.5

Петров А.С., Минин А.В.

СТЕГАНОГРАФИЯ. МЕТОД LSB ДЛЯ ГРАФИЧЕСКИХ ФАЙЛОВ

Рассматривается применение стеганографии для безопасной передачи информации в графических файлах. В основу взят метод LSB. Проведены исследования для повышения его стегостойкости. Приводится стегоанализ данного метода, и выдвигаются предложения по противодействию наиболее эффективным из известных методов стегоанализа. Предлагаются две модификации исходного метода для изображений, в которых возможно выделение областей монотонной заливки. Показывается, что использование предложенных модификаций значительно повышает стегостойкость.

Введение

Для сокрытия информации методом стеганографии первым делом выбирается тип контейнера. Наиболее удобными в данном случае являются BMP (изображение). Обычно в структуре мультимедийных файлов есть биты, которые слабо влияют на качество изображения или звука и при их изменении общая картина практически не меняется. Например, в звуковых файлах стандарта WAV имеются так называемые «младшие биты», которые, по существу отвечают за самые тихие звуки. Именно эти биты и заменяются на «секретные». Специальные программы внедряют сообщение в тело файла, при этом предлагают дополнительные возможности по шифрованию и сжатию встраиваемой информации, ее защиту с помощью пароля.

Файлы с секретной информацией в нормальных условиях ведут себя также, как и обычные, то есть могут отображаться и воспроизводиться. Для открытия секретных данных пользователь должен знать файл, в котором они находятся, иметь пароль и программу для вскрытия контейнера [1, 2].

В контейнеры можно помещать абсолютно любые данные, начиная от текстовых сообщений и заканчивая музыкой, графикой и анимацией. Внешний файл контейнера является ничем иным как хранилищем, в котором можно разместить все, что угодно.

При этом нужно отметить и тот факт, что любой контейнер можно освобождать от данных и заполнять его заново.

На сегодняшний день наиболее популярным методом сокрытия информации в изображениях является метод LSB (Least Significant Bits) [3, 4]. К существенным недостаткам этого метода можно отнести то, что одна и та же техника внедрения секретной информации применяется без изменений ко всем видам графических изображений, порой даже без предварительного их анализа. Поэтому представляется актуальной задача создания модификации метода LSB, которая бы учитывала структуру скрывающего изображения.

Постановка задачи

В работе рассмотрены две новые методики использования метода LSB, осуществляющие внедрение информации в полном соответствии со структурой скрывающих изображений. Последнее обстоятельство позволяет значительно повысить стегостойкость базового метода к наиболее эффективным методам стегоанализа [5, 6, 7].

Краткие сведения о классическом методе LSB

Метод LSB (Least Significant Bits) или метод замены младших бит был предложен Е. Адельсоном в 1990 г. [3] (см. также [4]). На сегодняшний день он является одним из наиболее широко используемых методов сокрытия информации. Идея метода заключается в замене от одного до четырех младших битов в байтах цветового представления точек исходного изображения битами скрываемого сообщения. Возможность такой замены обусловлена некоторой избыточностью представления цвета и, как отмечается, возможно, случайным поведением младших битов.

Далее мы, в основном, будем оперировать файлами, содержащими изображения в режиме True Color, т.е. полноцветными изображениями, в которых под хранение информации о цвете каждой точки отводится по 3 байта. Каждый из байтов содержит информацию об интенсивности одной из трех составляющих цвета (палитра RGB): красной, синей, зеленой. Так как под хранение каждой из составляющих отводится по одному байту, то соответствующие им интенсивности цветов изменяются в пределах от 0 до 255. Таким образом, общее число возможных цветов равно $256^3 \approx 1.6 \cdot 10^7$. Известно [4], что человеческий глаз способен различить лишь порядка четырех тысяч цветов, а для хранения такого количества достаточно всего четырех бит. При применении метода LSB предполагается, что цвет точки практически в полной мере определяется старшими четырьмя битами каждого из трех байтов представления RGB, а, следовательно, оставшиеся четыре младших бита можно использовать для внедрения скрываемой информации, назовем их стегобитами.

Стегоанализ метода LSB. Рассмотрим метод визуального анализа битовых срезов, приведенный в [5], [4. С.131-133] и [6]. Он заключается в том, что с помощью несложной программы изображение просматривают по слоям, т.е. берутся битовые срезы изображения. Учитывая то, что интенсивность каждого цвета определяется ровно одним байтом, всего необходимо будет просмотреть 8 таких срезов. Для каждого из трех цветов первый срез – это изображение, построенное самыми младшими битами, второй срез – изображение, построенное вторыми битами и т.д. Для большей четкости битового среза в те байты, в срезе которых стоит единица, заносят максимальное значение (255). Далее полученное изображение битового среза просматривают и визуально сравнивают с исходным изображением. На рис.1 приведен пример подобного анализа.

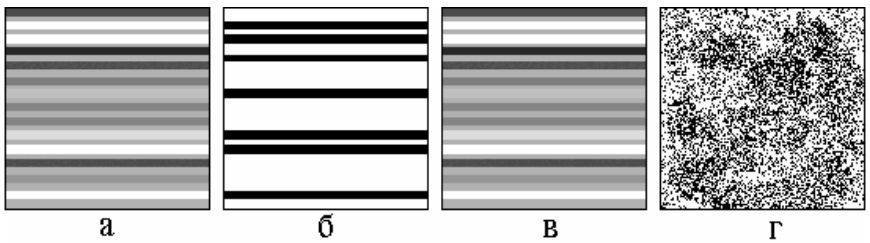


Рис. 1. Сравнение битовых срезов: а – исходное изображение; б – битовый срез по последнему биту; в – изображение с внедренным в последние биты сообщением; г – битовый срез полученного изображения.

Как видно из примера, здесь нарушается предположение о том, что младшие биты всегда случайны. Более того, между младшими битами существуют некоторые закономерности, и их поведение вовсе непохоже на случайное, а изображение, построенное ими, на шум. Так, в результате проведенного нами анализа более четырех сотен изображений выяснилось, что в изображениях очень часто встречаются длинные серии из одинаковых бит и практически любое изображение содержит серию минимум из 14 одинаковых бит. В случае, если в младшие биты изображения происходит внедрение информации, эти закономерности нарушаются.

Следует также учесть и тот факт, что в отличие от изображений, другие данные, которые могут оказаться внедряемыми сообщениями, не содержат столь длинных серий из одинаковых бит. Кроме того, довольно часто внедрение сообщений в изображения осуще-

ствляется побайтно. При таком способе внедрения длинные серии могут получиться только в случае, если сообщение содержит рядом расположенные байты, равные 0 или 255. Однако практически всегда до встраивания сообщения в контейнер проводится его предварительное шифрование и (или) сжатие. В результате сообщение представляет собой нечто похожее на случайную последовательность бит. Как следствие, в срезе, в который внедряется полученное в результате шифрования и (или) сжатия сообщение, число длинных серий, равно как и их длина, сильно сокращается. На этом факте основывается и целый ряд методов статистического стегоанализа. Мы не будем подробно рассматривать эти методы, так как в их основе лежит уже рассмотренный нами принцип и большинство из них достаточно хорошо описаны в [4, 6].

Уточнение местоположения и числа стегобит. Исследования в области особенностей человеческого зрения [7] показали, что порог чувствительности глаза к изменению освещенности при средних ее значениях составляет $\Delta I = 0.01 - 0.03I$ или 1~3% (рис.2). Заметим, что использование для внедрения информации четырех младших разрядов в байтах исходного изображения может привести к изменению интенсивности порядка 6%, что в два раза превышает порог чувствительности человеческого глаза.

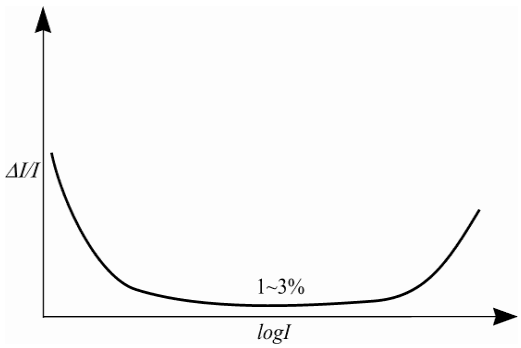


Рис. 2. Порог чувствительности человеческого глаза.

Проведенные нами исследования подтвердили, что замена не четырех, а даже трех младших битов (~3%) вносит заметные для человеческого глаза искажения. Изменение же яркости в пределах 1–1,5% в действительности оказалось незаметным. Следовательно, для того чтобы внедрение в изображение дополнительной информации оказалось незаметным для человеческого глаза, наиболее оптимальным будет подвергнуть модификации либо первый и второй разряды (максимальное искажение 1,17%), либо только третий разряд (искажение 1,56%) каждого из трех байтов, отвечающих за цвет точки.

Модификация метода LSB для изображений, содержащих области монотонной заливки большой площади. Наиболее эффективным методом стегоанализа изображений рассматриваемого типа является метод визуального анализа битовых срезов. Его основная идея заключается в сравнении изображения в целом с изображениями его битовых срезов. То есть человек сначала смотрит на изображение, отмечает для себя некоторые элементы этого изображения и пытается сопоставить их с элементами изображения конкретного битового среза. Так, в случае, если изображение содержит большие области, закрашенные одним цветом, то человек пытается найти соответствующие области и на срезе. И если на срезе человек видит ту же область, что и на исходном изображении, но разбитую на множество белых и черных точек, то у него возникают вполне обоснованные подозрения. Однако, в случае, если вся область целиком будет залита либо черным, либо белым цветом, никаких подозрений не возникнет. Дело в том, что человек, проводящий анализ, не знает, каков был исходный цвет той или иной области. Не зная исходного цвета точек области, нельзя определить и значение соответствующего бита в цветовом представлении. А не зная значения этого бита, нельзя ничего сказать и о цвете области на битовом срезе. Последнее наглядно показано на рис.3.

Из всего описанного выше можно сделать вывод о том, что внедрять информацию в изображение, содержащее области монотонной заливки, желательно сохраняя эти области. То есть, если нам необходимо внести изменение в биты одной из точек некоторой области, то точно такие же изменения нужно внести и во все оставшиеся точки той же области. Что касается выделения монотонных областей, то для этой цели можно использовать старшие разряды, которые не используются для сокрытия информации. Так как они не подвергаются изменению, то области, выделенные кодером, могут быть однозначно определены и декодером, т.е. исключается вероятность неоднозначного извлечения информации. В качестве алгоритма, отвечающего за выделение областей, рекомендуется использовать алгоритм выделения четырехсвязной области.

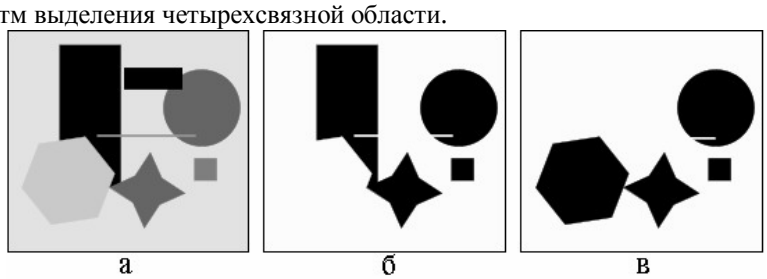


Рис. 3. Возможные битовые срезы: а – исходное изображение; б – битовый срез изображения, не содержащего дополнительной информации; в – возможный битовый срез при внедрении сообщения 01101100.

Теперь постараемся определить, в каких именно битах наиболее целесообразно производить сокрытие информации. Ранее отмечалось, что для незаметного для человеческого глаза внедрения информации можно использовать либо два младших бита, либо только третий бит. Однако отметим тот факт, что противник не располагает исходным изображением (пустым контейнером), в противном случае стегоанализ любой стегосистемы становится тривиальным. Если также учесть и то, что изображение не содержит плавных переходов цветов, то в качестве стегобит можно смело выделить все три последних бита. Возможное максимальное изменение интенсивности исходного цвета в этом случае будет порядка 3%. Хотя подобное отклонение и находится на пороге чувствительности человеческого глаза и может быть обнаружено при сопоставлении цветов, в данном случае оно будет незаметно, так как изменению будет подвергаться целая область, и противнику будет просто не с чем сравнивать. Что же касается требования отсутствия плавных переходов цветов, то в этом случае оно обязательно, так как именно последние биты и отвечают за плавное изменение цвета.

Отметим, что для упрощения программной реализации желательно использовать не все 9 возможных бит (по три младших бита каждой составляющей цвета), а лишь восемь из них. Это даст возможность не разбивать сообщения на биты, а производить внедрение сообщений побайтно. То есть, в каждую точку, вернее область изображения, будет внедряться ровно один байт сообщения. Предлагается в байтах, отвечающих за интенсивность красного и синего цветов, для внедрения сообщения использовать по три бита, а в байте, отвечающем за интенсивность зеленого, два бита. При этом, как оказалось, желательно выделять не два последних бита, а последний и третий биты. Выбор зеленой составляющей под внедрение двух, а не трех бит обусловлен большей чувствительностью человеческого глаза именно к зеленому диапазону видимого спектра. Что же касается выделения именно первого и третьего бита, то это позволяет получить наибольшую точность выделения границ монотонных областей.

В заключение отметим, что этот метод обладает высокой стойкостью не только против метода визуального анализа битовых срезов, но и против статистических методов стегоанализа. Последнее обусловлено, прежде всего, тем, что не нарушается естественность контейнера. Битовые срезы, по которым возможно проведение статистического анализа, содержат в большом числе длинные последовательности, и число переходов от нуля к единице и от единицы к нулю находится в допустимом диапазоне.

Модификация метода LSB для изображений, содержащих области монотонной заливки и плавные переходы цветов. В случае использования предыдущего метода для строго определенных типов изображений он дает достаточно хорошие результаты, но в случае, если изображение обладает плавными переходами цветов, его использование нежелательно. Дело в том, что в описанном методе выделение областей осуществляется по старшим разрядам байтов представления цвета. А если учесть то, что за плавные переходы цветов отвечают младшие биты, безжалостно затираемые сообщением, то в результате плавные переходы цветов в изображениях исчезают. Как следствие, появляется возможность обнаружить факт внедрения посторонней информации даже визуально, хотя реально это отмечено лишь для небольшого числа изображений. При анализе гистограммы на ней также выделяются характерные всплески. Причина всплесков – увеличение размеров предполагаемых областей монотонной заливки за счет захвата соседних, незначительно отличающихся по цвету, областей. Устранить указанный недостаток можно за счет более точного выделения областей.

По результатам проведенного сравнительного анализа было выявлено, что наибольшая точность выделения областей обеспечивается при использовании маски FB (11111011). То есть в том случае, когда под скрываемое сообщение выделяются только третьи биты, а все остальные используются для определения границ областей. Точность выделения областей монотонной заливки в данном случае составляет 0,9952, а возможное искажение исходной интенсивности цветов не превышает 1,56%. Для выделения областей при внедрении информации также рекомендуется использовать метод заливки четырехсвязной области.

Таким образом, данная модификация основана на тех же принципах, что и предыдущая, но лишена ряда недостатков, связанных с использованием в качестве контейнеров изображений, содержащих как области монотонной заливки, так и плавные переходы цветов. Данный метод также весьма стоек к различным методам стегоанализа и может использоваться со всеми форматами графических файлов, не производящих сжатие изображений с потерей качества.

Выводы. В данной статье представлены две новые методики сокрытия информации в изображениях, основанные на методе LSB. Их отличительной особенностью является то, что внедрение информации осуществляется в соответствии со структурой используемых в качестве контейнеров изображений. Одна методика предназначена для работы с изображениями, содержащими обширные области монотонной заливки, вторая – для работы с изображениями, содержащими как области монотонной заливки, так и области с плавными переходами цветов. Использование предложенных методик позволяет значительно повысить стегостойкость базового метода.

Литература

1. Генне О. В. Основные положения стеганографии // Защита информации. Конфидент. – 2002. – №3. – С.20-24;
2. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с;
3. E. Adelson: Digital Signal Encoding and Decoding Apparatus. – U.S. Patent. – No. 4,939515 (1990);
4. Кустов В. Н., Федчук А. А. Методы встраивания скрытых сообщений // Защита информации. Конфидент. – 2002. – №3. – С.34-37;
5. Andreas W., Andreas P. Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools — and Some Lessons Learned / Proceedings of the Workshop on Information Hiding, 1999. PP. 61-76;
6. Johnson N.F., Jajodia S. Steganalysis of Images Created Using Current Steganography Software / Proceeding of 2nd Workshop on Information Hiding // Lecture Notes in Computer Science, Springer, 1998. Vol. 1525. PP. 273-289;
7. Girod B. The information theoretical significance of spatial and temporal masking in video signals / Proceedings of the SPIE Symposium on Electronic Imaging, 1989. Vol. 1077. PP. 178-187.

УДК 681.32(075)

Дубровкина М. В.

КОМПЛЕКС ИДЕНТИФИКАЦИИ И КОНТРОЛЯ ИЗДЕЛИЙ ДЛЯ АСУ ТП КОЖЕВЕННОГО ПРОИЗВОДСТВА.

В статье представлены результаты по разработке комплекса идентификации и контроля изделий для АСУ ТП обработки кожи. При разработке комплекса исследуется процесс обработки кожи, выбирается наилучший метод маркировки кожи, разрабатывается метод считывания кода, разрабатываются основные составляющие комплекса.

Одним из наиболее важных факторов, влияющих на спрос продукции, является её качество, что обуславливает необходимость постоянного контроля качества продукции на всех этапах технологического процесса. Особенность технологического процесса кожевенного производства состоит в том, что в процессе технологической обработки каждое изделие (в соответствии с маршрутной картой техпроцесса) попадает в различные партии. Следовательно, для того чтобы обеспечить высокое качество изготавливаемой продукции, необходимо отследить качество сырья и работу всех звеньев производства, что обеспечивается однозначной идентификацией изделий на каждом этапе обработки.

Таким образом, разработка комплекса идентификации и контроля изделия, позволяющей отслеживать работу поставщиков сырья и работников производства и тем самым влиять на повышение качества продукции в процессе её изготовления, является весьма актуальной.

Цель: Разработать комплекс идентификации и контроля изделия для кожевенного производства.

Для достижения поставленной цели необходимо решить следующие основные задачи:

1. рассмотреть процесс обработки кож на кожевенном заводе с целью определения мест установки основных составляющих комплекса;
2. рассмотреть существующие методы маркировки кожи, выбрать наилучший метод;
3. разработать метод считывания кода с последующим его распознаванием;
4. разработать комплекс идентификации и контроля кожи, состоящий из устройства нанесения кода и устройства считывания кода.

Рассмотрим процесс обработки кожи и определим места установки основных составляющих комплекса: устройств нанесения и считывания кода, объем информации, которая должна быть в БД АСУ предприятия, обеспечивающая последующий анализ эффективности производства, выявления его «узких мест».

Важным фактором, влияющим на рациональное использование натуральный кож, является сорт [1].

На кожевенном заводе пять сортировок.

Первая сортировка – на кожсырьевом заводе, сортировка кож на производственные партии по целевому назначению, для обеспечения однородного характера их обработки, упорядочение учета. На данном этапе в базу данных заносится: дата, номер партии, поставщик, сортировщик, вес, сорт, группа сырья, вид сырья, развес, съем, консервирование, основные дефекты.

Вторая сортировка проводится в дубильном цехе после отжима вет-блу – это сортировка в «целых», при которой вводится новая информация: сорт полуфабриката, пороки, как ранее скрытые, так и технологические, вес и площадь полуфабриката. При данной сортировке происходит распределение полученных партий на два направления: продажа или дальнейшая обработка. На данной сортировке необходимо считывать нанесенный код, чтобы определить качество работы поставщиков, а так же, благодаря маркировке, точный выход полуфабриката по каждой коже.

Третья сортировка – сортировка в половинках, позволяет отследить качество работы механической обработки кож (двоение, строжка). При двоении кожа распиливается по толщине. В результате получается лицевой и бахтармяный спилок. Бахтармяный спилок формируется в отдельную партию. Наиболее часто возникающие при двоении и строжке дефекты - это неравномерное двоение, несоответствие толщины полуфабриката заданной. Считывание кода на данной сортировке оправданно при необходимости проведения анализа работы рабочих занятых механической обработкой кожи.

Четвертая сортировка – это сортировка краста, на которой, как правило, окончательно определяется сорт продукта. Полученная на данной сортировке информация позволяет проанализировать работу на предыдущих участках техпроцесса.

Пятая сортировка – это сортировка готовой кожи. На данной сортировке определяется не только сорт готовой продукции, но и ее площадь. Считывание кода на данной сортировке позволяет провести анализ работы предыдущих звеньев производства, определить удельные показатели работы предприятия - выход готовой кожи (отношение количества готовой кожи к массе сырья). [2]

Очевидно, что именно на этапах сортировки будут устанавливаться устройства нанесения и считывания кода. Потому что, во-первых, это места, в которых появляется одна из основных характеристик сырья, полуфабриката и готовой кожи – сорт, а в некоторых - их вес и площадь; во-вторых, это точки ввода информации в БД АСУ предприятия о перерабатываемых партиях; в-третьих, это места формирования новых партий.

Таблица 1.

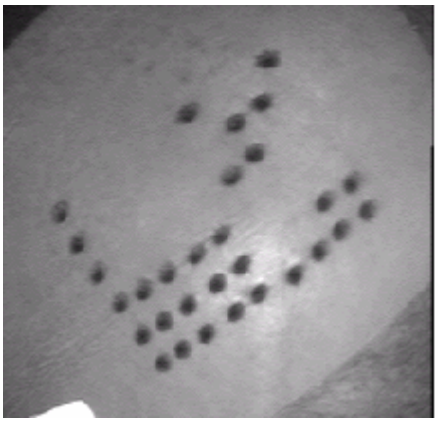
Сравнение различных методов нанесения кода

	Бирки с кодом	Электронный чип	Маркировка поверхности	Нанесение отверстий
Отсутствие средства крепления	НЕТ	НЕТ	ДА	ДА
Устойчивость к процессам обработки кожи	НЕТ	НЕТ	ДА	ДА
Четкое отображение и чтение	ДА	НЕТ	ДА	ДА
Остается ли после строжки и двоения	НЕТ	НЕТ	НЕТ	ДА
Считывание компьютером	ДА	ДА	НЕТ	ДА
Компьютерная маркировка	ДА	ДА	ДА	ДА
Секретность кодирования	ДА	ДА	НЕТ	ДА
Небольшая стоимость	ДА	НЕТ	ДА	ДА
Кодирование от шкуры до готовой кожи	НЕТ	НЕТ	НЕТ	ДА
Кодирование купленной партии	НЕТ	НЕТ	НЕТ	ДА

Метод маркировки кожи выбираем на основе проведенного анализа различных способов. В силу особенностей технологии кожевенного производства (в процессе обработки кожа подвергается различного рода химическим и механическим воздействиям) наиболее надежным маркером, сохраняющимся при проведении всех технологических операций, является сквозное отверстие. Выбранный метод маркировки обеспечивает неизменность кода при прохождении всех этапов обработки кожи (см. табл. 1). [3]

Исходя из реальных объемов производства на кожевенном заводе и кодируемой информации, в качестве наиболее надежного выбираем метод маркировки нанесением отверстий в виде двухмерной прямоугольной матрицы размерностью 6 на 9, в которой отверстия используются как метки (рис.1). Код должен считываться с обеих сторон шкуры

при любом её положении, поэтому крайний столбец по вертикали и крайний ряд по горизонтали выполнены сплошными и являются базовыми при распознавании кода. В каждом информационном столбце (а их у нас семь) пробиваются два отверстия (если не учитывать отверстие, расположенное в базовой строке). Место расположения этих двух информационных отверстий при считывании и распознавании соответствует цифре кода. Последний столбец - проверочный. В нем отверстия будут располагаться в тех строках, в которых информационных отверстий нечетное количество. В итоге, во всех строках (без учета отверстий базового столбца) будет получено четное количество отверстий.



Считан	Время	Код
Да	1.370	00008723

Рис. 1. Пример изображения маркировки и его считанный код.

Для считывания кода применим оптоэлектронный метод. Основные его достоинства: широкий круг материалов, универсальность, можно легко автоматизировать процесс, быстродействие, возможна передача информации одновременно на несколько устройств контроля, «картинка» легко преобразуется в цифровой код. А основной недостаток этого метода – зависимость результата от присутствия помех (посторонний свет, загрязнения поверхности, в которой нанесен код и др.) можно устранить.

Рассмотрим кратко принцип действия устройства считывания.

Телевизионное изображение участка кожи с маркировкой передается в память компьютера для дальнейшей обработки. Признаками отверстий как объектов изображения являются яркость и размер пятна, регулярность расположения. Автоматизированное распознавание кода сводится к решению следующих задач:

– выделение отверстий на фоне помех;

– определение матрицы отверстий, выявление базовых рядов матрицы;

– определение положения информационных отверстий в каждом ряду;

– декодирование информации.

На основе выбранного метода маркировки и исследования реального кожевенного производства разработаем комплекс, позволяющий автоматически наносить на поступающее в переработку сырьё код в виде матрицы отверстий и считывать его с полуфабриката и готовой кожи с последующим распознаванием кода и передачей его в АСУ предприятия.

Комплекс маркировки кожи состоит из устройства нанесения и устройства считывания кода.

Устройство нанесения кода состоит из перфоратора, интерфейсного блока и компьютера. Схема его размещения в цепи сортировки кож приведена на рис.2.

Маркировка производится следующим образом: оператор вносит в компьютер информацию по каждой коже (поставщик, сорт, масса, код сортировщика и т.п.), компьютер автоматически присваивает каждой коже номер, который передается в интерфейсный блок, затем вырабатывает команды для перфоратора для нанесения кода.

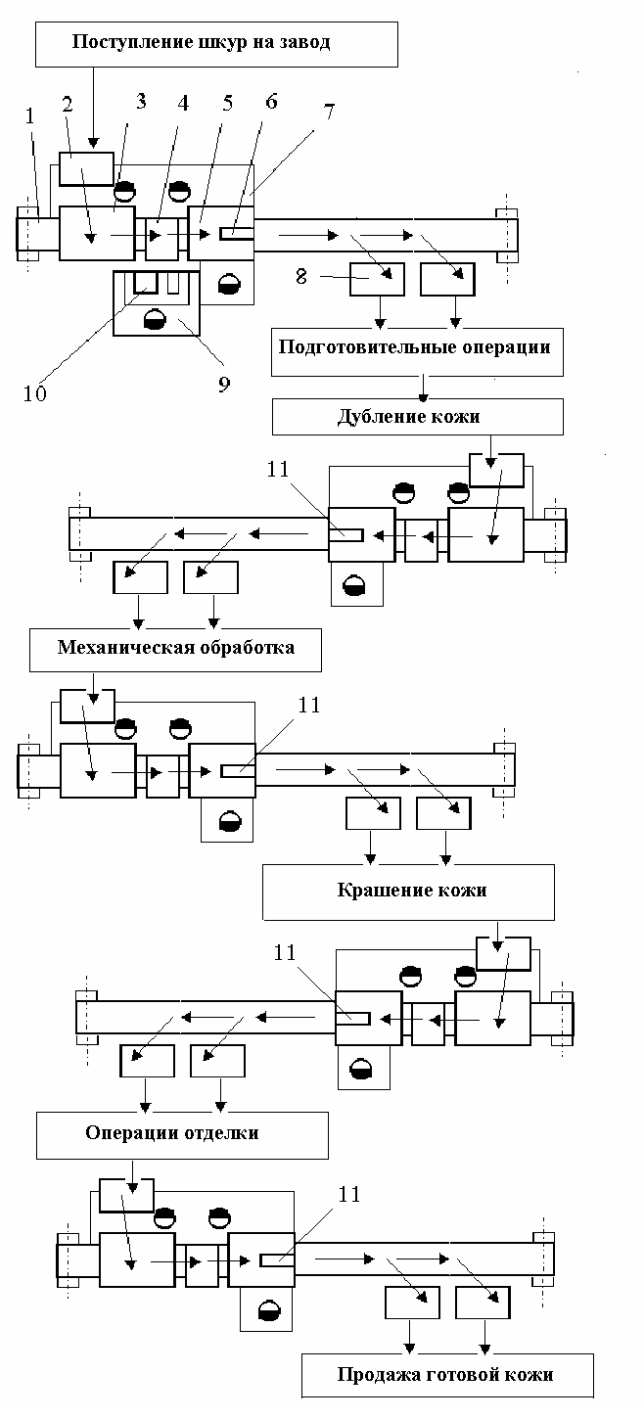


Рис. 2. Размещение устройства нанесения кода и устройства считывания кода в цепи сортировки кож:
1-ленточный конвейер; 2-поддон с кожей; 3-стол сортировщика;4-весы; 5-рабочий стол; 6-устройство нанесения кода;7-площадка обслуживания; 8-поддоны для отсортированных кож; 9-рабочее место оператора; 10-компьютер, 11- устройство нанесения.

Промаркированные кожи, рассортированные по партиям, поступают на обработку.

Считывание кодов осуществляется с использованием устройства считывания кода, которое при помощи интерфейсного блока подсоединяется к компьютеру.

Возможно подключение нескольких считывающих устройств, которые работают в параллельных технологических цепях, к одному компьютеру.

Схема размещения устройств считывания в цепи сортировки кож приведена на рис.2.

Считывание кода осуществляется после определения сорта, массы и площади кожи. Каждое из считывающих устройств устанавливается на перфорированный код и включается. Затем интерфейсный блок по очереди (в случае совпадений по времени работы считывающих устройств) получает информацию с телекамеры и передает ее через интерфейсный блок в компьютер. В компьютере информация обрабатывается и расшифровывается считанный код, дополнительно в компьютер с клавиатуры компьютера или считывающего устройства вносятся данные, полученные при сортировке кожи: сорт, масса и площадь. [3]

Выводы

В результате был разработан комплекс идентификации и контроля изделия для кожевенного производства, который обеспечивает нанесение кода на кожу, введение этого кода в базу данных (БД), считывание этого кода с полуфабрикатов и готовой кожи в процессе ее производства, введение в БД сведений по вновь приобретенным параметрам обрабатываемого изделия. Это позволяет отследить качество сырья и работу всех звеньев производства и в результате обеспечить высокое качество изготавливаемой продукции.

Разработанный комплекс может быть использован для учета и контроля изделий в различных отраслях промышленности.

Литература

1. Технология одежды из кожи: Учебное пособие / Л. А. Бекмурзаев, В. Ф. Водорезова, Е. И. Шайкевич – М.: Форум: ИНФРА, 2004. – 144 с;
2. Вопросы внедрения системы маркировки шкур./ Анчиполовский Б. Л., Хмеленко Н. Г.; НИПКИ «Искра». – Луганск, 2004. – 6с. Рус. – Деп. в ГНТБ Украины 15.12.04, № 76 – Ук 2004;
3. Методы кодирования в задачах маркировки кожевенного сырья./ Литвин В. П., Анчиполовский Б. Л.; НИПКИ «Искра». – Луганск, 2004. – 4с. Рус. – Деп. в ГНТБ Украины 15.12.04, № 75 – Ук 2004.

УДК 004.056

Соловьев В.И., Командина Т.В.

ЗАЩИТА “ОТ ИНФОРМАЦИИ” В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В статье исследована проблема эффективности больших информационных систем, предложена методика, позволяющая перевести такую систему в более устойчивое состояние и существенно снизить затраты на ее сопровождение.

На современном этапе развития информационных технологий внедрение и сопровождение больших систем требует серьезных финансовых затрат. Кроме стоимости самой системы, Заказчик оплачивает ее поддержку и сопровождение. Ежегодная сумма этих затрат составляет 25-30% от стоимости системы. То есть каждые три-четыре года к стоимости системы добавляется, как минимум, 100% от ее первоначальной стоимости. Это общемировая практика, и Украина не является исключением. Возникает вопрос: как повысить эффективность современных информационных систем с точки зрения соотношения эффективность – стоимость.

В течение последних трех лет с этой целью был произведен анализ функционирования и сопровождения полностью идентичных больших информационных систем на по-

лутора десятках предприятиях. Это – информационные системы бюро технических инвентаризаций Украины, а также другие большие информационные системы.

В результате этого исследования установлено: разработчики при сопровождении больших систем после небольшого переходного периода внедрения заняты в 90% случаев и более выявлением и устранением ошибок ввода информации, которые при компьютерном документообороте приводят к существенным негативным последствиям. Итак, задача фактически сводится к тому, как оценить и снизить количество таких ошибок.

Задача оценки количества ошибок ввода требует выбора критерия, что является само по себе неформальной задачей. В качестве ошибки ввода была принята наиболее простая мера ошибки – любой ошибочно (или неверно) введенный символ.

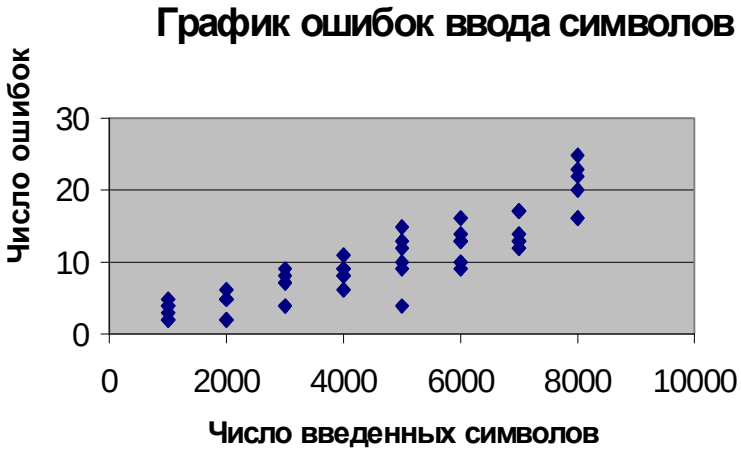


Рис.1. Зависимость числа ошибок от количества введенных символов.

Обработка большого статистического материала работы пользователей с разнообразными формами позволила в первом приближении оценить зависимость числа ошибок ввода от числа вводимых символов (рис.1). В этой зависимости не учитывается скорость ввода различных пользователей и другие возможные и необходимые дифференциации зависимостей. Фактически зависимость характеризует среднестатистическое количество ошибок ввода для среднестатистического пользователя в конкретной информационной системе и т. д.

Основным последствием ошибок ввода является потеря работоспособности системы. Это проявляется в виде явно неверных статистических отчетов в системе, которые визуально наблюдают Пользователи, невыполнении балансов, в ряде случаев – полной потере работоспособности и отсутствии возможности эксплуатации системы. Пользователи системы в большинстве случаев не в состоянии своими силами выявить причину неработоспособности системы. Они вынуждены сплошь и рядом обращаться к разработчикам.

Системы, в которых удается уменьшить число ошибок ввода до определенного уровня, становятся гораздо более устойчивыми в работе, т.о. требуя меньших затрат на их сопровождение.

На рис.2 представлен график зависимости человеко-часов затрачиваемых предприятием, сопровождающем однотипные промышленные системы от числа ошибок ввода на килобайт информации баз данных. Эти данные были получены в процессе длительного совершенствования и эволюции одной и той же системы. При этом существенно уменьшалось число ошибок ввода информации за счет программных и методических средств.

С точки зрения финансовых затрат на сопровождение очевидно, что они растут при росте ошибок на килобайт информации.

Система становится достаточно эффективной с финансовой точки зрения при сопровождении для Заказчика, если число ошибок ввода на килобайт информации падает до

0,5-0,6 ошибок ввода на один килобайт информации. При этом стоимость сопровождения такой системы падает до 5 % (и менее) в год от стоимости самой системы.

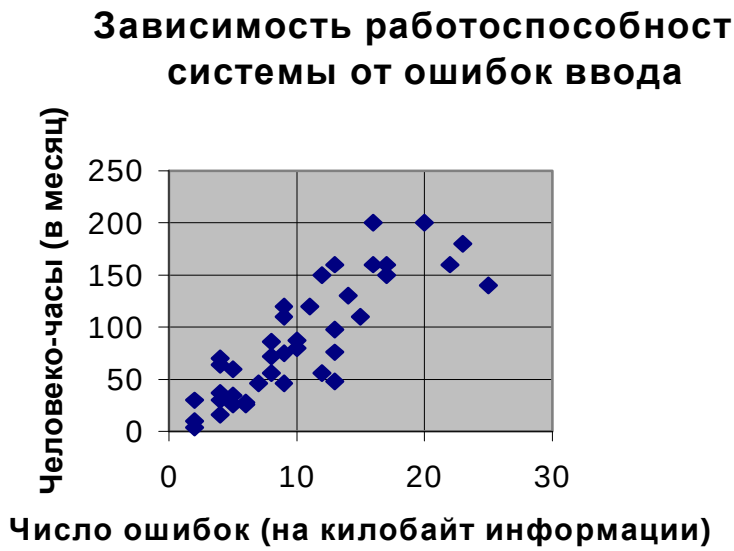


Рис. 2. Зависимость работоспособности системы от ошибок ввода.

Анализ различных типов ошибок позволил сгруппировать основные типы ошибок, которые оказывают наиболее существенное влияние на устойчивость систем всего в два типа.

Первый тип – это обычные символьные ошибки ввода. Второй тип – это так называемые числовые ошибки, связанные с различными числовыми балансами.

Основная причина большого количества ошибок ввода данных в современных информационных системах, как показывает анализ, является чисто научно-технической. Как правило, разработчики не придерживаются при разработке систем в реляционных базах данных базовых требований к разработке сформулированных Кодом [1] (основоположником теоретических аспектов баз данных). Это касается, в первую очередь, символьных ошибок ввода.

Первое, что обязательно необходимо делать в реляционных системах для резкого снижения ошибок ввода – выносить любую справочную информацию в справочники-словари (даже если они весьма небольшие). Пользователь Заказчика в этом случае резко ограничен в возможности ошибки, влияющей на работоспособность системы. А если даже допускает ее, то сам быстро исправляет. Последовательное применение этого требования уменьшает число ошибок в несколько раз, и как следствие, делает систему гораздо более устойчивой и работоспособной.

Вторая наиболее трудноразрешимая проблема ошибок ввода – числовые ошибки ввода, существенно влияющие на различные балансы. За редким исключением, в больших системах отсутствуют специальные программные средства для контроля над ошибками подобного рода в силу сложной реализации.

Наиболее распространенная числовая ошибка связана с так называемой проблемой округления и проблемой сохранения различных балансов.

Так, например, типичная задача, которая возникает при бухгалтерском и складском учете (но не только!!) следующая: необходимо рассчитать средневзвешенную (или среднеарифметическую) цену, которая постоянно изменяется во времени

$$\tilde{N}\tilde{n}\eth = \sum_{i=1}^{k} (\grave{a}_i * n_i) / m ,$$

где $\tilde{N}\tilde{n}\eth$ – средняя цена, $\grave{a}_i$ - цены партии изделия, n_i - количество изделий в партии, m – общее количество изделий.

Цена неизбежно округляется (другого не дано) до второго знака после запятой.

При дальнейшем использовании этой цены в расчетах накапливаются ошибки. При интегральных расчетах за месяц или большой период, естественным образом не бьются балансы.

Другой пример: на предприятие присылается по договору определенная сумма денег, и на эту сумму необходимо отгрузить различный ассортимент продукции по различной стоимости. Сотрудники предприятия должны добиться согласования в документах общей суммы и общей стоимости продукции.

Все подобные примеры сводятся к чисто математической проблеме решения Диофантова уравнения в целых числах.

$$M = \sum_{i=1}^{k} (a_i * n_i),$$

где M , a_i - заданные целые числа, n_i - неизвестные целые числа, которые удовлетворяют уравнения.

Известно, что в общем случае эта задача неразрешима строго математически.

Практически в любой бухгалтерской системе и системе автоматизации складского учета приходится реализовывать округление до определенного знака в процессе функционирования системы. Затем эта неизбежная операция сказывается на интегральных балансах предприятия. Причем, ошибки округления накапливаются за счет большой статистики.

Большинство же задач “подгонки баланса” имеют приближенное решение, достаточное для практики. Как правило, эти методы решения базируются на различных эвристических соображениях и требуют весьма трудоемких расчетов.

Программная реализация подобных методов существенно повышает эффективность функционирования систем.

Учет и решение перечисленных проблем в современных информационных системах, связанных с ошибками ввода, позволяет перевести их работу в существенно более устойчивое состояние.

Итак, современные большие информационные системы малоэффективны с точки зрения соотношения цена + цена сопровождения = эффективность.

Основная причина сравнительно низкой эффективности – неизбежные ошибки ввода информации.

Основными массовыми ошибками ввода, оказывающими самое существенное влияние на эффективность систем – стандартная символьная ошибка при наборе текста и числовые ошибки ввода, связанные с требованиями соблюдения самых различных балансов.

Для устранения массовых символьных ошибок необходимо максимизировать в системе применение справочников-словарей.

Для устранения числовых балансовых ошибок необходимы специализированные программные помощники, встроенные в системы.

Решение проблем указанных двух типов ошибок, по-видимому, позволяет перевести большую информационную систему в более устойчивое состояние и существенно снизить затраты на её сопровождение.

Литература

1. Т. Коннолли, К. Бегг, Базы данных, М., 2000 г., 1110 с.

УДК 681.3.07

Клюев С.А., Спирягин В.И., Спирягин М.И.

ИССЛЕДОВАНИЕ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СИСТЕМЫ ПЛАТФОРМЫ JAVACARD

В данной статье рассмотрены мероприятия по обеспечению безопасности на JavaCard платформе.

Механизм безопасности JavaCard

Текущая архитектура безопасности для смарт-карт имеет три центральных механизма, эти функции безопасности, необходимые, чтобы предотвратить логические нападения: межсетевой экран, верификация кода байта, формализация кода байта.

Прикладная платформа, которая развивается, формальная модель защиты, которая используется в Java Card технологии, как одна из тех, которая определяется временами выполнение в среде смарт-карты, то есть здесь учитывается память, связь, защита и прикладное выполнение дополнений на смарт-карте. JCRE (Java card runtime environment - JavaCard среда выполнения) отвечает смарт-карте, работающей со стандартом ISO 7816. Дополнения, разработанные на платформе Java Card, имеют очень небольшой программный код. Java Virtual Machine (JVM) - Java виртуальная машина, интерпретирует независимый от виртуальной машины байт-код, который сохраняется в ROM (Read Only Memory) памяти смарт-карты. Преимущество независимой от машины кода есть то, что дополнения могут быть разработаны и работать независимо от архитектуры смарт-карты и вычислительного устройства смарт-карты. Кроме того, этот код является переносным. Условия выполнения Java Card (JCRE) состоят из компонентов системы Java Card, которая работает на смарт-карте. JCRE отвечает за управление ресурсами карты, сетевую связь, выполнение апплета на смарт-карте и обеспечивает систему защиты апплета. Таким образом JCRE служит операционной системой смарт-карт. Как показано на рис.1 среда выполнения JavaCard находится на верхнем уровне аппаратных средств и операционной системы смарт-карты. JCRE состоит из Java Card виртуальной машины (байт-код интерпретатор), структура дополнения Java Card классифицирует классом Application Protocol Interface (APIs), стандартных программных средств и системных классов JCRE. В JCRE принято отделять апплеты от частных технологий смарт-карт, где используются стандартные системы, которые взаимодействуют с помощью API интерфейса для апплетов. В результате, апплеты более легко переносить и записывать на другую архитектуру смарт-карт.

Уровень непосредственно JCRE содержит Java Card виртуальную машину (JCVM) и родные методы. JCVM выполняет коды байта, управляет делением памяти, управляет объектами и осуществляет защиту во время их выполнения. Методы обеспечивают поддержку JCVM и следующий уровень системных классов. Системные классы предназначены для взаимосвязи по протоколам связи с нижним уровнем, управления памятью, осуществления криптографической поддержки, и т.д.[1].

Системы сетевой защиты апплета (межсетевые экраны)

Здесь используются два пакета javacard.security и javacardx.crypto, которые обеспечивают интерфейсы для классов криптографии, ключи и могут использоваться для вычисления подписи; обрабатывать сообщение и генерировать случайные данные. Дополнение или апплет на карте идентифицируются апплетом ID или AID (application identifier). Далее, идентификатор ресурса (RID (resource identifier)) используется вместе с AID, таким образом, они могут использоваться для уникальной идентификации из дополнений и файлов данных в файловой системе карты.

Защита дополнений достигнуты за счет использования системы сетевой защиты апплета [2]. В сущности, защищены объектные пространства, называемые состояниями, определяемые для каждого апплета, когда они выполняются. Системы сетевой защиты

(межсетевые экраны) апплета определяют границы к его состоянию или выделяют область в пространстве памяти. Это необходимые мероприятия для границы между двумя дополнениями. Когда образ апплета создан, JCRE назначает ему состояние.

Рис. 1. Системная архитектура смарт-карты.

Когда к объектам обращаются апплеты, состояние их взаимодействия (состояние, которые были назначены при создании) равнозначно активному состоянию в один момент времени. Несоответствие состояния означает исключение, и доступ отклоняет.

JavaCard также позволяет совместимое использование объекта, поперек состояниям, то есть устанавливая безопасный канал связи между двумя состояниями, через OS состояние, которое есть JCRE состоянием.

Верификация байт-кода

Верификация байт-кода - ключевая функция безопасности в архитектуре Java Card. Его цель заключается в том, чтобы проверить корректность выполнения апплета, его код, а также исключить возможность апплетов выполнить злоумышленные действия во время их выполнения. Этот процесс состоит из двух шагов. Первый, наиболее простой, есть структурный анализ последовательности CAP (Converted Applet — преобразованный аплет) - файла. Второй требует статического анализа программы и предназначенный для:

- значения используются вместе с правильным типом (во избежание неправильных указателей) и с методом, которому отдается преимущество;
- ни какой стек операндов не должен выйти за границы и опустошаться;
- методы (private, public, or protected) должны быть совместимые для использования;
- объекты и локальные переменные должны быть инициализированы перед вызовом.

Инициализация - одна из главных трудностей с точки зрения кода байта проверки.

Проверка кода байта - поточный анализ, выполняемый виртуальной машиной, использует стандартные операции и сам принцип JVM, если бы не две существенные особенности: тип виртуальной машины управляет типами вместо значений, используется один метод.

Поточный анализ стремится к вычислительным решениям поточных уравнений по схеме, полученной из отношения выделенных типов между типами JVM, используя при этом универсальный алгоритм из G. Kildall[3]. Внутри алгоритм управляет так называемыми stackmaps (путеводитель стеков), который хранит каждую точку программы, указывающие структуру хронологии, которая представляет программу, определяющая, что бы предварительно была достигнута точка программы. Хронологическая структура будет инициализироваться к начальному состоянию из метода, которое проверяется для первой точки программы, и к заданному по умолчанию состоянию для других точек программы. Первый шаг процесса итерации функции выполняемой виртуальной машиной находится на вершине хронологической структуры. Разные структуры хронологии могут использоваться в зависимости от необходимой точности анализа.

В монофазном анализе, структура хронологии хранит одно состояние программы, которое является меньше всего верхним связанным из состояний, которые были предварительно вычислены в этой точке программы. В таком анализе, размножено состояние в структуре хронологии составляет взятие меньше всего верхних связанных (на решетках типа виртуальной машины) типов, которые появляются в двух состояниях и хранящий результат обратно в тоже место.

Завершение анализа гарантируется, поскольку набор состояний не имеет бесконечной цепочки роста, и состояние сохранено в структуре хронологии увеличиваются. Как отмечено R. Stata и Г. Abadi [4], сведены структуры хронологии к единственному состоянию как сделано в анализе, который ведет к алгоритму проверки кода байта, но не обрабатывает подпрограммы, как приказано неофициальными спецификациями Sun. Точнее, монофазный байт-код отклоняет проверки программы кода байта, которые делают полиморфное использование подпрограмм. Такое использование подпрограмм может привести к двум исходам: для одной и той же точки программы, которая не имеет того же номера локальных переменных или того же номера элементов в стеке операнда. Это привело бы к объединению состояния и вызывало бы в этом состоянии ошибку, хотя выполнение такое допустимо.

Проверка на устройстве

В настоящее время апплеты проверяются вне карты и в случае успешной проверки, будут инициализироваться и загружаются на карте. Такое решение не оптимально в значении, которое оставляет критический компонент архитектуры защиты за смарт-карты. Однако, есть несколько предложений, чтобы ограничить достоверную вычислительную базу смарт-карт и использовать на карте проверку кода байта. Одно решение, принятое в KVM [5] заключается в том, чтобы положиться на легкую проверку кода байта, сначала предложенную E. Rose, в котором программа, занимается решением уравнений потока данных, а роль верификатора, проверить, что решения являются правильными. Другое предложение X. Leroy [6] где происходит превращение вне карты, которое позволяет проверить байт-код, который может быть выполненным за один шаг. В более поздних работах D. Deville и G. Grimaud [7] не требуют, чтоб программы были перезаписаны или аннотировались, но операции вместо этого эффективнее кодируется относительно структуры данных, управляемых верификатором кода байта.

Формализация байт-кода

Сейчас доступны несколько реализаций JavaCard платформы. Они отличаются сферой действия окружающей среды во время выполнения, и вычислительным механизмом формализации, на них ссылается стиль семантики, используемой для набора инструкции и специфического аспекта защиты, которая они стремятся поддерживать.

Следующая реализация платформы Java Card была написана в Coq [8] языка спецификаций. Однако формализация легко переносима и на другие языки программирования

типа CAML, а также проверенных помощников типа Isabelle и Prototype Verification System (PVS).

Начало функций, и конец соответственно возвращает для данного списка первый элемент, и список без первого элемента. Наша формализация использует тип список list во многих местах как тип упорядоченных наборов, для случаев с исключением стеков или массивов. Позволяют использовать все обратимые функции accessors (доступа) и lemmas (леммы) Coq и получить непосредственно выполнимую семантику. Однако, с новой системой модуля Coq, было бы также возможно объявить абстрактные модули для основного типа данных datatypes и давать выполняться этим модулям.

Записи представлены ключевым словом Record

Пакет javacard.security

Пакет обеспечивает базовую оболочку для криптографических функций. Пакет базируется на стандартном пакете Java java.security.

Пакет javacard.security определяет базовый класс keyBuilder и различные интерфейсы, используемые для вычисления ключей в симметричных (DES) и асимметричных (DSA, RSA) алгоритмах. Также поддерживаются абстрактные базовые классы RandomData , Signature и MessageDigest, которые используются для генерации случайных чисел и цифровых подписей.

Пакет javacardx.crypto

Пакет javacardx.crypto является дополнительным. Пакет содержит криптографические классы и интерфейсы, которые являются подчиненными Соединенным Штатам, и экспортируют регулирующие требования, предоставляет классы и интерфейсы для выполнения криптографических задач. Базовый класс Cipher собственно и поддерживает функции кодирования/декодирования. Пакеты javacard.security и javacardx.crypto предоставляют всем апплетам интерфейс для криптографии. Вместе с тем это именно интерфейс. Здесь не содержится никакой реализации. Производитель JCRE обеспечивает уже конкретную реализацию абстрактных классов RandomData, Signature , MessageDigest и Cipher. Обычно, смарт-карты содержат специальный сопроцессор для выполнения криптографических операций [1].

Преимущества защиты JavaCard

При программировании дополнений, которые используют технологию Java, разработчикам нужно следовать правилам защиты. Эти правила должны соответствовать программированию на языке, который используется для разработки дополнений. Это применяется, чтобы дополнить механизмы защиты, поддерживаемые платформой Java. Такие правила защиты охватывают широкий диапазон свойств, включая политику безопасности, которая не гарантируется платформой, свойства защиты, связанные с конфиденциальностью или управлением ресурса, также как свойства, которые гарантируют правильное и законное использование API.

Выводы

На основании проведенных исследований, можно сделать вывод, смарт-карты являются идеальной областью применения формальных методов защиты, и имеют существенные достижения и в области проверки платформы и проверке дополнений. Несмотря на такое научный процесс развития, формальные методы не получили широкое приложение в промышленности, в том числе и в использовании формальных методов для смарт-карт, поскольку персональные устройства разработчиков весьма часто ограничены R&D лабораториями. Согласно недавнему roadmap (сетевой график)[9], эффективность расширяемости и стоимости остается двумя узкими местами для более широкого применения формальных методов в промышленности смарт-карт. При обращении к этим узким местам - важен технический вызов, который будет занят формальным содружеством методов.

Кроме того, нарастающая сложность и возможность соединения надежных персональных устройств, поддерживают новые вызовы и возможности для формальных мето-

дов. Некоторые определенные технические вызовы уже были рассмотрены выше: распространение проверки платформы и методов проверки апплета, необходимо охватить организацию поточной обработки сообщений, развитие систематического шифрования свойств безопасности на языках спецификации интерфейса типа JML, объединения систем разных типов и логических методов проверки, установления функциональной правильности компонентов системы.

Эти определенные вызовы будут служить следующим шагом до намного большего приложения и лучшей интеграции формальных методов в архитектуре безопасности для проверенных персональных устройств, и в конечном счете защита архитектуры для больших сетей с поддержкой Java-устройств.

Будущий европейский проект “MOBIUS стремится к: Мобильности, Откровенности и Безопасности” [10] будут использовать многие из этих вызовов и возможностей в контексте больших и распределенных сетей с поддержкой Java-устройств, а также стремятся к обеспечению глобальных услуг, постоянных и надежных.

Литература

1. Java Card Technology Overview.pdf;
2. Макаренко С.М. Брусникін А. Алгоритм шифрування для передачі данних у відкритих мережах. - :М.: ПІТЕР, 2003-422с;
3. G. A. Kildall. A unified approach to global program optimization. In Proceedings of POPL’23, pages 194–206. ACM Press, 1923;
4. R. Stata and M. Abadi. A type system for Java bytecode subroutines. ACM Transactions on Programming Languages and Systems, 21(1):90–132, January 1999;
5. Connected Limited Device Configuration (CLDC) and the K Virtual Machine (KVM). http://java.sun.com/products/cldc;
6. X. Leroy. On-card bytecode verification for Java card. In I. Attali and T. Jensen, editors, Proceedings of e-SMART’01, volume 2140 of Lecture Notes in Computer Science, pages 150–164. Springer-Verlag, 2001;
7. D. Deville and G. Grimaud. Building an “impossible” verifier on a Java Card. In Proceedings of WIESS’02. Usenix Association, 2002;
8. Coq Development Team. The Coq Proof Assistant User’s Guide. Version 8.0, January 2004;
9. Roadmap for European Research on Smartcard Technologies. http://www.ercim.org/reset;
10. Mobius Project: http://mobius.inria.fr.

УДК 330.47.65.012

Соловьев В. И.

ИНФОРМАЦИОННЫЕ АСПЕКТЫ ОЩУЩЕНИЯ КРАСОТЫ МЕЛОДИИ

В статье рассматриваются вопросы (проблемы) математичекого моделирования красоты мелодии. Приведены результаты анализа ряда музыкальных произведений.

Объяснение красоты звучания мелодии, в конечном счете, является предметом исследования нейрофизиологии и психофизиологии. За последние десятилетия использование современных экспериментальных методов исследования нейронных образований мозга существенно продвинуло научные представления о механизмах запоминания, хранения и переработки информации [1,2,3]. Однако, эти результаты пока не предоставляют возможности понять ряд удивительных механизмов психофизиологии сенсорных процессов, таких например, как восприятие ощущения красоты музыкальной мелодии. Другое направление научных исследований, не связанное напрямую с нейрофизиологией, пытается обнаружить закономерности в музыкальных произведениях, которые позволили бы пролить свет на известные законы мелодий, выискивая паттерны методами динамических систем.

Также считая, что некоторые возможные подсказки для экспериментальных методов нейрофизиологии могут содержаться в закономерностях конкретных мелодий, расс-

мотрим процесс количественного математического анализа мелодии под несколько другим углом зрения.

В качестве исходных постулатов исследования музыкальных произведений рассмотрим следующие известные факты.

1. Человек распознает известную ему мелодию в довольно широком диапазоне изменений, как ритма исполнения, так и сдвига по частотному диапазону звучания на постоянную для данного музыкального произведения величину.

2. При этом степень консонанса (приятности звучания) изменяется, но мелодия узнаваема, в начальном ее звучании.

3. Все процессы переработки информации в мозгу носят дискретный характер. Это касается как нервных импульсов в нейронных сетях, так и собственно процессов долговременного запоминания при молекулярных изменениях в нервных клетках [1]. При этом не имеется в виду способ организации хранения памяти на нейронных структурах. Не важно – носит он волновой, дискретный или комбинированный характер с точки зрения организации [1].

В случае наличия аккордов на данном постановочном этапе исследования при анализе мелодии принимаются, как правило, ноты нижних частот. Понятно, что такое приближение, безусловно, оказывает влияние на красоту мелодии. Далее будет показано, что предлагаемая методика исследования легко обобщается на “полнокровные” музыкальные произведения.

Наконец, в качестве дополнительной гипотезы-постулата, которая существенно облегчает технические трудности анализа на этапе постановки задачи, предположим, что базовые механизмы запоминания мелодии могут иметь сравнительно простой характер и как-то отражаться в мелодии. Кроме того, в качестве объекта численных исследований будем использовать нотную нотацию конкретных произведений, которая уже по своему существу является формализованной моделью.

На основе этих принципов были исследованы различные классические музыкальные произведения и песенная музыка. Последовательность численного исследования была следующая:

Каждая нота нотной нотации произведения переводилась в ее частотный эквивалент. Определялась средняя длительность звучания музыкального произведения (в конкретном исполнении) и на этой основе производилась оценка средней длительности (в секундах) музыкального такта произведения и соответственно длительность звучания каждого звука.

С учетом длительности звучания каждой ноты в рамках нотной нотации вычислялось число звуковых колебаний для каждой ноты – как количество колебаний в секунду деленное на длительность звучания ноты. При этом учитывались и музыкальные паузы.

В соответствии с исходным постулатом 1, вычислялась разница числа колебаний следующих друг за другом нот (с учетом пауз), при этом определялось абсолютное значение разницы (без учета знака).

В таблицах 1,2. приведены фрагменты полученных числовых последовательностей для произведения И. С. Баха – “Токката и фуга ре минор” (обработка для фортепьяно Л. Брассена) и Л. Бетховена – “Соната №14 – для фортепьяно”.

В таблицах 1,2. нечетные строки – дискретная последовательность чисел, вычисленная для музыкального произведения, четные строки – ближайшие к каждому из чисел последовательности числа Фибоначчи.

Числовая последовательность (модель в данном подходе), рассматриваемых произведений, удивительным образом близка к числам числовой последовательности Фибоначчи. При этом относительно существенные отклонения соответствуют музыкальным паузам. Если учесть округления при вычислениях целых чисел до ближайшего целого по правилам арифметики, то совпадения с числами ряда Фибоначчи может оказаться еще выше. Природа не обязана использовать известные математические методы округлений.

Таблица 1.

Фрагменты числовой последовательности для произведения И. С. Баха – “Токката и фуга ре минор” (обработка для фортепьяноЛ. Брассена)

Последовательность чисел для произведения	220	24	2	1	3	35	21	73	110	110	21	1	5
Ближайшее число Фибоначчи	233	21	2	1	3	34	21	69	144	144	21	1	5
Последовательность чисел для произведения	20	37	175	175	21	3	12	1	29	14	58	330	0
Ближайшее число Фибоначчи	21	34	144	144	21	3	13	1	34	13	55	370	0

Таблица 2.

Фрагменты числовой последовательности для произведения Л. Бетховена – “Соната №14 – для фортепьяно”.

Последовательность чисел для произведения	17	13	30	17	13	30	17	13	30	17	13	30	17
Ближайшее число Фибоначчи	18	13	34	18	13	34	18	13	34	18	13	34	18
Последовательность чисел для произведения	13	30	17	13	30	17	13	30	17	13	27	14	13
Ближайшее число Фибоначчи	13	34	18	13	34	18	13	34	18	13	21	13	13
Последовательность чисел для произведе-ния	27	14	13	27	18	19	37	23	14	40	12	27	40
Ближайшее число Фибоначчи	21	13	13	21	18	18	34	21	13	34	13	21	34
Последовательностьчисел для произведения	17	13	30	17	9	32	16	16	37	11	17	17	17
Ближайшее число Фибоначчи	18	13	34	18	8	34	18	18	34	13	18	18	18

Учет аккордов в музыкальном произведении осуществляется по аналогии. В частности, производится вычисление всех разностей числа колебаний между всеми составляющими нотами последующего аккорда и предыдущего. Это приводит к совокупности (пакету) чисел на каждом музыкальном минифрагменте исполнения.

Исследования песенных произведений дают аналогичные результаты. Однако, близость полученных числовых рядов к числам последовательности Фибоначчи, нескольку хуже, чем для классических непесенных произведений. Так, в Таблице.3. приведен фрагмент числовой последовательности для песни “Два кольори”

Таблица 3.

Фрагменты числовой последовательности для песни “Два кольори”

Последовательность чисел для произведения	16	8	5	13	8	3	9	4	417	490	98	213	224
Ближайшее число Фибоначчи	13	8	5	13	8	3	8	13	377	377	89	233	233
Последовательность чисел для произведения	207	216	9	9	5	12	12	294	269	97	89	140	52
Ближайшее число Фибоначчи	233	233	8	8	5	13	13	233	233	89	89	13	55

Если данное исследование претендует хотя бы на какое-то соответствие реальным закономерностям обработки слуховой информации (в частности – музыкальных мелодий), то одна из возможных существенных причин следующая. Песенная музыка воспринимается в целом неразрывно с текстовой песенной частью. Ясно, что при восприятии песенной музыки ее корректный анализ должен учитывать и смысловую, вербальную часть. Хотя все же классика – есть классика.

При условии достоверности приведенных результатов (а они требуют проверки на множестве различных музыкальных произведений), возможно, гипотетически, сделать множество различных выводов-гипотез относительно возможных механизмов хранения и переработки музыкальных мелодий в мозгу. Понятно, что эти гипотезы будут иметь чисто спекулятивный характер без подтверждения экспериментальными данными нейрофизиологии. Однако невозможно не поддаться искушению привести ниже ряд из них. В конце концов, какие-то мысли, гипотезы на основе этих возможных закономерностей могут оказаться в какой-то степени полезными.

Запоминание мелодии на нейронных структурах, возможно, осуществляется в своем внешнем проявлении в виде совокупности дискретных физических ячеек, хранящих в эквивалентном представлении числа Фибоначчи.

Консонанс (красота мелодии) определяется в среднем степенью отклонения мелодии от ее идеала, конкретного для каждой индивидуальной мелодии, базирующегося на определенной траектории из различных последовательностей чисел Фибоначчи. Ощущение красоты мелодии есть следствие ее близости к определенной идеальной, которая может храниться на совокупности нейронных структур. Не исключено, что не любую частотную последовательность звуков и интервалов между ними способны хранить (и запоминать) нейроны. Понятно, что и при создании мелодии, у ее творца должен по вероятности генерироваться ансамбль, количественной характеристикой которого может являться по-

следовательность Фибоначчи. При этом, очевидно, что красота мелодии существенно зависит и от ее исполнителя. За счет собственного тонкого ощущения красоты при исполнении может изменяться длительность звучания нот (фиксированная в исходной записи нотной нотации произведения).

Появляется возможность ввести абсолютные математические меры красоты музыкальной гармонии (консонанса, диссонанса), в какой-то степени независимые от конкретного музыкального произведения.

Например, - в качестве такой меры может выступать среднеквадратическое отклонение (для конкретного исполнителя) числовой последовательности произведения, определяемой по приведенной выше методике, от последовательности ближайших чисел ряда Фибоначчи, приведенная к одному такту (либо нормированная по другому целесообразному базовому параметру.

Конечно, в столь простой постановке исследования не были затронуты различные другие аспекты исполнения музыкальных мелодий, влияющие на восприятие. Например, такие, как изменение громкости звучания и ряд других. Учет других факторов требует привлечения к развиваемой концепции ощущения красоты дополнительных экспериментальных данных и постулатов.

Безусловно, если эти результаты заслуживают внимания, исследования в направлении данной методики должны базироваться на результатах оцифровки звучания конкретных музыкальных произведений. Однако, технические трудности анализа при подобном, безусловно, более корректном подходе, существенно возрастают. В тоже время, запись музыкального произведения в виде современной нотной нотации прошла длительную эволюцию со времен Пифагора и аккумулировала в себе длительный опыт исследований гармоничности звуков и формальных моделей. В следствии этого, по-видимому, использование нотной нотации в качестве исходного материала для анализа более приемлемо. С другой стороны, здесь легко впасть в заблуждение, при интерпретации результатов анализа. В частности, числа Фибоначчи, возникающие при данном исследовании, могут в существенной мере оказаться следствием уже установившегося исторически гармонического ряда (до, ре, ми, фа…).

Однако, даже в этом случае, при условии подтверждения результатов после проверки на большом множестве музыкальных произведений возникает вопрос. Каким образом простые математические действия над формализованной записью сложного музыкального произведения в соответствии с общепринятыми представлениями об общих закономерностях восприятия мелодий могут приводить к простым числовым рядам или даже столь удивительной близости к ним?

Литература

1. Александров Ю. И. Психофизиология. Питер, 2006, 463 с;
2. Сомьен Дж. Кодирование информации в нервной системе млекопитающих. М. Мир1975, 386 с;
3. Роуз с. Устройство памяти. От молекул к сознанию. М. , Мир, 1995, 265 с;

УДК 621.4.016.1

Дядичев В.В., Капуста Л.В., Кулян Н.Р.

ИЕРАРХИЧЕСКИЙ ПОДХОД К ВЫБОРУ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Предлагается иерархический подход к выбору средств защиты информации в зависимости от степени ее доступности, места расположения информации и способов ее утечки.

Широкомасштабное использование компьютерной техники в рамках территориально-распределенных информационных систем, увеличение объемов обрабатываемой инфо-

рмации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости, поэтому особое значение предается вопросам безопасности информации, как важной части процесса внедрения новых информационных технологий во все сферы жизни общества.

Создание соответствующих средств защиты информации представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла информационной системы. При этом все средства, методы и мероприятия, используемые для защиты информации, объединяются в единый целостный механизм – систему защиты, выбор которой зависит от степени ее доступности и способов ее утечки.

По степени доступности информацию можно классифицировать на следующие виды:

- информация особой секретности – обычно используется в государственных учреждениях;
- информация повышенной секретности – используется в банках и других коммерческих организациях;
- несекретная информация – используется в учебных учреждениях, небольших торговых предприятиях и т.д.

Для информации особой секретности применяется целый комплекс программных и программно – аппаратных средств защиты информации в локальной сети, наряду с этим используются средства, обеспечивающие защиту информации от утечки по различным физическим полям.

На тех предприятиях, организациях и учреждениях где используется информация повышенной секретности, применяются программные методы защиты данных, в некоторых случаях рекомендуется использование программно – аппаратных средств защиты для повышения эффективности уже существующих систем безопасности.

Для несекретной информации используют способы защиты на уровне администрирования, такие как, идентификация и аутентификация пользователей, разграничение доступа уже зарегистрированных пользователей, использование антивирусных программ и т.д.

Информация может храниться на отдельных компьютерах или серверах в зависимости от конфигурации сети, передаваться по каналам связи (проводным, беспроводным) к пользователю.

Программно – аппаратные средства защиты информации определяются местом её расположения и способом её утечки:

- электронный замок «Соболь»/«Соболь-PCI» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети.
- программно – аппаратный комплекс Secret Net 4.0, который используется для обеспечения информационной безопасности в локальной вычислительной сети, рабочие станции и сервера которой работают под управлением следующих операционных систем: Windows'9x (Windows 95, Windows 98 и их модификаций); Windows NT версии 4.0; UNIX MP-RAS версии 3.02.00.
- программно – аппаратный комплекс Аккорд 2.0, который по сравнению с Secret Net имеет большее количество атрибутов доступа к программам и файлам
- устройства криптографической защиты данных (УКЗД) серии «КРИПТОН» — это аппаратные шифраторы для IBM PC-совместимых компьютеров. Устройства применяются в составе средств и систем криптографической защиты данных, для обеспечения информационной безопасности в государственных и коммерческих структурах [6].

В качестве каналов связи используются сетевые кабели, инфракрасные порты, радиопередатчики. Для обеспечения защиты информации на этом уровне рекомендуется использовать межсетевые экраны, устройства криптографической защиты информации,

средства анализа защищенности ОС и сетевых сервисов, средства обнаружения опасных информационных воздействий в сетях.

В качестве средств защиты рекомендуется использовать межсетевые экраны [2]:

- сетевой монитор безопасности IP Alert-1, основная задача этого средства, программно анализирующего сетевой трафик в канале передачи, состоит не в отражении осуществляемых по каналу связи удаленных атак, а в их обнаружении, протоколировании (ведении файла аудита с протоколированием в удобной для последующего визуального анализа форме всех событий, связанных с удаленными атаками на данный сегмент сети) и незамедлительным сигнализировании администратору безопасности в случае обнаружения удаленной атаки. Основной задачей сетевого монитора безопасности IP Alert-1 является осуществление контроля за безопасностью соответствующего сегмента сети;
- межсетевой экран безопасности Firewall, реализует следующие функции:

– многоуровневую фильтрацию сетевого трафика, которая позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику безопасности в выделенном сегменте IP-сети;

– proxy-схема с дополнительной идентификацией и аутентификацией пользователей на Firewall-хосте, которая позволяет при доступе к защищенному Firewall сегменту сети осуществить на нем дополнительную идентификацию и аутентификацию удаленного пользователя и является основой для создания приватных сетей с виртуальными IP-адресами. Смысл proxy-схемы состоит в создании соединения с конечным адресатом через промежуточный proxy-сервер на хосте Firewall;

– создание приватных сетей (Private Virtual Network - PVN) с "виртуальными" IP-адресами (NAT - Network Address Translation). Хостам в PVN-сети назначаются любые "виртуальные" IP-адреса, для того чтобы скрыть истинную топологию сети. Для адресации во внешнюю сеть необходимо либо использование на хосте Firewall proxy-серверов, либо применение специальных систем роутинга (маршрутизации).

Кроме того, для защиты информации по каналам связи используют устройства криптографической защиты информации:

- СКЗИ "Верба - OW" – обеспечивает криптографическую защиту данных. Зашифрованные данные становятся доступными только для того, кто знает соответствующий ключ, с помощью которого можно расшифровать сообщение, и поэтому похищение зашифрованных данных без знания ключа является бессмысленным. Используемые в СКЗИ "Верба-OW" методы шифрования гарантируют не только высокую секретность, но и эффективное обнаружение искажений или ошибок в передаваемой информации;
- СКЗИ КРИПТОН – шифрование позволяет шифровать файлы, обеспечивая их конфиденциальность. Зашифрованную информацию можно хранить на любых носителях (в т.ч. дисках персонального компьютера), передавать по сети Internet и другим открытым каналам связи, не опасаясь, что с содержимым зашифрованных файлов ознакомятся посторонние [6];
- Средства анализа защищенности ОС и сетевых сервисов, средства обнаружения опасных информационных воздействий в сетях – осуществляют проверку настроек и конфигурации доступа, идентификации и аутентификации, средств мониторинга и др. компонентов ОС; контроль целостности и неизменности программных средств и системных установок; проверку наличия уязвимостей системных и прикладных служб. К таким системам относятся Solaris ASET, которая используется при работе в ОС Solaris; COPS (Computer Oracle and Password System) – в UNIX – системах; System Scanner предназначен для операционных систем UNIX и Windows [5].

Для защиты информации, предназначенной для пользователя, предлагается применять методы администрирования.

Исходя из проведенных исследований, необходимо осуществлять выбор средств защиты информации, исходя из степени её секретности, места расположения и способов её утечки.

Литература

1. Зегжда П., «Теория и практика. Обеспечение информационной безопасности». - Москва, 2002;
2. Мельников В. ”Защита информации в компьютерных системах”. Москва. ”Финансы и статистика”. ”Электроинформ”. 1997;
3. Нанс Б. “Компьютерные сети”. Москва. Бином. 2004;
4. Уолкер В., Я.Блейк, «Безопасность ЭВМ и организация их защиты», - Москва, 2000;
5. Хофман Л.,«Современные методы защиты информации», Москва, 2004;
6. Штайнке С. “Идентификация и криптография”. LAN\Журнал сетевых решений. 2005. №2.

УДК 004.681

Орленко В.С.

ОБЗОР МЕТОДОВ И СРЕДСТВ НЕСАНКЦИОНИРОВАННОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Краткая характеристика возможных каналов утечки информации, которые можно отнести к разряду наиболее вероятных для любого государственного или коммерческого предприятия, фирмы, банка, организации, учреждения. Полученные сведения можно теперь использовать на первом этапе построения комплексной системы защиты информации, то есть при анализе угроз утечки конфиденциальной информации.

Получить достоверную информацию о деятельности фирмы незаконным путем маловероятно, если фирма с пониманием относится к сохранности коммерческой тайны и создания соответствующей системы защиты. В то же время многие под безопасностью понимают, прежде всего, физическую защищенность, иногда включая отдельные требования информационной защиты коммерческих интересов, что не способствует решению проблем безопасности в комплексе.

Вывод один - необходимо обеспечивать безопасность информации, благодаря которой субъекты предпринимательской деятельности являются участниками выгодного внутреннего и международного обмена товаром и знаниями, имея от этого прибыль. Причем каждый коммерческий объект должен строить свою систему защиты информации на концептуальной основе, исходя из назначения объекта, его размеров, условий размещения, характера деятельности и т.д.

При разработке концепции защиты необходимо исходить из детального анализа направлений деятельности предпринимательской структуры и комплексных требований защиты. Особенно, если структуры применяют в своей деятельности средства информатики.

Учитывая многообразие потенциальных угроз информации в системе обработки данных, сложность структуры и функций, а также участие человека в технологическом процессе обработки информации, цели защиты информации могут быть достигнуты только путем создания системы защиты информации на основе комплексного подхода. И начинать создание системы надо с оценки угроз безопасности деятельности коммерческого объекта, а исходя из полученных результатов анализа, принимается решение о построении всей системы защиты и выбираются необходимые средства.

Возможные каналы утечки информации можно разбить на четыре группы.

1-я группа- каналы, связанные с доступом к элементам системы обработки данных, но не требующие изменения компонентов системы. К этой группе относятся каналы образующиеся за счет:

- дистанционного скрытого видеонаблюдения или фотографирования;
- применения подслушивающих устройств;
- перехвата электромагнитных излучений и наводок и т.д.

2-я группа- каналы, связанные с доступом к элементам системы и изменением структуры ее компонентов. Ко второй группе относятся:

- наблюдение за информацией с целью ее запоминания в процессе обработки;

- хищение носителей информации;
- сбор производственных отходов, содержащих обрабатываемую информацию;
- преднамеренное считывание данных из файлов других пользователей;
- чтение остаточной информации, т.е. данных, остающихся на магнитных носителях после выполнения заданий;
- копирование носителей информации;
- преднамеренное использование для доступа к информации терминалов зарегистрированных пользователей;
- маскировка под зарегистрированного пользователя путем похищения паролей и других реквизитов разграничения доступа к информации, используемой в системах обработки;
- использование для доступа к информации так называемых "люков", дыр и "лазеек", т.е. возможностей обхода механизма разграничения доступа, возникающих вследствие несовершенства общесистемных компонентов программного обеспечения (операционных систем, систем управления базами данных и др.) и неоднозначностями языков программирования, применяемых в автоматизированных системах обработки данных.

3-я группа, к которой относятся:

- незаконное подключение специальной регистрирующей аппаратуры к устройствам системы или линиям связи (перехват модемной и факсимильной связи);
- злоумышленное изменение программ таким образом, чтобы эти программы наряду с основными функциями обработки информации осуществляли также несанкционированный сбор и регистрацию защищаемой информации;
- злоумышленный вывод из строя механизмов защиты.

4-я группа, к которой относятся:

- несанкционированное получение информации путем подкупа или шантажа должностных лиц соответствующих служб;
- получение информации путем подкупа и шантажа сотрудников, знакомых, обслуживающего персонала или родственников, знающих о роде деятельности.

Далее кратко рассмотрим наиболее распространенные каналы утечки информации.

Для перехвата и регистрации акустической информации существует огромный арсенал разнообразных средств разведки: микрофоны, электронные стетоскопы, радиомикрофоны или так называемые "радиозакладки", направленные и лазерные микрофоны, аппаратура магнитной записи. Набор средств акустической разведки, используемых для решения конкретной задачи, сильно зависит от возможности доступа агента в контролируемое помещение или к интересующим лицам. Применение тех или иных средств акустического контроля зависит от условий применения, поставленной задачи, технических, и прежде всего, финансовых возможностей организаторов подслушивания.

В том случае, если имеется постоянный доступ к объекту контроля, могут быть использованы простейшие миниатюрные микрофоны, соединительные линии которых выводят в соседние помещения для регистрации и дальнейшего прослушивания акустической информации. Такие микрофоны диаметром 2.5 мм могут улавливать нормальный человеческий голос с расстояния до 10-15 м. Вместе с микрофоном в контролируемом помещении, как правило, скрытно устанавливают миниатюрный усилитель с компрессором для увеличения динамического диапазона акустических сигналов и обеспечения передачи акустической информации на значительные расстояния. Эти расстояния в современных изделиях достигают до 500 метров и более, то есть служба безопасности фирмы, занимающей многоэтажный офис (или злоумышленник), может прослушивать любое помещение в здании. При этом проводные линии чаще всего от нескольких помещений сводятся в одно на специальный пульт и оператору остается лишь выборочно прослушивать любое из них и, при необходимости, записывать разговоры на магнитофон или жесткий диск компьютера для сохранения и последующего прослушивания. Для одновременной регистрации акустических сигналов от нескольких помещений (от 2-х до 16-ти) существуют многоканальные регистраторы, созданные на базе ПЭВМ. Такие регистраторы чаще всего

используются для контроля акустической информации помещений и телефонных разговоров. Они имеют различные дополнительные функции, такие как определение входящих и исходящих номеров телефонов, ведение журналов и протоколов сеансов связи и др. Подобных регистраторов, как простых, так и сложных с большим набором дополнительных функций в настоящее время разработано и изготавливается у нас в Украине и за рубежом великое множество, есть из чего выбирать исходя из поставленной задачи и финансовых возможностей. Микрофоны могут быть введены через вентиляционные каналы на уровень контролируемого помещения, которое может прослушиваться с другого помещения, чердака здания или с крыши в местах выхода вентиляционного колодца. При этом не обязательно, как Карлсону, сидеть на крыше, достаточно установить диктофон с возможностью записи на несколько часов и имеющему возможность управления записью по уровню акустического сигнала, и все разговоры в контролируемом помещении будут записываться довольно длительное время без смены кассет. Кроме непосредственного перехвата звуковых колебаний отдельные микрофоны (т.н. микрофоны-стетоскопы) могут воспринимать звуковые колебания, распространяющиеся из контролируемого помещения по строительным конструкциям здания (стены, трубы отопления, двери, окна и т.п.). Их используют для прослушивания разговоров сквозь стены, окна, двери. Контрольный пункт для прослушивания разговоров с помощью микрофонов-стетоскопов может быть оборудован в безопасном месте здания на значительном удалении от контролируемого помещения. Современной промышленностью выпускаются многие модификации микрофонов направленного действия, которые воспринимают и усиливают звуки, идущие из одного направления, и ослабляют все другие звуки. Конструкции узконаправленных микрофонов - от формы трости до микрофонов, использующих параболические концентраторы звука. Так, направленный микрофон с параболическим концетратором диаметром 43 см, усилителем и головными микрофонами позволяет прослушивать разговоры на открытом месте с расстояний до 1 км.

Если агенты не имеют постоянного доступа к объекту, но имеется возможность его кратковременного посещения под различными предлогами, то для акустической разведки используются радиомикрофоны, миниатюрные диктофоны и магнитофоны закамуфлированные под предметы повседневного обихода: книгу, письменные приборы, пачку сигарет, авторучку. Кроме этого, диктофон может находиться у одного из лиц, присутствующих на закрытом совещании. В этом случае часто используют выносной микрофон, спрятанный под одеждой или закамуфлированный под часы, авторучку, пуговицу. Скрыто установленный в атташе-кейс малогабаритный магнитофон может незаметно включаться с помощью простой шариковой ручки. Современные диктофоны обеспечивают непрерывную запись речевой информации от 30 минут до нескольких часов, они оснащены системами акустопуска (Vox, Vas), то есть управлением по уровню акустического сигнала, автореверса, индикации даты и времени записи, дистанционного управления. В некоторых моделях диктофонов в качестве носителя информации используются цифровые микрочипы и мини-диски. Записанную на таком диктофоне речевую информацию можно переписывать на жесткие диски компьютеров для хранения, архивации и последующего прослушивания. Серьезным преимуществом цифровых диктофонов является то, что они не обнаруживают себя при работе, в отличие от кассетных, которые обнаруживаются специальными приборами по электромагнитным излучениям работающего двигателя лентопротяжного механизма, и при переходе на другую дорожку в режиме автореверса слышны характерные щелчки, которые могут демаскировать скрытно работающий диктофон.

Радиомикрофоны являются самыми распространенными техническими средствами съема акустической информации. Их популярность объясняется простотой пользования, относительной дешевизной, малыми размерами и возможностью камуфляжа.

Прием сигналов с радиомикрофонов осуществляется на стандартные FM - радиоприемники или специально изготовленные контрольные пункты с возможностью звукозаписи. Чаще всего для приема акустических сигналов от радиомикрофонов применяют сканирующие приемники. Используют также бытовые радиоприемники с установленным конвертером для приема сигналов в нужном диапазоне частот. Предпочтитель-

ным является применение магнитол, т.к. появляется возможность одновременного одновременного прослушивания и ведения записи. Для приема от радиомикрофонов с закрытым каналом используют приемники с конвертером и демаскиратом типа инверсия или декодером сигнала с цифровой дельта-модуляцией. Сканирующие приемники и создаваемые на их основе комплексы, кроме функций обычного радиоприема, выполняют радиомониторинг широкого спектра радиочастот. Совместно с программами управления они обеспечивают в автоматизированном и автоматическом режимах отображение радиообстановки на экране компьютера, накопление информации о принимаемых сигналах, анализ текущей и архивной информации с формированием отчетов о проделанной работе.

Утечка информации при использовании средств связи и различных проводных коммуникаций

В данном случае, когда речь заходит о возможности перехвата информации при использовании линий связи и проводных коммуникаций, следует иметь в виду, что перехват может осуществляться не только с телефонных линий и не только речевой информации. В этот раздел можно отнести:

– прослушивание и запись переговоров по телефонным линиям;
– использование телефонных линий для дистанционного съема аудио- информации из контролируемых помещений;
– перехват факсимильной информации;
– перехват разговоров по радиотелефонам и сотовой связи;
– использование сети 220 В и линий охранной сигнализации для передачи акустической информации из помещений;

Прослушивание и запись переговоров по телефонным линиям

Телефонные абонентские линии обычно состоят из трех участков: магистрального (от АТС до распределительного шкафа (РШ)), распределительного (от РШ до распределительной коробки (КРТ)), абонентской проводки (от КРТ до телефонного аппарата). Последние два участка - распределительный и абонентский являются наиболее уязвимыми с точки зрения перехвата информации. Подслушивающее устройство может быть установлено в любом месте, где есть доступ к телефонным проводам, телефонному аппарату, розетке или в любом месте линии вплоть до КРТ. Наиболее простой способ подслушивания это подключение параллельного телефонного аппарата или "монтерской" трубки. Используются также специальные адаптеры для подключения магнитофонов к телефонной линии. Адаптеры сделаны таким образом, что диктофон, установленный на запись в режиме акустопуска, включается только при поднятой трубке телефонного аппарата. Это дает возможность экономно расходовать пленку на кассете, не сматывая ее вхолостую. Подключение к телефонным линиям осуществляется не только гальванически (прямым подсоединением), а и с помощью индукционных или емкостных датчиков. Такое подсоединение практически не обнаруживается с помощью тех аппаратных средств, которые широко используются для поисковых целей. Самыми распространенными из подобных средств прослушивания являются телефонные контроллеры радиоретрансляторы которые чаще называются телефонными передатчиками или телефонными "закладками". Телефонные закладки подключаются параллельно или последовательно в любом месте телефонной линии и имеют значительный срок службы, так как питаются от телефонной сети. Эти изделия чрезвычайно популярны в промышленном шпионаже благодаря простоте и дешевизне.

Большинство телефонных "закладок" автоматически включается при поднятии телефонной трубки и передают разговор по радиоканалу на приемник пункта перехвата, где он может быть прослушан и записан. Такие "закладки" используют микрофон телефонного аппарата и не имеют своего источника питания, поэтому их размеры могут быть очень небольшими. Часто в качестве антенны используется телефонная линия. Для маскировки телефонные "закладки" выпускаются в виде конденсаторов, реле, фильтров и других стандартных элементов и узлов, входящих в состав телефонного аппарата. Чаще всего телефонные "закладки" стараются устанавливать за пределами офиса или квартиры, что существенно снижает риск. Для упрощения процедуры подключения подслушивающих уст-

ройств и уменьшения влияния на телефонную линию используются изделия с индуктивным датчиком съема информации. Особенностью подобных устройств является то, что требуется автономный источник питания и устройство должно иметь схему автоматического включения при снятии телефонной трубки. Качество перехватываемой информации практически всегда хуже.

Использование телефонных линий для дистанционного съема аудиоинформации из контролируемых помещений

Отдельное место занимают системы, которые предназначены не для подслушивания телефонных переговоров, а для использования телефонных линий при прослушивании контролируемых помещений, где установлены телефонные аппараты или проложены провода телефонных линий. Примером такого устройства может служить "телефонное ухо". "Телефонное ухо" представляет собой небольшое устройство, которое подключается параллельно к телефонной линии или розетке в любом удобном месте контролируемого помещения. Для прослушивания помещения необходимо набрать номер абонента, в помещении которого стоит "телефонное ухо". Услышав первый гудок АТС, необходимо положить трубку и через 10-15 секунд повторить набор номера. Устройство дает ложные гудки занято в течение 40-60 секунд, после чего гудки прекращаются и включается микрофон в устройстве "телефонное ухо" - начинается прослушивание помещения. В случае обычного звонка "телефонное ухо" пропускает все звонки после первого, выполняя роль обычной телефонной розетки и не мешая разговору. Кроме того, возможно использование телефонной линии для передачи информации с микрофона, скрытно установленного в помещении. При этом используется несущая частота в диапазоне от десятков до сотен килогерц с целью не препятствовать нормальной работе телефонной связи. Практика показывает, что в реальных условиях дальность действия подобных систем с приемлемой разборчивостью речи существенно зависит от качества линии, прокладки телефонных проводов, наличия в данной местности радиотрансляционной сети, наличия вычислительной и оргтехники и т.д. Из числа так называемых "беззаходовых" систем съема речевой информации с контролируемых помещений, когда используются телефонные линии, следует отметить возможность съема за счет электроакустического преобразования, возникающего в телефонных аппаратах, и за счет высокочастотного (ВЧ) навязывания. Но эти каналы утечки используются все реже. Первый из-за того, что современные телефонные аппараты не имеют механических звонков и крупных металлических деталей, а второй из-за своей сложности и громоздкости аппаратуры. Но тем не менее меры защиты от утечки информации по этим каналам применяются, они общеизвестны и не дорогие.

Перехват факс-сообщений принципиально не отличается от перехвата телефонных сообщений. Задача дополняется только обработкой полученного сообщения.

Обычно комплексы перехвата и регистрации факсимильных сообщений состоят из:

– ПЭВМ с необходимыми, но вполне доступными рессурсами;
– пакет программного обеспечения;
– стандартный аудиоконтроллер (SoungBlaster);
– устройство подключения к линии (адаптер).Комплексы обеспечивают автоматическое обнаружение (определение речевое или факсимильное сообщение) регистрацию факсимильных сообщений на жесткий диск с последующей возможностью автоматической демодуляции, дескремблирования зарегистрированных сообщений и вывода их на дисплей и печать.

Перехват разговоров по радиотелефонам не представляет трудности. Достаточно настроить приемник (сканер) на частоту несущей радиотелефона, находящегося в зоне приема, и установить соответствующий режим модуляции. Для перехвата переговоров, ведущихся по мобильной сотовой связи, необходимо использовать более сложную аппаратуру. Комплексы позволяют обнаруживать и сопровождать по частоте входящие и исходящие звонки абонентов сотовой связи, определять входящие и исходящие номера телефонов абонентов, осуществлять слежение по частоте за каналом во время телефонного разговора, в том числе при переходе из соты в соту. Количество задаваемых для контроля

абонентов определяется составом аппаратуры комплекса и версией программного обеспечения и может достигать до 16 и более. Имеется возможность вести автоматическую запись переговоров на диктофон, вести на жестком диске ПЭВМ протокол записей на диктофон, осуществлять полный мониторинг всех сообщений, передаваемых по служебному каналу, а также определять радиослышимость всех базовых станций в точке их приема с ранжировкой по уровням принимаемых от базовых станций сигналов. Стоимость подобных комплексов в зависимости от стандарта контролируемой системы связи и объемов решаемых задач может составлять от 5 до 60 тысяч долларов.

Перехват GSM-связи значительно сложнее.

Использование сети 220 В для передачи акустической информации из помещений

Для этих целей применяют так называемые сетевые "закладки". К этому типу "закладок" чаще всего относят устройства, которые встраиваются в приборы, питающиеся от сети 220 В, или сетевую арматуру (розетки, удлинители и т.д.). Передающее устройство состоит из микрофона, усилителя и собственно передатчика несущей низкой частоты. Частота несущей обычно используется в диапазоне от 10 до 350 кГц. Передача и прием осуществляется по одной фазе или, если фазы разные, то их связывают по высокой частоте через разделительный конденсатор. Приемное устройство может быть изготовлено специально, но иногда применяют доработанные блоки бытовых переговорных устройств, которые сейчас продаются во многих специализированных магазинах электронной техники. Сетевые передатчики подобного класса легко камуфлируются под различного рода электроприборы, не требуют дополнительного питания от батарей и трудно обнаруживаются при использовании поисковой аппаратуры, широко применяемой в настоящее время.

Для дистанционного перехвата информации (речи) из помещений иногда используют лазерные устройства. Из пункта наблюдения в направлении источника звука посылается зондирующий луч. Зондирующий луч обычно направляется на стекла окон, зеркала, другие отражатели. Все эти предметы под действием речевых сигналов, циркулирующих в помещении, колеблются, и своими колебаниями модулируют лазерный луч, приняв который в пункте наблюдения, можно путем несложных преобразований восстановить все речевые сигналы, циркулирующие в контролируемом помещении. На сегодняшний день создано целое семейство лазерных средств акустической разведки. Такие устройства состоят из источника излучения (гелий-неоновый лазер), приемника этого излучения с блоком фильтрации шумов, двух пар головных телефонов, аккумулятора питания и штатива. Наводка лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Съем речевой информации с оконных рам с двойными стеклами с хорошим качеством обеспечивается с расстояния до 250 метров.

Вопросы безопасности обработки информации в компьютерных системах пока еще волнуют в нашей стране не слишком широкий круг специалистов. Это, конечно, во многом обусловлено нашим отставанием в применении компьютерной техники вообще. Однако жизнь поставила всех в такие условия, что всеобщая компьютеризация перестала быть зарубежной экзотикой. Это вдохновляет. Но следует понимать, что компьютеризация, кроме очевидных и широко рекламируемых выгод, несет с собой, во-первых, значительные затраты усилий и ресурсов, а во-вторых, многочисленные проблемы.

В особую группу следует выделить специальные закладки для съема информации с компьютеров.

Миниатюрный радиомаяк, встроенный в упаковку, позволяет проследить весь путь следования закупленной ЭВМ, транслируя сигналы на специальный передатчик. Узнав таким путем, где установлена машина, можно принимать любую обработанную компьютером информацию через специально вмонтированные электронные блоки, не относящиеся к ЭВМ, но участвующие в ее работе. Самая эффективная защита от этой закладки - экранированное помещение для вычислительного центра.

По мнению специалистов универсальных "компьютерных закладок" сегодня не бывает. Те закладки, которые удавалось обнаружить, можно условно разделить на три типа:

те, которые выбирают информацию по ключевым словам или знакам, те, которые передают всю информацию, находящуюся на винчестере ЭВМ, и просто уничтожающие ее.

Утечка информации за счет ПЭМИН

Одной из наиболее вероятных угроз перехвата информации в системах обработки данных считается утечка за счет перехвата побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами.

ПЭМИН существуют в диапазоне частот от единиц Гц до полутора ГГц и способны переносить (распространять) сообщения, обрабатываемые в автоматизированных системах. Дальность распространения ПЭМИ исчисляется десятками, сотнями, а иногда и тысячами метров.

Наиболее опасными источниками ПЭМИН являются дисплеи, проводные линии связи, накопители на магнитных дисках и буквопечатающие аппараты последовательного типа.

Например, с дисплеев можно снять информацию с помощью специальной аппаратуры на расстоянии до 500-1500 метров, с принтеров до 100-150 метров. Перехват ПЭМИН может осуществляться и с помощью портативной аппаратуры. Такая аппаратура может представлять собой широкополосный автоматизированный супергетеродинный приемник. В качестве устройств регистрации принятых сигналов (сообщений) может использоваться магнитный носитель или дисплей.

Итак, была представлена краткая характеристика возможных каналов утечки информации, которые можно отнести к разряду наиболее вероятных для любого государственного или коммерческого предприятия, фирмы, банка, организации, учреждения. Полученные сведения можно теперь использовать на первом этапе построения комплексной системы защиты информации, то есть при анализе угроз утечки конфиденциальной информации.

УДК 681.3

Арлинский О.Ю., Дегтярева Л.Н.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БЕСПРОВОДНЫХ СЕТЯХ

В статье анализируются ключевые проблемы процесса создания беспроводной связи, обеспечение безопасности итоговой инфраструктуры локальной сети и предлагаются методы, позволяющие сделать эту работу эффективной.

В настоящее время устройства беспроводной связи на базе стандартов 802.11x продвигаются на рынках сетевого оборудования очень интенсивно. Процедура развертывания беспроводной сети подразумевает ряд мероприятий, направленных на обеспечение безопасности итоговой инфраструктуры. Пренебрежение проблемами несанкционированного доступа вызвано некоторой инерционностью внедрения беспроводных технологий, но популярность данного вида связи растет быстрыми темпами, т.к., если безопасности не уделять должного внимания, то такую сеть можно считать публичной, что неизбежно приведет к нарушению ее функционирования.

Сам принцип беспроводной передачи данных заключает в себе возможность несанкционированных подключений к точкам доступа. При разработке корпоративной сети администраторы в первую очередь заботятся о качественном покрытии территории офисов, не учитывая того, что «взломщики» сети могут подключиться к ней даже из автомобиля, припаркованного на улице. Не менее опасная угроза - вероятность хищения оборудования. Часто несанкционированное подключение точек доступа к ЛВС выполняется самими работниками предприятия. Защиту информации при подключении к сети таких устройств сотрудники обеспечивают тоже самостоятельно, не всегда задумываясь о последствиях.

Решение подобных проблем требует комплексного подхода. В данной статье не рассматриваются организационные мероприятия - они чаще всего выбираются исходя из условий работы каждой конкретной сети. А к мероприятиям технического характера можно отнести использование обязательной взаимной аутентификации устройств и внедрение активных и пассивных средств контроля.

Но нужно отметить, что методы обеспечения безопасности сетей 803.11x на этапе их начального развития (1997-98 годы) использовались не совсем неудачные. Только в 2001 году появились первые реализации драйверов и программ, позволяющих справиться с шифрованием WEP.

Пользователь может быть спокоен, если у него появится возможность обеспечить решение трех проблем для своего трафика: конфиденциальность (данные должны быть надежно зашифрованы), целостность (данные гарантированно не должны быть изменены третьим лицом) и аутентичность (надежная проверка того, что данные получены от правильного источника).

В настоящее время в различном сетевом оборудовании, в том числе в беспроводных устройствах, широко применяется более современный, по сравнению со стандартами 1997-1998 годов, способ аутентификации, который определен в стандарте 802.1x. Принципиальное отличие его от прежних способов аутентификации заключается в следующем: пока не будет проведена взаимная проверка, пользователь не может ни принимать, ни передавать никаких данных. Стандарт предусматривает также динамическое управление ключами шифрования, что, естественно, затрудняет пассивную атаку на WEP. Принято считать, что разграничение доступа, основанное на разделении аппаратных MAC-адресов беспроводных сетевых адаптеров на "своих" и "чужих", является эффективным средством противодействия атакам. Это действительно так, но лишь при обеспечении дополнительных мер безопасности.

Кстати, аутентификация беспроводного клиента по MAC-адресу - исключительно инициатива конкретного производителя, спецификации беспроводных стандартов 802.11b/g такой меры безопасности не предусматривают. То есть подобный метод аутентификации может либо присутствовать, либо нет, - в зависимости от желания и маркетинговой политики производителя.

Даже если существует возможность "отсеивания" чужих беспроводных клиентов, полностью полагаться на эту меру не стоит - ее взлом занимает считанные минуты и доступен даже начинающему хакеру с неоконченным средним образованием. Суть взлома такова: при помощи специальной утилиты прослушивается радиообмен точки доступа на канале, по которому происходит обмен информацией с клиентами, и в полученном трафике выделяется список "своих" клиентов. Затем остается лишь программно подменить аппаратный адрес своего беспроводного адаптера на один из списка валидных адресов (в подавляющем большинстве случаев это можно сделать даже стандартными средствами драйвера) - и "чужой" адаптер стал "своим".

На сегодняшний день разумными считаются три средства, дополняющие уже имеющиеся, - стандарты IEEE 802.1x, 802.11i и протокол WPA.

IEEE 802.1x применяется для авторизации, аутентификации и аккаунтинга пользователей, чтобы проверить возможность предоставления доступа к сети. В случае 802.1x используются уже динамические ключи шифрования, что является несомненным плюсом. 802.1x предназначен для работы со сторонними средствами, такими как сервер RADIUS (Remote Access Dial-In User Server) и протокол EAP (Extensive Authentication Protocol).

Сервер RADIUS - своего рода "проходная", вахтер на которой самостоятельно решает, пустить пользователя в сеть или нет. К чести некоторых производителей беспроводного доступа (например, D-Link и U.S. Robotics), возможность авторизации и аутентификации пользователя на сервере RADIUS с помощью 802.1x предусмотрена даже в достаточно старых устройствах стандарта 802.11b.

В настоящее время есть несколько популярных реализаций RADIUS-серверов: FreeRadius, GNU Radius, Cistron Radius, Radiator Radius, Microsoft IAS, Advanced Radius. Некоторые из них - коммерческие продукты, некоторые - доступны для бесплатного испо-

льзования с соблюдением соответствующих лицензионных требований. При этом часто используются такие термины, как "авторизация", "аутентификация" и "аккаунтинг". Под аутентификацией понимается процесс определения тождественности пользователя, в наиболее общем виде - посредством имени ("логина") и пароля. Авторизация - это определение сетевых сервисов, доступных конкретному пользователю, и сервисов, к которым доступ запрещен. Наконец, аккаунтинг – «журналирование» использования сетевых ресурсов и сервисов.

В общем случае алгоритм привязки RADIUS-сервера к беспроводной сети может быть таков:

1. Сетевой администратор дает команду RADIUS-серверу завести новую учетную карточку пользователя с занесением в нее имени пользователя, под которым он будет проходить аутентификацию, и его пароля.
2. Внесенный в базу RADIUS-сервера пользователь с помощью беспроводной связи подключается к точке доступа, чтобы проверить электронную почту.
3. Точка доступа запрашивает у пользователя его имя и пароль.
4. Точка доступа связывается с RADIUS-сервером и дает запрос на аутентификацию пользователя.
5. RADIUS-сервер находит валидные имя пользователя и пароль, дает добро на новую сессию и заводит в журнале соответствующую запись о начале новой сессии.
6. Точка доступа предоставляет пользователю возможность работать с теми сервисами, которые ему предписаны (это и есть авторизация).
7. По окончании сессии, которая может быть прервана либо самим пользователем, либо RADIUS-сервером (например, истек "нарезанный" по регламенту промежуток времени работы), RADIUS-сервер делает в журнале запись об окончании сеанса.

Эта процедура достаточно строгая, но в тоже время логически верная - хотя и относится лишь к управлению доступом.

Следует отметить, что до сих пор удачных попыток взлома 802.1x не зафиксировано, поэтому можно сделать вывод, что развитие идет в верном направлении. 802.11i предусмотрен в качестве глобальной замены WEP (его иногда называют также WPA2). 802.11i является как бы "надмножеством" WPA - сочетает все его возможности со своими оригинальными. 802.11i использует гораздо более мощный, нежели RC4 у WEP, алгоритм шифрования - это AES (Advanced Encryption Standart).

В действительности построить хорошо защищенную сеть можно и при помощи уже имеющихся средств - даже несмотря на WEP, SSID broadcasting и MAC-доступ. Хорошо зарекомендовавшее себя решение - Virtual Private Network, виртуальная частная сеть, в которую можно "завернуть" всю беспроводную сеть вместе с ее огрехами в области безопасности. Средства VPN работают на глобальном сетевом уровне, поэтому, видимо, в настоящее время это один из немногих способов обеспечения достойной безопасности - благо технология IPSec портирована с IPv6 на IPv4.

Выводы

При условии использования современного оборудования и программного обеспечения, в настоящее время вполне возможно построить на базе стандартов серии 802.11x защищенную и устойчивую к атакам беспроводную сеть.

Однако почти всегда беспроводная сеть связана с проводной, а это, помимо необходимости защищать беспроводные каналы, является побуждением к внедрению новых методов защиты в беспроводных сетях. В противном случае сеть будет иметь фрагментарную защиту, что, по сути, является угрозой безопасности. Желательно использовать оборудование, имеющее сертификат Wi-Fi Certified, то есть подтверждающий соответствие WPA. Категорически недопустимо в серьезных беспроводных сетях, устанавливая в локальную сеть устройства, оставлять настройки производителя по умолчанию.

В случае смешанной сети следует использовать виртуальные локальные сети; при наличии внешних антенн применяется технология виртуальных частных сетей VPN.

Необходимо сочетать как протокольные и программные способы защиты, так и административные.

При планировании защищенной беспроводной сети необходимо учитывать, что любое шифрование или другие манипуляции с данными неизбежно приводят к дополнительным задержкам, увеличивают объем служебного трафика и нагрузку на процессоры сетевых устройств. Безопасность – важный фактор в современных сетях, но он теряет всякий смысл, если трафик пользователя не получает должной полосы пропускания. Сети создаются, в конечном счете, не для администраторов, а для пользователей.

Литература

1. Беспроводные линии связи и сети. Столлингс В. - М, СПб, К: Вильямс, 2003 г. - 640 с.
2. Сети и системы радиодоступа. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. - М: Эко-Трендз, 2005 г. - 384 с.
3. Основы построения беспроводных локальных сетей стандарта 802.11: Практическое руководство по изучению, разработке и использованию беспроводных ЛВС стандарта 802. Рошан П., Лиэри Дж. - К,М,СПб: Вильямс, 2004 г. - 304 с.
4. Безопасность беспроводных сетей: Идентификация угроз, присущих беспроводным системам; Разработка и внедрение плана мобильной безопасности, защита от нападения хакеров. Максим М., Поллино Д. - М: ДМК Пресс /Компания АйТи, 2004 г. - 288 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМАХ

УДК 656.073

Гусев Ю.В., Слободянюк М.Э.

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНЫХ НОРМАТИВОВ ВЗАИМОДЕЙСТВИЯ СМЕЖНЫХ ЗВЕНЬЕВ ЛОГИСТИЧЕСКИХ ТЕХНОЛОГИЙ ПРЕДПРИЯТИЙ

Поставка сырья, отгрузка продукции и межцеховые перевозки рассматриваются как логистические технологии, которые взаимодействуют между собой, обслуживаются одними и теми же аппаратами и занимают общие зоны простоя и хранения. Рис. 1. Ист. 2.

Транспортная система промышленного предприятия, являясь частью производственно-транспортной системы (ПТС), может рассматриваться как совокупность исполнительных (обеспечивающих) подсистем, объединенных в последовательные технологические линии или логистические технологии (ЛТ). Такое выделение позволяет решать проблему повышения эффективности функционирования ПТС за счет оптимизации работы звеньев ЛТ.

Логистическая технология (технологическая последовательность транспортно-грузовых, коммерческих и информационных операций) представляет собой совокупность обслуживающих аппаратов и накопителей, которые характеризуют производительную силу ПТС. К обслуживающим аппаратам относятся маневровые локомотивы, погрузочно-разгрузочные машины и комплексы, автомобильный транспорт и др., к накопителям — резервные емкости путей сортировочного парка и зоны хранения, а также дополнительное количество погрузочных средств производственных цехов, которое задействуется для освоения потока перерабатываемых грузов.

В качестве первого условного накопителя, размеры которого не оптимизируются, принимается поток поездов, поступающих в зону сортировочного парка в расформирование. К первому обслуживающему аппарату и второму накопителю соответственно относятся маневровые локомотивы и пути сортировочного парка. Перечисленные элементы являются общими для всех ЛТ, включающих в себя железнодорожный транспорт. Следует отметить, что в качестве подобных условных накопителей могут выступать в зависимости от вида ЛТ и другие элементы внешней среды ПТС, нормативы которых не оптимизируются в данном случае. В то же время совокупность этих нормативов должна строго соблюдаться при оптимизации функционирования ПТС.

В рамках активного стратегического управления на базе возможной интеграции с отдельными элементами внешней среды должна предусматриваться система совершенствования и оптимизации нормативов внешней среды, к которым можно отнести параметры графика движения поездов, тарифы, спрос на транспортные услуги, параметры работы смежных с железнодорожным видов транспорта и др.

В зависимости от рода перерабатываемого груза и схемы механизации и автоматизации погрузочно-разгрузочных работ в зоне хранения число аппаратов и накопителей в технологических линиях может быть различным. Так, если на грузовом фронте тарно-штучные грузы перерабатываются электропогрузчиками, а в зоне хранения – кранами-штабелерами, то в этом случае для оптимального согласования производительностей двух типов ПРМ в зоне хранения могут присутствовать накопители.

Следует отметить, что при существующих условиях поставок сырья и отгрузки продукции производительность обслуживающих аппаратов подвержена случайным колебаниям, и могут быть заданы лишь вероятности, с которыми размеры перерабатываемых потоков вагонов и грузов принимают те или иные значения. Игнорирование случайного характера входящих потоков транспортных средств и грузов при выборе параметров, ха-

рактеризующих техническое оснащение и технологию подсистем ПТС, может вызвать значительные сбои в работе. Это будет выражаться в непроизводительном простое транспортных средств, погрузочно-разгрузочных машин и нарушении ритмичного протекания производственного процесса.

В этих условиях, чем больше размеры накопителей, тем легче преодолеть любые колебания размеров входящих потоков транспортных средств и грузов, оказывающих влияние на перерабатывающую способность подсистем комплекса. Однако с увеличением размеров накопителей возрастают затраты на строительство и эксплуатацию ПТС. Поэтому возникает задача нахождения таких размеров накопителей, которые минимизируют величину логистических затрат, при заданном количество вагонов и грузов, необходимых для стабильной работы предприятия.

Обслуживающие аппараты и накопители задействуются одновременно несколькими ЛТ, поэтому основным технологическим критерием выбрана величина грузопотока, перерабатываемого одним элементом ПТС (рис. 1).

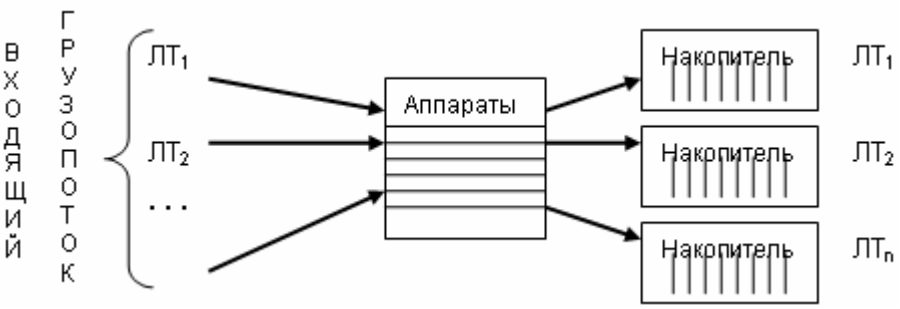


Рис. 1. Смежные звенья логистических технологий, перерабатываемые i-м элементом ПТС.

Экономико-математическая модель определения оптимальных нормативов взаимодействия смежных звеньев ЛТ включает в себя математическое ожидание размера перерабатываемого грузопотока за U временных интервалов ЛТ $F_{ср}$ и определяется по выражению

$$F_{\text{ñð}}\left(B_{J_k+1},\bar{b}_i\right)=\sum_{u=1}^{U}\sum_{k}^{K}\sum_{j_k=1}^{j_k}\alpha\sum_{P_{J_k}^u\in M_{J_k}}P_{J_k}^u\,\bar{a}^u\left(P_{J_k}^u\middle|B_{J_k}\right),\qquad(1)$$

где B_{j_k+1} - вектор оптимизируемых параметров, составляющими которого являются размеры резервных накопителей;

$\bar{b}_i$ - вектор неуправляемых параметров, характеризующих i-е звено ЛТ;

$J_k = 2, \ldots, J_k+1$ – число резервных накопителей k-й ЛТ, размеры которой оптимизируются (k = 1, …, K – количество ЛТ);

α – заданные интервалы дискретности в пространстве состояний фактической производительности звеньев ЛТ;

$P_{J_k}^u$ - фактическая производительность обслуживающего аппарата k-й ЛТ за u-й временной интервал;

$\bar{a}^u\left(P_{J_k}^u\middle|B_{J_k}\right)$ - вероятность различных состояний фактической производительности при условии, что вектор оптимизируемых нормативов резервов (размеров резервных накопителей) примет значение B_{Jk}.

Введение условной вероятности позволяет учесть, что производительность маневровых локомотивов, ПРМ в определенный момент времени зависит от мощности входя-

щего потока вагонов, отгружаемой продукции, количества хранимого груза, которые, в свою очередь, определяются вместимостью сортировочных путей, зоны хранения. Например, фактическая производительность ПРМ характеризуется размером входящего потока вагонов на грузовой фронт и свободной вместимостью зоны хранения для аккумуляции перерабатываемого грузопотока.

Максимизация приведенного выше функционала осуществляется при следующих ограничениях. Перерабатываемый грузопоток k-й ЛТ за u временных интервалов должен быть не менее задаваемой основным производством величины. Возможности сооружения сортировочных путей и развития зон хранения ограничены имеющимися размерами территории.

Проблема обеспечения гарантии качественного обслуживания непосредственно связана с задачей определения оптимальных размеров резервов. Управление качеством транспортного обслуживания означает управление резервами технических средств, перерабатывающей способности комплекса, которое обеспечивало бы переработку заданного объема работы и максимизировало эксплуатационную надежность данного предприятия. Вместе с тем, при определении оптимальных резервов в области коммерческой деятельности необходимо учитывать фактор ограничения на используемые ресурсы. Определение оптимального сочетания размеров перерабатывающей способности (производительной силы) подсистем ПТС и размера получаемой прибыли в условиях действия рыночных факторов (в частности, риска) является важным фактором устойчивого функционирования любой логистической системы.

Литература

1. Концепция повышения эффективности управления вагонопотоками на предприятии. // В.Э. Парунакян, В.А.Бойко, Ю.В.Гусев // Вестник ПГТУ: Сб. науч. тр. Вып. 13 – Мариуполь, 2003;

2. Логистические транспортно-грузовые системы: Учебник для студ. высш. учеб. заведений/ В.И.Апатцев, С.Б.Лёвин, В.М.Николашин, Издательский центр «Академия», 2003.-304с.

УДК 621.372

Глущенко В.Ю.

КОНЦЕПЦИЯ ВНЕДРЕНИЯ СТРАТЕГИЧЕСКОГО ПЛАНИРОВАНИЯ И УПРАВЛЕНИЯ НА ПРЕДПРИЯТИЯХ ЖИЛИЩНО-КОММУНАЛЬНОЙ СФЕРЫ

Рассматривается концепция формирования организационной структуры предприятий жилищно-коммунального хозяйства региона при внедрении на них стратегического планирования и управления.

Постановка проблемы

На сегодняшний день, спустя годы реформ в сфере жилищно-коммунального хозяйства, многие проблемы и противоречия только обострились, что требует выбора более активной позиции, эффективных и взвешенных действий со стороны муниципальных властей в решении задач управления развитием сектора жилищно-коммунальных услуг.

Проблемы регионального развития и реорганизации жилищно-коммунального хозяйства нашли свое отражение в научных работах ученых-экономистов и практиков. Значительный вклад в разработку данной проблемы сделали: С.И. Бандур, В.Н. Лексин, М.Я. Лемешев, Л.В. Мельник, А.З. Пронин, В.А. Смирнов, В.О. Солодкий, М.Ф. Тимчук, Л.Н. Чернышев, М.Г.Чумаченко, Я.Я. Шепель, П.И. Кассиди, Б.К. Кетс, П. Ликинс, Р.Л. Кемп и др., в работах которых приводится широкий спектр подходов к решению данных проблем.

Однако в современных условиях реформирования жилищно-коммунального хозяйства (ЖКХ) Украины одной из наиболее актуальных проблем становится разработка методологических и методических основ стратегического управления предприятиями

всех уровней данной сферы. Это объясняется тем, что состояние ЖКС сегодня характеризуется как "катастрофическое" [1, 2].

Цель статьи

Обоснование концепции на формирование организационной структуры предприятий жилищно-коммунального хозяйства региона при внедрении на них стратегического планирования и управления.

Предлагаемая концепция базируется на принципах и методах системного подхода, ключевыми положениями которого являются:

1. Любой объект ЖКХ регионального уровня рассматривается в качестве целостной социально-экономической системы (ЦСЭС), для функционирования и развития которой характерны определенные закономерности и тенденции.

2. Функционирование и развитие ЦСЭС осуществляется в тесной взаимосвязи и взаимодействии с внешней средой (внешним окружением).

В современных условиях приоритетным направлением деятельности любой ЦСЭС становится обеспечение ее жизнеспособности и устойчивого развития на долгосрочную перспективу. С этой целью органы управления любого уровня иерархии должны выполнять ряд функций, основными из которых являются:

1. Функция адаптации, означающая умение любой ЦСЭС достаточно быстро реагировать на постоянно изменяющиеся условия внешней среды в целях обеспечения доступа к необходимым ресурсам при одновременном сохранении своей самостоятельности и самобытности.

2. Функция целенаправленности, предусматривающая обоснование и выбор целей деятельности (целеполагание), а также разработку механизма реализации поставленных целей.

3. Функция интеграции, связанная с формированием достаточно четкой организационной структуры управления ЦСЭС, которая обеспечивала бы сохранение целостности организационных действий внутри нее, включая контроль за деятельностью отдельных ее элементов (подсистем).

4. Функция состоятельности, предполагающая необходимость учета действия социальных факторов при разработке стратегии развития любой ЦСЭС.

Однако на практике обеспечение жизнеспособности любой ЦСЭС регионального уровня и ее устойчивого развития в значительной мере зависит от следующих факторов:

• сложившегося механизма взаимоотношений между государственными органами управления различных уровней (федеральными, региональными и муниципальными);

• существующего механизма взаимоотношений между государственными органами управления всех уровней и предприятиями ЖКХ.

Механизм управления предприятиями ЖКХ должен иметь индикативный характер, в основе которого возложены экономические интересы производителей и потребителей, которые гибко регулируются государством и местными органами власти и создают условия для улучшения качества жилищно-коммунальных услуг. В таком механизме применяются прямые и косвенные экономические и правовые рычаги управления. К прямым экономическим рычагам следует отнести целевое финансирование конкретных направлений деятельности, проектов и мероприятий; хозяйственные договоры; местные заказы и контракты. Косвенными регуляторами являются местные налоги, платежи, льготные кредиты, договорные тарифы и цены. Составными элементами механизма являются также и организационные рычаги, обеспечивающие выполнение обязательных требований и условий. Они необходимы для организации разработки прогнозов, планов, заключения договоров на выполнение работ, проведения налоговой и финансово-кредитной политики управления областью. Формирование механизма управление ЖКХ следует осуществлять на следующих принципах:

– приоритет социальных, региональных и местных интересов над ведомственными, отраслевыми и локальными;

– антимонопольная политика;

– распределение функций заказчика и исполнителя и привлечение к области подчинительных организаций разных форм собственности, создание конкурентных условий деятельности;

– нормативный принцип ресурсосбережения и выделение разных уровней обеспечения потребителей;

– использование разных источников финансирования: централизованных и децентрализованных финансовых ресурсов.

Применение такого механизма возможно в организациях жилищно-коммунального хозяйствования, построенных на иных, чем сейчас существующих, концептуальных подходах.

Для развивающихся и обновляющихся предприятий характерно усиление стратегической направленности их деятельности. Постепенно осуществляется переход от традиционных к адаптивным стратегическим организационным структурам [3]. Для успешного стратегического развития предприятие должно иметь четкое стратегическое видение или эффективную стратегическую обобщающую цель своей деятельности.

Стратегия не возникает стихийно, она является результатом формулирования компанией своих целей, которые вытекают из ее миссии.

Поэтому проблема пересмотра и формулирования эффективной миссии предприятий ЖКХ является сегодня весьма актуальной.

Связь таких основных понятий как «миссия», «цель» и «стратегия» представлена на рисунке.

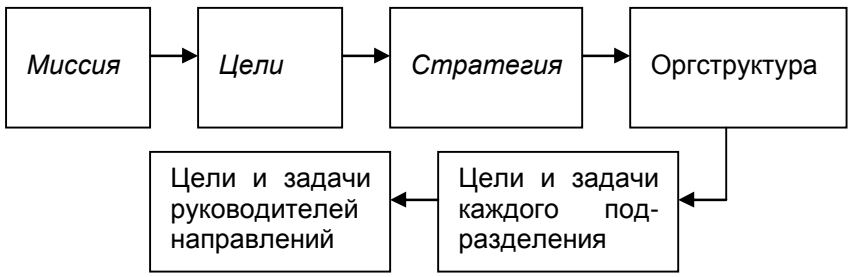


Рис. Схема формирования цели руководителей направлений.

Основополагающим фактором формирования миссии предприятий ЖКХ является придание данной области экономики Украины статуса социально-экономической сферы, основное назначение которой - полное удовлетворение потребностей населения в жилищно-коммунальных услугах.

Как показывает опыт и практика зарубежных стран, в первую очередь, бывших социалистических, для предприятий ЖКХ наиболее перспективными оказались миссии, ориентированные на конечный результат и клиента.

Очевидно, что говорить о приватизации и реструктуризации предприятий жилищно-коммунальной сферы Украины можно лишь после того, как будет повышена эффективность этой отрасли. Кроме того, в разных регионах вопрос о приватизации должен решаться по-разному. Во многих секторах жилищно-коммунальной сферы конкуренция и не возникнет. Так что для реформы ЖКХ нужна целевая программа модернизации, базируемая на использовании современных технологий.

Для достижения положительных результатов на предприятиях необходима активизация его внутренних возможностей, изменение стратегии, реорганизация и создание эффективной системы управления, иначе говоря - его реформирование. Это требует включения целой цепочки последовательных изменений, которые ведут от старой формы хозяйствования к новой, позволяют создать новый внутренний экономико-хозяйственный механизм, отвечающий происходящим изменениям во внешней среде.

Подчеркнем, что одним из направлений реформирования предприятий ЖКХ является его структурная реорганизация. Этот процесс содержит в себе повышение хозяйствен-

ной самостоятельности подразделов, достижение той или другой степени их экономического обособления, а также связанные с этим процессы изменения ассортимента работ и услуг, кадровой, финансовой и маркетинговой политики предприятия.

Одним из эффективных инструментов оптимизации организационно-экономической структуры предприятия и достижения сбалансированности всех его систем управления является реинжиниринг бизнес-процессов с ориентацией на клиента.

Сегодня реинжиниринг является важным фактором успешного и стабильного развития, мощным управленческим инструментом, главным потенциалом менеджмента. Это делает его чрезвычайно важным элементом повседневной жизни для многих компаний в условиях перехода к рыночным отношениям.

Другой важной характеристикой реинжиниринга является способ осуществления изменений. Реинжиниринг означает отказ от сложившихся традиций, устоявшихся правил и подходов и воспроизводит новый деловой процесс «с чистого листа». Это позволяет преодолеть прошлый стереотип экономического мышления, негативное воздействие сложившихся хозяйственных догм, что особенно актуально для давно работающих предприятий, плохо адаптированных к рыночным условиям. Именно такими унитарными предприятиями являются предприятия ЖКХ Украины. Реформируя деловой процесс с его истоков, реинжиниринг радикально меняет деловую внутрифирменную среду, снимает остроту проблемы разрушения вертикальных или горизонтальных связей, сложившихся на предприятии [4].

В качестве центрального звена при реинжиниринге выступают современные информационные технологии, играющие в данном случае роль конструктивного фактора. Само по себе использование компьютерных технологий в управлении не дает нового качества и количества хозяйственной деятельности в целом. Реинжиниринг по-новому организует бизнес-процессы и интегрирует в новые бизнес-процессы компьютерные технологии и современные коммуникации. Реальная сила технологии заключается не в том, что она позволяет старым процессам функционировать лучше, а в том, что она дает возможность сломать старые правила и создать новые способы работы.

Возможность такой революции обусловлена, в первую очередь, новейшими достижениями в области информационных технологий, специалисты которой начинают играть ведущую роль в конструировании бизнеса.

Реинжиниринг является направлением, возникшим на стыке двух различных сфер деятельности - управления (менеджмента) и информатизации. Именно поэтому реинжиниринг требует новых специфических средств представления и обработки проблемной информации, понятных как менеджерам, так и разработчикам информационных систем. Подобные средства требуют интеграции ключевых достижений информационных технологий и создания соответствующих инструментальных средств поддержки реинжиниринга.

В настоящее время в сегменте регионального рынка ЖКУ исходными моментами хозяйственной деятельности являются непосредственное оказание услуги, оплата клиентом услуги, способ доведения услуги до потребителя и т.д., то есть в основе разделения хозяйственной деятельности на отдельные процессы лежит функциональный принцип.

С точки зрения бизнес-процессов, необходимо отметить, что услуги, в отличие от товаров, исторически имеют более конкретную направленность на клиента. Учитывая стремление производящих компаний к сопровождению своих товаров определенной совокупностью услуг, усматривая в этом финансовую выгоду и укрепление конкурентных позиций, предложение услуг в последнее время равнозначно предложению товаров.

В этом смысле понимание бизнеса не как совокупности простейших задач, а как единого бизнес-процесса, в качестве которого может выступать обслуживание клиента, не сопровождается коренной ломкой управленческой структуры и сознания менеджеров. То есть услуги более органично вписываются в базовое понятие реинжиниринга, нежели хозяйственные структуры. Это означает, что, с одной стороны, реинжиниринг в сфере услуг может быть осуществлен относительно безболезненно, а, с другой, резко повышается вероятность его успеха и создает условия и предпосылки для диверсификации.

Диверсификация сегодня стала столь популярна среди теоретиков и практиков управления, что быстро заняла место одной из стратегических «панацей» постсоветской экономики.

Под диверсификацией для предприятий ЖКХ будем понимать увеличение числа производств и номенклатуры товаров или услуг, производимых в новых для них сферах.

Принятие программы инновационного развития ЖКХ Украины инициализировало внедрение новых энергосберегающих технологий, средств контроля и современных разработок во всех сферах услуг, предоставляемых населению.

Выделяют следующие виды диверсификации:

• интеграция вперед по технологической цепочке – компания берет на себя обязанности и функции, ранее выполнявшиеся третьей стороной;

• интеграция назад по технологической цепочке – организация производств или покупка предприятий, аналогичных тем, которыми владеют поставщики фирмы;

• концентрическая диверсификация – когда компания ищет новые товары и рынки, обладающие сходными чертами с уже принадлежащими ей;

• конгломератная диверсификация – когда компания пытается пробиться на совершенно новый для нее рынок с новым товаром.

Результаты анализа, проведенного автором, свидетельствуют, что для предприятий ЖКХ Украины целесообразны концентрическая и конгломератная диверсификации. Это объясняется тем, что развитие рынков новых строительных технологий, внедрение современных ресурсосберегающих технологий и устройств практически происходит без участия предприятий ЖКХ.

Использование для преобразования организационно-экономической структуры предприятия реинжиниринга, диверсификации или их одновременно, в определенном сочетании, должно регламентироваться задачами, стоящими перед каждым конкретным предприятием ЖКХ.

Выводы

Таким образом, когда говорится о структурной перестройке ЖКХ, нужно понимать, что это только часть сложного и многопланового процесса организационного, экономического реформирования с совершенствованием внутрихозяйственного расчета, конечная цель которого - добиться безубыточной работы предприятий ЖКХ. Все эти меры должны создать условия для инвестиционной привлекательности сферы жилищно-коммунальных услуг, выхода предприятий ЖКХ на новые рынки услуг.

Совершенствование организационно-экономической структуры субъекта хозяйственной деятельности должно осуществляться путем трансформации его вертикальных и горизонтальных связей. Для реформы ЖКХ нужна целевая программа его модернизации с использованием современных технологий.

Литература

1. Паршин А. Ледниковый период в Алчевске. Кто виноват и что делать? // Жизнь Луганска - 2006 - №13. С.8
2. Родионов Д.Г. Экономико-организационные основы реформирования жилищно-коммунального хозяйства.- Калуга, 2000 - 203 с.
3. Ритвельдт Д., Качалин В. Сравнительный анализ эффективности предприятий как инструмент стратегического планирования.
4. Проблемы теории и практики управления - 2000 -№3. С.40-44.
5. Тельнов Ю.Ф. Реинжиниринг бизнес-процессов: Компонентная методология. М.: Финансы и статистика. 2004 - 319 с.

УДК 621.372

Глущенко В.Е., Глущенко Ю.В.

ПОСТРОЕНИЕ МОДЕЛИ ФИНАНСОВОГО АНАЛИЗА ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СФЕР

Рассматривается концепция формирования организационной структуры предприятий жилищно-коммунального хозяйства.

Постановка проблемы

Вопрос реформирования социально-экономической системы на сегодняшний день является одним из приоритетных направлений политики правительства Украины. Базовые теоретические и практические вопросы реформирования жилищно-коммунального хозяйства (ЖКХ) нашли отражение в нормативных документах Президента, Верховной Рады и правительства Украины [1,2], в научных и практических работах отечественных ученых и специалистов, таких как: С.И. Бандур, В.Н. Лексин, Л.В. Мельник, А.З. Пронин, В.А. Смирнов, В.О. Солодкий, М.Ф. Тимчук, Л.Н. Чернышев, М.Г.Чумаченко, Я.Я. Шепель и др., в работах которых приводится широкий спектр подходов к решению данных проблем.

Однако вопросы исследования финансовой деятельности предприятий социально-экономической системы региона в условиях экономической и финансовой нестабильности, дефиците государственных и городских бюджетных средств на основе комплекса экономико-математических моделей на сегодняшний день недостаточно изучены, и их решение актуально.

Цель статьи

Построение модели анализа финансовой деятельности предприятий жилищно-коммунальной сферы.

Переориентация предприятий ЖКХ на конечный результат и клиентско-ориентированную стратегию деятельности показывает, что традиционные подходы бухгалтерского учета уже не соответствуют кардинально изменяющейся деловой среде.

В настоящее время перспективной стала система нового поколения Balanced Scorecard (BSC), «система сбалансированных показателей» и управленческая система учета и контроля, или management accounting and control system (MACS), представляет собой внутреннюю среду для принятия решений и управления организацией.

Предприятие находится под контролем, если оно следует в направлении достижения своих стратегических целей. Процесс поддержания организации в состоянии контроля состоит из следующих стадий [3].

1. Планирования, заключающегося в выработке организационных целей, выборе видов деятельности для достижения целей и отборе показателей, с помощью которых можно определить, насколько полно поставленные цели были достигнуты.

2. Исполнения — воплощения плана в жизнь.

3. Мониторинга — процесса измерения текущего исполнения.

4. Анализа — сравнения полученной информации о текущем уровне, достигнутом системой, с запланированным уровнем для того, чтобы установить любые расхождения и наметить корректирующие действия.

5. Исправление положения заключается в принятии соответствующих мер, с целью вернуть систему в управляемое состояние (состояние контроля).

Каждое предприятие ЖКХ является уникальным, однако чем бы ни занималось каждое из них в отдельности, все они применяют один и тот же основной процесс контроля. Единственное ключевое различие состоит в определении наиболее подходящих показателей оценки исполнения, используемых предприятием. Этот выбор определяется средой, в которой оно функционирует.

При выборе и проектировании системы управленческого учета и контроля в организации следует помнить о двух ее аспектах: поведенческом и техническом.

Учет поведенческого аспекта в MACS предполагает:

–ориентацию на кодекс этического поведения организации;

–использование сбалансированной системы показателей;

–наделение сотрудников полномочиями принимать решения и участвовать в разработке самой системы контроля;

–разработку адекватной системы стимулирования за достигнутые результаты.

С технической стороны MACS характеризуется масштабом системы и релевантностью генерируемой ею информации. Что касается масштаба, то многие MACS измеряют и оценивают результат только в одном звене цепочки ценностей, а именно, в текущем производственном процессе. Главным недостатком таких систем является то, что они игнорируют предпроизводственные и послепроизводственные затраты, связанные с продуктами и услугами.

Поскольку такие затраты на предприятиях ЖКХ достигают внушительных размеров, отсутствие информации о них ставит организации в заведомо невыгодное положение. Менеджеры в этом случае пытаются выяснить уровень полных затрат жизненного цикла продукта или услуги, когда затраты предопределены и управлять ими поздно.

Роль информации состоит в том, чтобы помочь менеджменту оценить, достигает ли организация своих целей.

Оценивая современное состояние систем управленческого учета на предприятиях ЖКХ Украины, можно сказать, что служба, обеспечивающая учетно-аналитическую функцию, например, служба контроллинга, практически на всех из них все еще не выделена в качестве самостоятельной структурной единицы.

Большинство предприятий ориентируются на традиционные для них структуры. Некоторые предпочитают передать функции контроллера организации подразделениям, оказавшимся не у дел в результате краха плановой государственной системы и проводимой на предприятии реструктуризации, а именно, планово-экономическим службам, другие создают в рамках бухгалтерии направление управленческого учета с теми же задачами.

Процесс реформирования ЖКХ показывает, что потребности менеджеров в профессиональных услугах бухгалтеров-аналитиков уже давно вышли за пределы только информационной поддержки. Руководители нуждаются в аналитической обработке учетной информации для принятия решений. Им также нужна система обратной связи и раннего оповещения для оперативного контроля и оценки исполнения. Качественную и надежную информацию для принятия управленческих решений, планирования и контроля должна генерировать и предоставлять менеджменту служба управленческого учета или контроллинга.

В зависимости от решаемых задач предприятие может быть рассмотрено с различных точек зрения, например: как логистическая система; как система движения финансов; как система движения документов и т. д. Естественно, каждая точка зрения инициируется возникновением определенных проблем на предприятии, связанных с планированием, контролем, учетом и управлением ресурсами. Чтобы разобраться с этими проблемами, в первую очередь, нужно отразить протекающие на предприятии бизнес-процессы в определенной осязаемой для менеджера форме. Другими словами, современное предприятие должно иметь свою бизнес-модель. Бизнес-модель предприятия - это система графических и текстовых описаний, позволяющих понимать суть процесса управления предприятием [3].

Международные стандарты ISO серии 9000:2000 представляют собой мощный стимул для развития моделирования деятельности организации.

К основным современным методам и средствам моделирования деятельности предприятий относятся:

- совокупность подходов и методов (языков), объединенных общим названием "интеграционная дефиниция" (integration definition, IDEF), в частности, методы функциональ-

ного моделирования IDEF0, информационного моделирования IDEF1, моделирования процессов IDEF3 и т.д.;

- унифицированный язык моделирования (Unified Modeling Language, UML), в основе которых положены различные языки объектно-ориентированного программирования, но, тем не менее, включающий в себя средства, выходящие далеко за их рамки.

Исследование основных требований к данному классу моделей показывает, что при классическом подходе к внедрению процессной модели управления необходимо создавать две бизнес-модели: исходную ("как есть") и целевую ("как должно быть"). Описание исходной модели (в заранее выбранной стандартной форме) требуется для того, чтобы выявить возможные недостатки в существующей системе управления предприятием. Данная модель необходима на стадии анализа и предназначена для оптимизации бизнес-процессов. Но здесь может возникнуть нюанс, связанный со временем, которое затрачивается на создание модели "как есть". Чем динамичнее развивается предприятие, тем меньше времени остается на ее описание (теряется актуальность). Как показывает практика, если достоверность модели к моменту ее завершения составит не более 70%, возможно, имеет смысл описать только основные бизнес-процессы, которые раскрывают последовательность шагов предприятия на пути достижения поставленных целей.

Любое знание и бизнес-модель имеют смысл, если используются постоянно на практике. Поэтому для поддержания бизнес-модели в актуальном состоянии необходимо создать условия, когда существование документации, формализующей бизнес предприятия, жизненно необходимо для функционирования самого бизнеса. Это возможно при условии, если на предприятии господствует устойчивое мнение, что бизнес-модель:

- вырабатывает общий язык взаимопонимания между центрами ответственности, принятия управленческих решений и исполнения;
- позволяет вырабатывать пошаговый план развития предприятия;
- обязательный этап внедрения информационной системы управления;
- единственно правильный путь к сертификации по стандарту ISO 9001:2000 (ДСТУ ISO 9001-2001);
- позволяет быстро и эффективно обучать новых работников конкретному направлению деятельности предприятия, т. к. диаграммы бизнес-процессов по сути являются наглядными должностными инструкциями; доступна для широкого круга пользователей и удобна в использовании.

Основываясь на этих принципах, авторами разработана модель финансового анализа деятельности предприятия ЖКХ.

Для реализации функций бизнес-моделей "как есть" и "как должно быть" модель представлена двумя основными блоками "Статистики" и "Анализ и прогнозы". Для представления зависимостей показателей и результатов анализа модель включает блок "Презентации".

В таблице приведены основные блоки модели и используемые ими данные.

Таблица

Раздел	Используемые данные
Статистики - входные данные; - бухгалтерские отчеты; - различные счета; - инструмент для вывода записи.	1. Статистическая отчетность о деятельности предприятий. 2. Бухгалтерские отчеты. 3. Тарифы. 4. Доходы предприятий. 5. Основные фонды, амортизация. 6. План инвестиций. 7. Данные анализа: - по горизонтали - по вертикали - анализ коэффициентов

продолжение таблицы

Анализ и прогнозы	1. Данные прогноза из раздела "Статистики". 2. Финансовые отчеты. 3. Планируемые тарифы. 4. Структура доходов. 5. Структура платежей. 6. План капитальных вложений. 7. План инвестиций. 8. Задолжники.
Презентации	1. Финансы и бюджет. 2. Источники финансирования. 3. Денежные потоки. 4. Коэффициент ликвидности. 5. Структура доходов. 6. Структура платежей. 7. Тарифы.

Блоки информационно связаны между собой базами данных и знаний, что обеспечивает гибкость модели, ее универсальность и легкость настройки на конкретные условия.

Блок "Статистики" использует данные о финансовой и хозяйственной деятельности предприятия, которые берутся из бухгалтерских отчетов за период не менее чем за три финансовых года. Поэтому структура таблиц этого раздела аналогична структуре форм статистической отчетности предприятия с добавлением колонок для записи данных трех предыдущих финансовых годов. Такая форма таблиц обеспечивает возможность накопления материала для оценки финансовой деятельности предприятия и динамики особо важных для прогнозирования показателей.

Оценка финансового состояния предприятия проводится с помощью:

- анализа коэффициентов - вычисление разных отношений между показателями отдельных статей отчетности;

- горизонтального анализа - определение параметров и тенденции их изменения, путем сравнения величин показателей за рассматриваемый интервал времени;

- вертикального анализа - определения удельного веса отдельных статей финансового отчета и их соотношения.

В модели реализован комплексный подход, учитывающий преимущества каждого из перечисленных методов.

Блок "Прогнозы" состоит из следующих двух частей: «Презентации» и «Анализ и прогнозы».

Процессы прогнозирования осуществляются поэтапно. На первом этапе проводится анализ фактических данных за прошедший период. Эти данные берутся из отчетов предприятий. Основные финансовые показатели, которые используются при анализе, берутся из стандартных форм квартальной и годовой бухгалтерской отчетности.

На втором этапе проводится согласование данных, получаемых в процессе анализа, с фактическими отчетными данными с целью определения характера тенденций изменения общеэкономических показателей.

На третьем этапе проводится непосредственно прогнозирование. Прогнозирование проводится в такой последовательности: прогнозирование доходов; прогнозирование затрат; прогнозирование изменений бухгалтерского баланса; пересмотр результатов и формирование детальной стратегии плана действий для достижения финансовой цели предприятия.

Презентационная часть представлена совокупностью таблиц, содержащих сводные данные блока "Статистики" и основные результаты прогнозов. По данным этих таблиц строятся диаграммы следующего содержания: финансирование из бюджета; источники

финансирования; денежные потоки; основные фонды; коэффициенты ликвидности; структура доходов и платежей; тарифы.

Диаграммы в наглядной форме демонстрируют результаты прогнозов.

Адаптация предприятия представляет процесс целенаправленного изменения параметров и структуры в ответ на происходящие изменения. Процесс адаптации носит импульсный характер, потому предприятие должно располагать удобным инструментом финансового планирования и контроля.

Рассмотренная модель является эффективным инструментом для проведения анализа финансового состояния, планирования и прогнозирования производственной деятельности коммунальных предприятий в условиях, когда остро ощущается отсутствие программ прогнозирования в рамках стратегического планирования и управления предприятием.

Модель реализована в стандартном программном пакете Microsoft Office 2000 и использует генератор электронных таблиц Excel. Все данные, используемые в различных разделах модели, представлены в виде таблиц, структура которых определяется видом документов и форм, из которых берутся эти данные.

Таким образом, модель представляет собой гибкий программный продукт, который можно дополнять и изменять с учетом потребностей конкретного пользователя.

Использование данной модели позволяет осуществлять выбор эффективного управления предприятием путем всестороннего анализа его финансовых возможностей и выделения финансов на решение первоочередных задач его развития.

Литература

1. Про схвалення Програми реформування і розвитку житлово-комунального господарства на 2002 - 2005 роки та на період до 2010 року. Постанова Кабінета міністрів України від 14.02.2002 р. № 130.// Офіційний вісник України.- 2002. - № 20.- С.977-998;

2. Про Стратегію та основні завдання підвищення ефективності роботи житлово-комунального господарства України. Рішення Держбуду від 23.07.2002 р. № 1. // Інформаційний бюлетень Держбуду.-2003, №1.- С.4-20;

3. Стерлин А. Р. Стратегическое планирование в промышленных корпорациях США. - М. Наука, 1990 - 256 с.

УДК 62:20

Махинько М.В.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ СИСТЕМНОГО ПРОЕКТУВАННЯ ПАКУВАЛЬНИХ АВТОМАТІВ

У статті розглянуто розробку інформаційної технології системного проектування пакувальних автоматів. Запропоновано структуру моделей об'єктів проектування в задачах підтримки прийняття проектних рішень. Розглянуто схеми евристичної підтримки процесу автоматизації проектування. Розглянуто перспективи впровадження технології в машинобудівну промисловість.

Вступ

В сучасних умовах розвитку економіки України великого значення набуває конкурентоспроможність продукції, що випускається на ринок. Для досягнення цієї мети необхідним є скорочення строків випуску, підвищення якості та зменшення собівартості. Як відомо, при налагодженні виробництва нового обладнання одним із ключових моментів є конструкторсько-технологічна підготовка виробництва даного обладнання. Актуальним у даній ситуації є створення інформаційних технологій, що орієнтовані на підвищення ефективності проектування нового обладнання.

У загальному вигляді конструювання нових пакувальних автоматів (НПА) – складний процес, що включає в себе задачі, які є складними на етапі формалізації та у більшості випадків вирішуються учасниками проекту емпіричними методами на базі власного досвіду. В даній ситуації доцільною є розробка інформаційної технології підтримки прийняття проектних рішень, в основі якої покладено *системні методи проектування*. Даний підхід на своїй меті має накопичення проектного досвіду, підвищення рівня культури проектування за рахунок збільшення використання аналітично розв'язаних проектних задач та забезпечення ефективності повторного використання накопичених проектних знань.

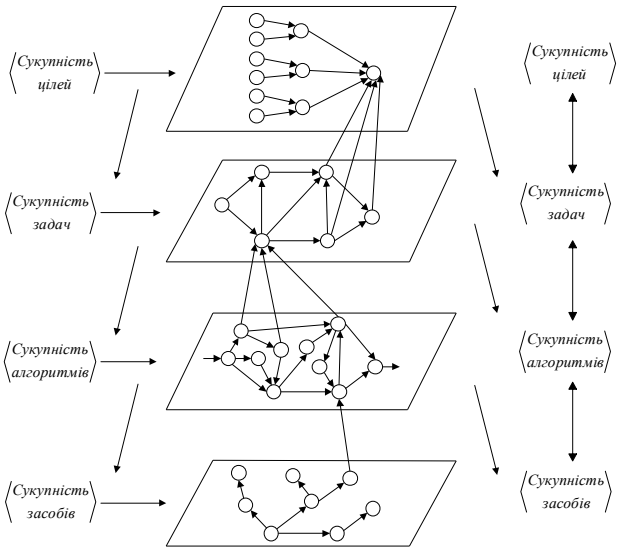


Рис. 1. Системна модель.

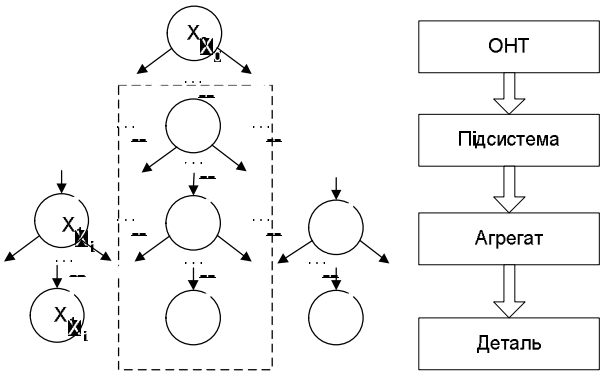


Рис. 2. «Машинобудівна» модель.

Єдина інформаційна модель процесу системного проектування НПА

Складність процесу проектування НПА співвідносна з великою кількістю слабкоструктурованих задач. На методах *системного проектування* (формалізації, структуризації та цілеорієнтації), що описані в [1], основано побудову системних моделей, які являють собою структуру порядку. Системна модель становить складну багаторівневу структуру, кожний рівень якої є визначеним етапом (аспектом зображення системи), що виражений та зафіксований мовою даного рівня (рис. 1).

Іншим аспектом представлення НПА є «машинобудівна» модель. В даній моделі одним із основних відношень є відношення <частина - ціле> і характерною є багатоярусна піраміда таких відношень (рис. 2). Являючись по своїй суті морфологічною моделлю, «машинобудівна» модель забезпечує учасника проекту відображенням майбутнього технічного обладнання у звичному для конструктора вигляді.

Системна та «машинобудівна» моделі пропонуються у якості базових при побудові єдиної інформаційної моделі НПА в системах підтримки прийняття проектних рішень (СППРР). Процес проектування розгортається навколо системної моделі, на основі якої відбувається довизначення інших моделей - машинобудівної, функціональної та ін.

На основі згаданих вище системних моделей відповідно до описаного в [3] процесу пакування відбувається розгортання проекту відносно його учасників – множини осіб, що приймають рішення.

Модельне забезпечення

При проектуванні НПА системними методами досліджень доцільним є створення банків системних та «машинобудівних» моделей. Ефективний аналіз існуючих банків моделей на предмет вже існуючих проектних рішень підвищує ефективність проектування вцілому. У складі СППРР пропонується інструмент аналізу банків моделей. Проектант, забезпечений аналітичними висновками, що поставляються йому процедурами направленого пошуку, має можливість робити більш обґрунтовані проектні рішення.

Важливою задачею при розробці банків системних та «машинобудівних» моделей є виділення в їх структурах не тільки формалізованих основних складових моделей, але й інтегральних елементів, що забезпечать ідентифікацію елемента процедурами направленого пошуку проектних рішень. Ідентифікаційні інтегральні елементи (ІІЕ) складових моделі надають структурі моделі у складі банку моделей властивості *селективного розпізнавання*. Дана властивість дозволяє пошуковій процедурі виділити прийнятне проектне рішення з контексту моделі іншого проекту, відкидаючи заздалегідь неприйнятні варіанти рішень.

Евристичне забезпечення

Іншим методом розв’язання слабкоструктурованих задач є застосування евристик. Для того, щоб не вибирати, який з методів кращий: аналітичний чи евристичний, в складі

СППРР пропонується застосування їх обох. З однієї сторони - це банки системних та «машинобудівних» моделей, а з іншого - база знань та модуль її інтерпретації.

База знань формується користувачами системи і наповнюється відповідно до предметних областей по мірі виконання проектів. Таким чином від проекту до проекту наповнення системи відбувається самими користувачами, а досвід фахівців концентрується та зберігається.

Пропонується інтелектуальна інтерпретація евристик, яка не тільки дає поради користувачу, але й забезпечує можливість перебудови моделей. Такий підхід розширює можливості автоматизації СППРР та удосконалює сам евристичний підхід.

База знань формується на основі удосконалених продукцій. Для продукційної бази знань було зроблено наступні удосконалення :

– кожне правило може бути забезпечено ІІЕ, які дають можливість не перебирати всю базу знань;

– кожне правило може бути забезпеченим в наслідковій частині набором інструкцій по роботі з моделлю (перебудова моделі, запуск сервісних модулів аналізу розрахунків та ін.).

Направлений пошук прийнятних проектних рішень

Інтегральні властивості банків моделей та удосконалене застосування евристик у поєднанні з формалізованим представленням інформаційної моделі НПА є основою інформаційної технології удосконалення процесу проектування.

Пошукові процедури при аналізі банків системних моделей розгортають стратегічні напрямки пошуку відповідно до логічних схем проектування [1]. В даному випадку початок проектування відповідає постановці задачі, яка виникає із заданої необхідності. Для майбутнього пакувального автомату визначається перелік критеріалльних функцій та їх межі. Далі пошукові процедури розгортають пошук по банкам моделей через всі етапи проектування :

– розв’язання задач формування структури та компонування;

– розв’язання задач узгодження підсистем у рамках системи (ОНТ), формування загальних режимів їх взаємодії;

– розв’язання задач синтезу законів функціонування та алгоритмів управління у відповідності до розробленої структури системи;

– розв’язання задач синтезу засобів управління.

В інтерактивному режимі користувач має змогу вибирати альтернативні сценарії проекту, запропоновані пошуковими процедурами, або відхиляти їх та розробляти самостійно етап проекту.

В пошукових процедурах запропоновано застосування багатовимірного аналізу даних при аналізі функціоналів, що дає можливість користувачу візуалізувати відношення між ними.

В результаті роботи пошукових процедур відбувається наповнення інформаційної моделі НПА, що уточнюється відповідно до розвитку проекту(рис. 3).

Організація процесу проектування НПА визначається етапами технології системних досліджень, а саме, розв’язком задач:

- синтезу(системної оптимізації);
- аналізу (системного моделювання);
- та прийняття рішень (вибору варіантів).

Відповідно до заданої множини задач пропонується базова структура СППРР. В рамках даного дослідження задачам синтезу відповідають модулі побудови машинобудівної та системної моделі НПА. Проектант має змогу визначати елементи і функціонали бажаної системи та визначати їх пріоритети. Задачі аналізу та прийняття рішень реалізуються при побудові пошукових процедур проектних рішень.

Основні результати

В результаті проведених вище теоретичних досліджень було розроблено прототип СППРР НПА.

В даній системі реалізовано побудову системної та машинобудівної моделі. Було забезпечено можливість автоматичної побудови одної моделі з іншої шляхом довизначення.

Розроблено структури для сутностей <Ціль>, <Задача>, <Операція>, <Виконавець> для системної моделі, та <ОНТ>, <Підсистема>, <Агрегат>, <Деталь> для машинобудівної.

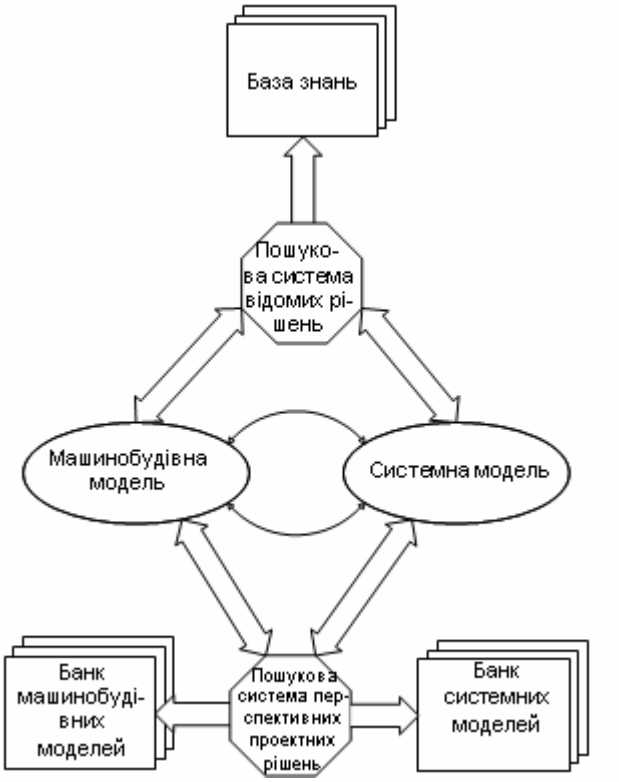


Рис. 3. Схема пошуку проектних рішень.

Представлення інформаційної моделі НПА даною парою моделей дає можливість проектанту розробляти проект в прийнятному для нього форматі представлення проекту. А також надає гнучкості пошуковим процедурам. Побудовані дерева зберігаються в банки моделей.

Розроблений апарат підтримки евристичних баз знань дозволяє їх створювати, редагувати та застосовувати при направленому пошуку проектних рішень.

Висновки

В даній статті запропоновано інформаційну технологію системного проектування НПА. Запропоновано нову структуру інформаційної моделі НПА. Удосконалено системні моделі в плані їх інтегральних характеристик. Запропоновано нові пошукові процедури проектних рішень. Впровадження даної інформаційної технології в галузі промисловості забезпечить створення єдиного інформаційного простору модельного та евристичного забезпечення. Такий підхід дозволить концентрувати та використовувати знання окремих проектних організацій для подальшого їх використання.

Література

1. Основи системного проектування та системного аналізу складних об’єктів: Підручник: Книга 1. Основи САПР та системного проектування складних об’єктів/ За ред. В. І. Бикова. – К.: Либідь, 2000. - 272 с;

2. А.А. Тимченко, М. В. Махинько, Системна модель процесів проектування пакувального обладнання в системах підтримки прийняття проектних рішень// Вісник технологічного університету поділля. - 2005. - №4. – Ч.1. - С. 44-46;

3. А.А. Тимченко, М.В. Махинько. Технологія системного моделювання процесів пакування. Міжнародний семінар з індуктивного моделювання. Збірник праць. // Київ: Міжнародний науково-навчальний центр інформаційних технологій та систем НАН та МОН України, 2005.–326-333 с.

УДК 656.073:004.001.891.57

Губенко В.К., Лямзин А.А.

МОДЕЛЬ ЛОГИСТИЧЕСКОГО РАСПРЕДЕЛИТЕЛЬНОГО ЦЕНТРА ЗЕРНОВЫХ И МАСЛЕНИЧНЫХ КУЛЬТУР

Разработана потоковая модель логистического распределительного центра зерновых и масленичных культур, которая позволяет управлять потоковыми процессами, а также учитывает их бинаправленный характер. Рис. 2. Табл. 1. Ист. 4.

Эффективное функционирование логистических распределительных центров тесно связано с решением задачи управления грузопотоками. Это возможно путем разработки потоковой модели логистического распределительного центра (ЛРЦ). Моделирование работы логистического распределительного центра и анализ потоковых процессов дает возможность проанализировать динамические характеристики, найти оптимальное решение задачи управления грузопотоками во многом зависящее от их величины, направленности, реверсивности. Существует достаточно большое разнообразие потоковых моделей: имитационные потоковые модели [1], модели потоков данных (data flow) [2] и ряд других. Системы моделирования потоковых задач имеют самые разнообразные средства их построения и основаны на различных принципах моделирования. Отличительной особенностью существующих потоковых моделей, от рассматриваемых нами, является однонаправленность потока. Разрабатываемая потоковая модель работы логистического распределительного центра зерновых и масленичных культур, учитывает возможность реверсивности грузопотока (рис.1.).

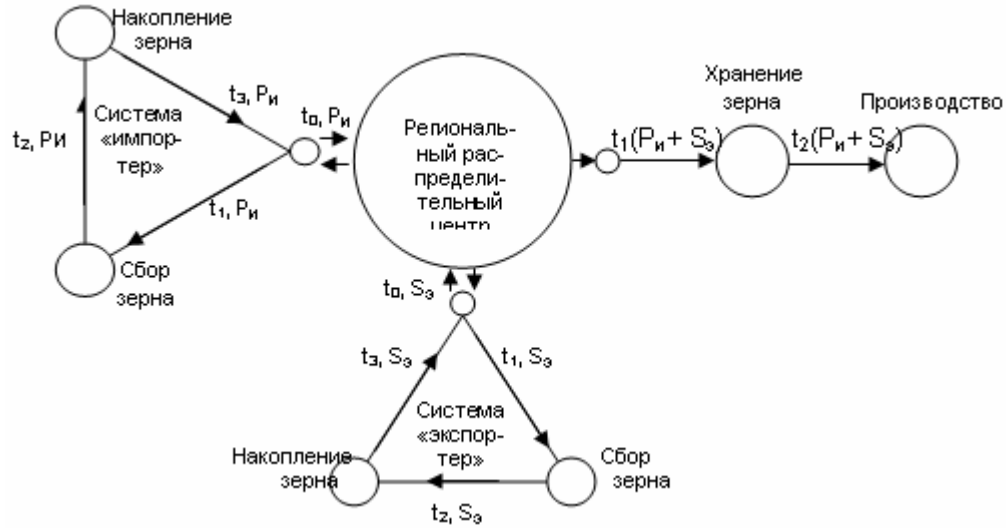
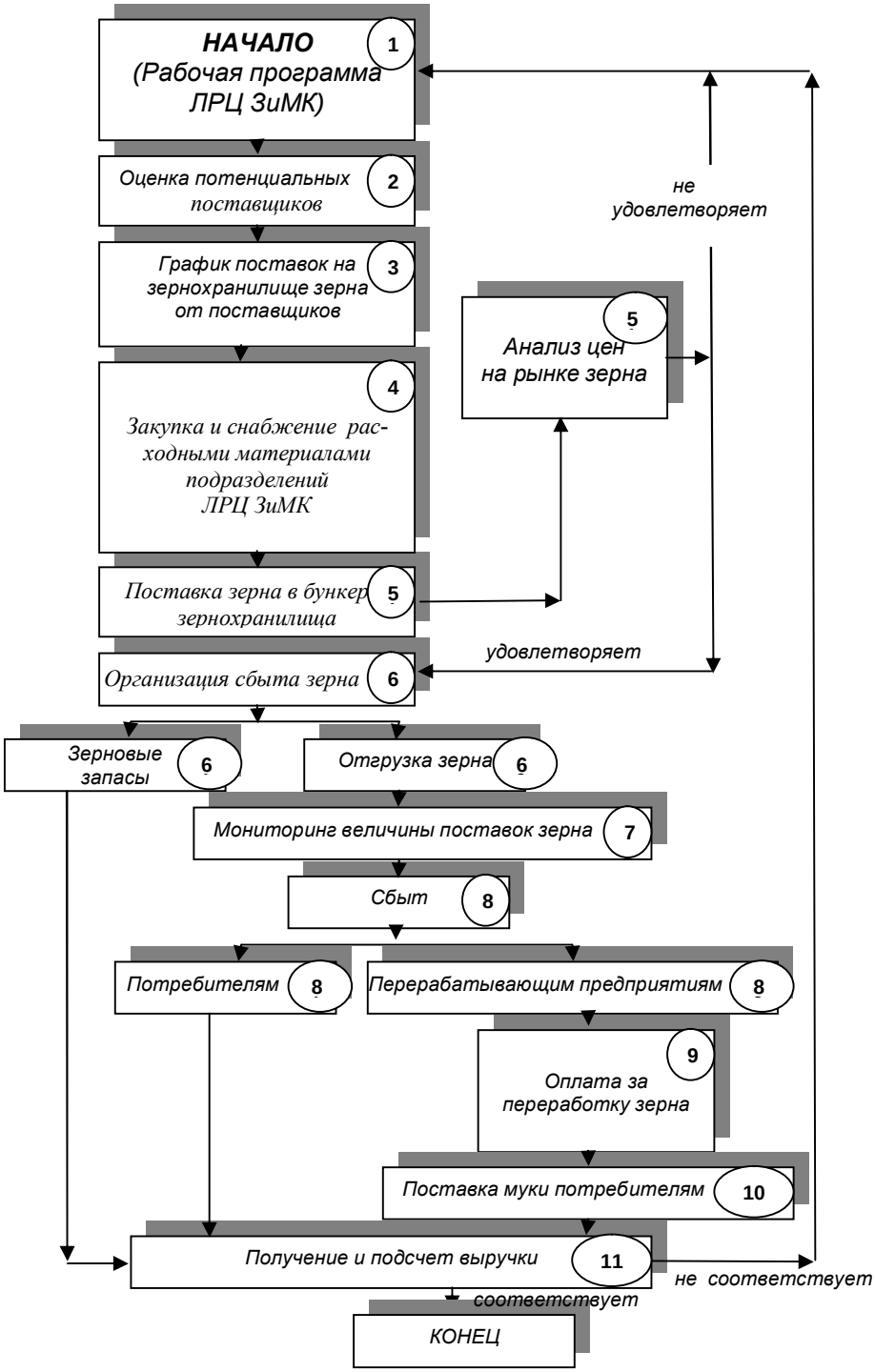


Рис. 1. Бинаправленный граф логистической системы зерновых и масленичных грузопотоков. $P_и$,$S_э$ – грузооборот зерна импортера (и), экспортера (э)соответственно; $t_0 \ldots t_3$ – время, определяющее длительность операций (t_0 – время на выполнение операции транспортировки зерна, t_1 – время операции поставок зерна для проведения посевных работ, t_2 – время проведения операций входящих в технологический цикл накопления зерна, t_3 – время на операции транспортировки зерна в ЛРЦ).



1,2,…11-номера блоков алгоритма; $5^1,6^{1,2}\ldots8^{1,2}$ – варианты развития событий.

Рис. 2. Алгоритм функционирования логистического распределительного центра зерновых и масленичных культур.

Разработка потоковой модели ЛРЦ ЗиМК заключается в моделировании потоков событий (процессов), протекающих в нем за определенный временной промежуток. Для

определения процессов, протекающих в ЛРЦ ЗиМК, воспользуемся алгоритмом, описывающим его функционирование (рис.2.).

Основным признаком потокового процесса является смена состояний потока - его реверсивность. Это позволяет рассматривать потоковые процессы во временном и в фазовом пространстве, которое отражает качественные изменения потоков. Под фазовым пространством понимается совокупность всевозможных мгновенных состояний ЛРЦ ЗиМК, имеющего определенную структуру и являющегося сложной системой.

Анализ процессов, протекающих в системе ЛРЦ ЗиМК (рис.2.), и понятие потокового процесса, позволяет сделать вывод о том, что разрабатываемая потоковая модель должна обладать равновесием.

Под равновесием понимается такое состояние системы ЛРЦ ЗиМК, при котором функция, определяющая эффективность ее работы, достигает максимума. Т.е. когда величина характеризующая перерабатывающую способность ЛРЦ ЗиМК с учетом определенных экономических затрат на его работу, не зависит от реверсивности грузопотоков и равноэффективна на всем временном отрезке.

Проводя аналогию с физическими (термодинамическими) системами, в системе ЛРЦ ЗиМК в качестве функции полезности может быть принята энтропия, характеризующая распределение вероятностей состояний системы. Таких состояний как:

– система имеет возможность обеспечить обработку реверсивных грузопотоков;

– система загружена настолько, что ее производственных мощностей не достаточно для эффективной работы;

– наличие внешних факторов не позволяет эффективно работать системе (перезагруженность примыкающих транспортных коммуникаций и т.п.).

Метод максимизации энтропии приписывает равные вероятности всем состояниям системы ЛРЦ ЗиМК. Исходя из этого, потоковой моделью ЛРЦ ЗиМК может являться так называемая гравитационная модель[3], которая выражается следующей зависимостью:

$$G_{э,и} = \mu \frac{S_э P_и}{C^2_{э,и}}, \qquad (1)$$

где $G_{э,и}$ – оценка эффективности работы ЛРЦ ЗиМК, характеризующая его способность переработать такой объем грузопотоков зерновых и масленичных культур из региона э (экспортера) в регион *и* (импортер), при котором экономические затраты на его деятельность будут соответствовать планируемым, тонн/грн.;

$S_э$ – объемы производства зерновых и масленичных культур в регионе «э»- *экспортер, тонн*;

$P_и$ – объемы потребления зерновых и масленичных культур в регионе «*и*»- *импортер, тонн*;

$C_{э,и}$– затраты на транспортировку из региона «*э*» в регион «*и*», *грн.*

μ– уровень несогласованности в работе ЛРЦ ЗиМК ($УНР_{ЛРЦ\ ЗиМК}$), обслуживающего регионы «*э*» и «*и*».

В развернутом виде показатель УНР μ определяется соотношением:

$$\mu = \frac{\sum_{i=1}^{k} (S_э \times t_э^{сд} + P_и^{пл} \times t^{сд}_и)}{\sum_{i=1}^{m} (S_э^{пл} \times t_э^{пл} + P_и^{пл} \times t_и^{пл})}, \qquad (2)$$

где $S_э$, $P_и$ – объем заказов, по которым допущены срывы сроков подготовки (сдачи, отгрузки), для экспортера «э» и импортера «и», тонны;

$t_{э,и}^{ср}$ - продолжительность срывов сроков подготовки каждого из указанных сортиментов (заказов) для экспортера «э» и импортера «и», дн;

$S^{пл}_{э}$, $P^{пл}_{и}$ – объемы заказов, запланированные к складированию в ЛРЦ ЗиМК в данном отчетном периоде для экспортера «э» и импортера «и» , тонны;

$t_{э,и}^{пл}$ — плановая продолжительность каждого заказа для экспортера «э» и импортера «и», дн;

k – количество заказов, срок выполнения которых превысил планируемый срок, ед.;

m – количество заказов, выполненных в планируемый срок, ед.

Обозначив знаменатель выражения (2) через С, а числитель через П, получим упрощенный способ для вычисления $УНР_{ЛРЦ\ ЗиМК}$:

$$\mu = \tilde{N} / \ddot{I} \ , \qquad (3)$$

где С – число дней, на протяжении которых был сорван срок подготовки приемки, отгрузки зерновых и масленичных культур того или иного конкретного заказа;

П – плановый срок подготовки того же заказа, дн.

На величины $S_э$ и $P_и$ накладываются ограничение. Данные ограничения заключаются в том, что суммы по строкам и столбцам матрицы оценки эффективности работы ЛРЦ ЗиМК должны совпадать с объемом грузопотоков, исходящих из каждой зоны, и с грузопотоком, входящим в каждую зону. Разработанная потоковая модель применена при анализе работы разрабатываемого логистического распределительного центра ООО «СРЗ» по переработке зерновых и масленичных культур г. Мариуполь [4].

Результаты применения данной модели приведены в таблице 1.

Таблица 1.

Наименование фирмы на рынке зерновых и масленичных культур	Кол-во импортируемого зерна, тыс. т	Кол-во зерна отправляемого на экспорт, тыс. т	Ср.время плановых поставок зерна, сут.	Ср. время задержки по поставке грузов, сут.	Ср. затраты на транспортировку зерновых и масленичных культур, тыс. грн.	Величина грузооборота из региона производителя в регион потребитель, тыс. т
ЛРЦ г. Мариуполь	500	500	2	1	65	1923
.....						

Выводы

Результаты анализа работы ЛРЦ ЗиМК, полученные с применением потоковой модели, позволяют сделать следующие выводы:

– для разрабатываемого ЛРЦ ЗиМК ООО «СРЗ», с учетом перерабатывающей его способности и затрат на его функционирование, требуется ряд мероприятий по повышению его эффективности. Данные мероприятия должны повысить его перерабатывающую способность с сохранением экономических затрат, что даст возможность обрабатывать реверсивные грузопотоки импортеров и экспортеров в размере 1 млн. тонн в год;

– разработанная потоковая модель ЛРЦ ЗиМК является адаптированной к рынку зерновых и масленичных культур, а именно, реверсивности зерновых и масленичных потоков, и имеет возможность учитывать несогласованность в работе ЛРЦ.

Литература

1. Шебеко Ю. Ожидании BPR.http://www.bizcom.ru/rus/bt/1997/nr8/21.htm.
2. Иванищев В.В. Автоматизация моделирования потоковых систем. - Л.: Наука, 1986.
3. Вильсон А. Дж. Энтропийные методы моделирования сложных систем. Перев. с англ. М.: Наука, 1976.
4. Губенко В.К. и др. Анализ возможного объема переработки зерновых и масленичных культур ООО «СРЗ».– г. Мариуполь, 2004.

УДК 621.313

Киричков А.В., Невзлин Б.И.

НАХОЖДЕНИЕ ТЕМПЕРАТУРЫ СРАБАТЫВАНИЯ ТЕРМОДЕТЕКТОРА

Модернизирована тепловая схема замещения асинхронного двигателя путем дополнения в схему термодетектора, составлена и решена система уравнений для модернизированной схемы, определено место размещения термодетектора, где наиболее адекватно определяется средняя температура обмотки статора. Рис. 4, ист. 21.

Введение

В [1] показано, что наиболее полно требованиям защиты двигателей, имеющих тяжелые режимы работы, отвечает защита с кодом ТР 221, т.е. двухуровневая защита для медленно и быстро нарастающих перегрузок, имеющая повышенную чувствительность к перегреву двигателя.

Создать тепловую защиту такого уровня возможно только применением малогабаритных и малоинерционных датчиков. Этим требованиям удовлетворяют только полупроводниковые датчики, позволяющие измерять температуру обмотки в нескольких локальных точках электродвигателя.

Но температурная защита, построенная по принципу контроля температуры в нескольких точках, не позволяет оценить среднее превышение температуры защищаемой обмотки, в соответствии требованиям стандарта ГОСТ 27888.

Для определения среднего перегрева обмоток необходимо использовать модель двигателя либо аналоговую, либо цифровую.

Задача модели: определение соотношений температуры, измеренной термодетектором в точке установки, и средней температуры обмоток электродвигателя.

Для определения температуры срабатывания термодетектора на основе разработанной модели необходимо определить температуру в точке установки термодетектора, соответствующую заданной по ГОСТ 27888-88 температуре среднего перегрева обмотки. На эту температуру и должна быть рассчитана температура срабатывания термодетектора.

Современное состояние проблемы

Моделью для определения этого соотношения может служить тепловая схема замещения электродвигателя, позволяющая определить средний перегрев обмоток, в одной из точек которой установлен термодетектор.

В настоящее время имеется достаточно много различных тепловых моделей асинхронных двигателей, в частности, Счастливого Г.Г. [2], [3], [4], [5], [6], Богаенко И.Н. [7], Борисенко А.И. [8], [9], Бурковского А.Н. [10], [11], [12], [13], [14], Выговского В.И. [15], Гуревича Э. И. [16], [17] Данько В.Г. [8], Ковалева Е.Б. [11], [12], [13], [14], [18], Федоренко Г.М. [3], [4],[5] [19], Яковлева А.И. [8], [9], [20], [21], [22], [23] и др. каждая из которых разрабатывалась применительно к определенным видам машин с соответствующей конструкцией и технологией изготовления.

Основное содержание исследования

В нашем случае, поскольку рассматриваются взрывонепроницаемые электродвигатели, целесообразно взять существующую модель Бурковского А.Н., Ковалева Е.Б. [12], [13], [14], рис. 1, разработанную и отлаженную именно для таких электродвигателей.

В данной схеме точки относятся: 1. Пазовая часть обмотки статора; 2. Лобовая часть обмотки статора; 3. Обмотка ротора; 4. Зубцы железа статора; 5. Корпус статора над пакетом сердечника статора; 6. Корпус статора над лобовыми частями обмотки статора; 7. Внутренний воздух в машине.

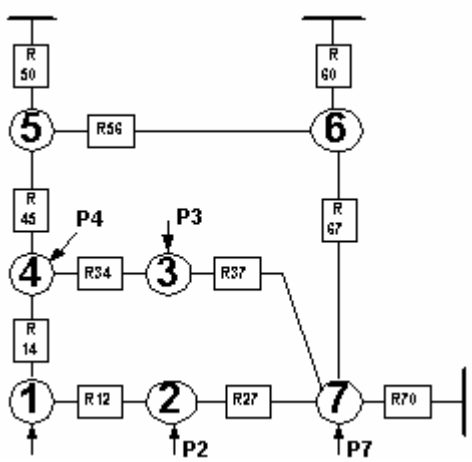


Рис. 1. Тепловая модель электродвигателя.

Эта модель содержит семь точек (тел) в электрической машине обдуваемого исполнения и не предусматривает установки термодетектора и определение температуры обмотки в точке его установки, поэтому ее необходимо усовершенствовать.

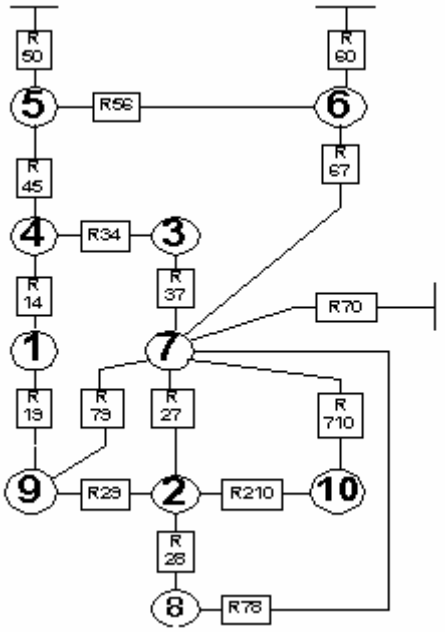


Рис. 2. Тепловая модель электродвигателя с термодетектором в лобовой части обмотки статора.

При определении температуры срабатывания термодетектора можно выделить следующие варианты установки термодетектора в лобовой части обмотки:

1. Термодетектор установлен между пакетом и точкой обмотки, соответствующей средней температуре лобовой части обмотки, т.е. на расстоянии lуд< 0.15*lл от пакета статора.

2. Термодетектор установлен в точке обмотки, соответствующей средней температуре лобовой части на расстоянии lуд> 0.15*lл от пакета сердечника статора.

3. Термодетектор установлен за точкой обмотки, соответствующей средней температуре лобовой части обмотки, т.е. на расстоянии lуд> 0.15*lл от пакета статора.

Для моделирования этих вариантов установки термодетектора используем тепловую модель элемента обмотки с термодетектором по [2], содержащую три элемента обмотки и один элемент, соответствующий термодетектору.

Модифицированная тепловая схема замещения для термодетектора установленного в лобовой части обмотки, приведена на рис. 2.

Первые семь точек соответствуют схеме [12], [13], [14], 8 – термодетектор, и 9 и 10 точки добавлены в модифицированной модели.

В данной схеме точки относятся: 1. Пазовая часть обмотки статора; 2. Участок лобовой части обмотки под термодетектором; 3. Обмотка ротора; 4. Зубцы железа статора; 5. Корпус статора над пакетом сердечника статора; 6. Корпус статора над лобовыми частями обмотки статора; 7. Внутренний воздух в машине; 8. Термодетектор; 9. Лобовая часть обмотки статора между сердечником и точкой установки термодетектора; 10. Лобовая часть обмотки статора за точкой установки термодетектора.

Таким образом, после модернизации схема будет вместо одной точки в лобовой части обмотки иметь три, и одну точку - термодетектор, т.е. для стационарного режима работы двигателя описываться 10 алгебраическими уравнениями.

Составим для нее уравнения:

1. $a11 * \theta1 – a14 * \theta4 - a19 * \theta9 = P10$
2. $a22 * \theta2 - a27 * \theta7 – a28 * \theta8 - a29 * \theta9 – a210 * \theta10 = P20$
3. $a33 * \theta3 – a34 * \theta4 – a37 * \theta7 = P30$
4. $-a14 * \theta1 – a34 * \theta3 + a44\ \theta4 – a45 * \theta5 = P4$ (1)
5. $-a45 * \theta5 + a55 * \theta5 – a56 * \theta6 = 0$
6. $-a56 * \theta5 + a66 * \theta6 – a67 * \theta7 = 0$
7. $-a27 * \theta2 – a37 * \theta3 - a67 * \theta6 + a77 * \theta7 – a78 * \theta8 – a79 * \theta9 – a710 * \theta10 = P7$
8. $- \theta28 * \theta2 – a78 * \theta7 + a88 * \theta8 = P80$
9. $–a19 * \theta1 – a29 * \theta2 – a79 * \theta7 + a99 * \theta9 = 0$
10. $- a210 * \theta2 – a710 * \theta7 + a1010 * \theta10 = P100$

Этой системе уравнений соответствует симметричная матрица проводимостей, у которой $aij = aji$, $aii = \Sigma\, aij + ai0 – \beta r * \theta$,

где

$$P = Pi0 * (1+ \beta r * \theta), \quad (2)$$

Pi0 – потери, зависимые от температуры (электрические потери в обмотках) при окружающей температуре.

Этой схеме соответствуют следующие тепловые проводимости и сопротивления:

Для точки схемы 1:

a14 - 1/R14 теплопроводность между точкой обмотки статора, имеющей среднюю температуру пазовой части обмотки, и точкой, имеющей среднюю температуру железа зубца статора.

a19 – 1/R19 теплопроводность между точкой обмотки статора, имеющей среднюю температуру пазовой части обмотки, и точкой, имеющей среднюю температуру участка лобовой части от пакета статора до места установки термодетектора.

$$a11 = a14 + a19 – \beta r * P10 \quad (3)$$

Для точки схемы 2:

a27 - 1/R27 теплопроводность теплоотдачи с поверхности лобовых частей статора.

a28 – 1/R28 продольная теплопроводность обмотки статора, между точками 2 и 8 (термодетектором).

a29 – 1/R29 продольная теплопроводность обмотки статора, между точками 2 и 9 лобовой части в месте установки термодетектора.

a210 – 1/R210 продольная теплопроводность обмотки статора, между точками 2 и 10 лобовой части в месте установки термодетектора.

$$a22 = a27 + a28 + a29 + a210 - \beta r * P20 \quad (4)$$

Для точки схемы 3:

a34 - 1/R34 тепловая проводимость между точкой обмотки ротора, имеющей среднюю температуру обмотки, и точкой, имеющей среднюю температуру железа зубца статора.

a37 - 1/R37 тепловая проводимость теплоотдачи с поверхности лобовых частей ротора.

$$a33 = a34 + a37 - \beta r * P30 \quad (5)$$

Для точки схемы 4:

a45 – тепловая проводимость между точкой, имеющей среднюю температуру железа зубца статора, и точкой, имеющей среднюю температуру поверхности статора над пакетом железа.

$$a44 = a14 + a34 + a45 \quad (6)$$

Для точки схемы 5:

a50 – тепловая проводимость между точкой, имеющей среднюю температуру поверхности статора над пакетом железа, и окружающей температурой.

a56 – тепловая проводимость между точкой, имеющей среднюю температуру поверхности статора над пакетом железа и точкой имеющей среднюю температуру поверхности корпуса статора над лобовыми частями.

$$a55 = a50 + a45 + a56 \quad (7)$$

Для точки схемы 6:

a60 – тепловая проводимость между точкой, имеющей среднюю температуру поверхности статора над лобовыми частями обмотки статора, и окружающей температурой.

a67 – тепловая проводимость, имеющей среднюю температуру поверхности статора над лобовыми частями обмотки статора и температурой внутреннего воздуха.

$$a66 = a60 + a56 + a67 \quad (8)$$

Для точки схемы 7:

a70 - тепловая проводимость между внутренним воздухом и окружающей температурой.

a78 - тепловая проводимость между внутренним воздухом и термодетектором.

a79 - тепловая проводимость между внутренним воздухом и участком лобовой части, на котором установлен термодетектор.

a710 - тепловая проводимость между внутренним воздухом и лобовой частью со средней температурой в точке 10.

$$a77 = a70 + a27 + a37 + a67 + a78 + a79 + a710 \quad (9)$$

Для точки схемы 8:

$$a88 = a28 + a78 \quad (10)$$

Для точки схемы 9:

$$a99 = a19 + a29 + a79 - \beta r * P90 \quad (11)$$

Для точки схемы 10.

$$a1010 = a710 + a210 - \beta r * P100 \quad (12)$$

Потери в точках схемы определяются при окружающей температуре для половины машины и равны:

P10 – потери в пазовой части обмотки статора.

P20 – потери в элементе лобовой части статора под термодетектором.

P90 – потери в лобовой части обмотки в точке 9.

P100 – потери в лобовой обмотки в точке 10.

$$Рлоб0 = P20 + P90 + P100 \quad (13)$$

Средняя температура лобовой части в этом случае равна:

$$\theta л = (\theta 2 * l2 + \theta 9 * l9 + \theta 10 * l10)/(l2+l9+l10) \quad (14)$$

где l9, l2, l10 по рис. 3.

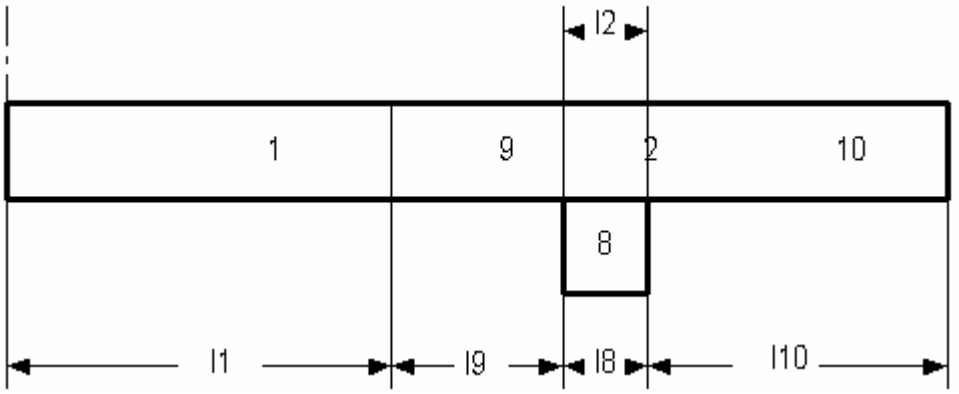


Рис. 3. Эскиз стержня обмотки статора.

Средняя температура обмотки равна:

$$\theta об = (\theta л * lл + \theta 1 * l1) / (lл + l1), \quad (15)$$

где: lл = l8 +l9 + l10, т.е. находится в области температур от θ1 до θл, а, следовательно, расположена в обмотке между точками 8 средних нагревов лобовой и пазовой частей обмотки.

Поэтому при установке термодетектора между точкой выхода секции из паза и точкой, соответствующей среднему нагреву лобовой части, расположенной согласно [8] на расстоянии равном 0.15 lлоб от пакета, показания термодетектора будут ближе всего соответствовать среднему нагреву обмотки статора.

При установке термодетектора над точкой обмотки со средней температурой лобовой части тепловая схема замещения машины упрощается и отличается от схемы модели по [12], [13], [14] одну точку, на термодетектор. Тепловая схема замещения для этого случая приведена на рисунке 4.

Из выражения (14) можно получить зависимость для определения коэффициента приведения температуры термодетектора:

$$Kpr = \theta 8 / \theta об \quad (16)$$

В этом случае при выборе позистора необходимо его температуру срабатывания определять из выражения:

$$\theta поз \leq \theta ГОСТ * Kpr \quad (17)$$

где θГОСТ – максимальная температура срабатывания защиты по ГОСТ 27888-88.

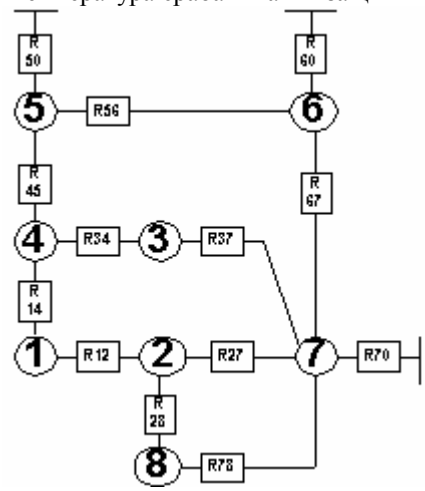


Рис. 4. Тепловая схема замещения электродвигателя при установке термодетектора в точке среднего нагрева лобовой части обмотки.

Вывод

Предложена тепловая модель позволяющая определять температуру срабатывания позистора, установленного в любой точке лобовой части обмотки, обеспечивающая срабатывание защиты при температуре обмотки, соответствующей максимальной допустимой температуре обмотки по ГОСТ 27888-88.

Литература

1. Загирняк М.В., Невзлин Б.И., Киричков А.В. Современные тепловые защиты электродвигателей в горных условиях // Вісник Кременчуцького державного політехнічного університету. – 2006;
2. Счастливый Г. Г. Нагревание закрытых асинхронных электродвигателей. - Киев, «Наукова думка», 1966, 196 с;
3. Счастливый Г.Г., Федоренко Г.М., Выговский В.И. и др. Расчет нагрева электрических машин. – К.: Техника, 1986. - 34 с;
4. Счастливый Г.Г., Федоренко Г.М., Семак В.Г. Погружные асинхронные электродвигатели. -М: Энергоатомиздат.-1983, 169 с;
5. Математические модели теплопередачи в электрических машинах /Счастливый Г.Г., Бандурин В.В., Остапенко В.Н., Остапенко С.Н. / К.: Наукова думка,-1986. - 182 с;
6. Богаенко И.Н. Контроль температуры электрических машин. / К.: Техніка, 1975. - 176 с;
7. Борисенко А.И., Данько В.Г., Яковлев А.И. Аэродинамика и теплопередача в электрических машинах.– М.: Энергия, 1974.–560 с;
8. Борисенко А. И., Костиков О.И., Яковлев А.И. Охлаждение промышленных электрических машин.– М.: Энергоатомиздат, 1983.– 296 с;
9. Бурковский А.Н. Расчет температурного поля статора обдуваемого взрывозащищенного асинхронного двигателя с внутренней аксиальной вентиляцией / Взрывозащищ. электрооборуд. / Укр. н.-и. проект.-конструкт. и технол. ин-т взрывозащищ. и руднич. электрооборуд. - Донецк, 1997. - С. 156-164;
10. Бурковский А.Н., Ковалев Е.Б. Аналитический способ определения коэффициентов влияния различных составляющих потерь на нагрев электрической машины // Взрывозащищенное электрооборудование: Сб. науч. тр. ВНИИВЭ.- М.: Энергия 1976.- Вып. II.-С. 25-28;
11. Бурковский А.Н., Ковалев Е.Б., Коробов В.К. Нагрев и охлаждение взрывозащищенных электродвигателей М.: Энергия, - 1970. - 198 с;
12. Ковалев Е.Б., Бурковский А.Н., Голянд Б. С. Методика тепловых расчетов взрывонепроницаемых электродвигателей // Электропромышленность, I970,- № 1;
13. Ковалев Е.Б., Бурковский А.Н. Исследование тепловых сопротивлений электрических машин // Электропромышленность 1968. - №342.- С. 18-19;
14. Выговский В.И. Методы и программные комплексы расчета трехмерных температурных полей турбогенераторов и электродвигателей переменного тока. Автореферат дисс. докт. техн. наук, 1994., 39с;
15. Гуревич Э. И., Рыбин Ю. Л. Переходные тепловые процессы в электрических машинах.– Л.: Энергоиздат, 1983.– 216 с;
16. Гуревич Э. И., Рыбин Ю. Л. Расчетные модели нестационарных тепловых процессов в обмотках электрических машин.–«Электротехника», 1975, № 12, С. 35–38.;
17. Ковалев Е.Б., Расков Ю.В., Голянд Б.С. Статистический анализ и расчет нагрева асинхронного электродвигателя // Электричество, 1975.- № 11.- С. 37-40;
18. Федоренко Г.М. Научные основы локальной интенсификации охлаждения и температурной диагностики турбогенераторов и жидкостно-заполненных электрических машин. Автореферат дисс. докт. техн. наук, Киев, 1990;
19. Математическая модель для исследования нагрева асинхронных двигателей, работающих в повторно-кратковременном режиме / Артанов С. Г., Мосина И.И., Пантюхов Л.Л., Яковлев А.И./ В кн. Аэродинамика и теплопередача в электрических машинах. – Харьков, 1976. - Вып. 6. - С. 11-27;
20. Мосина И. И., Травкина Т. Н., Яковлев А. И. Неравномерность нагрева обмоток статора закрытого обдуваемого электродвигателя. // Электротехническая промышленность. Серия «Электрические машины», 1972, вып. 2 (12);
21. Яковлев А. И. Исследование распределения температуры во взрывозащищенных асинхронных двигателях с двухсторонней аксиальной вентиляцией. // Изв. вузов. Электромеханика, 1969, № 11.

УДК 625

Попов С.В.

РАСЧЕТ УПРУГИХ ХАРАКТЕРИСТИК ОТДЕЛЬНЫХ ЭЛЕМЕНТОВ ОПОРНО-ВОЗВРАЩАЮЩЕГО УСТРОЙСТВА

В статье представлена методика расчета упругих характеристик блока резинометаллических элементов, с любым заранее заданным количеством элементов и его конструктивным исполнением.

В связи с ростом скорости движения на железных дорогах вопросы выбора конструкции и параметров упругого подвешивания являются важной составной частью проблемы создания высокоскоростных локомотивов, поскольку во многом именно от работы рессорного подвешивания зависят как динамические показатели локомотивов, так и их тяговые возможности.

В настоящее время на отечественных локомотивах для разделения массы кузова и тележек в вертикальном направлении широко применяются комбинированные резинометаллические опорно-возвращающие устройства. Конструкция такой опоры включает в себя роликовый аппарат и блок резинометаллических элементов (РМЭ) [1]. Опорно-возвращающие устройства устанавливаются на тележки таким образом, что относительное перемещение кузова и тележек в горизонтально-поперечном направлении (рис. 1) происходит вследствие упругих деформаций РМЭ опор. Максимально возможное горизонтально-поперечное относительное перемещение тележки под кузовом ±40 мм выбрано из условия размещения оборудования внутри кузова по ширине и обеспечения вписывания его в габарит. На первой части хода ±20 мм (рис. 1.а) возвращающий эффект создается упругими деформациями РМЭ опор. На следующей части хода (рис. 1.б) возвращающий эффект усиливается параллельным включением комплекта пружин шкворневого узла. Боковые опоры кузова с такими элементами имеют ряд преимуществ перед другими типами опор. Они дают возможность существенно упростить конструкцию связей кузова с тележками, обеспечить улучшение вертикальной динамики экипажа, снижение вибраций и шума, передающихся от ходовой части.

При движении локомотива возникают случаи нагружения боковых опор, когда на них одновременно действуют вертикальные и поперечные силы. Такое воздействие сил на комплект РМЭ вызывает значительные смещения опорных поверхностей блоков РМЭ, а в некоторых случаях даже потерю устойчивости. Учитывая указанный факт, существующие методы расчета упругих характеристик резиновых элементов необоснованно применяют и для расчета характеристик блока из нескольких элементов, установленных друг на друге [2]. При этом предполагается, что остальные пластины резинометаллических элементов остаются параллельными опорным поверхностям, независимо от величины относительного смещения тележек под кузовом.

В связи с этим, определение упругих характеристик опор, состоящих из комплекта резинометаллических элементов и обеспечивающих требуемые динамические качества, на стадии проектирования представляет немалый практический.

Для определения упругих характеристик комплекта РМЭ особый интерес представляет определение горизонтальной и вертикальной деформации среднего резинометаллического элемента при поперечном смещении опорных поверхностей с учетом поворота на угол ρ рис. 2.

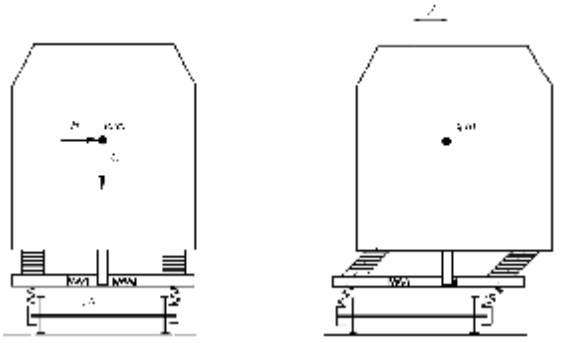
Предположим, что к среднему резинометаллическому элементу приложены вертикальная сила Q_0 и горизонтальная сила $P_{гв}$. Параллельность этих пластин свидетельствует о том, что резиновая шайба не воспринимает каких-либо изгибающих моментов. Тогда равнодействующая сил Q_0 и $P_{гв}$ может быть заменена нормальным давлением N и сдвигающей силой $P^*_{гв}$:

$$N = Q_0 \cdot \cos\rho - P_{\tilde{a}\hat{a}} \cdot \sin\rho; \qquad (1)$$

$$P^{*}_{\tilde{a}\hat{a}} = P_{\tilde{a}\hat{a}} \cdot \cos\rho + Q_0 \sin\rho\,. \qquad (2)$$

С увеличением угла наклона ρ резинометаллического элемента, сила сжатия уменьшится на величину ΔQ_0 :

$$\Delta Q_0 = Q_0 - Q_0 \cdot \cos\rho + P \cdot \sin\rho\,. \qquad (3)$$



а б

Рис. 1. Схема относительного перемещения кузова и тележек в горизонтально-поперечном направлении: а) перемещение тележки под кузовом в пределах ±20 мм; б) перемещение тележки под кузовом в пределах ±40 мм.

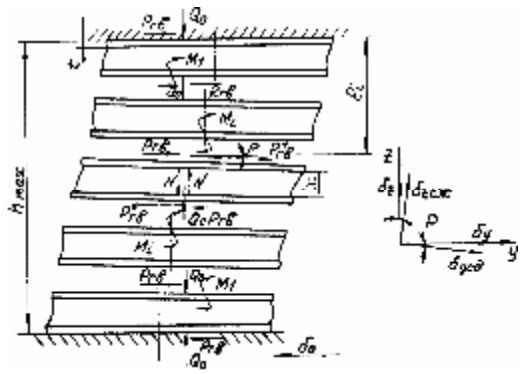


Рис. 2. Расчетная схема блока опоры, состоящего из резинометаллических элементов.

Соответственно, полная деформация резинового элемента по толщине уменьшится на величину:

$$\delta^{*}_{z\,\tilde{n}\tilde{a}\tilde{e}} = \frac{\Delta Q_0}{Æ_{\tilde{n}\tilde{a}\tilde{e}}}\,.$$

где $Æ_{\tilde{n}\tilde{a}\tilde{e}}$-жесткость на сжатие резинового элемента, значение которой определим из как:

$$Æ_{\tilde{n}\tilde{a}\tilde{e}} = \frac{\pi\left(R^2 - r^2\right)E_{\tilde{n}\tilde{a}\tilde{e}}}{h_0} \qquad (4)$$

где R - радиус резинового элемента; h_0 - толщина резинового элемента; k -коэффициент формы резинового элемента; $E_{\tilde{n}\tilde{a}\tilde{e}}$-модуль упругости на сжатие резинового элемента значение которого можно определить по формуле [3]:

$$E_{\tilde{n}\tilde{a}\tilde{e}} = 6 \cdot G(1 + k^2)\,. \qquad (5)$$

где G - модуль упругости на сдвиг резинового элемента.

Для резинового элемента, представляющего собой полую шайбу с внутренним диаметром d, коэффициент формы k будет равен [4]:

$$k = \frac{D-d}{4h}. \qquad (6)$$

В то же время, деформация сдвига вдоль пластины станет равной:

$$\delta^*_{y\ ñä} = \frac{P^*_{ãâ}}{Æ_{ñä}} \qquad (7)$$

$$Æ_{ñä} = \frac{\pi\left(R^2 - r^2\right)G}{h_p};$$

$$h_p = h_0\left(1 - \frac{Q_0}{Æ_{ñæ}}\right).$$

где $Æ_{ñä}$ - жесткость на сдвиг резинового элемента; G - модуль упругости на сдвиг резинового элемента; h_p - толщина резинового элемента под нагрузкой.

Полная вертикальная деформация наклонного резинового элемента получится равной:

$$\delta_z = -\delta^*_{z\ ñæ} \cdot \cos\rho + \delta^*_{y\ ñä} \cdot \sin\rho. \qquad (8)$$

Горизонтальная деформация наклонного резинового элемента равна:

$$\delta_y = -\delta^*_{z\ ñæ} \cdot \sin\rho + \delta^*_{y\ ñä} \cdot \cos\rho. \qquad (9)$$

Величину поперечного смещения других резинометаллических элементов в блоке опоры с достаточной точностью можно определить по углу наклона стальных пластин данного РМЭ:

$$\delta_{yi} = -\delta^*_{z\ ñæ} \cdot \sin\rho_i + \delta^*_{y\ ñä} \cdot \cos\rho_i; \qquad (10)$$

$$\rho_i = \frac{\rho^*_{i-1} + \rho^*_i}{2}. \qquad (11)$$

где ρ^*_{i-1}-угол наклона наружной от центра блока пластины i-го РМЭ; ρ^*_i - угол наклона внутренней пластины i-го РМЭ.

Для нахождения угла наклона РМЭ резиновую шайбу рассмотрим как деформируемый стержень, находящийся под действием поперечной силы $P_{гв}$ и момента сил M_i в условиях жесткого крепления одним концом к неподвижной поверхности. По формулам малых деформаций из закона Гука следует, что расчетное значение угла наклона одной стальной пластины относительно другой может быть определено по формуле:

$$\rho^*_i = \frac{P_{ÃÂ}h_p^2}{2EI_X} + \frac{M_i h_p}{EI_X} = \frac{h_p}{EI_X}\left(\frac{P_{ÃÂ}h_p}{2} + M_i\right). \qquad (12)$$

где I_X -момент инерции резиновой шайбы относительно оси OY, проходящей через ее геометрический центр; M_i- момент сил, действующий на резино-металлический элемент и зависящий от его местонахождения в резиновом столбе, значение которого можно определить по формуле:

$$M_i = P_{ÃÂ}L_i + Q_0\frac{\delta_0 \cdot l_i}{h_{max}} = \left(P_{ÃÂ} + Q_0\frac{\delta_0}{h_{max}}\right)\cdot(h_p + 2t)\cdot i; \qquad (13)$$

$$h_{max} = (h_p + 2t)\cdot n.$$

где n-количество РМЭ элементов в блоке; t- толщина стальной пластины; i-количество РМЭ от центра блока.

Тогда относительное угловое перемещение стальных пластин одного РМЭ равно:

$$\rho_i = \frac{h_p}{EI_X}\left[\frac{P_{ÃÂ}h_p}{2} + \left(P_{ÃÂ} + Q_0\frac{\delta_0}{h_{max}}\right)(h_p + 2t)\cdot i\right]. \qquad (14)$$

Так же следует иметь в виду, что деформация резинового столба увеличивается в поперечном направлении на величину, равную:

$$\delta_i^* = \frac{P_{ГВ} h_p^2}{3EI_x} + \frac{M_i h_p^2}{2EI_x} = \frac{h_p^2}{2EI_x}\left[\frac{2P_{ГВ} h_p}{3} + (P_{ГВ} + Q_0 \frac{\delta_0}{h_{max}})(h_p + 2t)i\right]. \quad (15)$$

Величина полного поперечного перемещения опорных поверхностей, вызванная силами $P_{ГВ}$ и Q_0, действующими на одну опору кузова, складывается из углов поворота и поперечного смещения всех резино-металлических элементов блока. Так, для опоры состоящей из 7 элементов, полное поперечное перемещение опорных поверхностей определяется по формуле:

$$\delta_0 = 2(\delta_{y1} + \delta_{y2} + \delta_{y3}) + \delta_{y4} + 2(\delta_1^* + \delta_2^* + \delta_3^*) + \delta_4^*. \quad (16)$$

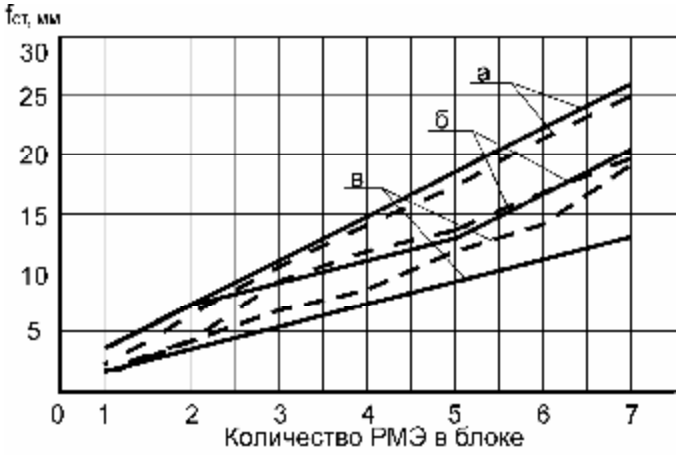
$$\text{или } \delta_0 = \sum_{i=1}^{n} \delta_{yi} + \sum_{i=1}^{n} \delta_i^*.$$

Жесткость сдвига блока РМЭ определяется как результат деления величины возвращающей поперечной силы $P_{ГВ}$ на поперечное перемещение его опорных поверхностей

$$Æ_{ñäî} = \frac{P_{ГВ}}{\delta_0}. \quad (17)$$

Таким же образом получены формулы для расчета жесткости для блоков, состоящих из различного количества РМЭ.

Результаты расчетов, проведенные по предложенной методике определения упругих характеристик опор, состоящих из комплекта резинометаллических элементов, представлены на рис. 3, 4.



– – – – экспериментальные данные ——— – расчетные данные

Рис. 3. Зависимость статического прогиба опоры от варианта конструктивного исполнения блока РМЭ и количества РМЭ в нем:
а) все РМЭ имеют отверстия диаметром 90 мм;
б) два верхних и два нижних РМЭ имеют отверстия диаметром 90 мм;
в) все РМЭ без отверстий (серийная опора тепловоза 2ТЭ116).

Сравнивая значения упругих характеристик блока РМЭ, полученные по предлагаемой методике, со значениями, получаемыми по существующей методике [2, 4], когда $Æ_{ñäïï} = \frac{Æ_{ñä}}{n}$, где n – количество РМЭ в блоке, определяем, что разница между значениями жесткости сдвига блока РМЭ может достигать 44%. В то же время с увеличением горизонтальной силы $P_{гв}$ значения статического прогиба могут отличаться на 16%, в слу-

чае же отсутствия горизонтальной силы такой разности практически не существует. Таким образом, упругие характеристики блока РМЭ, определяемые по существующей методике, отличается от предлагаемой тем, что она не учитывает различий в условиях деформаций отдельных его элементов.

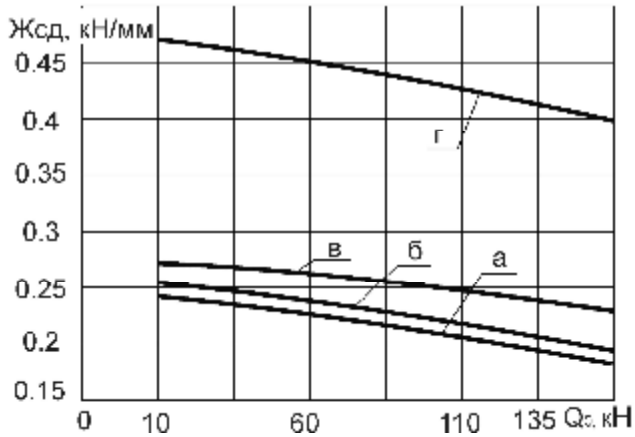


Рис. 4. Зависимость горизонтальной жесткости опоры от варианта конструктивного исполнения блока РМЭ и вертикальной нагрузки.
а) все РМЭ имеют отверстия диаметром 90 мм;
б) два верхних и два нижних РМЭ имеют отверстия диаметром 90 мм;
в) все РМЭ без отверстий (серийная опора тепловоза 2ТЭ116);
г) работа трех верхних РМЭ на сдвиг блокирована ограничителем горизонтальных перемещений.

Анализ результатов расчета показывает, что при различном конструктивном исполнении блока РМЭ опоры удается изменять как вертикальную, так и горизонтальную жесткость опор. Таким образом, использование предлагаемой методики расчета позволяет более точно определять упругие характеристики блока РМЭ с любым заранее заданным количеством элементов и его конструктивным исполнением.

Литература

1. Механическая часть подвижного состава: Учебник для вузов ж.-д. трансп. / И.В. Бирюков, А.Н. Савоськин, Г.П. Бурчак и др.; Под ред. И.В. Бирюкова. – М.: Транспорт, 1992.-440 с;
2. Тепловозы. Под ред.Н.И. Панова. М., Машиностроение, 1976. 544 с. с ил;
3. В.Н. Потураев Резиновые и резино-металлические детали машин. М.: «Машиностроение», 1966;
4. Конструкция, расчет и проектирование локомотивов: Учебник для студентов втузов, обучающихся по специальности «Локомотивостроение»/А.А. Камаев, Н.Г. Апанович, В.А. Камаев и др.; Под. ред. А.А. Камаева. – М.: Машиностроение, 1981, 351 с., ил.

УДК 625

Кашура А.Л.

УРОВЕНЬ СКОЛЬЖЕНИЙ В КОНТАКТЕ КОЛЕСА С РЕЛЬСОМ И СОПРОТИВЛЕНИЕ ДВИЖЕНИЮ

Рассмотрены качественные и количественные различия различных теорий взаимодействия колеса локомотива и рельса. Проведено сравнение теоретических величин скольжений поверхности колеса локомотива относительно рельса и величин скольжений, которые могут возникнуть в процессе эксплуатации.

Описание процессов взаимодействия колеса локомотива с рельсом имеет важное значение как с точки зрения обеспечения тяговых возможностей тягового экипажа, так и снижения сопротивления движению и износа взаимодействующих поверхностей.

Классификация гипотез о сцеплении подробно приведена в [3]. Здесь же проанализированы их принципиальные отличия. Отметим, что теории или гипотезы о сцеплении колеса локомотива с рельсом, основанные на предположении о существовании зоны «сцепления» в контакте колеса с рельсом названы «классическими». Основным принципиальным положением этих теорий является наличие в пятне контакта колеса с рельсом двух зон. В одной из них величина скольжения S точек поверхности колеса по поверхности равна нолю. Эта зона названа зоной «сцепления». В другой величина скольжения $S > 0$. Эта зона названа зоной «скольжения».

Рассмотрим процесс качения колеса локомотива по рельсу (рис.1).

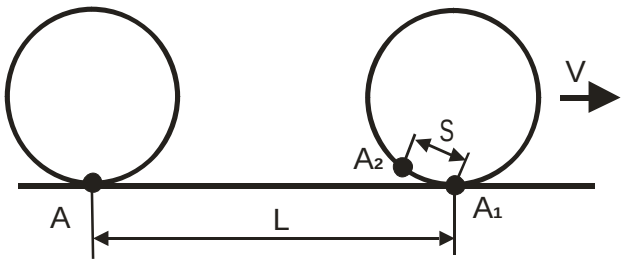


Рис. 1. Схема скольжения поверхности колеса относительно рельса.

За один оборот колеса точка **A** проходит расстояние **L** и должна занять положение $\mathbf{A_1}$. Но, вследствие проскальзывания, точка **A** займет положение $\mathbf{A_2}$. Разность положений точек $\mathbf{A_1}$ и $\mathbf{A_2}$ представляет собой величину абсолютного скольжения **S**. На железнодорожном транспорте чаще используют понятие относительного скольжения e.

$$\varepsilon = \frac{S}{L} \quad \text{или} \quad \varepsilon = \frac{dS\ /\ dt}{dL\ /\ dt} = \frac{\Delta V}{V},$$

где **V** – скорость движения колеса, $\Delta\mathbf{V}$ – скорость скольжения поверхности колеса относительно рельса.

Рассмотрим причины возникновения скольжения поверхности катания бандажа колеса относительно рельса в процессе эксплуатации.

Допуск на максимальную разность диаметров колес в колесной паре локомотива составляет 4 мм. Это значит, что за один оборот абсолютное скольжение одного колеса относительно другого может составить 3,14*4=12,56 мм. Величина относительного скольжения при диаметре колес 1050 мм составит 0,38%.

Определим разность диаметров колес от поперечного смещения в рельсовой колее. При зазоре в колее в прямом участке пути, равном 14 мм, и конусности поверхности катания колеса 1:20 разность диаметров колес может составить 14/20=0,7 мм. Тогда величина абсолютного скольжения составит 2,2 мм, а относительного 0,07%.

В кривых участках пути существует так называемое уширение или увеличенный зазор для облегчения прохождения экипажем кривой. Кроме того, вследствие кривизны, разный путь проходят колеса по внутреннему и по наружному рельсу. Несложные расчеты показывают, что величина относительного скольжения по этой причине может вполне составить примерно 0,3%.

Таким образом, только вследствие кинематики движения и эксплуатационных факторов величина относительного скольжения колес рельсового экипажа по рельсам в продольном направлении может составить 0,75%.

Теперь проанализируем результаты экспериментальных исследований, направленных на изучение аспектов «классической» теории сцепления.

В [2] сделан анализ экспериментальных данных по величинам микро-скольжений в контакте трущихся тел. Переходу колеса в полное скольжение относительно рельса пред-

шествует предварительное смещение точек поверхности контакта, определяемое как явление малого относительного перемещения. Это предварительное смещение ξ_{max} измерено на экспериментальной установке в [1] для образцов из материалов, идентичных материалам колеса и рельса и идентичных нагрузках. Максимальная величина ξ_{max} составила 14 мкм.

Очень важным моментом является то, что эти эксперименты проводились для чистых обезжиренных контактирующих поверхностей.

Анализ одной из самых характерных «классических» теорий – Ф.Картера [2, 4] – показывает, что максимум на характеристике сцепления соответствует уровню максимальных предварительных смещений и составляет 0,1-0,2% величины относительного скольжения поверхности бандажа колеса по рельсу. Аналогичные результаты дают и другие модификации этой или других теорий [5]. Все они построены на аналогичных предположениях о существовании зоны «сцепления» в контакте колеса с рельсом. Поэтому их результаты не имеют принципиальных ни количественных, ни качественных отличий.

Результаты этих теорий подтверждаются приведенными выше результатами экспериментов. Но они подтверждают только правильность решения поставленной задачи с учетом сделанных допущений. Существуют ли на железнодорожном пути условия, соответствующие сделанным допущениям? В [6] и многих других источниках указывается на наличие загрязнений как на рельсах, так и на колесах. Причем большинство из них имеет минерально-углеводородное происхождение. Это позволяет говорить как минимум о граничном трении колеса по рельсу [3].

В таких условиях реализации силы сцепления говорить о «классическом» подходе не представляется возможным. Более того, экспериментальные исследования на пути показывают, что высокий уровень сцепления сохраняется при стабильном скольжении в 10-15% [7].

Вывод: так называемая «классическая» теория сцепления не может объяснить результаты экспериментальных исследования процессов в контакте колеса локомотива с рельсом. Для более достоверного моделирования процессов сцепления и сопротивления движению необходимы более тщательные исследования с применением трибологического подхода.

Литература

1. Пинегин С.В. Трение качения в машинах и приборах. – М.: Машиностроение, 1976. – 264 с;
2. Голубенко А.Л. Сцепление колеса с рельсом: Монография. – К.: «ВИПОЛ», 1993. – 448 с;
3. Костюкевич А.И. Численная и экспериментальная идентификация процесса сцепления колес локомотива с рельсами: Дис. канд. техн. наук: - Луганск, 1991. – 232 с;
4. Медель В.В. Взаимодействие электровоза и пути. – М.: Трансжелдориздат, 1956. – 336 с;
5. Математическое моделирование колебаний рельсовых транспортных средств / Ушкалов В.Ф., Резников Л.М., Иккол В.С., Трубицкая Е.Ю., Редько С.Ф., Залеский А.И./ Под ред. В.Ф.Ушкалова .-Киев: Наукова думка, 1982.- 240 с;
6. Лужнов Ю.М., Попов В.А., Студентова В.Ф. Потери энергии их роль при реализации сцепления колес с рельсами // Трение, износ и смазочные материалы: Докл. Междуннар. Науч.-техн.конф. Ташкент, май 1985 г. – М., 1985. – Т.1. – с.133-138;
7. Асадченко В.Р. Характеристика сцепления колес с рельсами при торможении и ее особенности / Железнодорожный транспорт // Траспорт Урала. № 1. – 2004. – с.48 – 52.

УДК 621.318.38

Яковенко В.В., Букреев В.В., Корбан Н.П.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ МАГНИТОМОДУЛЯЦИОННОГО ПРЕОБРАЗОВАТЕЛЯ

В статье представлена математическая модель взаимодействия поля внешнего источника с магнитной системой магнитомодуляционного преобразователя, использующая интегральное уравнение Фредгольма первого рода. Предложен метод расчета, основанный на этой модели, который позволяет наиболее полно, по сравнению с существующими методами, учесть геометрические и магнитные параметры магнитных систем магнитомодуляционных датчиков.

Введение

Существующие методики расчета функции преобразования магнитомодуляционных датчиков (МД) основываются на методах анализа электрической цепи, содержащей нелинейную индуктивность. То есть под функцией преобразования МД понимается зависимость выходного сигнала модулятора от величины магнитного потока в сердечнике МД, само значение потока считается известным. В некоторых случаях величина магнитного потока рассчитывается методом магнитных цепей. Однако, поскольку входным сигналом МД является не магнитный поток, а некоторая физическая величина, для измерения которой и предназначен МД, то естественным является под функцией преобразования понимать зависимость выходного напряжения модулятора от значения физической величины.

Сложность определения магнитного потока в магнитопроводе магнитной системы датчика заключается в том, что требуется расчет магнитного поля системы, включающей в себя магнитопровод и источник поля, расположенный вне магнитопровода. Геометрическая конфигурация такой системы является сложной и расчет поля требует больших затрат времени, особенно в том случае, когда магнитная система датчика и источник магнитного поля перемещаются относительно друг друга. Источником поля, генерирующим магнитный поток в магнитопроводе датчика, может быть постоянный магнит (ПМ), ферромагнитное тело (ФТ), ступенчатая или зубчатая поверхность ФТ. Ферромагнитное тело может быть предварительно намагничено отдельным источником или полем Земли, или индуцировать поле под воздействием поля магнитной системы датчика.

В статье приводятся принципы построения расчетных схем по определению магнитного потока в магнитопроводе магнитной системы датчика, основанные на применении принципа взаимности К.М. Поливанова[1].

Математическая модель магнитного потока

Математическая модель взаимодействия поля внешнего источника и магнитной системы датчика основывается на теореме о взаимности [1], суть которой выражается соотношением:

$$\Phi = \frac{\mu_0}{iw}\int_V \overline{H}(P)\cdot\overline{M}(P)dV\,, \qquad \boldsymbol{P}\in\boldsymbol{V}\,, \tag{1}$$

где Φ - магнитный поток в магнитопроводе датчика;

$\overline{H}(P)$ - вектор напряженности магнитного поля, создаваемого размещенной на магнитопроводе обмоткой с намагничивающей силой iw;

iw - намагничивающая сила обмотки;

$\overline{M}(P)$ - вектор намагниченности в объеме V;

$\mu_0 = 4\pi\cdot 10^{-7}$ Гн/м – магнитная постоянная;

V - объем ферромагнитного тела.

Если ферромагнитное тело представляет собой постоянный магнит или ферромагнитное тело с известным распределением намагниченности, то магнитный поток в магни-

топроводе датчика может быть рассчитан путем непосредственного использования формулы (1).

Если имеются насыщенные и ненасыщенные ферромагнитные тела, то применяется общая формула [3]:

$$\Phi = \frac{m_0}{iw}\left[\int_V \overline{H}(P)\cdot\overline{M}(P)dV - \int_S j(K)M_n(K)dS\right],\ K\in S, \qquad (2)$$

здесь $j(K)$ - скалярный магнитный потенциал ферромагнитного тела;

$M_n(K)$ - нормальная составляющая намагниченности на поверхности магнитного тела;

S – площадь поверхности ферромагнитного тела.

Функция $\overline{H}(P)$ определяется путем решения интегрального пространственного уравнения [2]

$$4\pi\overline{H} = grad\left[\int_V \frac{div\overline{M}}{R}dV - \int_S M_n\cdot\frac{dS}{R}\right], \qquad (3)$$

которое при разбиении намагниченного пространства тела на элементарные объемы, представляющие собой параллелепипеды, и при допущении того, что в каждом элементарном объеме $div\overline{M} = 0$, сводится к системе алгебраических уравнений

$$\overline{H}_i = L\overline{M}_j + \sum_{k=1}^{K}\overline{H}_{\delta k}, \qquad (4)$$

где

$$L = \frac{1}{4\pi}\sum_{j=1}^{N}\overline{1}_n\int_{S_l}\frac{\bar{r}_{ij}}{\left|r_{ij}\right|^3}dS_l,$$

здесь N – общее количество элементарных объемов;

i,j – номера точек наблюдения и источника;

l – номер грани S_l, по которой производится интегрирование;

$\overline{1}_{nl}$ - внешняя нормаль к l – ой грани;

$\bar{r}_{ij}$ - радиус-вектор, проведенный из точки наблюдения в точку источника;

$\overline{H}_{\delta k}$ - вектор напряженности магнитного поля, создаваемого током в k-ой обмотке.

Система уравнений (4) решается итерационным способом по алгоритму:

$$\overline{M}^{k+1} = \overline{M}^{k} + \alpha(\overline{H}^{k} - \overline{H}^{k}_{\beta}), \qquad (5)$$

здесь k – номер итерации;

α - число, подбираемое эмпирически, $0 \le \alpha \le 2$;

$\overline{H}_{\beta}$ - вектор напряженности, соответствующий намагниченности $\overline{M}^{k}$;

$\overline{H}$ - суммарный вектор напряженности, создаваемый всеми элементарными объемами.

Алгоритм расчета величины выходного сигнала МД

При расчете величины выходного сигнала МД принимаются следующие допущения:

- петля гистерезиса магнитного материала аппроксимируется одной линией;
- магнитопровод МД разбивается на N элементарных объемов.

Один из вариантов конструкции магнитной системы показан на рис. 1.

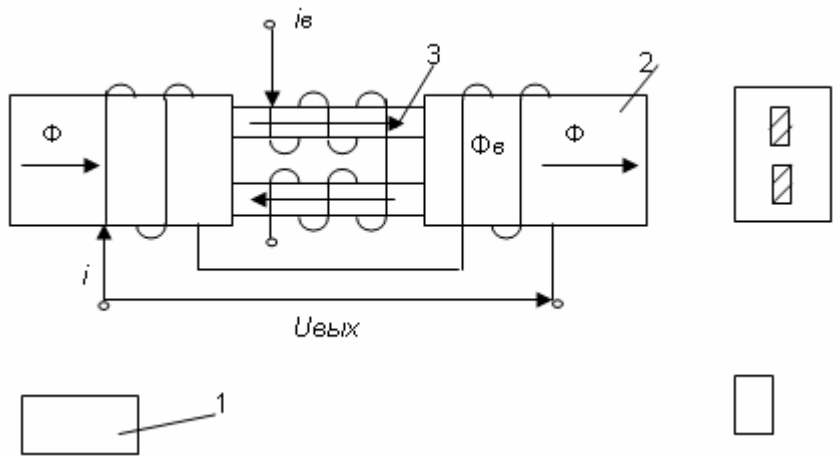


Рис. 1. Конструкция магнитной системы МД.
1 – ферромагнитное тело, 2 – сердечник, 3 – модулятор.

Алгоритм расчета функции преобразования МД следующий. Задаются геометрические и магнитные параметры магнитопровода. Петля гистерезиса магнитного материала аппроксимируется линией, а затем кубическими сплайнами. Задается число витков обмотки возбуждения и выходной обмотки, руководствуясь тем, что ток возбуждения должен доводить стержни модулятора до насыщения. При такой конструкции значение K в формуле (4) равно 2.

Задаются геометрические параметры намагниченного ферромагнитного тела, его координаты в пространстве и функция вектора намагниченности его материала.

Принимается, что обмотка возбуждения запитывается от источника синусоидального тока $i_{â} = I_{mâ} \sin \omega t$. Полупериод функции тока разбивается на n частей, в результате чего функция тока возбуждения дискретизуется $i_в = i_в[n]$.

Значение тока i в выходной обмотке МД устанавливается так, чтобы было $i << I_m$, что соответствует реальным условиям измерений.

Устанавливается в обмотке возбуждения значение тока $i[1]$ и путем решения системы уравнений (4) определяется значение $H[1]$, затем по формуле:

$$j_{\boldsymbol{i}} = \frac{1}{4p} \sum_{\boldsymbol{j}=1}^{\boldsymbol{N}} \sum_{\boldsymbol{l}=1}^{6} \overline{\boldsymbol{M}_{\boldsymbol{l}}} \cdot \bar{1}_{\boldsymbol{n}} \int_{\boldsymbol{S}_{\boldsymbol{l}}} \frac{\boldsymbol{dS}}{\boldsymbol{r}_{\boldsymbol{ij}}} + \sum_{\boldsymbol{k}=1}^{\boldsymbol{K}} j_{\boldsymbol{dk}}, \qquad (6)$$

где j_{dk} - потенциал, созданный обмотками с током, находится значение $j[1]$.

Катушки МД располагаются в пространстве различным образом и имеют, в основном, прямоугольное сечение. Кроме того, катушки имеют определенную толщину обмоток, которую необходимо учитывать. Поэтому целесообразно при расчете полей потенциала j_d и вектора напряженности $\overline{H}$ придерживаться двух правил. Формулы для расчета полей приводить в локальной системе координат, а затем встраивать их в глобальную систему координат. Обмотки по толщине разбивать на слои, как это предлагается в [3], а поле аппроксимировать суммой полей бесконечно тонких слоев тока, число слоев определять по формуле:

$$m \geq \frac{\Delta l}{0{,}025(p_1 + p_2)},$$

где p_1, p_2 – внутренний и внешний периметры катушки;

$\Delta \boldsymbol{l}$ - расстояние между токовыми слоями.

В этом случае магнитный потенциал считается по формуле:

$$j_d = \sum_{i=1}^{m} d_i a_i(m),$$

а вектор напряженности магнитного поля – по формуле:

$$\bar{H}_\delta = \sum_{i=1}^{m} \delta_i \bar{\beta}_i(m),$$

где δ_i - линейная плотность ампер-витков в бесконечно тонкой обмотке, которая равна:

$$\delta_i = \frac{IW}{mL_k},$$

здесь L_k – длина катушки;

IW – ампер-витки;

$\alpha_i(m), \bar{\beta}_i(m)$ - скалярная и векторная функции, которые определяются взаимным расположением точки наблюдения и i - ой бесконечно тонкой обмотки.

Внутри катушки, как показано на рис.2, выделяется фиктивный виток с размерами du, dv, dw площадью dS и током $I=idw$, где i – поверхностная плотность тока.

Поскольку для витка с током скалярный магнитный потенциал равен [1]:

$$j_d = \frac{IS\cos\Theta}{4p\boldsymbol{R}^2},$$

где Θ - угол между векторами $\bar{S}$ и $\bar{R}$, то потенциал в точке Q от элементарного витка с координатами u', v', w' внутри объема катушки будет иметь вид:

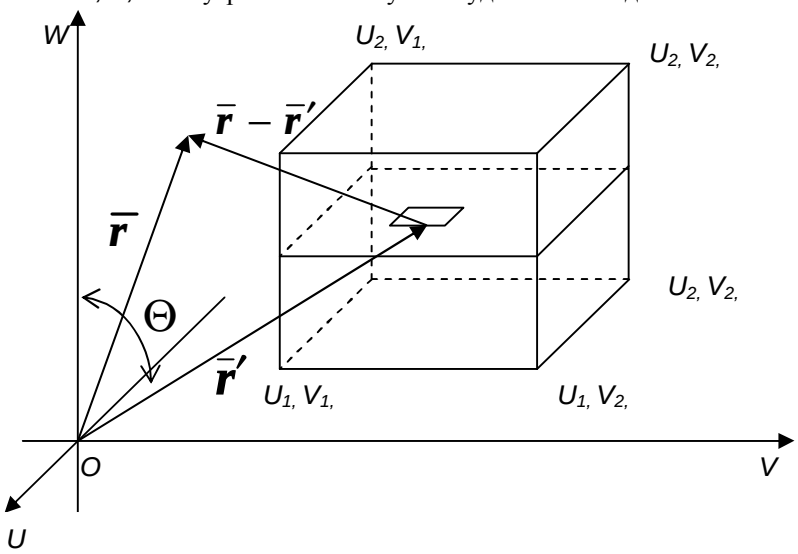


Рис. 2. К расчету скалярного магнитного потенциала катушки прямоугольного сечения.

$$dj_d = \frac{idwdS\cos\Theta}{4p\boldsymbol{R}^2} = \frac{iwdudvdw}{4p[(u-u')^2 + (v-v')^2 + (w-w')^2]^{\frac{3}{2}}},$$

а от всей катушки

$$j_d = \frac{1}{4p}\int_{u_1}^{u_2}\int_{v_1}^{v_2}\int_{w_1}^{w_2} \frac{iwdudvdw}{[(u-u')^2 + (v-v')^2 + (w-w')^2]^{\frac{3}{2}}}. \qquad (7)$$

Интеграл (7) рассчитывается численными методами. Значение вектора напряженности магнитного поля вычисляется по формуле Био-Савара [1].

По такому же алгоритму определяются все значения потока $\phi[n]$ за половину периода тока возбуждения, после чего путем численного дифференцирования определяется выходной сигнал датчика $U_{вых}[n]$.

Последовательно перемещая ферромагнитное тело относительно МД, можно найти функциональную зависимость между амплитудным значением выходного сигнала и величиной перемещения ферромагнитного тела по одной из координат.

Выводы

1. Существующие методы расчета МД не учитывают многих геометрических и магнитных параметров магнитных систем МД, что снижает достоверность результатов расчета. Для учета всех геометрических и магнитных параметров необходим полевой метод расчета, в основу которого положена математическая модель, использующая интегральное уравнения Фредгольма первого рода.

2. Предложен алгоритм расчета выходного сигнала, основанный на численном методе расчета поля в магнитной системе МД при дискретном изменении тока в обмотке модулятора.

Литература

1. Поливанов К.М. Теоретические основы электротехники. Т.3. – М.: Энергия, 1985 – 296 с. ил;
2. Курбатов П.А. Метод ограниченных областей для решения задач нелинейной магнитостатики. Электромагнитные поля и системы: Сб. научн. трудов. – МЭИ. - 1986. - №118. - С. 31 – 37;
3. Поляченко Е.Ю., Яковенко В.В., Тарасенко О.В. Импульсное устройство электропитания аппаратуры на вращающихся объектах//Вестник национального технического университета «ХПИ». - 2004. - №22. - С.41 – 44.

УДК 629.4.015.57

Губачева Л.А.

ГЕОМЕТРИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПОДВИЖНЫХ СОПРЯЖЕНИЙ РЕЛЬСОВЫХ ЭКИПАЖЕЙ ЖЕЛЕЗНЫХ ДОРОГ

Произведено геометрическое моделирование подвижных сопряжений рельсового экипажа на примере главной пары трения фрикционного гасителя колебаний пассажирской тележки с применением пакета прикладных программ MSC.NASTRAN.

Среди большого количества разработанных численных методов механики особое место занимает метод конечных элементов (МКЭ).

К числу универсальных пакетов МКЭ могут быть отнесены ППП ANSYS, MSC.NASTRAN, MSC.MARC, ALGOR, COSMOS, LS-DYNA и ряд других. По своему основному предназначению эти пакеты выполняют одинаковые функции и могут использоваться в зависимости от возможностей их приобретения. На последнее влияет их коммерческая цена (весьма высокая), наличие сервисных центров, региональных дилеров и др. Анализ работ, представленных на 13-м конгрессе по колесным парам (Рим, 2001), показал, что на фирмах, производящих продукцию для нужд железнодорожного транспорта, чаще всего используются пакеты ANSYS, COSMOS и MSC.NASTRAN [1-3].

Пакеты ANSYS и MSC.NASTRAN имеют более исследовательский характер. Их главное отличие заключается в том, что ANSYS имеет свой графический интерфейс, который позволяет полностью проводить создание и анализ модели средствами самого пакета. MSC.NASTRAN изначально был ориентирован на пакетный режим обработки информации. И первоначально NASTRAN являлся решателем, для которого пользователь должен был подготовить по определенным правилам информацию о рассматриваемой модели, а затем, после проведенных вычислений, обрабатывать ее либо вручную, либо с помощью дополнительных средств, которые не входили в саму программу. Таким образом, процесс

анализа любой модели состоит из 3 этапов: подготовка информации о рассматриваемой модели (препроцессинг); ее численный анализ с использованием метода конечных элементов; численная или графическая обработка результатов расчета (постпроцессинг). У фирмы MSC.Software Corporation есть два NASTRANa. Один в качестве пре- и постпроцессора использует программный продукт PATRAN той же фирмы, а второй - пре- и постпроцессор FEMAP фирмы Structural Dynamic Research Corp. И здесь возникают определенные сложности для пользователя, связанные с предпочтительностью выбора программного продукта. Следует отметить, что наиболее удобный графический интерфейс, который полностью ориентирован на возможности как Windows 98, так и Windows 2000, имеют пакет FEMAP и соответственно интегрированный пакет MSC.NASTRAN for Windows. Указанные пакеты имеют еще одно преимущество: они позволяют импортировать геометрию рассматриваемой модели из практически любой CAD-системы или проводить импорт модели целиком, если она была создана в FEA-системе. Полная аналогия с экспортом. Эти качества позволяют многим пользователям предпочесть указанный выше программный продукт. К сожалению, этот пакет имеет недостатки, связанные с тем, что FEMAP не полностью реализует возможности базового пакета MSC.NASTRAN. Например, отсутствует возможность задания сложных (зависящих от температуры) реологических свойств материала. Использование же пакета MSC.PATRAN в качестве пре- и постпроцессора позволяет реализовать возможности базового пакета MSC.NASTRAN в полном объеме.

В данной работе рассматривается решение задачи геометрического моделирования с помощью пакета прикладных программ (ППП) MSC.NASTRAN for Windows, которое выполняется при помощи программного пакета FEMAP 9.0.1. Рассматривается контакт двух деталей – втулки 1 и сухаря 2 (рис.1), пару трения образуют втулка и 6 сухарей, работающих одновременно.

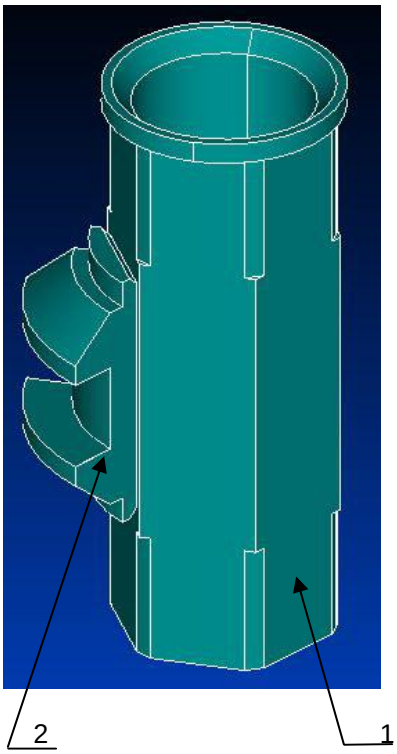


Рис. 1. Пара трения: 1-втулка, 2-сухарь.

Геометрическая модель втулки создавалась по частям, как набор четырех трехмерных тел, которые показаны на рис.2. После их создания при помощи операции булевого суммирования создавался единый трехмерный объект.

Наиболее просто создается модель фланцевой части. Для этого необходимо задать геометрию ее радиального сечения, преобразовать эту геометрию в объединенную поверхность типа Boundary Surface и вращением вокруг центральной оси создать трехмерное тело.

Наиболее сложными для моделирования частями являются нерабочие части втулки. Покажем последовательность действий при создании геометрии этого объекта. Сначала задается правильный шестиугольник, лежащий в основании, вписанный в окружность диаметром 87 мм (рис. 3), который затем преобразуется в поверхность Boundary Surface. Затем «выдавливаем» эту поверхность на расстояние 50 мм в направлении оси Z, в результате чего получаем первое трехмерное тело – правильную шестигранную призму (рис. 4).

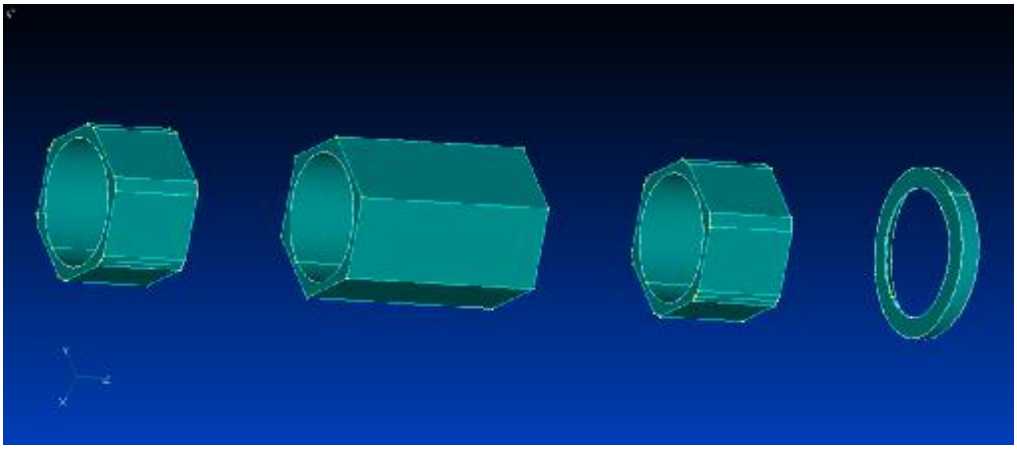


Рис. 2. Геометрическое моделирование втулки, как состоящей из 4 трехмерных объектов.

Следующая операция: совершенно аналогично сначала рисуем в плоскости XOY окружность диаметром 67,5 мм – внутреннее отверстие втулки, затем преобразуем его в поверхность типа Boundary Surface и выдавливаем его. В результате получаем второе трехмерное тело – цилиндр. Далее выполняются булевы операции логического вычитания из первого тела второго. Полученный в результате объект представлен на рис. 3.

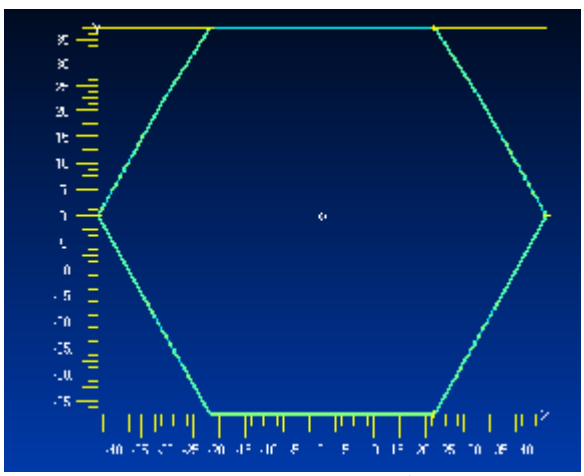


Рис. 3. Задание поверхности типа Boundary Surface в основании призмы.

Осталось у полученного объекта «снять фаски». Здесь стоит подчеркнуть, что чаще всего геометрические модели деталей могут создаваться различными способами. Например, указанную операцию можно было бы выполнить следующим образом: создать дополнительное тело – полый цилиндр с внешним диаметром достаточно большим, например, 100 мм и с внутренним диаметром 83 мм. Последующая булева операция вычитания позволила бы «снять фаски». Но в качестве примера рассмотрим другую технологию. Зададим в плоскости XOY окружность диаметром 83 мм, преобразуем ее в поверхность типа Boundary Surface и выдавим ее, создав обычную поверхность. Операция булевого вычитания из трехмерного объекта (рис. 5) созданной поверхности приводит к разбиению трехмерного тела на 7 частей: центральную и «фаски». Далее эти «фаски» могут быть удалены. Процесс их удаления показан на рис. 6, где половина «фасок» уже удалена.

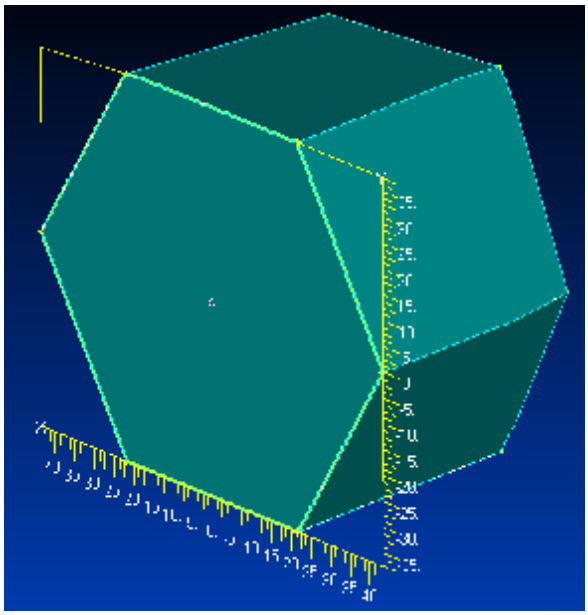


Рис. 4. Создание первого трехмерного объекта – шестигранной призмы.

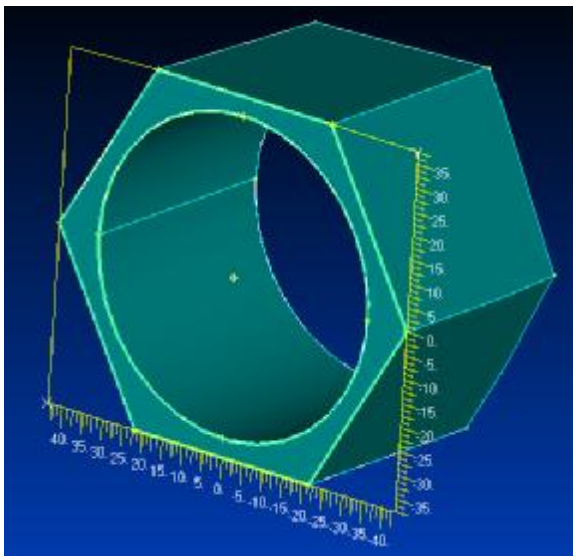


Рис. 5. Шестигранная призма с центральным отверстием.

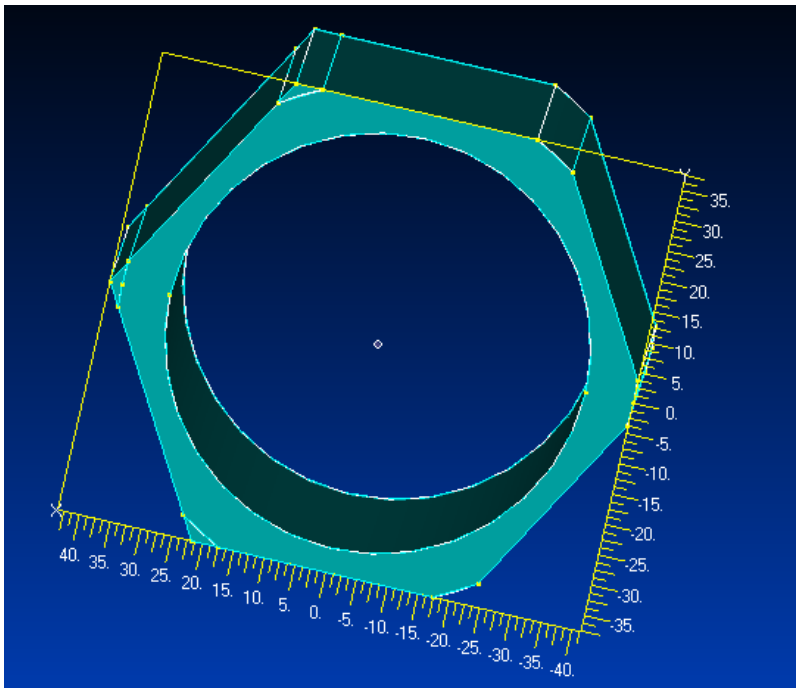


Рис. 6. Удаление «фасок» - трехмерных объектов, образовавшихся после выполнения булевой операции вычитания.

На геометрическом моделировании сухаря подробно останавливаться не будем, подчеркнем только, что оно значительно сложнее, требует выполнения значительно большего числа построений. Отметим только основной принцип. Сначала создается тело вращения, которое должно быть по своим размерам больше комплекта из 6 сухарей. Затем при помощи многочисленных булевых операций лишний «металл» убирается, как бы моделируется механическая обработка. И, наконец, единый трехмерный объект разрезается на 6 частей. На рис. 7 показана геометрическая модель сухаря, а на рис. 8 показана геометрическая модель сборки узла трения (втулки и 6 сухарей).

Конструкция данного узла трения центрально симметрична. Это позволяет рассматривать КЭ модель не всего узла, а только его шестую часть. С учетом того, что уменьшение количества узлов означает для пространственных задач соответствующее уменьшение числа степеней свободы, а значит и количества уравнений, то такой подход позволяет существенно уменьшить время решения задачи. Поскольку рассматриваемая задача относится к классу контактных задач связанной термоупругости, то ее решение даже для одной итерации требует значительного времени счета даже на очень мощных ЭВМ. Поэтому следует рассматривать только шестую часть узла трения, задав на границах втулки необходимые граничные условия.

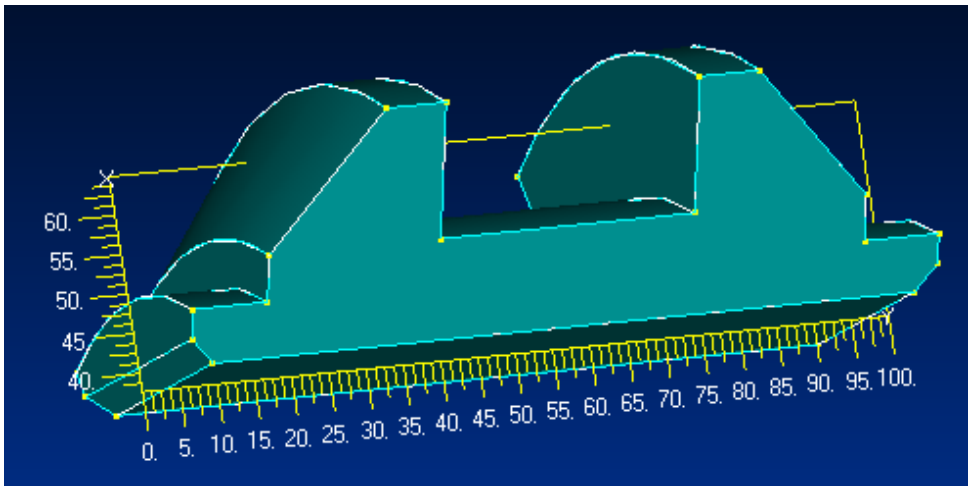


Рис. 7. Геометрическая модель сухаря.

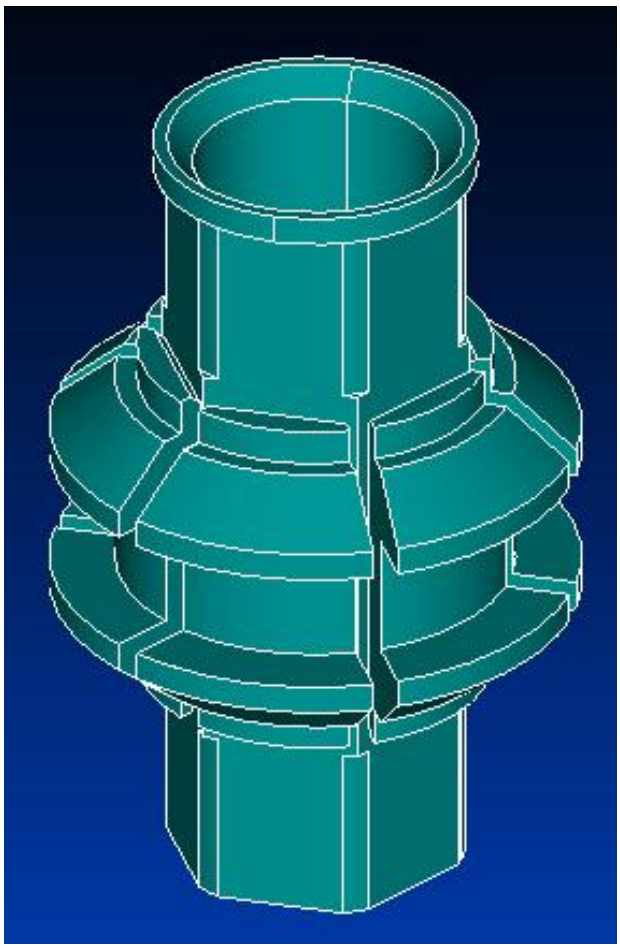


Рис. 8. Геометрическая модель сборки.

В плане геометрического моделирования это также означает, что геометрическая модель, представленная на рис. 8, должна быть рассечена плоскостями, проходящими че-

рез ребра основной шестигранной призмы и лишние части должны быть отброшены. На рис. 9 показана геометрическая модель шестой части рассматриваемого узла трения.

После этого можно приступать к следующему этапу - генерации КЭ сеток.

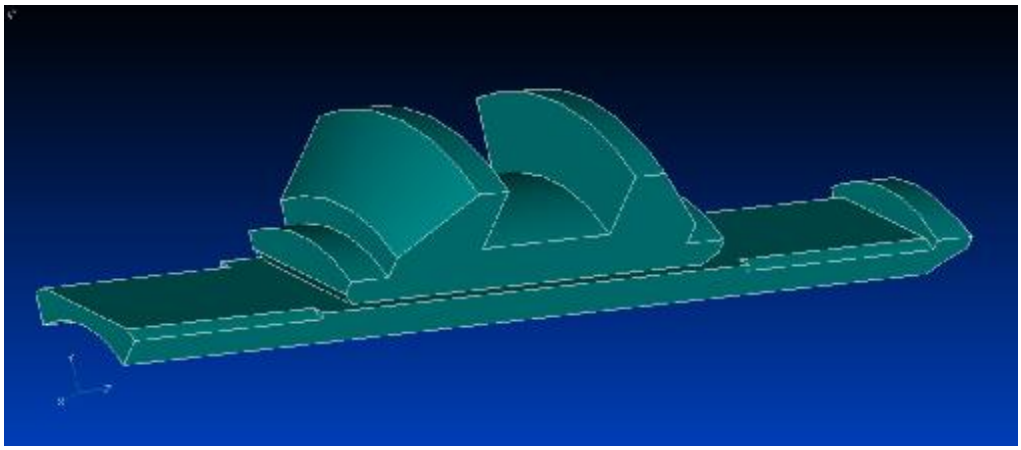


Рис. 9. Геометрическая модель шестой части рассматриваемого узла трения.

Выводы

Приведенная методика позволяет максимально использовать преимущества традиционного проектирования, создавая контуры сечений, а затем с помощью операций твердотельного моделирования, например, выдавливания, получать виртуальные заготовки частей деталей, которые максимально приближены к реальным конструкциям.

Литература

1. Есаулов В.П. Применение MSC.NASTRAN for Windows для расчета железнодорожных колес //Опыт применения передовых компьютерных технологий инженерного анализа фирмы MSC.Software на предприятиях России, Белоруссии, Украины /Вторая Российская конф. пользователей MSC.- М.: Постоянное представительство MSC.Software Corporation в СНГ, 2001.-С. 154-156;
2. Аксёнов Ю.Н., Богачёв А.Ю., Петров С.Ю. Опыт и практические результаты использования программных продуктов MSC для оценки работоспособности объектов ж.д. транспорта // Повышение эффективности применения передовых компьютерных технологий инженерного анализа фирмы MSC.Software на предприятиях России, Белоруссии, Украины /Четвертая Российская конференция пользователей MSC. – М.: Постоянное представительство MSC.Software Corporation в СНГ, 2001;
3. Сладковский А.В., Ситаж М., Мартыненко Ю.Р. Решение задач механики железнодорожного транспорта с помощью МКЭ. – Днепропетровск: Новая идеология, 2002. – 220 с.

УДК 546. 289

Рубан Р. В., Гоптарев М. Н., Кожемякин Г. Н.

ВЛИЯНИЕ ОТЖИГА НА СОВЕРШЕНСТВО СТРУКТУРЫ МОНОКРИСТАЛЛОВ ТВЕРДЫХ РАСТВОРОВ $GA_XIN_{1-X}SB$

Изучено влияние отжига на совершенство структуры в монокристаллах твердых растворов $Ga_xIn_{1-x}Sb$ с содержанием Ga от x=0,03 до x=0,07. Измерена плотность дислокаций в кристаллах, отожженных в области температур 170-300°С. Рис. 4. Ист. 7.

Твердые растворы $Ga_xIn_{1-x}Sb$ являются одними из перспективных материалов оптоэлектроники. Во всей области концентраций компонентов от InSb до GaSb величина запрещенной зоны кристаллов изменяется от 0,17 до 0,73 эВ, благодаря чему они могут работать в инфракрасной области длин волн соответственно 7-1,7 мкм при комнатной тем-

пературе. Это обеспечивает применение их в качестве высокочувствительных фотодатчиков, светоизлучающих диодов и лазеров [1,2].

Совершенство структуры монокристаллов $Ga_xIn_{1-x}Sb$ существенно влияет на их электрофизические и оптические свойства. В процессе роста монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$ методами направленной кристаллизации в них, как правило, образуются трещины [3]. Это обусловлено существенным изменением параметров кристаллической решетки до 6% при варьировании в кристаллах концентрации компонентов [4-5]. Экспериментально установлено, что легирование теллуром кристаллов $Ga_xIn_{1-x}Sb$ уменьшает количество трещин в них [6]. Впервые было показано в работе [7], что отжиг монокристаллов $Ga_{0,03}In_{0,97}Sb$ при температуре 150°С устраняет трещины длиной более 1 мм. Однако ранее более детально не изучалось влияние отжига на совершенство структуры монокристаллов $Ga_xIn_{1-x}Sb$, одним из критериев которого является плотность дислокаций.

Целью данной работы является изучение влияния отжига на плотность дислокаций легированных монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$ с содержанием Ga до x=0,07.

Монокристаллы твердых растворов $Ga_xIn_{1-x}Sb$ диаметром от 7 до 18 мм были выращены методом Чохральского. При выращивании монокристаллов $Ga_{0,03}In_{0,97}Sb$ в качестве затравки использовали монокристалл InSb с ориентацией <111>B. Для выращивания монокристаллов $Ga_{0,05}In_{0,95}Sb$ в качестве затравки использовали монокристалл $Ga_{0,03}In_{0,97}Sb$, а монокристаллов $Ga_{0,07}In_{0,93}Sb$ - монокристаллическую затравку состава $Ga_{0,05}In_{0,95}Sb$. Скорость вытягивания монокристаллов $Ga_xIn_{1-x}Sb$ составляла 2-3 мм/ч при частоте вращения кристаллов 8-10 об/мин. Тигель с расплавом, масса которого не превышала 85 г, в процессе роста не вращался. Исходным материалом для выращивания монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$, легированных теллуром, являлись галлий, индий, сурьма и теллур особой чистоты 99,9999 вес. %. Концентрация теллура в выращенных кристаллах составляла $1\cdot10^{18}$ $см^{-3}$. Процесс роста осуществляли в среде аргона высокой чистоты при избыточном его давлении 0,4 атм.

После выращивания, каждый монокристалл $Ga_xIn_{1-x}Sb$ разрезали параллельно оси роста, после чего их травили в травителе СР4А и подвергали отжигу в печи при температурах 170°С и 300°С в течение 12 ч. После отжига монокристаллы вновь разрезали параллельно оси роста вдоль первоначально отрезанной поверхности (рис. 1).

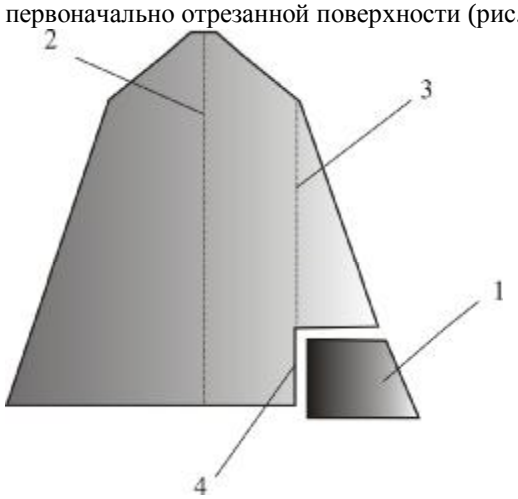


Рис. 1. Схема разрезания монокристаллов $Ga_xIn_{1-x}Sb$:
1 – часть монокристалла, отрезанная до отжига; 2, 4 – поверхности, отрезанные до отжига; 3 – поверхность, отрезанная после отжига.

Для подсчета плотности дислокаций поверхности 3 и 4 образцов кристаллов шлифовали с использованием порошка Al_2O_3 с размером зерна до 40 мкм. После шлифовки образцы полировали окисью хрома до получения зеркальной поверхности. Для выявления дислокаций отполированные поверхности кристаллов подвергали травлению в смеси кислот $3HF:3CH_3COOH:5HNO_3:1H_2O$ в течение 5-20 с при комнатной температуре. Наблюде-

ние количества и размеров трещин, а также подсчет плотности дислокаций по ямкам травления осуществляли под металлографическим микроскопом ММР-2Р.

Плотность дислокаций в монокристаллах твердых растворов $Ga_xIn_{1-x}Sb$ определяли как среднеарифметическое значение количества ямок травления из 20 измерений в отожженной и не отожженной областях кристаллов. Ошибка определения плотности дислокаций не превышала ±20%.

Поверхности монокристаллов $Ga_{0,03}In_{0,97}Sb$ и $Ga_{0,05}In_{0,95}Sb$ до и после отжига представлены на рис. 2.

На поверхности монокристаллов, отрезанных до отжига (рис. 2, а, в), видны трещины размером более 1 мм, вытянутые, как правило, перпендикулярно оси вытягивания. На поверхности этих же монокристаллов, отрезанных после отжига, трещины размером более 1 мм отсутствовали (рис. 2, б, г).

Глубокие трещины вдоль боковых поверхностей этих монокристаллов, а также аналогичные трещины в кристалле $Ga_{0,07}In_{0,93}Sb$ (рис. 3) устранить отжигом при 300°С не удалось. Вероятно, эти трещины образовались в процессе роста кристаллов из-за существенного отличия осевого и радиального градиентов температур.

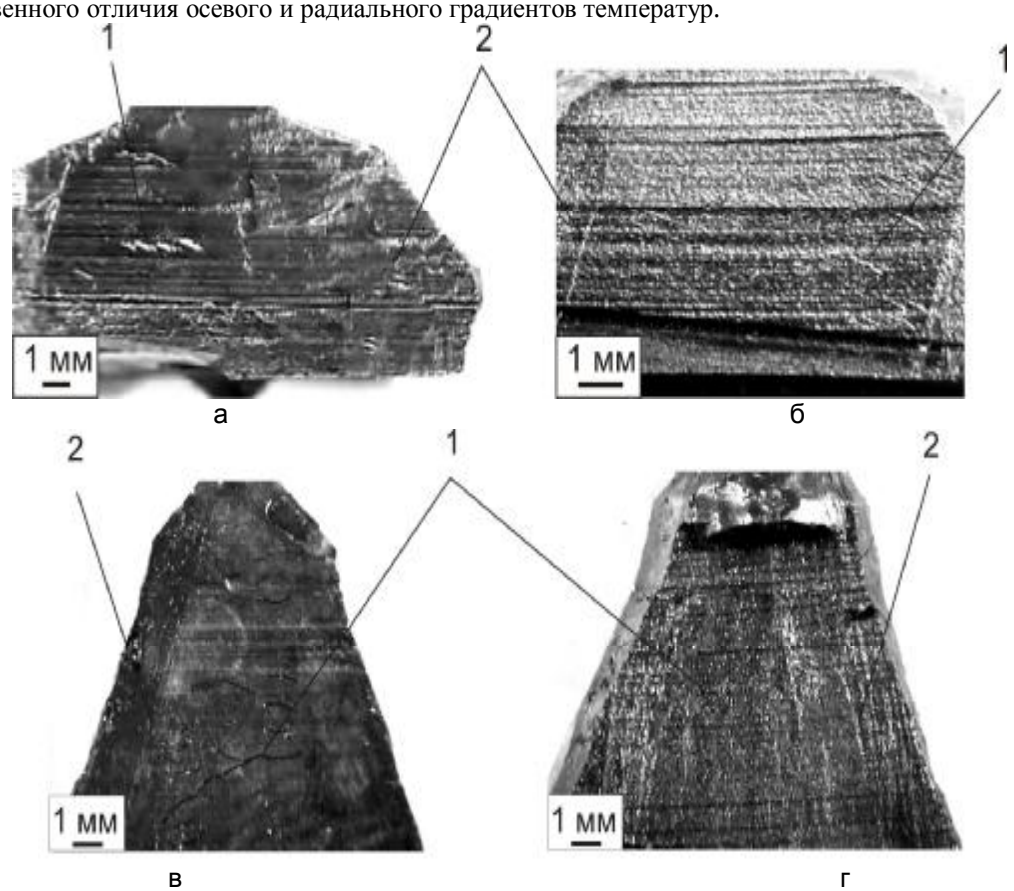


Рис. 2. Монокристаллы $Ga_{0,03}In_{0,97}Sb$ и $Ga_{0,05}In_{0,95}Sb$
а – $Ga_{0,03}In_{0,97}Sb$ до отжига; б – $Ga_{0,03}In_{0,97}Sb$ после отжига; в - $Ga_{0,05}In_{0,95}Sb$ до отжига; г - $Ga_{0,05}In_{0,95}Sb$ после отжига; 1-2 – трещины.

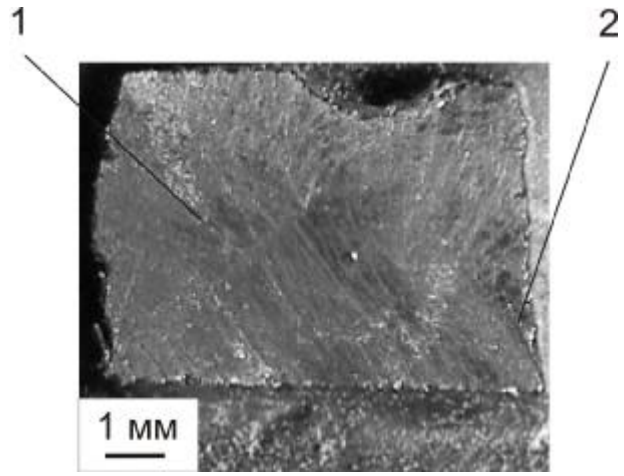


Рис. 3. Монокристалл $Ga_{0,07}In_{0,93}Sb$ после отжига;
1-2 – трещины.

Зависимость плотности дислокаций от содержания галлия в исследуемых монокристаллах $Ga_xIn_{1-x}Sb$ представлена на рис. 4.

Плотность дислокаций в кристаллах возрастает с увеличением содержания галлия от x=0,03 до x=0,07 как в не отожженной, так и в отожженной областях. В не отожженных областях вышеуказанных кристаллов плотность дислокаций увеличивается с $1{,}1\cdot10^6$ $см^{-2}$ до $1{,}51\cdot10^6$ $см^{-2}$, а в отожженных - от $8{,}55\cdot10^5$ до $1{,}05\cdot10^6$ $см^{-2}$. Надо полагать, отжиг при температурах до 300°C уменьшает внутренние напряжения в кристаллах $Ga_xIn_{1-x}Sb$, что способствует снижению количества дислокаций в них.

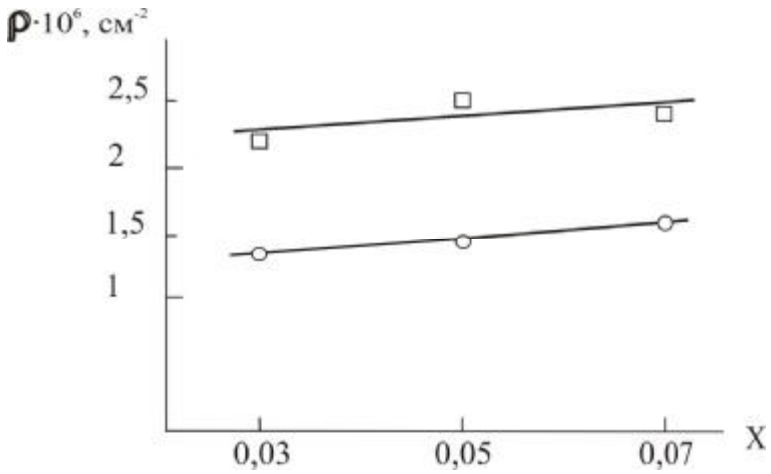


Рис. 4. Плотность дислокаций в монокристаллах $Ga_xIn_{1-x}Sb$
О – поверхности кристаллов, отрезанные после отжига;
– поверхности кристаллов, отрезанные до отжига.

Выводы

1. Отжиг монокристаллов твердых растворов $Ga_{0,03}In_{0,97}Sb$ и $Ga_{0,05}In_{0,95}Sb$ при температуре 170°C в течение 10-12 часов снижает количество трещин внутри кристаллов и устраняет трещины, размером более 1 мм.

2. Отжиг монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$ с x до 0,7 при температурах до 300°C в течение 12 часов не позволяет устранить трещины, появляющиеся на боковой поверхности вытянутых монокристаллов. Вероятно, образование таких трещин может

быть результатом превышения градиентов температуры выше оптимальных в твердой фазе.

3. Отжиг монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$ с содержанием галлия до x=0,07 при температурах 170°С и 300°С снижает плотность дислокаций на 30-40%.

Литература

1. Gong Xiuying, Kazuhiko Okitsu, Tctsuo Ozawa, Yasuhiro Hawarawa, Tomou Yamaguoii, Masashi Kumagawa. LPE Growth of Ga1-xInxSb Multi-grading Layers. Research Institute of Electronics. Shizuotca University Johoku. Hamamatsu, Japan. Cryst. Res. Technol. 1992;
2. P. S. Dutta, H. L. Bhat, V. Kumar, J. Appl. Phys. 81 (1997) 5821;
3. C. Barat, T. Duffar, J.P. Garandet. Chemical segregation in vertical Bridgman growth of GaInSb alloys // Cryst. Res. Technol. – 1999. – V. 34, № 4 – P. 449-456;
4. Solid-solution hardening and Vegard's rule of In1-xGaxSb. M. Schenk, C. Silber. / J. of Materials science: materials in electronics, 9 (1998), 313-316;
5. Axially linear slopes of composition for "delta" crystals. P. Gille, M. Hollatz, H. Kleessen, M. Schenk. / J. of Crystal Growth, 139, (1994), 165-171;
6. Burstein-Moss shift in impurity-compensated bulk Ga1-xInxSb substrates. R. Pino, Y. Ko, and P. S. Dutta, Shekhar Guha, Leonel P. Gonzalez./ J. of Applied Physics, v.96, November, 2004;
7. Г. Н. Кожемякин, Л. В. Золкина, М. В. Афанасьева. Исследование влияния отжига на трещины в монокристаллах твердых растворов $Ga_xIn_{1-x}Sb$. Весник ВНУ им. В. Даля, №3, 2005, стр. 119-122.

УДК 546.289

Золкина Л.В., Кожемякин Г.Н., Ром М.А.

СОВЕРШЕНСТВО СТРУКТУРЫ И ЭЛЕКТРОФИЗИЧЕСКИЕ СВОЙСТВА МОНОКРИСТАЛЛОВ $GA_XIN_{1-X}SB$

Изучены структурное совершенство, основные электрофизические свойства монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$ с содержанием галлия x до 0,03, выращенных в ультразвуковом поле. Рентгенографически установлено, что исследуемые монокристаллы $Ga_xIn_{1-x}Sb$ обладают высоким совершенством структуры. Обнаружено положительное воздействие ультразвука на электрофизические свойства: удельное электросопротивление, подвижность носителей заряда и термо-э.д.с. полученных монокристаллов $Ga_xIn_{1-x}Sb$. Рис. 4. Табл. 1. Ист. 14.

В настоящее время большое количество исследований посвящено получению монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$ высокого качества, которые относятся к перспективным материалам оптоэлектроники [1-4]. Применение классического и модифицированных методов Бриджмена, традиционного метода Чохральского не принесло положительных результатов, так как полученные кристаллы $Ga_xIn_{1-x}Sb$ являлись поликристаллами и имели достаточно высокую неоднородность распределения компонентов вдоль слитка и в его поперечном сечении, а также трещины [1-4]. Изучение результатов экспериментов роста монокристаллов $Ga_xIn_{1-x}Sb$ при воздействии внешних полей показало, что наименьшими энергозатратами, наибольшими простотой и эффективностью характеризуется выращивание кристаллов в ультразвуковом поле [5-6]. Оптимальные условия роста и введение ультразвуковых волн с частотой 1,44 МГц в расплав позволили значительно снизить слоистую неоднородность распределения компонентов в вытянутых монокристаллах твердых растворов $Ga_xIn_{1-x}Sb$ с содержанием галлия x до 0,03 [7-8]. Положительное воздействие ультразвукового поля на рост монокристаллов $Ga_xIn_{1-x}Sb$, которое заключалось в устранении слоев с периодом более 14 мкм в центральных областях и на периферии кристаллов, было подтверждено с помощью оптической микроскопии и селективного травления [7-8]. Однако для оценки качества полученных монокристаллов $Ga_xIn_{1-x}Sb$ необходимы дополнительные исследования. Поэтому целью настоящей работы является изучение структурного совершенства исследуемых в работах [7-8] монокристаллов $Ga_xIn_{1-x}Sb$ и ос-

новных электрофизических свойств данных кристаллов, выращенных в ультразвуковом поле.

Образцы для рентгенографических исследований имели форму пластин толщиной до 2 мм, вырезанных из слитка вдоль оси роста <111> параллельно боковой грани (211) и обработанных механически для удаления искаженного приповерхностного слоя. Определение совершенства структуры образцов проводилось с помощью метода кривых качания [9]. Измерения были выполнены на дифрактометре ДРОН-3 в $CuK_{\alpha 1}$-излучении (монохроматор Ge(111)) по схеме (n, -m) на рефлексе (422). Применяемое линейное пошаговое сканирование позволило изучить совершенство структуры образцов по их сечению.

Эксперименты, посвященные определению основных электрофизических свойств монокристаллов $Ga_xIn_{1-x}Sb$ с содержанием галлия x до 0,03 включали измерение концентрации носителей заряда, удельного электросопротивления и термоэлектродвижущей силы. Данные измерения проводились при температуре 300 К как на образцах монокристаллов, выращенных без ультразвукового воздействия, так и на образцах монокристаллов, вытянутых при воздействии ультразвуковых волн на расплав. Кроме того, для получения сравнительных данных основных электрофизических параметров монокристаллов InSb и $Ga_xIn_{1-x}Sb$ дополнительно были выполнены измерения концентрации носителей заряда, удельного электросопротивления и термо-э.д.с. в образцах монокристалла InSb, полученного вытягиванием из расплава, для которого были использованы исходные материалы: индий и сурьма высокой чистоты, как и для роста монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$. Исследуемые образцы монокристаллов $Ga_xIn_{1-x}Sb$ и InSb имели прямоугольную форму с размерами 1,6×1,6×7 мм и 2×1×13 мм соответственно и были вырезаны параллельно направлению вытягивания монокристаллов. Измерение концентрации носителей заряда в вышеуказанных монокристаллах осуществлялось с помощью эффекта Холла, который возникает при помещении образца в электрическое и магнитное поля [10]. В образце монокристалла электрическое поле создавалось источником постоянного тока, имеющим высокое выходное сопротивление. Полюса постоянного магнита, между которыми помещался образец, позволяли получить магнитную индукцию 0,18 Тл. Направление вектора магнитной индукции и положение контактов подводимого тока показаны на рис. 1. Падение напряжения на эталонном сопротивлении, включенном последовательно с образцом, соответствовало холловскому напряжению и было измерено с помощью микровольтметра Щ300. Для получения точных данных определения э.д.с. Холла в процессе эксперимента были проведены четыре измерения при двух направлениях тока через образец и двух направлениях магнитного поля, а контакты измерительной схемы были выполнены методом точечной сварки.

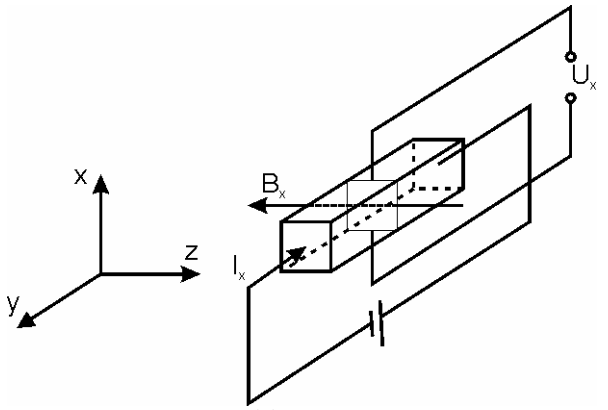


Рис. 1. Схема возникновения эффекта Холла в образце монокристалла.

С целью измерения удельного электросопротивления монокристаллов $Ga_xIn_{1-x}Sb$ и InSb применялся двухзондовый метод, необходимым условием которого является создание омических контактов на образце [11]. Через данные контакты вдоль образца пропус-

кали электрический ток, величина которого составляла 0,5 А. Подача электрического тока осуществлялась от источника постоянного тока Б5-46, включенного последовательно с сопротивлением. В качестве потенциальных зондов использовали медную проволоку с острозаточенными концами. Медные зонды, установленные на одной из поверхностей образца вдоль линий тока, позволяли определить возникающее падение напряжения на образце (рис. 2). Относительная погрешность измеряемых величин концентрации носителей заряда и удельного электросопротивления составляла: $\frac{\Delta n_k}{n_k} = \pm 3\%$ и $\frac{\Delta \rho_y}{\rho_y} = \pm 2\%$.

Величина термоэлектродвижущей силы в образцах монокристаллов $Ga_xIn_{1-x}Sb$ и InSb была определена путем измерения разности потенциалов на концах образца при создании некоторого градиента температуры в кристалле. Подготовка следуемых образцов включала выполнение на одной из боковых граней кристаллов, параллельной оси вытягивания, углублений диаметром до 0,3 мм и глубиной до 0,4 мм для крепления медных контактов и медь-константановых термопар. Диаметр медной и константановой проволок, применяющихся в экспериментах, был равен 0,1 мм, что позволяло минимизировать тепловые потери через эти контакты. На одном из концов образца крепился резистивный нагреватель, а на втором его конце – медный радиатор. Такая конструкция позволяла обеспечить создание градиента температуры на образце монокристалла до 1,8 К/см (рис. 3). С целью определения точного значения градиента температуры расстояние между подпаянными к образцу медными контактами и термопарами было измерено с помощью оптического микроскопа с точностью 0,05 мм. Показания медь-константановых термопар, расположенных вблизи медных контактов и контролирующих температуру, фиксировались цифровым прибором ЩС300 с точностью 0,1 мкВ. При этом точность определения температуры на образце монокристалла $Ga_xIn_{1-x}Sb$ составляла 0,05 К. Знак термо-э.д.с. в исследуемых монокристаллах определяли по известному отрицательному значению термоэлектродвижущей силы в монокристаллах висмута [12].

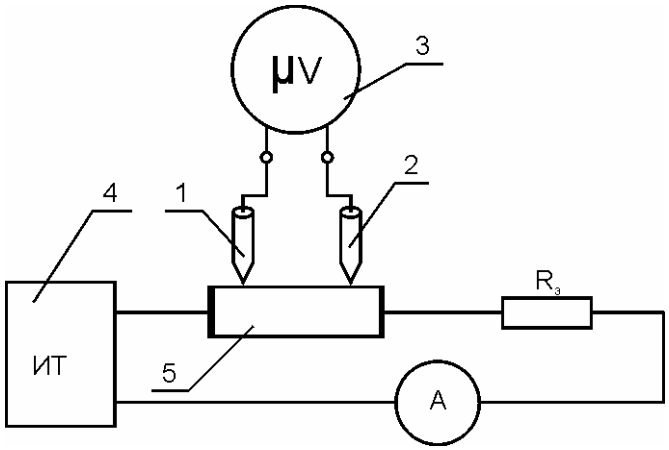


Рис. 2. Схема измерений удельного сопротивления двухзондовым методом:
1, 2 – потенциальные зонды;
3 – микровольтметр ЩС300;
4 – источник постоянного тока;
5 – образец монокристалла.

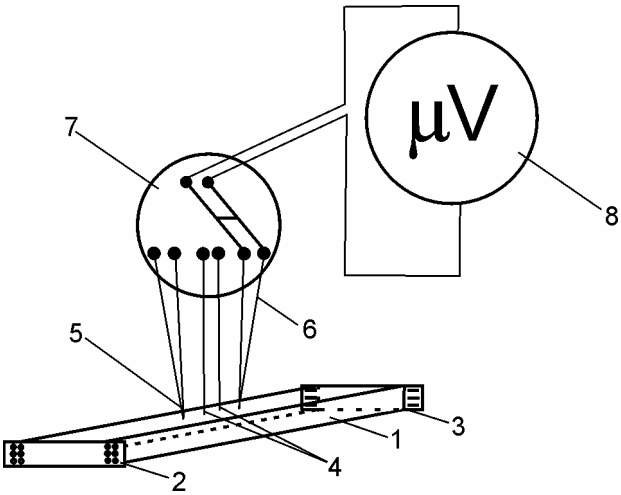


Рис. 3. Схема измерения термо-э.д.с.:
1 – кристалл;
2 – нагреватель;
3 – медный радиатор;
4 – медные контакты;
5, 6 – медь-константановые термопары;
7 – переключатель ПМТ-8;
8 – микровольтметр.

Оценка погрешности измерений была выполнена по результатам 8 измерений термо-э.д.с. при температуре 300 К на образце монокристалла $Ga_xIn_{1-x}Sb$. Перед каждым измерением проводился демонтаж и монтаж медных контактов, термопар и других измерительных проводов. Относительная погрешность измерения термо-э.д.с. составляла ±2 %.

На рис. 4 приведены кривые качания кристаллов с областями, выращенными без ультразвука и при его воздействии на расплав. В точке 1, которая располагалась в верхней части слитка, обнаружены блоки мозаики с углами разориентации 0,015÷0,03° при полуширине кривой качания β ~0,05°. В точке 2 блочная структура не наблюдалась, а величина β составляла ~0,065°. Блоки с разориентацией менее 0,1° обнаружены в точке 3. Подобная структура со сравнительно крупными блоками и малыми углами разориентации свидетельствует о высоком совершенстве структуры исследуемых монокристаллов.

Для определения концентрации носителей заряда в монокристаллах $Ga_xIn_{1-x}Sb$ и InSb на основе усредненного по образцу значения холловского сигнала был вычислен коэффициент Холла, равный [11]:

$$R_X = 10^8 \cdot \frac{U_X \cdot}{I_X \cdot B_X}, \qquad (1)$$

где U_x – холловское напряжение;

v – размер образца по оси x;

I_x – сила тока, протекающего через образец;

B_x – магнитная индукция.

Тогда концентрацию носителей заряда можно определить из соотношения [11]:

$$n_k = 6{,}25 \cdot 10^{18} / R_X \qquad (2)$$

Полученные значения концентрации носителей заряда в монокристаллах твердого раствора $Ga_xIn_{1-x}Sb$, выращенных в ультразвуковом поле и без воздействия ультразвука на расплав, незначительно отличаются и являются достаточно близкими к измеренной вели-

чине концентрации носителей заряда, равной $2{,}3\cdot10^{16}$ см$^{-3}$ в исследуемых монокристаллах InSb.

В результате измерений падения напряжения на образцах монокристаллов $Ga_xIn_{1-x}Sb$ и InSb двухзондовым методом удельное электросопротивление вычисляли согласно выражению [10]:

$$\rho_y = \frac{U_p \cdot S_o}{I_o \cdot s_o}, \qquad (3)$$

где U_p – разность потенциалов между измерительными зондами;

S_o – площадь поперечного сечения образца;

I_o – постоянный ток, протекающий через образец;

s_o – расстояние между зондами.

Определенные таким образом значения концентрации носителей заряда и удельного электросопротивления были применены для вычисления подвижности носителей заряда в монокристаллах $Ga_xIn_{1-x}Sb$ и InSb по соотношению [10]:

$$m_n = \frac{1}{e \cdot n_k \cdot r_y}, \qquad (4)$$

где e – заряд электронов, равный $1{,}602\cdot10^{-19}$, Кл.

Результаты определения концентрации носителей заряда, удельного электросопротивления, подвижности носителей заряда и термо-э.д.с. в исследуемых монокристаллах приведены в таблице 1.

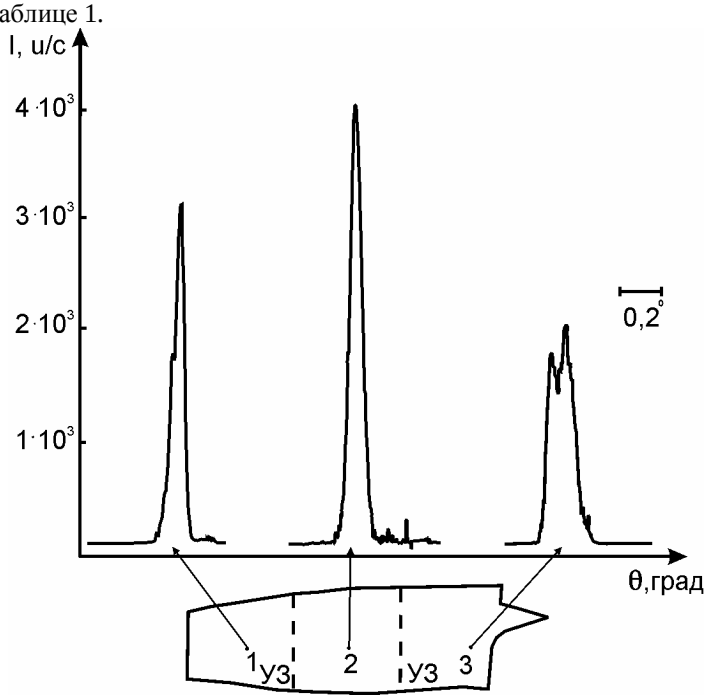


Рис. 4. Кривые качания монокристалла $Ga_xIn_{1-x}Sb$.

Полученные значения подвижности носителей заряда в монокристаллах твердого раствора $Ga_xIn_{1-x}Sb$, выращенных без ультразвука и при ультразвуковом воздействии отличаются на 23-46 %. Более высокая подвижность носителей заряда в кристаллах, вытянутых в ультразвуковом поле, характеризует их более высокое качество. Это может быть результатом уменьшения рассеяния носителей заряда, которое обусловлено однородным распределением компонентов, обнаруженным при помощи оптической микроскопии и

селективного травления, в вышеуказанных монокристаллах. Данные значения также достаточно близки к величине подвижности носителей заряда в монокристаллах InSb, которая согласно экспериментам измерения составила $6{,}6\cdot10^4$ см^2/В·с. Кроме того, подвижность носителей заряда в монокристаллах твердого раствора $Ga_xIn_{1-x}Sb$ с содержанием галлия x до 0,03 значительно выше подвижности носителей заряда, равной $4\cdot10^4$ см^2/В·с в кристаллах твердого раствора такого же состава и легированных теллуром до концентрации $2{,}6\cdot10^{18}$ см$^{-3}$ [13]. Значения концентрации и подвижности носителей заряда в монокристаллах $Ga_xIn_{1-x}Sb$, которые близки к значениям данных характеристик в совершенных монокристаллах InSb, также подтверждают высокое совершенство структуры выращенных монокристаллов.

Дифференциальная термо-э.д.с. в монокристаллах $Ga_xIn_{1-x}Sb$ и InSb была найдена согласно выражению [14]:

$$\alpha_{1,2} = \lim_{\Delta T_{\hat{e}} \to 0} \frac{U_{1,2}}{\Delta T_{\hat{e}}} \qquad (5)$$

где $U_{1,2}$ – разность потенциалов, возникающая в полупроводнике;

$\Delta T_к$ – разность температур.

Таблица 1

Электрофизические свойства в монокристаллах твердых растворов $Ga_xIn_{1-x}Sb$ и InSb.

№ п/п	Состав кристаллов / Параметр	Монокристалл InSb	Монокристалл GaxIn1-xSb, выращенный без ультразвукового воздействия	Монокристалл GaxIn1-xSb, вытянутый при воздействии ультразвуковых волн на расплав
1.	Концентрация носителей заряда, n_k, см$^{-3}$	2,3·1016	$(2{,}53\pm0{,}05)\cdot10^{16}$	$(2{,}57\pm0{,}05)\cdot10^{16}$
2.	Удельное электросопротивление, r_y, Ом·см	40,9·10-4	$(49{,}6\pm1)\cdot10^{-4}$	$(36{,}5\pm0{,}7)\cdot10^{-4}$
3.	Подвижность носителей заряда, m_n, см^2/В·с	6,6·104	$(5\pm0{,}2)\cdot10^4$	$(6{,}7\pm0{,}3)\cdot10^4$
4.	Термоэлектродвижущая сила, $a_{1,2}$, мкВ/К	–183	–130±3	–165±3

Согласно экспериментальным данным термоэлектродвижущая сила в образцах монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$, выращенных без ультразвукового воздействия, была равна –130±3 мкВ/К. Значительное отличие данной величины было обнаружено в образцах монокристаллов $Ga_xIn_{1-x}Sb$, полученных в ультразвуковом поле. Так, термо-э.д.с. в монокристаллах, которые выращены при воздействии ультразвука, составила 165±3 мкВ/К, что на 22-32% больше значения термоэлектродвижущей силы в образцах кристаллов, вытянутых без ультразвукового воздействия. Более высокое значение термо-э.д.с. в кристаллах, вытянутых в ультразвуковом поле, может быть обусловлено отсутствием слоев с расстоянием более 14 мкм. Надо полагать, что в случае наличия слоистости в монокристаллах увеличивается рассеяние носителей заряда, которое отрицательно влияет на основные электрофизические параметры. Это подтверждает и более высокое значение подвижности носителей заряда в монокристаллах $Ga_xIn_{1-x}Sb$, выращенных при воздейст-

вии ультразвука. В монокристаллах InSb с близкой концентрацией носителей к монокристаллам твердого раствора $Ga_xIn_{1-x}Sb$ величина термо-э.д.с. составила –183 мкВ/К, что хорошо согласуется с данными, приведенными в работе [14]. Отличие значений термо-э.д.с. в монокристаллах $Ga_xIn_{1-x}Sb$ в сравнении с кристаллами InSb указывает на характерное для неупорядоченных твердых растворов снижение структурного совершенства. Однако по результатам проведенных измерений одной из структурно-чувствительных характеристик полупроводниковых материалов – термо-э.д.с. в исследуемых монокристаллах можно также утверждать о положительном влиянии вводимых в расплав в процессе роста ультразвуковых волн на совершенство структуры вытянутых монокристаллов $Ga_xIn_{1-x}Sb$.

Выводы

1. Рентгеноструктурный анализ монокристаллов твердых растворов $Ga_xIn_{1-x}Sb$ с содержанием галлия x до 0,03 показал наличие мозаичных блоков с углами разориентации не превышающими 0,1° , что свидетельствует о высоком совершенстве структуры.

2. Установлено положительное воздействие ультразвука на удельное электросопротивление и подвижность носителей заряда, которое состоит в снижении удельного электросопротивления на 23-29% и увеличении подвижности носителей заряда на 23-46% в монокристаллах $Ga_xIn_{1-x}Sb$, полученных в ультразвуковом поле в отличие от монокристаллов $Ga_xIn_{1-x}Sb$, которые выращены без ультразвука.

3. Показано, что дифференциальная темо-э.д.с. в монокристаллах $Ga_xIn_{1-x}Sb$, вытянутых в ультразвуковом поле, на 22-32% больше данной величины в монокристаллах, которые получены без ультразвука.

Литература

1. Pino R., Ko Y. and Dutta P.S. Burstein-Moss shift in impurity-compensated bulk $Ga_{1-x}In_xSb$ substrates // J. Appl. Phys. – 2004. – V. 96. – № 9 – P. 5349 – 5352;
2. Barat C., Duffar T., Garandet J.P. Chemical segregation in vertical Bridgman growth of GaInSb alloys // Cryst. Res. Technol. – 1999. – V. 34. – № 4 – P. 449 – 456;
3. Tanaka A., Shintani J., Kimura M. Multi-step pulling of GaInSb bulk crystal from ternary solution // J. Cryst. Growth. – 2000. – V. 209. – P. 625 – 629;
4. Tsaur S.C., Kou S. Growth of $Ga_{1-x}In_xSb$ alloy crystals by convectional Czochralski pulling // J. Cryst. Growth. – 2003. – V. 249. – P. 470 – 476;
5. Okitsu K., Hayakawa Y., Hirata A. Gravitation effects on mixing and growth morphology of an $In_{0.5}Ga_{0.5}Sb$ system // Cryst. Res. Techol. – 1996. – V. 31. – № 8 – P. 969 – 978;
6. Tsuruta T., Yamashita K., Adachi S. Effect of ultrasonic vibrations on the growth of $In_xGa_{1-x}Sb$ mixed crystals (III) // Jpn. J. Appl. Phys. – 1992. – V. 31. – P. 23 – 25;
7. Zolkina L.V., Kozhemyakin G.N. Effect of ultrasound on the growth striations in $Ga_xIn_{1-x}Sb$ single crystals // Functional Materials. – 2005. – №4(12), – P. 25 – 29;
8. Золкина Л.В., Кожемякин Г.Н. Влияние ультразвукового поля на слоистую неоднородность в монокристаллах твердых растворов $Ga_xIn_{1-x}Sb$ // Вестник ВНУ им. В. Даля, Луганск – 2004.– №6(76) – С. 90 – 93;
9. Русаков А.А. Рентгенография металлов. – М.: Атомиздат. – 1977. – 480 с;
10. Фистуль В.И. Введение в физику полупроводников. – М.: Высш. шк., 1984. – 352 с;
11. Павлов Л.П. Методы определения основных параметров полупроводниковых материалов. – М.: Высш. шк., 1975. – 206 с;
12. Регель А.Р., Глазов В.М. Физические свойства электронных расплавов – М.: Наука, 1980. – 296 с;
13. Pino R., Ko Y. and Dutta P.S. Burstein-Moss shift in impurity-compensated bulk $Ga_{1-x}In_xSb$ substrates // J. Appl. Phys. – 2004. – V. 96. – № 9 – P. 5349 – 5352;
14. Тауц Я. Фото- и термоэлектрические явления в полупроводниках – М.: Изд-во иностранной литературы, 1962. – 253 с.

УДК 622.7

Яковенко В.В, Бранспиз М.Ю., Букреев В.В.

РАСЧЕТ НЕОБХОДИМОЙ СИЛЫ ИЗВЛЕЧЕНИЯ БАРАБАННЫХ МАГНИТНЫХ СЕПАРАТОРОВ С БОКОВОЙ ПОДАЧЕЙ СЕПАРИРУЕМОГО МАТЕРИАЛА

Для магнитных сепараторов барабанного типа с боковой подачей сепарируемого сыпучего материала описана методика расчета необходимой силы извлечения, позволяющая учесть основные эксплуатационные факторы, влияющие на рабочий процесс сепаратора.

Введение

Для магнитных сепараторов барабанного типа известны две схемы подачи сепарируемой среды [1–4]:

1) верхняя подача (рис. 1а), когда сыпучий материал подается сверху на вращающуюся обечайку сепаратора;

2) боковая подача (рис. 1б), при которой сепарируемый материал совершает свободное падение рядом с обечайкой сепаратора.

В то время как для сепараторов с верхней подачей имеются методики инженерных расчетов необходимой магнитной силы, обеспечивающей надежное извлечение ферромагнитных включений [1–3], для сепараторов с боковой подачей такие методики лишь только разрабатываются [4]. Создание такой методики является актуальной задачей, так как именно значение необходимой извлекающей силы определяет основные геометрические и электротехнические параметры барабанного магнитного сепаратора, являясь исходным при проектировании его магнитной (или электромагнитной, в зависимости от типа возбуждения) системы.

В данной работе представлены результаты разработки методики расчета необходимой извлекающей силы для сепараторов, эксплуатируемых по второй схеме.

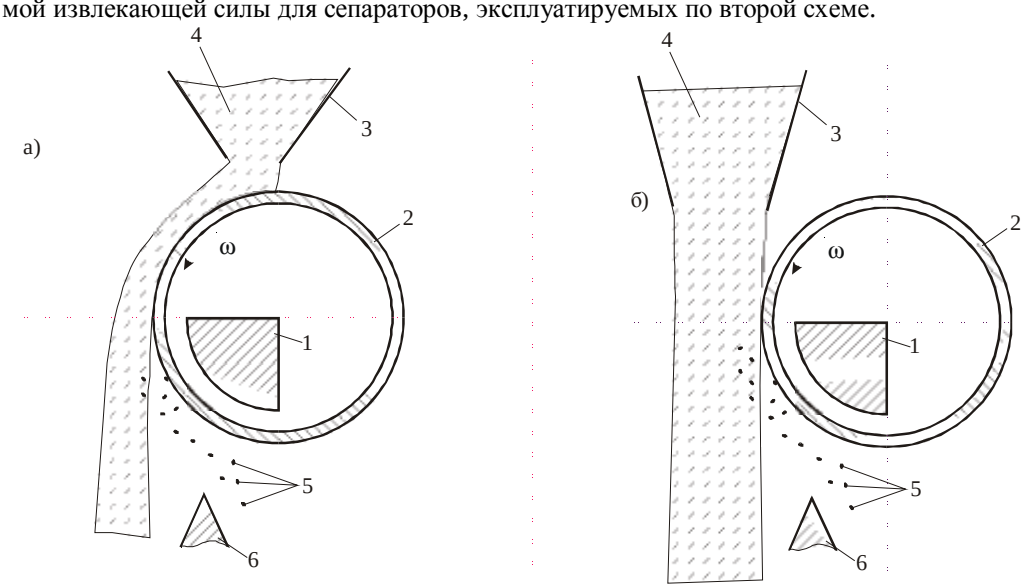


Рис. 1. Схемы барабанного магнитного сепаратора с верхней (а) и боковой (б) подачей материала в рабочую зону:
1 – неподвижная магнитная система; 2 – вращающаяся обечайка барабана;
3 – бункер питателя;
4 – сепарируемая сыпучая среда;
5 – ферромагнитные тела;
6 – разделительный шибер.

1. Расчетная схема сепарации

С этой целью учтем, что процесс извлечения ферромагнитных тел наиболее труден для тех тел, попавших в зону извлечения, которые находятся на наибольшем удалении от поверхности барабана на максимальном расстоянии от нее, равном толщине сепарируемого слоя h_M (точка А на рис. 2). При чем этот процесс является успешным, если траектория движения извлекаемого тела, начавшись в точке А, заканчивается в точке В на поверхности барабана (рис.2). При этом, ввиду существенной неравномерности распределения магнитной силы F_M в рабочей области сепаратора, под необходимой силой извлечения будем понимать для определенности значение радиальной составляющей силы F_M именно в точке А (обозначим эту силу F_A).

В качестве базы для определения силы F_A примем методику разложения движения извлекаемого ферромагнитного тела на два независимых движения, как это сделано в [5] применительно к магнитным шкивам. В рассматриваемом случае такими независимыми движениями являются:

- переносное движение ферромагнитного тела в вертикальном направлении под действием силы тяжести и частиц сыпучей среды;
- относительное движение тела под действием извлекающей магнитной силы в радиальном направлении к поверхности обечайки барабана магнитного сепаратора сквозь слой сыпучего немагнитного материала.

Как ясно из рис. 2 сила магнитного поля F_M, действующая на ферромагнитное тело в любой точке траектории извлечения, имеет вертикальную составляющую, направленную против поля тяжести, что приводит к торможению ферромагнитного тела в свободно падающем потоке сыпучего материала. В результате переносное движение тела по вертикали будет происходить за большее время, по сравнению со временем свободного падения. В дальнейших расчетах, однако, этим торможением пренебрежем, что, ввиду уменьшения расчетного времени переносного движения, приводит к завышению необходимой силы извлечения, а, следовательно, не снижает надежности извлечения.

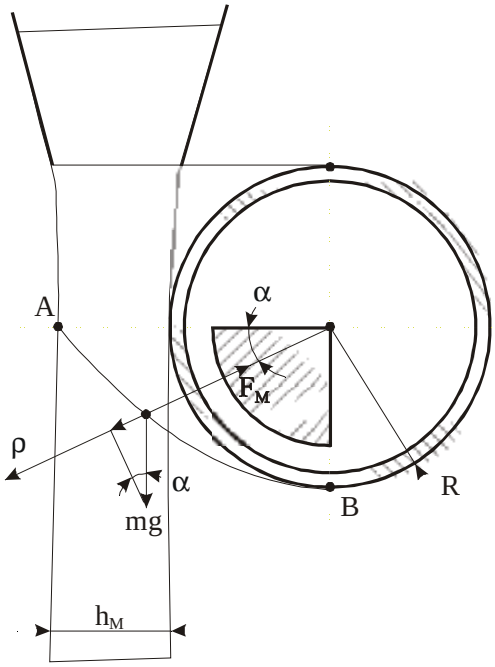


Рис.2. Расчетная схема извлечения ферромагнитного тела барабанным магнитным сепаратором.

2. Уравнение переносного движения и его решение

Итак, если считать переносное движение свободным падением, то путь, пройденный ферромагнитным телом, определяется выражением [6]

$$\frac{1}{2} g t_{âåðò}^2 + V_A \cdot t_{âåðò} = R, \qquad (1)$$

где g – ускорение свободного падения; V_A – начальная скорость тела в точке А, $t_{âåðò}$ – время, переносного движения, в течение которого тело проходит по вертикале путь *R*, равный наружному радиусу обечайки (см. рис.2).

Решая (1), находим:

$$t_{âåðò} = \sqrt{\left(\frac{V_A}{g}\right)^2 + 2\frac{R}{g}} - \frac{V_A}{g}. \qquad (2)$$

Для дальнейших выкладок учтем следующее: при подаче сепарируемого материала в рабочую зону барабанного магнитного сепаратора из выпускного отверстия соответствующего бункера – питателя необходимо предусматривать технологический зазор между корпусом бункера и вращающейся обечайкой барабана сепаратора. Как следствие, выпускное отверстие соответствующего бункера располагается в рассматриваемом случае на некотором расстоянии от точки А, равном радиусу R обечайки барабана (рис. 2).

Если теперь принять, что начальная скорость выхода сыпучего материала из бункера – питателя приблизительно равна нулю, то для скорости V_A, как скорости свободного падения тела после прохождения определенного расстояния [6], можно записать следующую формулу:

$$V_A = \sqrt{2 \cdot g \cdot R}, \qquad (3)$$

подстановка которой в (2), после несложных преобразований, позволяет записать формулу для $t_{âåðò}$ в таком виде:

$$t_{âåðò} = \sqrt{\frac{R}{g}} \cdot (2 - \sqrt{2}). \qquad (4)$$

3. Уравнение относительного движения и его решение

Далее учтем, что наличие у ферромагнитного тела относительной скорости $V_{îòí}$ обуславливает уменьшение его радиальной координаты ρ

$$V_{îòí} = -\frac{d\rho}{dt}. \qquad (5)$$

В общем случае, конечно, скорость $V_{îòí}$ является сложной функцией координаты ρ, вид которой существенно определяется видом функциональной зависимости радиальной силы от координаты ρ.

Однако, если реальную радиальную силу $F_M - mg\cos\alpha$ (см. рис.2), уменьшающую координату тела ρ в относительном движении, заменить некоторой постоянной силой, равной F_A, то это приведет к завышению расчетного времени относительного движения и, как следствие, к завышению необходимой силы извлечения. После такой замены в соответствии с [5], можно записать

$$V_{îòí} = -\frac{F_A}{\gamma}, \qquad (6)$$

где γ – некоторый коэффициент, интерпретируемый в [5] как коэффициент сопротивления относительному движению ферромагнитного тела.

Подставляя (6) в (5), получаем

$$\frac{d\rho}{dt} = \frac{F_A}{\gamma}.$$

Решая это дифференциальное уравнение с учетом того, что за время $t_{отн}$ координата ρ изменяется от $R+h_M$ до R, найдем:

$$t_{îòí} = \frac{\gamma}{F_A} \cdot h_M . \qquad (7)$$

4. Оценка необходимой силы извлечения

Окончательно, учитывая очевидное условие извлечения, которое в веденных символах может быть записано как:

$$t_{îòí} \le t_{âåðò} , \qquad (8)$$

для необходимой силы извлечения, после подстановки в (8) выражения (4) и (7), несложно получить следующее соотношение:

$$F_A \ge \frac{\sqrt{g}}{2-\sqrt{2}} \cdot \gamma \cdot \frac{h_M}{\sqrt{R}} , \qquad (9)$$

которое и рекомендуется для использования в инженерной практике расчетов барабанных магнитных сепараторов, эксплуатируемых по рассмотренной схеме.

Относительно входящего в соотношение (9) коэффициента γ отметим, что его удельное (на единицу массы) значение $\gamma^* = \gamma / m$ может изменяться в пределах 50…250 $с^{-1}$ в зависимости формы ферромагнитного тела и материала сыпучей среды [5]. С учетом этого, для повышения эксплуатационной надежности проектируемых барабанных магнитных сепараторов с боковой подачей сепарируемого материала, можно рекомендовать принимать в качестве расчетного значения коэффициента γ максимальное его значение. Это, с учетом приведенного численного значения коэффициента γ, дает следующую завышенную оценку (в ньютонах) для необходимой силы извлечения некоторого ферромагнитного тела массой m из потока сепарируемого материала в рассматриваемом случае

$$F_A = 1500 \cdot m \cdot h_M / \sqrt{R} . \qquad (10)$$

При этом и (9) и (10) служат исходными соотношениями для перехода к соответствующей оценке параметров магнитного поля магнитной системы барабанного сепаратора (напряженность, градиент напряженности) по известным формулам для механической силы магнитного поля [1, 3, 5]. Разработка методики такого перехода может рассматриваться в качестве направления для дальнейших исследований.

Вывод

Получена верхняя оценка необходимой силы извлечения для магнитных сепараторов барабанного типа с боковой подачей сепарируемого сыпучего материала, позволяющая учесть основные эксплуатационные факторы, влияющие на рабочий процесс магнитного сепаратора: толщина струи ссыпки сепарируемого материала, радиус барабана сепаратора, масса извлекаемых ферромагнитных тел.

Литература

1. Деркач В.С. Специальные методы обогащения. –М.: Недра, 1966.–338 с;
2. Сумцов В.Ф. Электромагнитные железоотделители. –М.: Машиностроение 1978. –174 с;
3. Кармазин В.И., Кармазин В.В. Магнитные методы обогащения. –М.: Недра, 1984. –416 с;
4. Букреев В.В. Совершенствование систем с постоянными магнитами железоотделителей барабанного типа: Дис. канд. техн. наук. –Донецк, 2000. – 160 с;
5. Бранспиз Ю.А. Совершенствование методов расчета и конструкций электромагнитных шкивных железоотделителей: Дис. канд. техн. наук. –Ворошиловград, 1989. –261 с;
6. Россель Ж. Общая физика. – М.: Мир, 1964.–506 с.

УДК 539.12.04

Калюжный А.В.

ИССЛЕДОВАНИЕ СПЕКТРОВ ОТКЛИКА РАДИАЦИОННОГО МЕТОДА КОНТРОЛЯ СКРЫТЫХ ПУСТОТ

В данной статье исследуются спектры отклика различных материалов с целью определения оптимального энергетического окна.

1. Введение

При проведении спецслужбами оперативно-следственных мероприятий практически всегда возникают проблемы контроля скрытых полостей, а также определения количества и состава материала в этих полостях. Отсюда несомненная актуальность задачи создания приборного обеспечения для интроскопии помещений (контроля материала дистанционно без механического разрушения оболочки) при досмотрах и обысках, скрытых полостей в вагонах, каютах морских и речных судов, полостей в салонах автомобилей и автобусах.

Чаще всего при этом применяются интроскопы с рентгеноскопической системой зондирования и задача решается путем контроля неоднородности материала.

Однако в этом случае источник и детектор излучения должны находиться по разные стороны объекта исследования, что резко ограничивает область применения рентгеновских интроскопов.

В отличие от рентгеноскопического способа, радиометрический метод контролирует плотность путем измерения степени ослабления рассеянного потока гамма-излучения в веществе [1]. Объектом исследований, изложенных в данной статье, являются приборы реализующие данный метод радиационного контроля. Целью исследования является определение оптимального спектрального окна регистрации отраженного гамма-излучения.

Цель исследования – исследование спектров отклика радиационного метода контроля скрытых пустот.

Задачи исследования - определение оптимального энергетического окна для различных материалов.

2. Методика проведения экспериментов

Блок – схема экспериментальной установки приведена на рисунке 1.

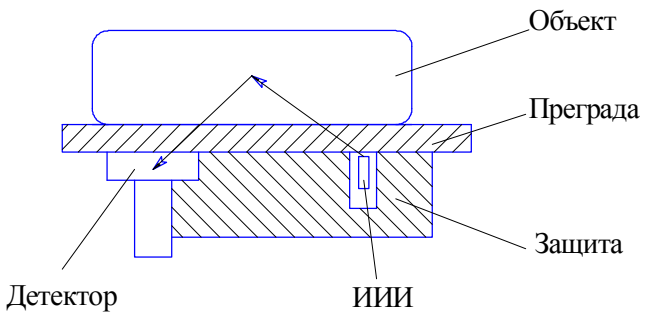


Рис. 1. Схема проведения эксперимента.

На некоторый участок обследуемого объекта направляется излучение источника ионизирующего излучения (ИИИ). В качестве источника использовался Ba^{133} активностью 1.0 MBq. Поток излучения, отраженный [2] в обратном направлении, попадает на детектор. В качестве детектора использовалась сборка на базе ФЭУ 9112В фирмы Electron

Tubes и сцинтиллятора (CsI(Tl) ∅40x5 мм. Спектры снимались на спектрометр «Фортуна».

Сигнал с детектора служит мерой усредненной плотности объекта на обследуемом участке [3].

Исследования проводились с целью выявления энергетических окон, в которых отклик от исследуемых композиций (преграда + искомый объект) наиболее информативный с точки зрения максимально эффективного определения наличия искомых объектов за различными преградами. Энергетические окна вычислялись путем исследования спектров отклика различных композиций материалов.

Так как схема проведения всех экспериментов предполагает нахождение изотопа в непосредственной близости к блоку детектирования, то природный фон в данной ситуации будет изменен, поэтому в начале был накоплен спектр, который фактически представляет собой сумму природного фона, части излучения Ba^{133}, которую не полностью поглотила защита, флюоресценции материала защиты и флюоресценции воздуха. Этот спектр будем считать изначально фоновым.

В ходе серии экспериментов использовалось четыре типа преград: сталь сечением 1.5 мм, сталь сечением 6 мм, дерево толщиной 15 мм и резина сечением 4 мм. Так как материал преграды также частично поглощает и отражает излучение изотопа, то перед тем, как помещать за преграду исследуемый образец, снимались спектры материалов преград, которые фактически переставляют сумму фонового спектра и спектра материала преграды. Затем за преграду помещался исследуемый образец и снимался спектр. Для получения спектра отклика от исследуемого образца, помещенного за преграду, из полученного спектра вычитался спектр преграды.

Дальнейшая математическая обработка заключалась в поиске такого энергетического окна в котором отношение общей счетности сигнала от исследуемого образца, за вычетом сигнала от преграды, к сигналу от преграды было бы максимальным. Это соотношение назовем контрастностью.

Под оптимальным энергетическим окном подразумевается окно, в котором получена максимальная контрастность для данной схемы,

Под усреднённым подразумевается окно, взятое для всех схем, исходя из перекрытия всех энергетических окон, для него тоже вычисляется контрастность.

Под полным энергетическим окном подразумевается окно, в котором излучает Ba^{133}.

Контрастность вычисляется по ниже приведенной формуле:

$$K = \frac{\sum_W S_W}{\sum_W F_W},$$

где К – контрастность, S_W – спектр отклика от исследуемого образца в выбранном окне регистрации, S_F – спектр фонового излучения в том же окне регистрации.

Мерой достоверности обнаружения была выбрана статистическая погрешность Пуассоновских процессов, оцениваемая при помощи параметра σ, который вычисляется следующим образом:

$$\sigma = \sqrt{\sum_i S_i},$$

где S_i – счетность выбранном окне регистрации.

Результаты проведенных исследований приведены в таблице 1.

Таблица 1.

Условия эксперимента		Оптимальное энергетическое окно KeV	Контрастность в оптимальном энергетическом окне		Контрастность в усредненном энергетическом окне (12-375 KeV)		Контрастность в энергетическом окне 0…400 KeV	
Материал преграды	Исследуемый образец		N раз	σ	N раз	σ	N раз	σ
	Парафин	12-215	19,2	93,25	17,9	92,35	17,3	90,8
	Сталь 1,5 мм	125-375	1,47	5,3	0,82	4,23	0,86	4,5
	Сталь 6 мм	19-327	3,8	19,6	3,77	19,4	3,76	19,75
	Древесина 15 мм	19-262	3,7	18,7	3,6	18,6	3,5	18,2
	Резина 4 мм	19-297	2,3	11,9	2,3	11,9	2,25	11,8
	Оргстекло 25 мм	19-297	7,8	39,7	7,7	39,6	7,4	39
	Книга 35 мм	19-268	10,3	52,1	10	51,5	9,6	50,7
	Оргстекло на расстоянии 50 мм	19-208	5,7	27,7	5,05	26	4,9	25,6
	Оргстекло на расстоянии 75 мм	19-208	3,5	17	3,1	15,9	3	15,6
	Оргстекло на расстоянии 125 мм	19-179	1,09	5,03	0,89	4,6	0,86	4,5
	Оргстекло на расстоянии 150 мм	31-167	0,59	2,6	0,48	2,5	0,47	2,4
	Оргстекло на расстоянии 200 мм	31-149	0,25	1,05	0,21	1,09	0,2	1,08
Сталь 1,5 мм	Оргстекло 25 мм	42-256	2,9	18,4	2,5	17,7	2,3	16,8
Сталь 1,5 мм	Свинец 20 мм	31-90	1,3	4,1	0,54	3,77	0,51	3,7
Сталь 1,5 мм	Свинец на расстоянии 75 мм	31-78	1,1	3,15	0,33	2,3	0,28	2,03
Сталь 1,5 мм	Оргстекло на расстоянии 75 мм	31-161	1,41	7,2	0,82	5,7	0,73	5,3
Сталь 1,5 мм	Оргстекло на расстоянии 150 мм	90-149	0,44	1,6	0,19	1,3	0,15	1,1
Сталь 1,5 мм	Оргстекло на расстоянии 200 мм	31-137	0,25	1,1	0,1	0,68	0,07	0,5
Сталь 6 мм	Оргстекло 25 мм	31-208	0,7	6,3	0,45	5,1	0,42	4,8

продолжение таблицы 1.

Сталь 6 мм	Свинец 20 мм	31-208	0,1	0,9	0,04	0,41	0,02	0,22
Сталь 6 мм	Книга 35 мм	31-208	0,82	7,6	0,54	6,1	0,5	5,7
Резина 4 мм	Парафин	19-238	5,2	46,3	4,7	44,3	4,5	43,5
Резина 4 мм	Свинец 20 мм	31-90	0,64	3,2	0,09	0,9	0,09	0,85
Резина 4 мм	Оргстекло 25 мм	31-268	3,24	29,3	3,14	29,5	3,03	29
Резина 4 мм	Оргстекло на расстоянии 75 мм	31-179	0,94	7,04	0,59	5,6	0,57	5,4
Дерево 15 мм	Свинец 20 мм	31-90	1,9	11,4	0,75	8,3	0,73	8,2
Дерево 15 мм	Оргстекло на расстоянии 75 мм	31-161	0,58	5,14	0,41	4,6	0,4	4,5
Дерево 15 мм	Оргстекло 25 мм	19-208	2,4	25,1	2,2	23,9	2,1	23,6

Согласно данным таблицы 1 оптимальное энергетическое окно “плавает” в зависимости от материалов и размеров преград, а также геометрии измерений. Ширина этого окна варьируется от 59 до 308 KeV. Усредненное окно регистрации мало чем отличается от полного окна (12-375 KeV для усредненного окна и 0-400 KeV для полного окна).

На рисунке 2 представлена сравнительная характеристика спектров отклика различных материалов.

Из рисунка 2 можно сделать выводы, что для органических веществ характерной особенностью спектра отклика максимум отраженной энергии лежит в области низких энергий, для сталей оптимальное энергетическое окно лежит в области более высоких энергий, а для металлов с большим атомным числом (Pb, Au, Pt) максимальное излучение лежит в рентгено-флюоресцентной области металлов.

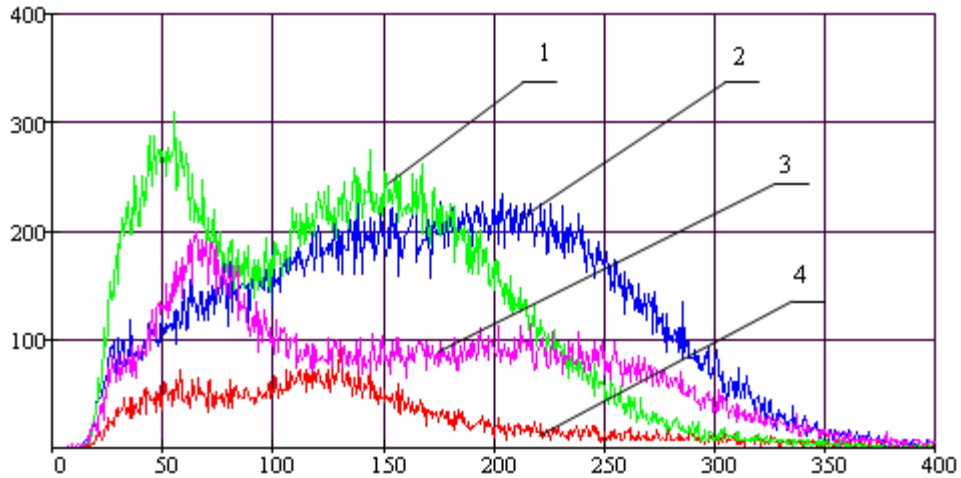


Рис. 2. Сравнительная характеристика спектров отклика различных материалов, где 1 – спектр отклика от образца из древесины толщиной 15 мм, 2 – спектр отклика от образца из стали сечением 6 мм, 3 – спектр отклика от образца из свинца толщиной 20 мм, 4 – спектр фонового излучения.

На рисунке 3 можно увидеть зависимость статистической погрешности Пуассоновских процессов от расстояния образца из оргстекла до детектора. При удалении исследуемого образца от детектора вероятность его обнаружения падает практически экспоненциально.

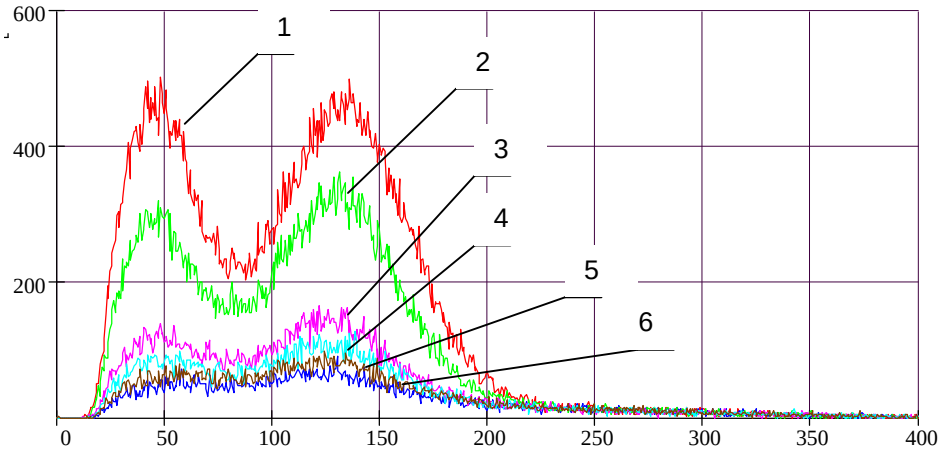


Рис. 3. Зависимость параметра σ от расстояния до детектора. 1 – спектр отклика образца из оргстекла на расстоянии 50 мм от детектора, 2 – спектр отклика образца из оргстекла на расстоянии 75 мм от детектора, 3 – спектр отклика образца из оргстекла на расстоянии 125 мм от детектора, 4 – спектр отклика образца из оргстекла на расстоянии 150 мм от детектора, 5 – спектр отклика образца из оргстекла на расстоянии 200 мм от детектора, 6 – спектр фонового излучения.

3. Выводы

На основе проведенных исследований были решены задачи по определению оптимального энергетического окна для различных образцов. Т.е. каждый образец излучает в своем диапазоне энергий и для того, чтобы его идентифицировать, необязательно, чтобы детектор работал во всем диапазоне энергий. Вполне достаточно оптимального энергетического окна, которое несет наибольшее количество информации. Идеальным случаем является “умный” прибор с плавающим энергетическим окном, который будет сам определять размер энергетического окна в зависимости от условий.

Проведенные исследования показывают, что возможны три варианта работы прибора с энергетическими окнами: первый – одно широкое, окно которое перекрывает весь энергетический диапазон при этом используется один дискриминатор нижнего уровня (ДНУ) и один дискриминатор верхнего уровня (ДВУ); второй вариант – предварительный сбор данных осуществляется при усредненном энергетическом окне, а уточнение ведется при помощи ряда переключаемых (более узких окон); третий вариант – изначально работа ведется в предварительно выбранном узком энергетическом окне (целенаправленный поиск) с возможностью переключения между рядом окон. Варианты два и три требуют наличия ряда переключаемых ДНУ и ДВУ (по количеству окон).

Литература

1. Вартанов В. А., Самойлов П. С. , Практические методы сцинтилляционной гамма-спектрометрии., М., “Атомиздат”, 1964 г;
2. Лейпунский А. И. , Новожилов Б. В., Сахаров В. Н., Распространение гамма-квантов в веществе., М., “Физматгиз”;
3. Арцыбашев В.А. , Гамма-метод измерения плотности., М., “Атомиздат”, 1965 г.

УДК 621.3.064

Ламанов С.Л., Михайлова Л.Ф., Яковенко В.В., Комісаренко О.І.

ВПЛИВ ФОРМИ КРИВОЇ СПАДАННЯ СТРУМУ НА ЕНЕРГОВИДІЛЕННЯ У КОМУТУЮЧОМУ ЕЛЕМЕНТІ

Досліджується вплив форми кривої спадання струму i(t) на енерговиділення на комутуючому елементі параметричної схеми заміщення нелінійного ланцюга з дугою відключення. Показано, що в реальному діапазоні зміни параметрів ланцюга, що відключається, для суттєвого зниження енерговиділення в дузі відключення, за інших рівних умов, достатньо, щоб коефіцієнт комутаційних перенапружень досягав значення Кп=2,3. Аналіз проводиться у відносних одиницях. Мал. 2, дж.2.

Проблема та її зв'язок з науковими й практичними задачами

Енергія, що виділяється в дузі відключення комутаційних апаратів, визначає ступінь термічної дії дуги на контактно-дугогасильну систему і апарат у цілому. Від кількості енергії, що виділяється в дузі, залежать гранична частота відключень, термін служби контактно-дугогасильної системи, розміри дугогасильного пристрою (ДП) та ін. Тому аналіз факторів, що впливають на енерговиділення, пошук шляхів зниження енергії дуги дозволяють виробляти рекомендації по конструюванню комутаційних апаратів із якнайкращими характеристиками.

Аналіз досліджень і публікацій

У [1], використовуючи розроблену методику [2], досліджено вплив форми кривої спаду струму i(t) на енерговиділення від джерела живлення (ДЖ). Проведений аналіз дозволив зробити висновки про те, що у розглянутому діапазоні зміни форми кривої i(t), величина енергії, що надходить від ДЖ - $W_{ДЖ}$ може змінюватися в десятки разів. Отже, змінюючи конструкцію і параметри ДП, від яких залежить форма кривої спаду струму i(t), можна суттєво впливати на кількість енергії, що надходить у ланцюг, що відключається, від ДЖ.

Постановка задачі

Якщо реалізувати в конструкції ДП комутаційних апаратів надані в [1] рекомендації, то можна знизити енерговиділення від ДЖ, що повинно вплинути і на виділення енергії на основному розсіючому елементі контуру – дузі відключення. Використовуючи ту ж методику, проаналізуємо вплив форми кривої i(t) на енерговиділення в дузі. Для цього замінимо нелінійний опір дуги відключення $r_д(i)$ параметричним опором комутуючого елементу (КЕ) $r_{КЕ}(t)$, напруга на якому визначається виразом у відносних одиницях [2]:

$$u^*_{КД}(t^*) = r^*_{КД}(t^*)\cdot i^*(t^*) = \left(1+\frac{n}{t^*}\right)\left(\frac{t^*}{t^*_к}\right)^n, \qquad (1)$$

де $i^*(t^*) = 1-\left(\frac{t^*}{t^*_к}\right)^n = 1-\left(\frac{K_n-1}{n}t^*\right)^n$ – струм в ланцюзі;

$t^*_к = \frac{n}{u^*_{КД}(t^*_К)-1} = \frac{n}{K_П-1}$ – відносний час комутації;

$K_П = u^*_{КД}(t^*_К)$ – рівень комутаційних перенапружень;

n – емпіричний коефіцієнт, що змінюється в межах $1 \le n \le 4$ залежно від типу дугогасильного пристрою.

Зробимо аналіз енергетичних характеристик процесу відключення (1).

Виклад матеріалу і його результати

Підставимо вирази для $u^*_{КД}(t^*)$ і $i^*(t^*)$ в інтеграл, що визначає енерговиділення на КЕ:

$$W^*_{\hat{E}\text{Å}} = \int_0^{t^*_K} u^*_{\hat{E}\text{Å}}\left(t^*\right)\cdot i^*(t^*)dt^* \qquad (2)$$

одержимо:

$$W^*_{\hat{E}\text{Å}} = \int_0^{t^*_{\hat{E}}} \left(1+\frac{n}{t^*}\right)\left(\frac{t^*}{t^*_{\hat{E}}}\right)^n\left[1-\left(\frac{t^*}{t^*_{\hat{E}}}\right)^n\right]dt^* \qquad (3)$$

або, після інтегрування:

$$W^*_{\hat{E}\text{Å}} = t^*_{\hat{E}}\,\frac{n}{(n+1)(2n+1)} + 0{,}5 = \frac{n^2}{(\hat{E}_{\text{Ï}}\ -1)(n+1)(2n+1)} + 0{,}5\,. \qquad (4)$$

На малюнку 1,а приведено графіки залежності $W^*_{\hat{E}\text{Å}} = f(K_{\text{Ï}})$ для різних n, побудовані по одержаній залежності. Для підтвердження правильності прийнятої методики теоретичних досліджень, на малюнку 1,б приведено графіки залежності енергії ДЖ від часу комутації $W^*_{\hat{E}\text{Å}} = f(t^*_{\hat{E}})$ для тих же значень n. Графіки малюнка 1,б малоінформативні, а аналіз графіків на малюнку 1,а дає цікаві результати.

Проведений в [1] аналіз показав, що енергія, що надходить у ланцюг від ДЖ, істотно залежить як від K_{Π}, так і від n у всьому прийнятому діапазоні їх зміни: $1 \le n \le 4$; $1{,}2 \le K_{\Pi} \le 5$ (для порівняння на мал.1а приведені криві $W^*_{\ddot{A}\text{Æ}} = f(\hat{E}_{\text{Ï}})$). Криві залежності, $W^*_{\hat{E}\text{Å}} = f(K_{\text{Ï}})$ приведені на малюнку 1,а, мають дві яскраво виражені області. Перша - визначається діапазоном зміни K_{Π}:

$$1{,}2 \le K\text{п} \le 2.$$

Тут, наприклад, зміна K_{Π} від 1,2 до 2, при n=2 , призводить до зменшення $W^*_{\hat{E}\text{Å}}$ приблизно в 2,4 раза (для порівняння - $W^*_{\ddot{A}\text{Æ}}$ зменшується при цьому в 4 рази). Зміна n від 4 до 1 призводить, наприклад, при K_{Π}=1,2, до зменшення $W^*_{\hat{E}\text{Å}}$ в 1,7 раза (для порівняння $W^*_{\hat{E}\text{Å}}$ - зменшується в 6, 4 раза).

Друга область визначається значеннями K_{Π}: $2 \le K_{\Pi} \le 5$.

Тут зміни K_{Π} від 2 до 5, при n=2, призводять до зменшення $W^*_{\hat{E}\text{Å}}$ приблизно в 1,35 раза ($W^*_{\ddot{A}\text{Æ}}$ зменшується при цьому в 4 рази). Зміна ж n від 4 до 1 при K_{Π}=3,5 зменшує $W^*_{\hat{E}\text{Å}}$ всього в 1,13 разу ($W^*_{\ddot{A}\text{Æ}}$ зменшується при цьому в 6,4 раза).

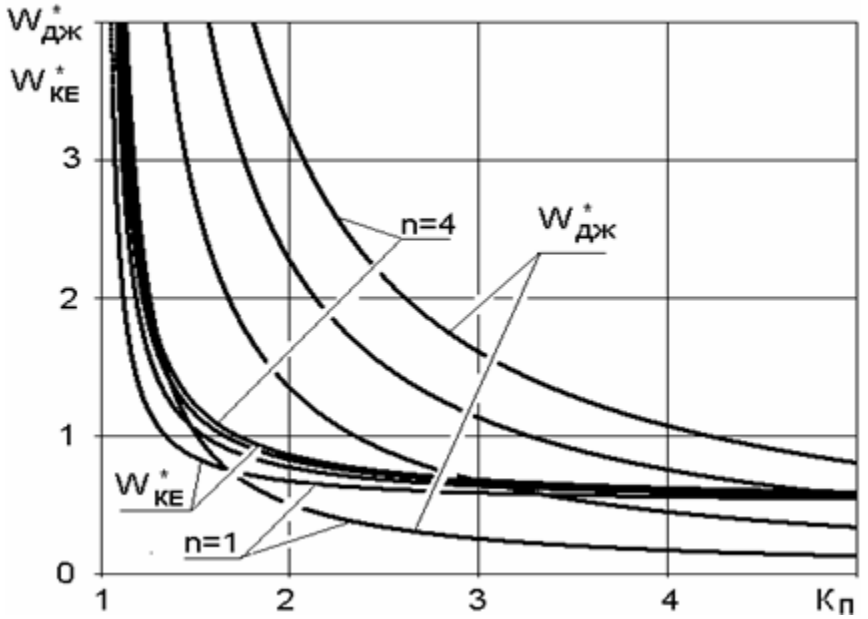
Для уточнення граничного значення Кп, при якому можна вважати вплив зміни коефіцієнта n несуттєвим, був розрахований відносний приріст у згаданому вище діапазоні зміни Кп та n. При значеннях Кп більше 2,3 зміна n від одного до чотирьох змінює $W^*_{\hat{E}\text{Å}}$ менш ніж на 10 відсотків. Таким чином, значення Кп=2,3 рекомендується як граничне для апаратів управління.

Спрощено можна вважати, що на практиці збільшення K_{Π} (при одних і тих же параметрах ДЖ і навантаження) можна досягти, збільшивши відповідно інтенсивність магнітного дуття. Також можна вважати, що зміни n на практиці можна добитися (при одному й тому ж K_{Π} й параметрах навантаження та ДЖ) відповідною зміною конструкції і параметрів ДП.

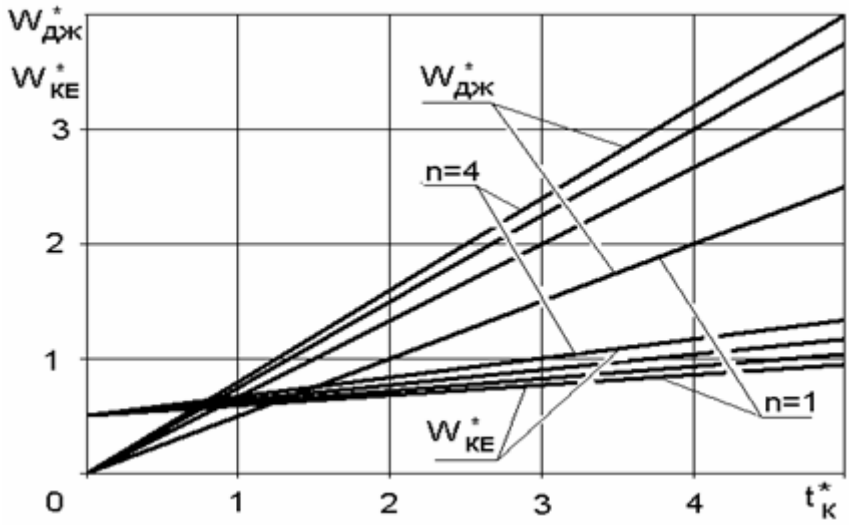
Висновки й напрям подальших досліджень

Проведений аналіз дозволяє зробити наступний висновок: при проектуванні апаратів, для яких важливим показником є енерговиділення на КЄ (наприклад, апарати управління), параметри й конструкції ДП слід вибирати й розраховувати так, щоб ДП забезпечував рівні комутаційних перенапружень близьки до Кп=2,3 і гладкі криві зміни $u_{Д}(t)$ (без

повторних запалювань дуги). Збільшення Кп понад указаний рівень збільшує ймовірність виникнення повторних запалювань дуги, ушкодження напівпровідникових елементів, може привести до неефективної витрати матеріалів системи магнітного дуття, збільшенню її габаритів і не приведе до помітного зниження енерговиділення. Зменшення ж $К_П$ може привести до значного збільшення енерговиділення в ДП.



а)



б)

Мал. 1.1 – Криві залежності $W^*_{ЕД} = f(K_П)$, $W^*_{ДЖ} = f(K_П)$,

(а), та $W^*_{ЕД} = f(t^*)$, $W^*_{ДЖ} = f(t^*)$, (б) при різних значеннях n .

Література

1. А.И. Комиссаренко, С.Л. Ламанов, Ю.С. Ткаченко О роли источника питания в энергетическом балансе отключаемой цепи постоянного тока. Вісн. Східноукр. нац. Ун-ту им В.Даля.-2003-№4(62); с. 110-114;

2. Комиссаренко А.И., Ламанов С.Л. Методика исследований процесса отключения цепей постоянного тока контактными коммутационными аппаратами. Вісн. Східноукр. нац. Ун-ту им В.Даля.-2002-№1(47); с. 18-24.

УДК 625.031:621.317.49

Смирный М.Ф., Малахов О.В., Седнева О.А., Малахова М.О.

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ИЗМЕНЕНИЯ ВЕКТОРА НАПРЯЖЕННОСТИ МАГНИТНОГО ПОЛЯ НА ПОВЕРХНОСТИ ФЕРРОМАГНИТНОГО ТЕЛА ПРИ УПРУГОМ СЖАТИИ

В статье представлены результаты экспериментальных исследований изменения характеристик магнитного поля при приложении к ферромагнитному телу сжимающей нагрузки.

Введение

Известно, что сложность явлений, протекающих при фрикционном взаимодействии колес локомотива и рельса, предопределяет многообразие методов их изучения. Так, определение зон концентрации напряжений в железнодорожном рельсе при силовом взаимодействии с колесом подвижного состава аналитическим путем рассматривалась авторами в [1,2,3,4,5], в работе [6] был предложен способ определения фактической площади контакта поверхностей тел с ферромагнитными свойствами. В работе [7] определена структура устройства, позволяющего использовать предложенный способ применительно к контактирующим поверхностям колеса и рельса. Однако оценка достоверности предложенного решения требует дальнейшего проведения экспериментальных исследований, начатых в [8].

Постановка задачи

С целью определения зависимости изменения топологии магнитного поля вблизи поверхности ферромагнитного тела в виде стальной пластины от его напряженно-деформированного состояния необходимо провести экспериментальное исследование по оценке напряженности магнитного поля при сжимающей нагрузке.

В связи с этим были поставлены следующие задачи:

- провести экспериментальное исследование изменения пространственной топологии напряженности магнитного поля в части ее горизонтальной составляющей стальной пластины, подвергающейся упругому сжатию;
- провести анализ полученных данных для оценки напряженно-деформированного состояния ферромагнитного тела и определить дальнейшие направления исследования в области силового взаимодействия колеса и рельса.

Основная часть

Для проведения эксперимента использована стальная пластина размером 400 х 200 х 3 мм, размеченная в центральной части в формате сетки 14 х 6 с шагом 10 мм, что обеспечило 84 точки, в которых проводились измерения.

В качестве информационно-измерительной системы применен микропроцессорный комплекс (рис. 1), состоящий из феррозондового датчика 1, расположенного горизонтально вдоль оси Y над поверхностью пластины 2, блока возбуждения феррозондового датчика 3, блока выборки-хранения аналогового сигнала 4, аналого-цифрового преобразователя 5, микропроцессора 6, блока согласования интерфейсов 7, через который измерительная информация передавалась в персональный компьютер 8.

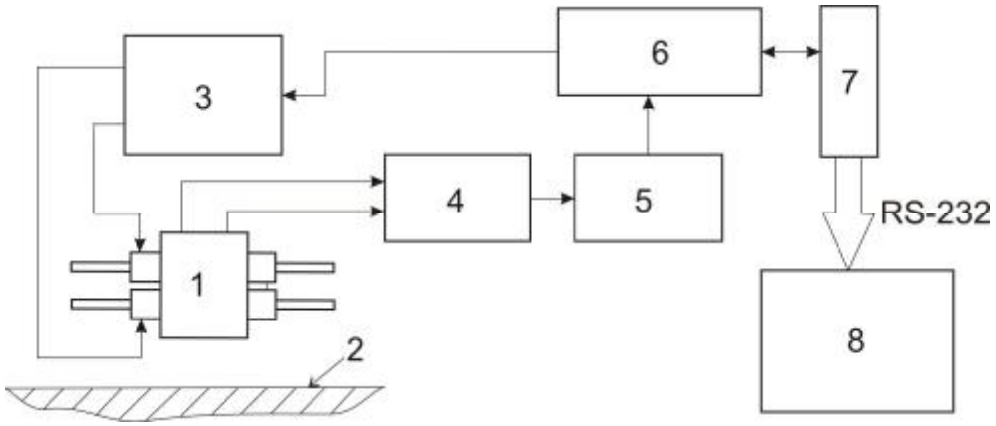


Рис. 1. Структурная схема информационно-измерительного комплекса.

После установки феррозондового датчика в первое положение на поверхности пластины 2 программа, работающая в персональном компьютере через COM порт и блок согласования интерфейсов RS232 подает запрос на микропроцессор 6. Микропроцессор запускает блок возбуждения 3, который формирует импульс в обмотке возбуждения феррозондового датчика 1. Сигнал с информационной обмотки феррозондового датчика 1 поступает на вход блока выборки-хранения аналогового сигнала 4, предназначенного для увеличения длительности сигнала во времени. С выхода блока выборки-хранения 4 сигнал подается на вход аналого-цифрового преобразователя. В комплексе использован 10 битный АЦП с быстродействием 200 тыс. операций в секунду. Оцифрованный сигнал с выхода АЦП считывается процессором и возвращается в персональный компьютер в виде пакета данных через блок согласования интерфейсов 7.

Далее датчик перемещается в следующую точку на поверхности пластины и цикл измерения повторяется. После получения информации со всех 84 точек программа формирует отчет в виде текстового файла с разделителями. Такой формат представления результатов эксперимента позволяет легко импортировать данные для их дальнейшей обработки.

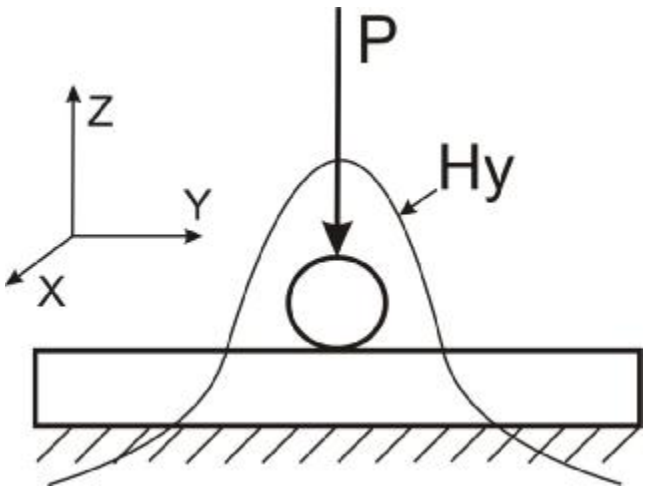


Рис. 2. Приложение нагрузки вдоль прямой на пластине.

Эксперимент был поставлен таким образом, что в каждой серии измерений определялась остаточная намагниченность пластины до и после нагружения пластины. Нагружение производилось путем прижатия к поверхности пластины стального цилиндра диамет-

ром 10 мм и длиной 200 мм с усилием 5 кН (рис. 2), горизонтальная составляющая вектора напряженности магнитного поля определялась для каждой из 84 точек. Изменение остаточной намагниченности нагруженной таким образом пластины получено в виде разницы между начальными и конечными их значениями (рис. 3).

Результаты измерения представлены в условных единицах, поэтому для тарировки датчика использовалось эталонное магнитное поле, создаваемое соленоидом с известной длиной провода l и количеством витков обмотки N с напряженностью магнитного поля в центре катушки:

$$H = N/l * I, \qquad (1)$$

где I – сила тока в цепи.

После сравнения расчетных данных и измеренных в условных единицах устанавливается коэффициент пересчета напряженности магнитного поля из условных единиц к размерности А/м.

На рис. 3 представлен характер изменения остаточной намагниченности в размерности А/м для одного из вариантов исследования, когда нагрузка в 5 кН была сосредоточена только в центре пластины (район 6-7-й точек). Видно, что в месте приложения нагрузки остаточная намагниченность увеличилась.

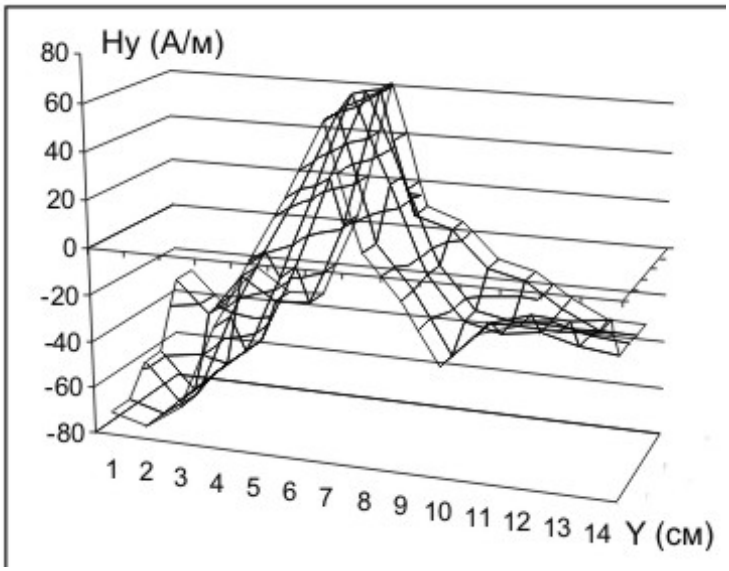


Рис. 3. Изменение остаточной намагниченности при приложении нагрузки в районе 6-7-й точек пластины.

Также было исследовано изменение остаточной намагниченности пластины при рассредоточенной равномерной нагрузке вдоль бруса в районе точек 5-8 с шириной контакта, равной 40 мм (рис. 4).

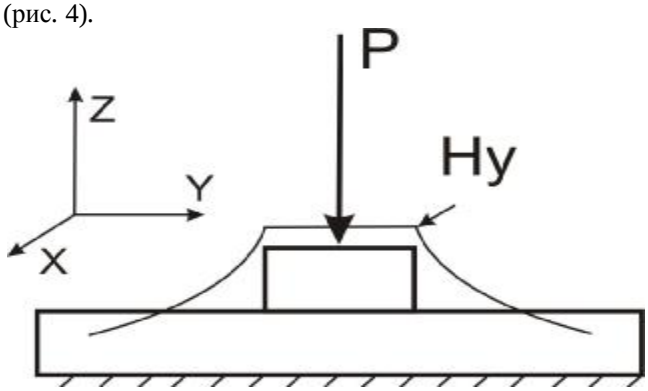


Рис. 4. Приложение нагрузки вдоль стального бруса.

Смена способа нагружения поверхности стального бруска с контактной линии (стальной цилиндр) на сосредоточенную поверхность (брус), находящейся в контакте с пластиной в диапазоне 5-8-й точек, приводит к тому, что остаточная намагниченность в местах контакта с брусом представлена менее однозначно из-за неравномерного распределения напряжений сжатия на поверхности бруса, однако граничная полоса контакта имеет достаточно четкие очертания (рис. 5).

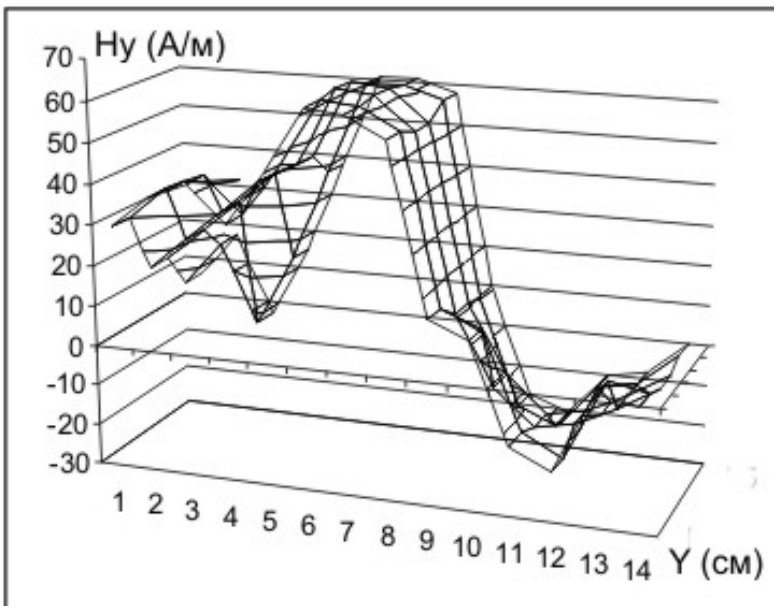


Рис. 5. Изменение намагниченности при равномерной нагрузке вдоль точек 5-8.

Выводы

В результате проведенного эксперимента можно сделать следующие выводы:

- Изменение горизонтальной составляющей вектора напряженности магнитного поля отражает произведенные в ферромагнитном теле упругие напряжения растяжения или сжатия, что позволяет использовать данный факт для оценки напряженно-деформированного состояния бездефектных металлоконструкций;
- Описанный метод измерения перераспределения остаточной намагниченности в ферромагнитных телах вследствие нагрузки позволяет проводить оценку напряженно-деформированного состояния головки рельса либо поверхности катания колеса, для чего необходимо проведение соответствующих экспериментов.

Литература

1. Вербек Г. Современное представление о сцеплении и его использовании // Железные дороги мира. – 1964. - № 24. – С. 23 – 53;
2. Голубенко А.Л. Сцепление колес с рельсами. – К.: ВИПОЛ, 1999. – 448 с;
3. Голубенко А.Л. Методика аналитического определения сил сцепления в контакте колес с рельсом // Конструирование и производство транспортных машин: Республ. межвед. научн.-техн. сб. – Харьков: Вища школа. – 1987. вып. 19. – С. 74 – 84;
4. Осенин Ю.И. Прогнозирование и управление характеристиками сцепления колес с рельсами. – К.: ВИПОЛ, 1999. – 100 с;
5. Смирный М.Ф., Солодовник М.Д., Малахов О.В. Аналитическая оценка зон концентрации напряжений железнодорожного рельса при боковом ударном воздействии на него колеса в реальных условиях движения транспортных средств. // Вісник Східноукр. нац. ун-ту ім. В. Даля. – Луганськ, СНУ, 2005.- №8(90). С. 89-93;
6. Малахов О.В., Смирний М.Ф., Осенін Ю.І. Спосіб визначення фактичної площі контакту поверхонь з феромагнітними властивостями // Заявка U 2005 08 208 від 22.08.2005;

7. Малахов О.В., Смирний М.Ф., Осенин Ю.І. // Пристрій для визначення механічних напружень у феромагнітних конструкціях // Деклараційний патент № 20041210108 від 15.07.2005. Бюл. №7. Київ. Деклараційний патент 2005;
8. Малахов О.В., Малахов В.Н., Седнева О.А., Малахова М.О. Экспериментальная оценка изменения пространственной топологии магнитного поля ферромагнитного тела в форме пластины, вызванного локальным ударным воздействием // Адаптивні системи автоматичного управління. Регіональний міжвузівський збірник наукових праць. Дніпропетровськ, 2005 – № 8 (28).

УДК 625.282:625.032.07

Петров А.С., Игнатьева О.В.

ПУТИ УМЕНЬШЕНИЯ ИЗНОСА КОЛЕСНЫХ ПАР ПОДВИЖНОГО СОСТАВА

В статье представлены результаты по определению износа бандажей колесных пар и пути совершенствования экипажной части моторного вагона электропоезда ЭПЛ9Т.

Многолетняя эксплуатация подвижного состава показала, что одними из слабых звеньев экипажей являются бандажи колес, ресурс которых определяется прокатом, и в большей мере – износом гребней. Это становится главным препятствием для увеличения среднемесячного пробега локомотивов. Так, при среднесетевом износе гребней 0,4 мм на 10 тыс.км пробега на отдельных участках пути износ гребней превышает его в несколько раз, что резко увеличивает время простоя локомотивов под обточкой бандажей, эксплуатационные затраты и расход металла. Следует отметить, что на части локомотивов наблюдаются аномальные износы гребней колес. Так, если на некоторых из них после пробега 4 – 10 тыс.км износа гребней нет вообще, то на других он недопустимо высок и достигает 8 мм/10 тыс.км пробега. Объяснить эти аномалии только наличием большого количества кривых участков – невозможно. Необходимо также учитывать влияние на износ гребней колес особенностей конструкции и режимов эксплуатации локомотивов.

Факторы, влияющие на износ бандажей, можно сгруппировать так:

1. Факторы, связанные с состоянием пути: большое количество кривых малого радиуса, разница в твердости материалов бандажей и рельсов, отклонение ширины колеи от номинальной и т.д.

2. Факторы, связанные с эксплуатацией подвижного состава: применение торможения поезда локомотивом, движение по кривым участкам со скоростями, существенно отличающимися от равновесных, увеличенные нагрузки от колес на рельсы, частые и длительные пробуксовки колес и т.д.

3. Факторы, связанные с конструкцией и техническим состоянием экипажей: несовершенство связей между кузовом локомотива, тележкой и колесными парами, неравномерное распределение нагрузки по колесам, неудовлетворительная работа устройств защиты от буксования колес, большая необрессоренная масса и кинематическое несовершенство приводов колес, большая разница диаметров колес в пределах одной колесной пары, перекосы и боковые смещения колесных пар и тележек относительно их номинального положения и т.д. Ряд факторов может усугубляться в процессе эксплуатации подвижного состава.

Для практики важно выяснить, какие из перечисленного многообразия факторов повышенного износа бандажей колес являются определяющими, а какие – второстепенными, а также выяснить степень их влияния на износ.

Поэтому в качестве метода для решения задачи по выявлению степени влияния вышеперечисленных факторов на ресурс бандажей целесообразно выбрать метод математического моделирования движения локомотива, позволяющий учитывать многие из перечисленных факторов и в процессе исследования выявлять влияние каждого из них в отдельности и в различных сочетаниях.

Опыт эксплуатации подвижного состава с повышенными скоростями показывает, что при этом увеличиваются силы, действующие на путь и элементы экипажей как в прямых, так и в кривых участках пути, от которых зависят безотказность работы локомотивов и вагонов и безопасность движения в целом.

Среди этих сил особое место занимают те, которые действуют в направлении, поперечном к продольной оси пути, и зависят от боковых колебаний системы «экипаж – рельсовый путь», поскольку они определяют работу сил трения в контактах гребней бандажей с боковыми гранями рельсов и, следовательно, ресурс бандажей по износу гребней.

В последние два десятилетия эта проблема превратилась в одну из самых актуальных, в первую очередь из-за многократного увеличения интенсивности износа гребней колес подвижного состава.

Были проведены эксплуатационные испытания электропоездов серии ЭПЛ2Т и ЭПЛ9Т в период от 2002 по 2004 гг. в локомотивных депо Ясиновато-западной донецкой железных дорог и депо Львов и Фастов для определения основных показателей надежности опытных образцов электропоездов и их функциональных систем (тягового электропривода, экипажной части, тормозной системы, систем вентиляции, кондиционирования, отопления и т.д.) в натурных условиях эксплуатации в пригородном сообщении, а также определения износа гребней колесных пар.

Согласно собранному статистическому материалу были отмечены преждевременные подрезы гребней бандажей, рис. 1 и рис. 2. На рис. 1 изображена динамика подреза гребня для первой колесной пары моторного вагона электропоезда ЭПЛ9Т. Переточка была произведена из-за остроконечного наката гребней при пробеге электропоезда равным 127.273 тыс. км. На рис. 2 изображена динамика подреза гребня для второй колесной пары моторного вагона электропоезда ЭПЛ9Т. Переточка была произведена из-за проката бандажей.

Согласно [1] основными факторами, влияющими на возникновение преждевременного износа, являются: 1 – кривизна пути; 2 – углы набегания гребней колес на рельсы; 3 – нагрузки в контактах колеса с рельсом; 4 – коэффициент трения (смазка контакта «гребень-рельс»); 5 – скорости скольжения в контактах колеса с рельсом; 6 – ширина рельсовой колеи.

Одним из путей уменьшения износа является подбор рациональных параметров ходовых частей подвижного состава с применением математической модели движения экипажа.

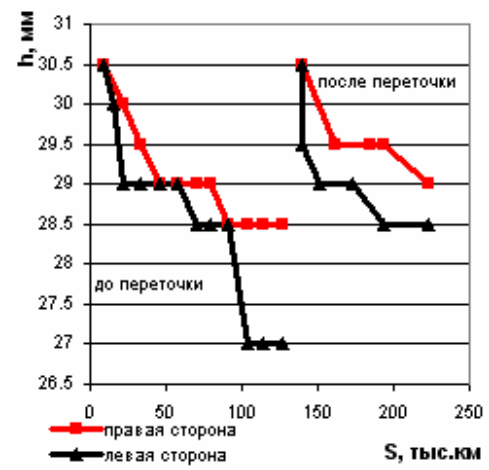


Рис. 1. Зависимость толщины гребня первой колесной пары от пробега S.

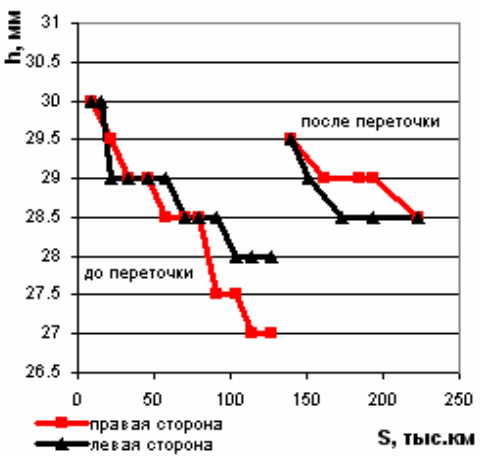


Рис. 2. Зависимость толщины гребня второй колесной пары от пробега S.

При разработке математической модели пространственных колебаний электропоезда ЭПЛ9Т были учтены следующие особенности:

- обязательный учет нелинейностей упругодиссипативных характеристик, зазоров, преднатягов, фрикционных пар с сухим трением при описании связей колесных пар с рамами тележек и тележек с кузовом;
- учет забегания точки контакта гребня колеса и рельса;
- имитация поверхностей профиля колеса и рельса с определением точек контакта по поверхности катания и гребню;
- динамическая система описывается с различным техническим состоянием ее элементов: перекосом колесных пар, разными диаметрами колес одной колесной пары, различными коэффициентами трения поверхностей катания и боковых поверхностей колес относительно рельсов;
- в кривых учитываются участки прямой, переходной кривой и круговой части кривой с неровностями в плане и профиле каждой рельсовой нити.

Для количественной оценки и ранжирования факторов, определяющих техническое состояние ходовой части локомотива, их влияния на показатели бокового износа гребней колес и динамических качеств локомотивов использовались подходы теории планирования эксперимента.

Применительно к электропоезду ЭПЛ9Т с двухосными тележками с двухступенчатым рессорным подвешиванием в качестве функции отклика для первой колесной пары (наиболее нагруженной при проходе кривых) принимались:

- направляющие и рамные силы;
- вертикальные и горизонтальные коэффициенты динамики;
- коэффициент запаса устойчивости от схода колес с рельсов;
- комплексный фактор износа гребня набегающего колеса.

Для расчета износа гребней бандажей колесных пар использовались формулы согласно [2]. Для кривых участков пути:

$$I_\Gamma = \chi_\Gamma \cdot N_{ijK} \cdot f_\Gamma \cdot V^2 \cdot \sqrt{h_\Gamma^2 + x_\Gamma^2 / \sin^2 \theta_\Gamma} \cdot \alpha \cdot d_{KP} L_y \cdot b_Э m_Э / \pi \sqrt{h_\Gamma^2 + x_\Gamma^2 / \sin^2 \theta_\Gamma} \cdot \sin \Theta_И . \quad (1)$$

Для прямых участков пути:

$$I_\Gamma = \chi_\Gamma \cdot N_{ijK} \cdot f_\Gamma \cdot V^2 \sqrt{h_\Gamma^2 + x_\Gamma^2 / \sin^2 \theta_\Gamma} \cdot 2\pi \cdot r_0 \cdot d_{ПР} \cdot L_y \cdot S_K / L_В^2 . \quad (2)$$

где χ_Γ, мм/кНм – коэффициент износа гребней, величину которого согласно опытным данным равна $2{,}7 \cdot 10^{-7}$ мм/кНм; N_{ijK} – направляющая сила, действующая на гребень колеса от рельса; f_Γ – коэффициент трения; h_Γ – расстояние от плоскости пути до точки контакта гребня с боковой гранью рельса; θ_Γ – угол между осью и образующей конуса гребня; r_0 – средний радиус круга катания колеса; $\Theta_И$ – средний угол наклона "путей трения" к плоскости пути; S_k – путь колеса в чистом качении за время *t*; V — скорость движения экипажа; L_y – участок пути; d_{KP} – «доли» кривых на участке пути; $d_{ПР}$ – «доли» прямых на участке пути; α – коэффициент, учитывающий «долю» гребней, контактирующих с рельсами, в общем количестве осей экипажа; $L_В$ – длина волны виляния.

С целью определения рациональных параметров ходовой части исследовано влияние на динамические показатели изменения конструкции, перечисленные в табл. 1, где даны пределы их изменения и рекомендованные значения.

Исследования выполнялись методами компьютерного моделирования пространственных колебаний экипажа во временной области по математической модели в режимах тяги с учетом случайных неровностей рельсов в плане и профиле, соответствующих удовлетворительному состоянию пути. Обработка расчетных осциллограмм динамических процессов выполнялась с усреднением трех абсолютных максимумов.

Динамические показатели, найденные при рекомендованных значениях параметров, заметно улучшились. Так, коэффициент вертикальной динамики второй ступени рессор-

ного подвешивания уменьшился для порожнего вагона на 13%, для груженого – на 12% , коэффициент вертикальной динамики первой ступени рессорного подвешивания уменьшился для порожнего вагона на 8%, для груженого – на 10%, рамная сила в прямых участках пути уменьшилась, для порожнего – на 3%, для груженого – на 5%, рамная сила в кривых участках пути R=600 м уменьшалась, для порожнего – на 17%, для груженого – на 6%.

Таблица 1.

Рекомендованные значения параметров ходовых частей электропоезда

№	Наименование параметра	Размерность	Численные значения	
			Диапазон значений	Рекомендуемые
1	Статический прогиб рессорного подвешивания : общий прогиб $\sum f$ перераспределение прогиба между ступенями χ	мм	150-175 0.346-0.426	170 0.356
2	Коэффициент демпфирования в гидравлическом гасителе колебаний в центральной ступени β_{II}	кНс/м	60-200	140
3	Угол наклона гидравлического гасителя колебаний в центральной ступени α	град	0-90	30
4	Коэффициент относительного трения фрикционного гасителя колебаний в буксовой ступени рессорного подвешивания $F_{фр}$	кН	0-6	2
5	Поперечная жесткость во второй ступени рессорного подвешивания k_y^{II}	кН/м	100-500	200
6	Параметр демпфирования автосцепного устройства β_a	кНс/м	1250-2000	2000

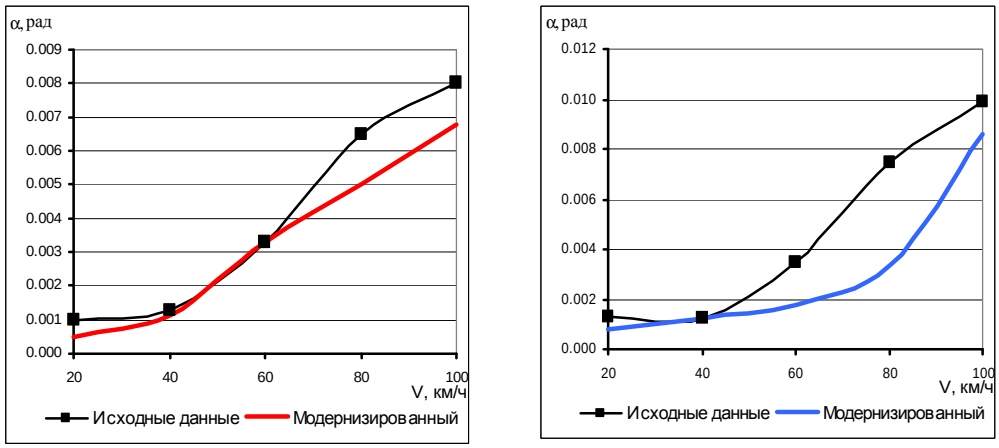
Для оценки предлагаемых решений были рассчитаны угол набегания колесной пары и значения износа гребней колесных пар в кривых и прямых участках пути для порожнего и груженого вагона электропоезда ЭПЛ9Т. Согласно проведенным исследованиям, за счет модернизации вагона удалось снизить угол набегания колесных пар для порожнего на 12% и для груженого – на 21% в прямых участках пути, и в кривых для порожнего – на 14% и для груженого – на 22%, рис. 3. Известно, что чем меньше угол набегания, тем лучше ходовые качества вагона. Износ бандажей колесных пар модернизируемого вагона электропоезда ЭПЛ9Т на участке пути в 100 тыс.км с протяженностью кривых менее 30% со скоростью до 100 км/ч для порожнего вагона составит $I_Г$ = 0,13 мм/10 тыс. км, а для груженого вагона – $I_Г$ = 0,2 мм/10 тыс. км. Прогнозируемый износ на текущий пробег электропоезда ЭПЛ9Т, равный 175 тыс. км, составит $\approx$ 3,5 мм для порожнего вагона, и $\approx$ 4,6 мм – для груженого. Со скоростями движения до 160 км/ч на текущий пробег электропоезда ЭПЛ9Т, равный 175 тыс. км, износ составит $\approx$ 4,6 мм для порожнего вагона, и $\approx$ 6 мм – для груженого. Таким образом, согласно исследованиям, у исходной конструкции моторного вагона электропоезда ЭПЛ9Т имеет место повышенный износ гребней бандажей колесных пар, что влечет за собой преждевременный выход из строя бандажа и уменьшает производительность электропоездов из-за неплановых простоев для преждевременной обточки колес.

Моторный вагон ЭПЛ9Т с исходной конструкцией экипажной части имеет пробег до обточки, согласно расчетам, около 130 тыс. км (рис. 4), то есть бандажи должны обтачиваться раньше, чем запланировано согласно текущему ремонту. Проведенные исследо-

вания позволили разработать рекомендации по предупреждению повышенного износа гребней колес, заключающиеся в выборе рациональных параметров упруго-диссипативных связей экипажной части.

Авторами были выведены зависимости уменьшения толщины гребня от пробега для различных скоростей движения вагона электропоезда, см. рис. 4.

Экономия годовых затрат от снижения расходов на ремонт вагона электропоезда с модернизированной экипажной частью и уменьшения простоев при обточке колес и продления срока службы бандажей составляет 16 тыс. грн. в год. Общий экономический эффект для ЭПЛ9Т – 78 тыс. грн. (на 1.02.2006 г).



а б

Рис. 3. Угол набегания колесной пары для:
а – порожнего и б – груженого моторного вагона в кривых R=600 м.

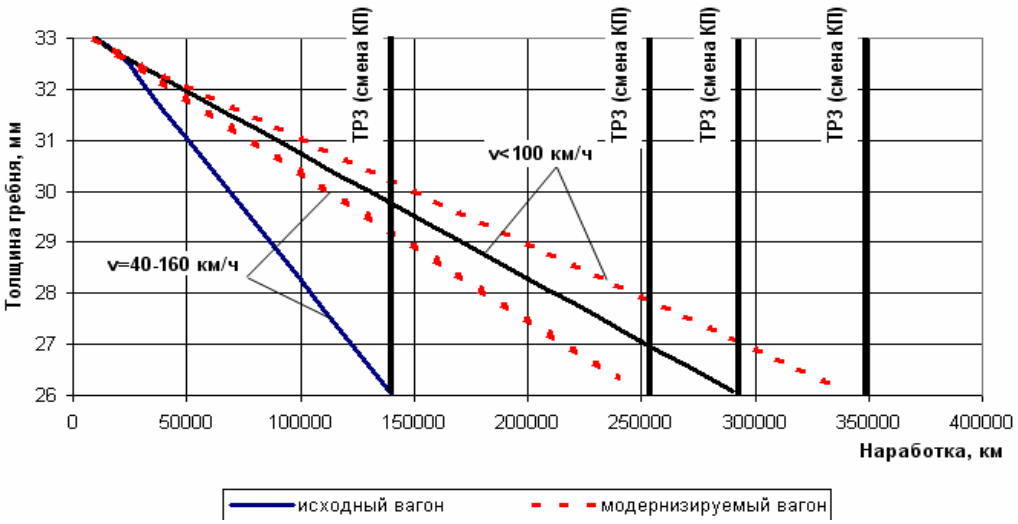


Рис. 4. Прогнозируемый износ бандажей колесных пар в зависимости от пробега для исходной и модернизированной конструкции моторного вагона электропоезда.

Таким образом, путем модернизации удалось улучшить основные динамические характеристики электропоезда и снизить износ гребней бандажей колесных пар, тем самым повысив технико-экономическую эффективность применения электропоезда ЭПЛ9Т и безопасность движения, а также снизить материальные и трудовые затраты на поддержание и восстановление подвижного состава.

Литература

1. Маслиев В.Г. Научные основы выбора конструкторско - технологических параметров устройств для уменьшения износа бандажей колес локомотивов: диссертация док. техн. наук. – Харьков, 2001 г.- 461 с;
2. Петров А.С., Романенко О.В., Игнатьев О.Л. Способ оценки износа колесных пар подвижного состава // Вісник Східноукраїнського нац. ун-ту ім. В. Даля. - Луганськ, СНУ ім. В.Даля, 2005.- № 8(90), ч.2. – С. 153-158.

УДК 629.423

Ладик Ю.Э., Ладик Д.А., Спирягин М.И., Спирягин В.И.

МИКРОПРОЦЕССОРНАЯ СИСТЕМА УПРАВЛЕНИЯ ТОРМОЗАМИ РЕЛЬСОВОГО ТРАНСПОРТНОГО СРЕДСТВА

Предложен вариант системы управления тормозами рельсового транспортного средства, что позволяет обеспечивать повышение эффективности использования тормозов за счет применения GPS и GPRS технологий.

Повышение эффективности торможения железнодорожного подвижного состава представляет собой сложную задачу, в основе которой лежит комплекс конструкторских и технологических мероприятий, значительная часть которых требует крупных капиталовложений. Кроме этого, реализация тормозных усилий также связана с вопросами ресурсосбережения и безопасности движения.

Анализ отечественного и зарубежного опыта подтвердил реальную возможность решения такой задачи за счет использования микропроцессорных систем управления для управления процессами торможения.

Однако наиболее важным элементом работы микропроцессорных систем являются аспекты их регулирования, для которых не в полной мере обоснованы и решены научно-практические задачи обеспечения устойчивой работы рельсового транспортного средства в режиме торможения [1-3].

С точки зрения тормозных систем, мы можем видеть, что наибольшее применение в Украине нашли электрические и пневматические тормозные системы на железнодорожном транспорте. Особый интерес представляет использование электромагнитных тормозов на городском рельсовом транспорте, но в данной работе этот вид тормозов авторами не рассматривался.

В связи с этим, авторами предлагается один из вариантов управления тормозной системы рельсового транспортного средства. Блок-схема системы управления показана на рис. 1.

Отличие от ранее применяемых систем - возможность совместного использования электрического и пневматического тормоза, а также использования GPS и GPRS-технологий.

GPS-приемник используется для определения местоположения рельсового транспортного средства в определенный момент времени. GPRS-модем осуществляет связь микропроцессорной системы с центром управления движением.

Принцип работы любой микропроцессорной системы заключается не только в выполнении функций по управлению работой своей системы, но также в обеспечении корректной и устойчивой работы всего микропроцессорного комплекса транспортного средства в целом. В ВНУ им. Даля этот вопрос уже изучался научными сотрудниками [4,5].

Предложенный вариант должен корректно работать с системой регулирования проскальзываний. Структурная схема системы регулирования показана на рис. 2. На данном рисунке $V_{ë}$ - линейная скорость рельсового транспортного средства, $V_{ë.ç}$ - задаваемая линейная скорость, $\omega_{ê}$ - угловая скорость колеса, $\omega_{З}$ - задаваемая угловая скорость колеса.

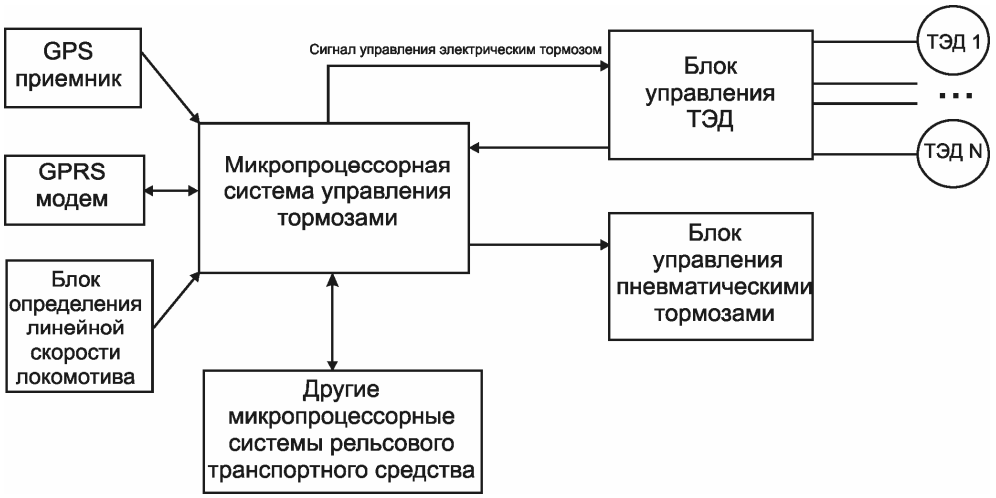


Рис. 1. Микропроцессорная система управления.

Регулирование режима работы тормозящих тяговых электродвигателей осуществляется с помощью блока управления ТЭД в двух режимах:

- поддержания заданных тормозных усилий по позициям контроллера;
- поддержание характеристик тяговых электродвигателей по позициям контроллера.

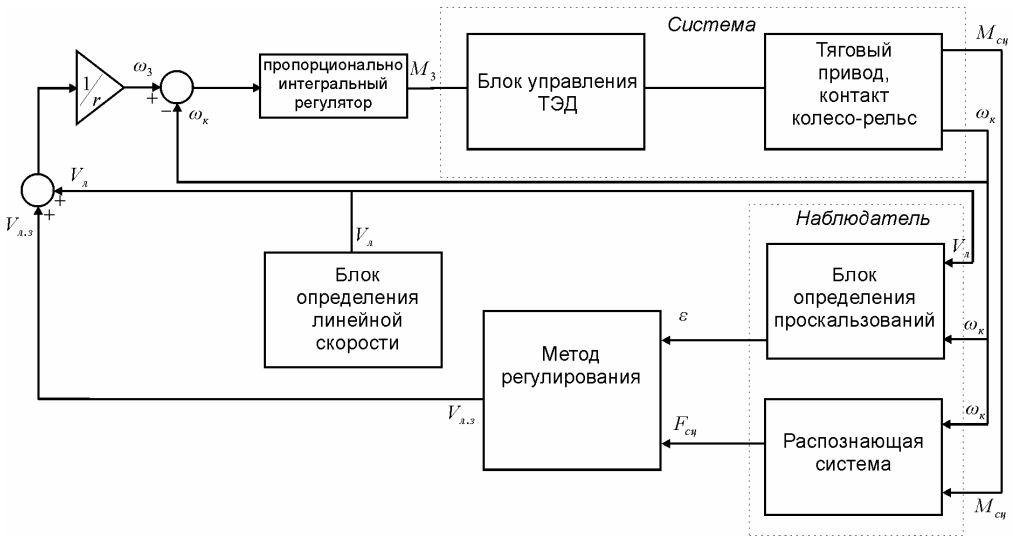


Рис. 2. Структурная схема регулирования.

Первый режим используется при ручном управлении электрическим тормозом, а второй при поддержании заданной скорости.

При наличии ограничений по характеристикам тяговых двигателей в работу режима торможения включается пневматический тормоз, который при отсутствии юза подтормаживает те колесные пары, которые не обеспечивают заданный режим торможения рельсового транспортного средства.

При наличии юза на одной или нескольких осях выше допустимого значения тормозная нагрузка на этой (этих) осях снижается за счет уменьшения электрического момента торможения, а для обеспечения режима торможения тормозное усилие увеличивают

на осях, не подверженных юзу, посредством увеличения тормозного электрического момента тормозящих двигателей, или, при наличии ограничений на электродвигателях, путём дополнительного включения пневматического тормоза.

При режиме торможения пневматическим тормозом, можно обеспечить практически те же режимы торможения, что и при применении электрического тормоза. Эта осуществляется с помощью блока управления пневматическими тормозами, путем регулирования давления в цилиндрах, применяя микропроцессорную систему для управления пневматическими позиционерами, что влечет за собой регулирование усилия нажатия тормозных колодок на колесо.

GPS-технология используется для определения проблемных участков движения, что позволяет сообщить системе управления о текущем месте нахождения, и в случае необходимости начать тормозить поезд заранее с низким замедлением (например, участки с ограничением скорости). Благодаря этому появляется возможность использовать преимущественно динамический тормоз и избежать износа пневматических тормозов. Заблаговременное отключение тяги дает некоторую экономию энергии.

В случае, если рельсовое транспортное средство приближается к запрещающему движение сигналу семафора, то для осуществления корректной работы системы предлагается использовать GPRS-технологии. Микропроцессорная система своевременно получает необходимую информацию посредством GPRS модема и также осуществляет торможение поезда заранее. Применение данной технологии также позволит использовать преимущественно динамический тормоз и избежать износа пневматических тормозов.

Для проверки работоспособности предложенной системы было проведено математическое моделирование ее работы, были введены блоки, эмулирующие внешнюю среду и датчики системы. В результате удалось получить удовлетворительный процесс регулирования.

За счет применения данной системы, общая микропроцессорная система строится на базе распределенной архитектуры. В результате мы имеем более сложную схему построения микропроцессорной системы управления рельсовым транспортным средством. Стоимость разработки такой архитектуры больше, если сравнивать с классической архитектурой. Это обусловлено расходами, связанными с необходимостью разработки более сложного программного обеспечения. С другой стороны, данный вариант обладает повышенной отказоустойчивостью.

Применение данного варианта микропроцессорной системы позволит обеспечить устойчивую работу локомотива в режиме наиболее эффективного торможения. Снижение расхода топлива можно отнести на счет оптимизации режима ведения поезда благодаря ускоренному и плавному торможению и отпуску и (в меньшей степени) на счет сокращения продолжительности работы компрессоров благодаря уменьшению общего расхода сжатого воздуха. Внедрение системы позволит избежать повышенного износа тормозных колодок и увеличить срок их службы.

Выводы

В данной статье представлены теоретические основы для построения микропроцессорной системы управления тормозами рельсового транспортного средства.

Результаты любых теоретических исследований и разработок, их конструктивность касательно практического применения всегда определяются их «выходными данными», в нашем случае – комплексом моделей объекта управления.

Поэтому предложенная конструкция системы нуждается в дальнейшем исследовании на стабильность, конвергенцию и устойчивость работы, так как относится к системам, отвечающим за безопасность движения. Это побуждает нас к дальнейшим исследованиям и более детальному ознакомлению с применением систем реального времени в данной области.

Литература

1. Система автоведения поездов на железных дорогах Чехии и ее взаимодействие с ETCS. // Железные дороги мира. – 2000. – №2;
2. Пневматические тормоза с электронным управлением. // Железные дороги мира. – 2002. – №7;
3. Izumi Hasegawa, Seigo Uchida Braking Systems. // Japan Railway & Transport Review. - June 1999. - No. 20 - pp.52–5;
4. Горбунов Н.И., Кашура А.Л., Спирягин В.И., Спирягин М.И. Улучшение тягово-тормозных свойств локомотивов за счет применения микропроцессорных систем// Сборник научных трудов «Перспективные задачи инженерной науки». – Днепропетровск: GAUDEAMUS. - 2002. – Вып. 4.- С.168-172;
5. Спирягин М.И. Повышение эффективности тяги и торможения за счет совершенствования алгоритма управления тяговой передачей рельсового транспортного средства. // Вісн. Східноукр. нац. ун-ту ім. В. Даля. - Луганськ: СНУ. - 2003. - Вип. 12(70). - С. 144-149.

УДК 620.179.14.05

Водолазский В.Н., Шведчикова И.А.

ПРИНЦИПЫ ПОСТРОЕНИЯ МЕТАЛЛОДЕТЕКТОРОВ (ОБЗОР)

Рассмотрены принципы построения некоторых типов металлодетекторов. Определены основные направления конструктивных усовершенствований приборов. Рис. 6, библ. 11.

Введение

В последние годы на предприятиях различных отраслей промышленности достаточно остро стоит проблема повышения качества выпускаемой продукции. Одним из условий, обеспечивающих решение указанной проблемы, является предупреждение попадания в готовые изделия металлических примесей, содержащихся в сырье в виде металлической пыли, окалины, мелких кусков оборудования. Для этих целей на практике широко применяются металлодетекторы, которые кроме своей основной функции, связанной с обнаружением металлических включений, нередко выполняют также функции управления различными исполнительными устройствами. В качестве таких устройств чаще всего используются либо магнитные сепараторы [1], обеспечивающие извлечение нежелательных металлических примесей, либо приводные электродвигатели ленточных транспортеров [2], изменяющие скорость или направление транспортировки материала.

Постановка задачи

К настоящему времени известен целый ряд методов обнаружения металлических включений, на основе которых разработаны разнообразные конструкции металлодетекторов. Подробный анализ методов обнаружения металлических включений в потоке технологического сырья и существующих конструкций промышленных металлодетекторов приведен, например, в работах [3, 4]. Однако до сих пор отсутствуют эффективные конструкции промышленных металлодетекторов, способные выявлять разные виды металлических включений (как магнитные, так и немагнитные), а также адаптироваться под любые размеры зоны контроля [3]. В этих условиях очевидна актуальность задачи по определению четких критериев, лежащих в основе выбора конструкций металлодетекторов применительно к конкретным условиям эксплуатации. Для ее решения необходима по возможности наиболее полная информация об уровнях чувствительности, областях применения и принципах построения металлодетекторов. С учетом вышеизложенного целью настоящей работы является сравнительный анализ принципов построения существующих конструкций металлодетекторов, необходимый для реализации поставленной задачи.

В современных условиях на предприятиях различных отраслей промышленности преимущественное распространение получили вихретоковый и магнитный (индукционный) методы обнаружения нежелательных металлических включений в потоке технологи-

ческого сырья, а в конструкциях металлодетекторов широко используются датчики проходного и накладного типов.

В работе [5] описан вихретоковый металлодетектор с датчиком проходного типа, предназначенный для обнаружения посторонних включений (металлических и неметаллических) в жидких и пластично вязких реальных средах, что является достаточно трудной задачей. Принцип построения указанного устройства поясняется с помощью рис. 1.

Контролируемая среда пропускается через приемные катушки 2, 3 и парные электроды 4, 5 или через одну приемную катушку и парные электроды 4 и 5. При отсутствии посторонних включений в среде токи через дополнительные катушки 6 и 7 равны, и на выходе преобразователя сигнал отсутствует. При попадании в контролируемую среду металлической частицы в ней наводятся от первичного поля излучающей катушки 1 вихревые токи, создающие вторичное поле, воспринимаемое приемными катушками 2 и 3, в результате чего на выходе преобразователя появляется полезный сигнал. При попадании в контролируемую среду неметаллической посторонней частицы (например, стекло, камень, дерево и т.д.) сопротивление между электродами, в зону действия которых попадают частицы, изменяется, соответственно изменяется ток в дополнительной катушке 6 или 7, что обуславливает появление полезного сигнала на выходе преобразователя.

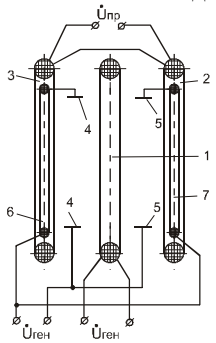


Рис. 1. Принцип построения датчика для контроля
жидких и пластично вязких реальных сред.

Металлодетекторы с датчиками проходного типа предназначены, как правило, для установки на конвейерных линиях. В этом случае металлические скобы (заклепки), которыми скрепляется конвейерная лента, являются причиной ложных срабатываний металлодетектора. Существует несколько способов решения этой проблемы, некоторые из них приведены в работе [6].

Так, при движении ненагруженной части транспортерной ленты со скобами через дополнительный датчик (рис. 2) возникает сигнал, который через время tз заблокирует сигнал с измерительного датчика. Время tз определяется из соотношения

$$t_З = l/V_{TP}, \qquad (1)$$

где l – расстояние между дополнительным датчиком и измерительным датчиком; VTP - скорость движения ленты.

С целью отстройки от ложных срабатываний, а также для повышения помехозащищенности и чувствительности металлодетектора применяют секционирование излучающей и приемной катушек проходного датчика (рис. 3).

Расположение секций катушек датчика в соответствии с рис.3 повышает чувствительность металлодетектора, т.к. устраняются зоны нечувствительности к протяженным металлическим предметам, и снижается влияние ориентации этих предметов на выходной сигнал металлодетектора. Дополнительная отстройка от помех осуществляется путем реализации алгоритма, когда считается, что через датчик прошло металлическое включение только в том случае, если через определенные промежутки времени сработало не менее двух секций датчика.

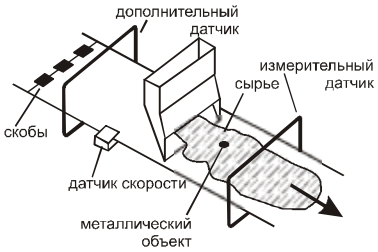


Рис. 2. К объяснению принципа отстройки от ложных сигналов.

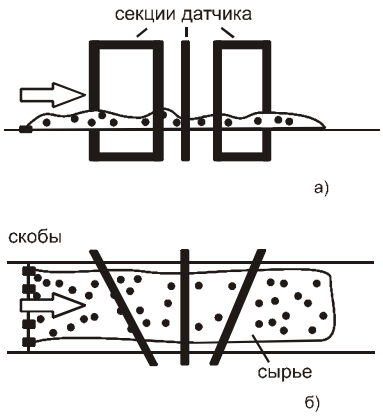


Рис. 3. Расположение секций датчика: а) вид сбоку; б) вид сверху.

Принцип определения момента прохождения скоб в вышеописанной конструкции металлодетектора основан на регистрации сигнала от металлических объектов, лежащих на одной линии, перпендикулярной направлению движения транспортерной ленты. В этом случае, если разница во времени получения сигналов со стороны секций 1 и 3 будет равна t=AC/V, где V - скорость движения ленты (рис. 4), то очевидно, что через секции датчика прошли металлические скобы.

Как уже указывалось выше, при нестабильности взаимного расположения датчика и металлических предметов технологического оборудования, например, при соединении ленты транспортера металлическими заклепками, необходима глубокая компенсация сигналов, которой можно добиться путем возбуждения, например, индукционного датчика генераторами одновременно на нескольких частотах [7].

Соотношения между одновременно излучаемыми частотами и их общим количеством определяются, исходя из требований к подавлению объектов, отличающихся от подлежащих обнаружению величиной индукционного параметра τ_0:

$$\tau_0 = \gamma\mu L^2, \qquad (2)$$

где γ- электропроводимость объекта; μ- магнитная проницаемость объекта; L- характерный размер объекта.

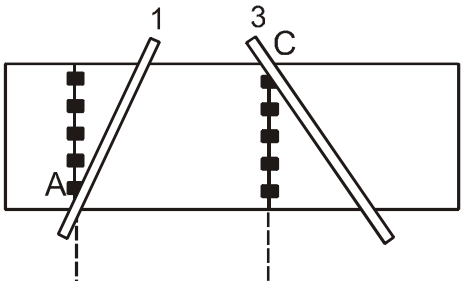


Рис. 4. К определению момента прохождения скоб через секции датчика.

При выборе рабочих частот следует руководствоваться соотношениями [7]:

$$\begin{cases} \omega_1 \cdot \omega_4 = \omega_2 \cdot \omega_3 = \dfrac{1}{\tau_0} \\ \omega_4 / \omega_3 = \omega_2 / \omega_1 = 2 \\ \log_2 \omega_3 / \omega_2 = m+1 \end{cases}, \qquad (3)$$

где m- целое число.

С целью повышения помехоустойчивости металлодетектора и получения равной и высокой чувствительности к металлическим предметам, находящимся в любой точке транспортируемого материала независимо от высоты и ширины его слоя, применяются накладные датчики. На рис. 5 представлен дифференциально-резонансный датчик металлодетектора с расположенными в одной плоскости под лентой конвейера приемными рамками 2, обмотки которых включены навстречу друг другу, и одной генераторной рамкой 1, установленной над лентой конвейера напротив приемных рамок. [8]. Однако такая установка катушек значительно усложняется монтаж датчика.

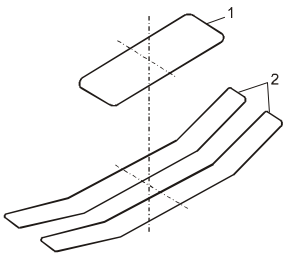


Рис. 5. Накладной датчик с двумя приёмными рамками.

К современным металлодетекторам зачастую предъявляется и такое требование, как определение координат металлического включения, что может быть обеспечено как с помощью проходных, так и с помощью накладных датчиков. Один из возможных вариантов конструкции металлодетектора с накладным датчиком представлен на рис. 6.

Масса сырья, которая подвергается контролю на содержание металлических включений, перемещается транспортной лентой. Направление перемещения сырья перпендикулярно плоскости (рис. 6). Наличие в зоне контроля посторонних металлических включений вызывает появление полезных сигналов (E1 и E2) на выходе приемных пар обмоток 2-3 и 4-5. Величины E1 и E2 зависят от местоположения частицы в контролируемой зоне. Отношение E2/E1 является функцией координаты x. Данное устройство позволяет получить нужное пространственное распределение чувствительности к внесению металличес-

кого объекта в разные точки зоны контроля за счет взаиморасположения как самих обмоток, так и их расположения относительно зоны контроля [9].

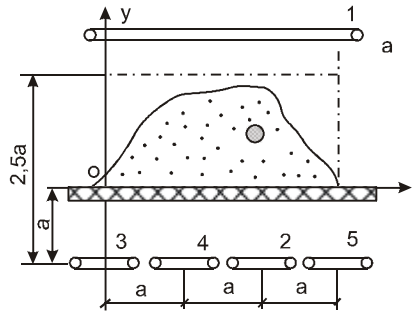


Рис. 6. Накладной датчик с двумя приёмными рамками.

Достаточно простой способ определения координат ферромагнитных включений был предложен в работе [10]. Над лентой транспортера, по которой перемещается контролируемый материала, располагается электромагнит, а под лентой - пластинки из ферромагнитного материала, которые крепятся к оси. Пластинки размещены в различных местах поперечного сечения транспортера, и их верхние кромки расположены по его контуру. Ферромагнитные предметы, проходя между электромагнитом и пластинами, экранируют последние, которые отклоняются от вертикальной плоскости и замыкают неподвижные контакты, сигнализируя о координате ферромагнитного предмета.

С целью повышения чувствительности и достоверности селективного обнаружения как ферромагнитных, так и немагнитных металлов в потоке, предлагается выполнять вихретоковый датчик в виде последовательно включенных секций на ферритовых сердечниках, расположенных ступенчато в плоскости контролируемой зоны с шагом перекрытия по ширине контролируемой зоны, равным половине длины ферритового сердечника [11]. При этом на центральном стержне Ш-образного ферритового сердечника намотана передающая, а на крайних стержнях – две приемные катушки, включенные последовательно-встречно.

Выводы

1. Как показал анализ информационных источников, для обнаружения посторонних металлических включений в потоке технологического сырья, перемещаемого транспортерными лентами, наибольшее распространение получили магнитный (индукционный, феррозондовый) и вихретоковый методы.

2. В современных конструкциях металлодетекторов находят применение датчики как накладного, так и проходного типов, выбор которых определяется условиями обеспечения требуемой чувствительности металлодетектора.

3. Основные направления конструктивных усовершенствований металлодетекторов связаны с повышением их чувствительности и помехозащищенности, а также с расширением функциональных возможностей путем одновременного обнаружения разных типов включений (металлических и неметаллических) и определения их положения на ленте транспортера.

Литература

1. Водолазский В.Н. Автоматизированный комплекс для обнаружения и извлечения ферромагнитных включений из потока угля. // Тези ІІІ Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених "Крок у майбутнє" (Київ, 25-27 червня 2003 р.). – Київ: НУТУ „КПІ". – 2003;

2. Способ удаления металла из непрерывного потока сыпучего груза; А.с. № 193387 1В, 5/01/ Матов А.Л., Мигуцкий Л.Р., Малюта Д.И. и др. - №1044247/27-11; Заявл. 17.12.65; Опубл. 13.03.67, Бюл. №7;

3. Швец С.Н. Анализ конструкций и разработка принципа построения модульных металлодетекторов. // Вісник СНУ імені Володимира Даля. – 2004. - № 6(76). – С. 15-20;
4. Порозов В.А. Металлообнаружители в пищевой промышленности. – М.: Пищ. пром., 1975. – 84 с;
5. Универсальный преобразователь; А.с. № 894652, G 01 V3/10/Дадунашвили А.С., Джапаридзе Т.Д., Марк Э.Э. - № 2920531/18-25; Заявл. 07.05.80; Опубл. 30.12.81; Бюл. № 48;
6. Шведчикова И.А., Водолазский В.Н. Повышение чувствительности и помехоустойчивости вихретокового металлодетектора // Вестник НТУ «ХПИ». - 2004. - №22. – С.107-112;
7. Металлоискатель; А.с. №688887 G 01 V3/10/Юзов В.И., Голосов А.А., Зархин Ю.Б.- №2618137/18-25; Заявл. 19.05.78; Опубл. 30.09.79; Бюл. №9;
8. Устройство для обнаружения металлических включений в массе неэлектропроводного материала; А.с. №187173 G 01 V3/10/ Гринштейн В.Я., Костолонов В.Ф.- №924328/29-14; Заявл. 12.10.1964; Опубл. 11.10.1966. Бюл. №20;
9. Устройство для определения координаты металлического объекта в массе сырья; А.с. №1651260 G 01 V3/10. /Гольдштейн А.Е., Жуков В.К., Калганов С.А. и др. - № 4645253/28; Заявл. 01.02.89; Опубл. 23.05.91; Бюл. №19;
10. Устройство для обнаружения магнитных частиц в немагнитных материалах; А с. № 102969 В 03 С 01/16/Макаров В.Е., Фисенко К.С. - №11094/9526/425051; Заявл. 27.07.53;
11. Устройство для обнаружения и селекции металлических частиц в потоке; А.с. №1295349 G 01 V3/08/ Бунько В.А., Лапицкий В.Н., Бакушев В.А. и др. - №3854153/31-25; Заявл. 10.01.85; Опубл. 07.03.87; Бюл. №9.

Лыфарь В.А., Рязанцев А.И.

МОДЕЛИРОВАНИЕ ФОРМИРОВАНИЯ ВЗРЫВООПАСНОЙ СРЕДЫ ПРИ ВОЗНИКНОВЕНИИ ПРОМЫШЛЕННЫХ АВАРИЙ.

Предложены модели прогнозирования масштабов аварийных выбросов, позволяющие рассчитать динамику формирования взрывоопасной среды или облака отравляющих веществ для газовой или жидкой фазы.

В большинстве технологических процессов химической и нефтехимической промышленности в оборудовании обращаются вещества в жидкой и газообразной фазе, находящиеся под давлением при высоких температурах. При разгерметизации оборудования происходит выброс опасных химических веществ (ОХВ), смешивание их с воздухом и образование взрывоопасных или токсичных смесей. В зависимости от того, как проходит такой процесс и как быстро формируются опасные смеси, возможны различные сценарии развития аварии с различными масштабами негативных последствий.

Для прогнозирования масштабов выбросов, интенсивностей истечения газовой и жидкой фазы из оборудования, выхода парогазовой фазы перегретой жидкости и испарения с поверхности пролива разработаны математические модели и программные модули комплекса оценки риска «РизЭкс-2».

Разработаны модели для следующих процессов:
- истечение газовой фазы из оборудования;
- истечение жидкой фазы из оборудования;
- испарение перегретой жидкой смеси;
- испарение с поверхности пролива;
- образование, истечение и испарение двухфазной смеси.

1. Модель истечения газовой фазы из оборудования

Принятые ограничения и допущения:

1. Истечение газа происходит из емкости постоянного и известного ограниченного объема V_{cap} при известных начальных условиях.

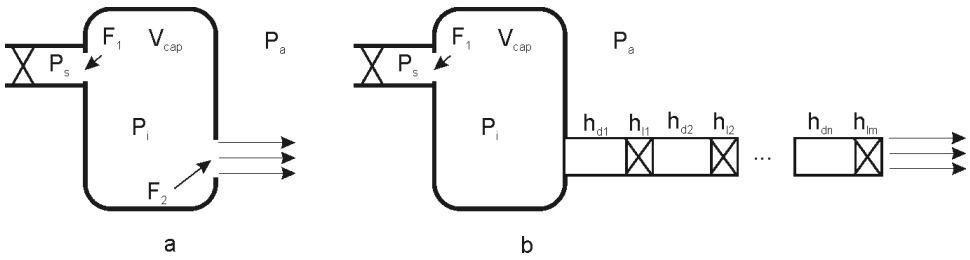


Рис. 1.1 – Два варианта истечения из емкости:
а – через отверстие или насадку; б – через систему соединений.

2. В процессе истечения давление в емкости регулируется двумя процессами: потерей массы газа из емкости в результате истечения через отверстие с известной (относительно небольшой) площадью F_2 в атмосферу и дополнительным приходом массы газа в емкость через отверстие с другой известной площадью F_1 (a) или истечения через систему местных и гидравлических сопротивлений (b) (трубопроводы h_{l_i} и запорная арматура h_{d_i}).

3. Все процессы происходят при постоянной температуре.

4. Начальное давление в емкости задается экспертом и равно P_s. Атмосферное давление равно P_a. Давление источника P_s остается постоянным в течение всего времени счета.

5. Источник может быть перекрыт в течение заданного экспертом времени.

В [1] рассмотрена задача истечения газа из емкости ограниченного объема. Предложено считать массовый расход как:

$$\frac{dM(t)}{dt} = m \cdot F \cdot y_i \sqrt{\frac{P_i}{v_i}}, \qquad (1.1)$$

где $\frac{dM(t)}{dt}$ - массовый расход, кг/сек;

m - коэффициент расхода отверстия;

F - площадь сечения отверстия истечения, м2;

P_i - давление в емкости в і-й момент времени, Па;

v_i - удельный объем в емкости в і-й момент времени, м^3/кг.

Коэффициент ψ_i определяется как:

$$y = \sqrt{2\left(\frac{k}{k-1}\right)\left[(b)^{\frac{2}{k}} - (b)^{\frac{k+1}{k}}\right]}, \qquad (1.2)$$

где β выбирается из условий:

$$b = \begin{cases} \frac{P_1}{P_2} \text{ если} \left(\frac{2}{k+1}\right)^{\frac{k}{k-1}} \le \frac{P_1}{P_2} \\ \left(\frac{2}{k+1}\right)^{\frac{k}{k-1}} \text{ если} \left(\frac{2}{k+1}\right)^{\frac{k}{k-1}} > \frac{P_1}{P_2} \end{cases}, \qquad (1.3)$$

где P_2 - давление в пространстве, откуда происходит истечение, Па;

P_1 - давление в пространстве, куда происходит истечение, Па;

В конечных разностях массовый расход из емкости можно записать как:

$$M_{t+1} = M_t - m_2 \cdot F_2 \cdot y_t \sqrt{\frac{P_t}{v_t}} \cdot \Delta t \ , \qquad (1.4)$$

где M_t - масса газа в емкости в предыдущий момент времени, кг;

M_{t+1} - масса газа в емкости в расчетный момент времени, кг.

Индексы і заменены на τ для обозначения принадлежности шага счета по времени.

Так как:

$$v_t = \frac{R \cdot T}{M \cdot P_t}, \qquad (1.5)$$

где R - универсальная газовая постоянная , 8314 $\frac{Дж}{моль \cdot град}$;

M - молекулярная масса выбрасываемого газа, кг/моль;

T - температура в емкости, К;

P_τ - давление в емкости в предыдущий момент времени, Па;

то выражение для изменения массы в емкости можно записать как:

$$M_{t+1} = M_t - m_2 \cdot F_2 \cdot y_t \cdot P_t \cdot \sqrt{\frac{M}{R \cdot T}} \cdot \Delta t \ . \qquad (1.6)$$

Вновь установившееся давление в емкости на следующем шаге по времени рассчитаем как:

$$P_{t+1} = \frac{M_{t+1} \cdot R \cdot T}{M \cdot V}, \qquad (1.7)$$

где V - объем емкости в м^3.

После этого необходимо определить «подпитку» из источника. Прибавочная масса, приходящая из источника будет рассчитана как:

$$\Delta M_t = m_1 \cdot F_1 \cdot y_{1t} \cdot P_s \cdot \sqrt{\frac{M}{R \cdot T}} \cdot \Delta t \ . \qquad (1.8)$$

При расчете β для истечения из емкости в атмосферу предполагаем, что $P_1 = P_a$, $P_2 = P_\tau$; для истечения из источника в емкость: $P_1 = P_{t+1}, P_2 = P$.

Делаем выбор: если массовый расход из источника ΔM_τ превышает производительность компрессора источника, то он становится равным массовому (кг/с) расходу компрессора, который вводится пользователем.

Окончательную массу вещества в емкости присваиваем как:

$$M_{\tau+1} = M_{\tau+1} + \Delta M_\tau . \qquad (1.9)$$

Вновь рассчитываем давление в емкости с учетом дополнительной массы:

$$P_{t+1} = \frac{M_{t+1} \cdot R \cdot T}{M \cdot V} . \qquad (1.10)$$

Расчет производим, пока счетчик по времени не превысит указанного экспертом времени окончания процесса или ручной остановки.

Подпитка из источника заканчивается в расчете по достижении времени перекрытия источника, введенного исследователем (сек).

Если выбрано истечение через систему местных и гидравлических сопротивлений, то предложено следующее решение:

Предполагаем истечение через круглые трубы (в иных ситуациях в [2] предложен метод определения необходимых коэффициентов).

Исследователь должен ввести (таблично) последовательный набор элементов в системе сопротивления потоку, начиная от элемента, расположенного у емкости, заканчивая элементом, через которое происходит истечение в атмосферу. Если элемент является гидравлическим сопротивлением, исследователь для каждого элемента вводит: l - длину тру-

бопровода в метрах, d - диаметр трубопровода в метрах, Δ - эквивалентную абсолютную шероховатость трубы (мм) [3], ν - кинематическую вязкость газа ($м^2/с$). Если элемент является местным сопротивлением, необходимо ввести коэффициент местного сопротивления ζ_l [4], молекулярную массу газа M (кг/моль), температуру газа внутри оборудования T (K).

Для расчета необходимо ввести начальное давление в оборудовании P_s (Па) и атмосферное давление (по умолчанию оно определено как 101000 Па), площадь отверстия источника подпитки F_1 ($м^2$),

Перепад давлений между емкостью истечения и средой истечения равен [2]:

$$P_s - P_a = \bar{\rho} \cdot g \cdot \frac{\bar{w}^2}{2 \cdot g} \cdot \left(\sum_{i=1}^{m} \lambda_i \cdot \frac{l_i}{d_i} \cdot + \sum_{j=1}^{n} \zeta_j \right), \qquad (1.11)$$

где $\bar{w}$ - средняя скорость потока (м/с);

$\bar{\rho} = \frac{P_s + P_a}{2} \cdot \frac{M}{RT}$ - средняя плотность потока ($кг/м^3$);

$l_i = 0.11 \left(\frac{\Delta \cdot 10^{-3}}{d} + \frac{68}{\mathrm{Re}} \right)^{0.25}$ - гидравлический коэффициент трения (формула Альтштуля).

Так как нас интересуют существенные выбросы, то предполагаем, что в дальнейшем будем иметь дело с турбулентными режимами, успешно описываемыми данной формулой:

$\mathrm{Re} = \frac{\bar{w} \cdot d}{n}$ – число Рейнольдса.

В действительности, неправильно определять гидравлическое сопротивление по средней скорости потока, так как на каждом участке системы скорости потоков разные и различные длины таких участков. Таким образом, давление в системе должно перераспределиться достаточно быстро (волна разрежения должна пройти по трубе со скоростью, близкой к звуковой) и установится на каждом участке свой перепад. Однако нас интересуют реальные системы, в которых произвольное изменение диаметра трубопроводов или несогласованные местные и гидравлические сопротивления недопустимы. Учитывая, что формула Альтштуля описывает турбулентные режимы и практически не зависит от перепадов скорости при значительных скоростях истечений, а в большей степени зависит от вязкости газа и шероховатости стенок трубы, ограничимся усредненным приближением скорости потока. Зная перепад давлений между емкостью и средой истечения, можно вычислить среднюю скорость из итогового уравнения:

$$\left(\frac{P_s - P_a}{P_s + P_a} \right) \cdot \frac{4RT}{m} = \bar{w}^2 \cdot \left(0.11 \cdot \sum_{i=1}^{m} \left(\frac{\Delta_i \cdot 10^{-3}}{d_i} + \frac{68 \cdot n}{\bar{w} \cdot d_i} \right)^{0.25} \cdot \frac{l_i}{d_i} \cdot + \sum_{j=1}^{n} z_j \right). \qquad (1.12)$$

Определить скорость $\bar{w}$ можно итерационно. Так как достижение критического режима истечения не позволяет скорости течения превысить скорость звука в обычных трубопроводах, то предполагаем, что средняя скорость истечения не превышает скорость звука.

Массовый расход системы равен:

$$\frac{\Delta M_t}{\Delta t} = \bar{w} \cdot \frac{p \cdot \left(\sum_{i=1}^{m} d_i \Big/ m \right)^2}{8} \cdot \frac{(P_s + P_a)m}{RT}. \qquad (1.13)$$

Потеря массы из емкости в единицу времени рассчитывается так же, как и в предыдущем примере. Все дальнейшие расчеты проводятся таким же образом.

2. Истечение жидкой фазы из оборудования

Истечение жидкости происходит в результате действия давления столба жидкости и давления над свободной поверхностью жидкости внутри аппарата. Истечение происходит при переменном или постоянном напоре через отверстия или насадки в газовую среду. Отверстие считается малым, если его максимальный размер не превосходит $0.1 \cdot H$.

Скорость истечения через малое отверстие из резервуара будет равна [2]:

$$v = j\sqrt{2g\left(H + \frac{P_0 - P_1}{rg}\right)}. \qquad (2.1)$$

При истечении через малое незатопленное отверстие струя при выходе претерпевает сжатие и площадь ее сечения равна S_c при начальной площади отверстия истечения S_0.

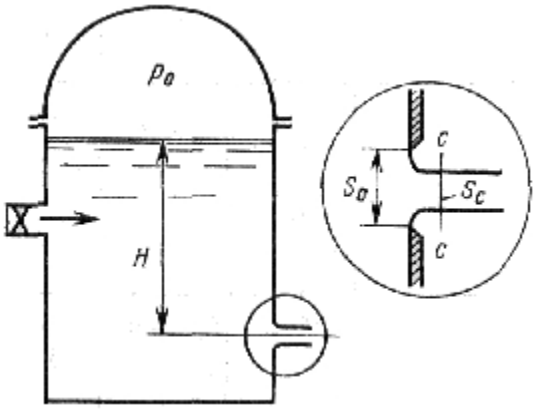


Рис. 2.1. Истечение жидкой фазы из емкости.

Алгоритм выполнения расчетов

Если выбирается «Истечение через длинный трубопровод», предполагается, что истечение происходит не через насадку или из отверстия, а через трубу, имеющую m участков постоянного диаметра и n местных сопротивлений.

Обозначение переменных:

H_p - начальная высота уровня жидкости в емкости, (м);

S_0 - площадь отверстия истечения (м^2);

h_s - высота расположения центра отверстия истечения над нижней частью емкости, (м);

ρ - плотность жидкости, $\left(\frac{кг}{м^3}\right)$;

– при выборе «истечения через круглое отверстие или насадки» μ (коэффициент расхода) определяется из справочников. Если выбрано «Истечение через длинный трубопровод», то μ определяется следующим образом:

(предполагаем последовательное соединение отдельных участков с различным гидравлическим сопротивлением)

$$m_C = \left(\sum_{i=1}^{m} l_i \frac{l_i}{d_i}\frac{S_0^2}{S_i^2} + \sum_{k=1}^{n} z_{м.к}\frac{S_0^2}{S_k^2}\right)^{-\frac{1}{2}}, \qquad (2.2)$$

где таблично задается n местных сопротивлений и m число участков постоянного диаметра;

S_0 - площадь поперечного сечения трубу на основном (расчетном) участке (в данном случае в месте выброса);

для каждого значения n и m задаются соответственно:

λ_i - гидравлический коэффициент трения [3-5];

l_i - длинна i -го участка постоянного диаметра d_i (м);

S_i, S_k - площади поперечного сечения i -го участка и k -го местного сопротивления соответственно;

$\zeta_{м.к}$ - коэффициент k -го местного сопротивления [3-5].

Коэффициент μ определяется из предлагаемого выбора, но может быть редактирован вручную. Более подробные сведения о гидравлических сопротивлениях можно найти в [3].

P_0 - давление над свободной поверхностью жидкости (в аппарате) (Па);

P_1 - давление во внешней среде истечения (Па).

Если $d_0 \le 0.1H_p$, то считается «малое отверстие», иначе «большое отверстие». Высота столба жидкости равна $H^\tau = H_p{}^\tau - h_s$.

Для «малого отверстия» объемный расход (м^3/с):

$$\nu_s{}^t = mS_0\sqrt{2g\left(H^t + \frac{P_0 - P_1}{rg}\right)}, \qquad (2.3)$$

где g - ускорение свободного падения 9,81 м/с^2.

Для «большого отверстия», заменяя H^τ на $H^\tau + {\omega_p}^2 \Big/ 2g$, где $\omega_p = \nu_s^\tau / S_p$ - скорость подхода,

$$S_p = \frac{pH_p^2}{4} \qquad (2.4)$$

получим мгновенное значение расхода:

$$\nu_b{}^t = \sqrt{\frac{2g\left(H^t + \frac{P_0 - P_1}{rg}\right)}{\left(\frac{1}{mS_0}\right)^2 - \left(\frac{4}{p\left(H^t + h_s\right)^2}\right)^2}},$$

где H^τ - переменная высота столба жидкости.

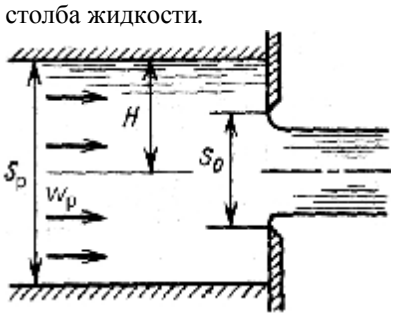


Рис. 2.2. «Подход» жидкости.

Контроль переменных значений столба жидкости считается для: вертикального цилиндра; горизонтального цилиндра, сферы, цилиндра и конуса с учетом геометрии заданных сосудов.

Выводится график функции $M(t)$. В отчет выводятся данные обо всех условиях эксперимента и выборах эксперта, а также график $M(t)$. В приложении 2 показан пример расчета (контрольной задачи) для истечения жидкости из емкости, выполненный при помощи счетного модуля.

Литература

1. Техническая термодинамика под ред. В. И. Крутова. Учебник для втузов. М., «Высш. школа» 1971. стр. 176;
2. Теоретические основы теплотехники. Теплотехнический эксперимент.: Справочник/Под общ. Ред. чл.-корр. АН СССР В. А. Григорьева, В. М. Зорина. – 2-е изд.- М.: Энергоатомиздат, 1988.-560 с;
3. Альтштуль А. Д. Гидравлическое сопротивление. М.: Стройиздат, 1973;
4. Идельчик И. Е. Справочник по гидравлическим сопротивлениям. М. Машиностроение, 1975;
5. Дейч М. Е. Техническая газодинамика. М.: Энергия, 1974.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В НАУЧНО-ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

УДК 371.315.7:159.942

Меняйленко О.С.

ДОСЛІДЖЕННЯ ПЕДАГОГІЧНИХ ВПЛИВІВ НА ФУНКЦІОНАЛЬНИЙ СТАН УЧНІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ НАВЧАННЯ

1. Постановка проблеми

Сьогодні загальновизнаною тенденцією в розвитку суспільства є інформатизація його різних сфер і, як наслідок цього, – підвищені вимоги до системи освіти. Сучасна система освіти також дедалі активніше використовує інформаційні технології навчання, що базуються на методах педагогіки, психології та кібернетики. Використання інформаційних технологій навчання дозволяє перейти від навчання, орієнтованого на „пересічного учня", до технологій, які враховують індивідуальні особливості учнів на основі гуманізації освіти і принципів значущості особи учня [1].

Однак на сьогодні проблему оцінки впливу як традиційних, так і інформаційних технологій навчання на учнів ґрунтовно не досліджено ні в науково-теоретичному, ні в методичному аспектах.

Одним з підтверджень цього є дані, наведені в роботі [2]: по Україні щорічно покінчують життя самогубством діти до 12 років – 70–80 осіб, а 12–15 років – 350–400 осіб. З них 25 % становлять учні, орієнтовані на безумовний успіх. Це „зразкові діти", „зубрили", для яких одна негативна оцінка може призвести до трагедії. Особливо це стає актуальним при використанні інформаційних технологій навчання.

Через недослідженість зазначеної проблеми неможливо науково обґрунтовано використовувати інформаційні технології навчання в різних навчальних закладах, урахувати індивідуальні особливості учнів.

Суперечність між вимогами створення високоефективних інформаційних технологій навчання та недостатнім рівнем наукового дослідження оцінки їх впливу на учнів дозволяє констатувати наявність проблеми і робить актуальним проведення досліджень у цьому напрямі.

2. Аналіз останніх досліджень і публікацій

У педагогіці і психології використовується ряд загальних підходів і методів для оцінки закономірностей оволодіння знаннями, уміннями й навичками, які ґрунтуються на використанні різних видів тестів, наприклад, робота [3] та ін. [4, 5].

Ці методи і підходи не дозволяють вести безперервний контроль стану учня в процесі навчання, отже, їх неможливо використовувати для об'єктивної функціональної діагностики учнів на різних етапах навчання.

Однією з перших спроб об'єктивної оцінки функціонального стану (поведінки) учнів при розв'язанні задач були роботи Лебедєва А.Н. [6], котрий намагався знайти ознаки інтелектуального розвитку за допомогою методів електроенцефалографії. Проте стосовно до умов використання як традиційних, так і інформаційних технологій навчання, функціональна діагностика впливу педагогічних дій на учнів не проводилася через відсутність формального опису педагогічних впливів та їх математичних моделей, а також методів дослідження об'єктивної реакції учнів на них.

Стосовно інформаційних технологій навчання вперше проведено формалізацію і класифікацію педагогічних впливів у роботах автора [7–9], розроблено математичні моделі базових педагогічних впливів (стратегій), у тому числі й моделі „гуманних" педагогічних стратегій [10]. Використання цих моделей дозволяє об'єктивно підійти до оцінки стану учнів в умовах інформаційних технологій, виявити особливості задання (вибору) педагогічних впливів для учнів з різними індивідуальними когнітивними характеристиками і,

отже, виключити можливі негативні наслідки застосування інформаційних технологій на учнів [2].

3. Формулювання цілей статті (постановка завдання)

Головною метою роботи є дослідження впливу педагогічних стратегій на учнів з різними когнітивними особливостями в умовах застосування інформаційних технологій навчання.

4. Виклад основного матеріалу

З використанням розроблених моделей педагогічних стратегій для об'єктивної (функціональної) оцінки впливу інформаційних технологій навчання скористаємося методами комп'ютерної електроенцефалографії (ЕЕГ), які дозволяють безперервно здійснювати сумарну реєстрацію електричної активності головного мозку учня.

Методика об'єктивної (функціональної) оцінки педагогічних впливів на учня в умовах інформаційних технологій навчання включає: 1) реєстрацію ЕЕГ учня на етапах навчання до початку роботи (фон 1), під час роботи і після завершення (фон 2); 2) виділення ділянок на ЕЕГ, що відповідають моментам педагогічних впливів; 3) виявлення та усунення артефактів на ЕЕГ [11]; 4) виявлення та виділення спайків на ЕЕГ при педагогічному впливі [11]; 5) спектральний аналіз на основі перетворення Фур'є виділених ділянок для δ-, θ-, α- і β-ритмів; 6) картрування електричної активності мозку (КЕАМ) учня; 7) виділення домінуючих ритмів і побудову схеми (карти) переходів; 8) оцінку статистичної значущості результатів, отриманих на основі спектрального аналізу.

Для зняття ЕЕГ використовувався комп'ютерний електроенцефалограф DX-400 Practic, який дозволяє здійснювати обробку ЕЕГ на основі міжнародних стандартів [11].

Схему розміщення електродів показано на рис. 1, а схему експериментальної установки – на рис. 2.

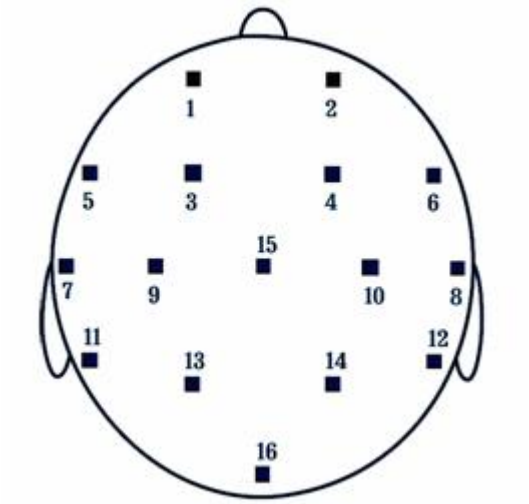


Рис. 1. Схема розміщення електродів.

Відповідно до розробленої методики проводились дослідження з учнями спеціалізованої фізико-математичної школи № 1 м. Луганська та студентами 1–3 курсів Луганського національного педагогічного університету на базі лабораторії функціональної діагностики Луганської обласної лікарні. Дослідженнями було охоплено 150 осіб. Оцінка статистичної значущості виділених на основі перетворення Фур'є δ-, θ-, α- і β-ритмів виконувалася за t-критерієм Стьюдента для залежних вибірок, використовуваним у таких дослідженнях [11].

Рис. 2. Експериментальна установка для оцінки (діагностики)
педагогічних впливів на учня.

На рис. 3–5 показано типові ЕЕГ учня O_1 в режимі фону (до навчання, див. рис. 3), навчання (див. рис. 4) і при педагогічному впливі PS_- (див. рис. 5).

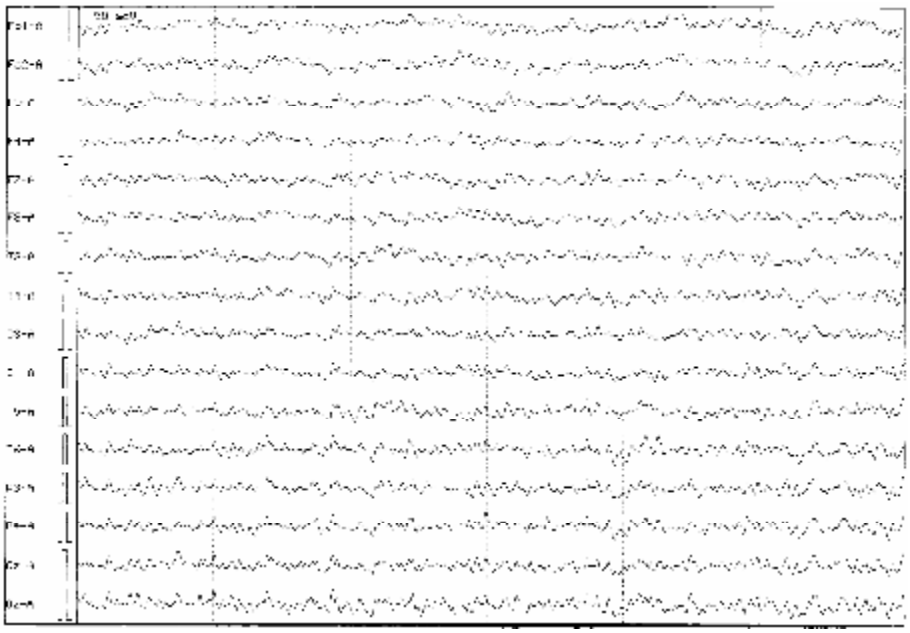


Рис. 3. Приклад ЕЕГ учня O_1 в режимі фону 1 (до навчання).

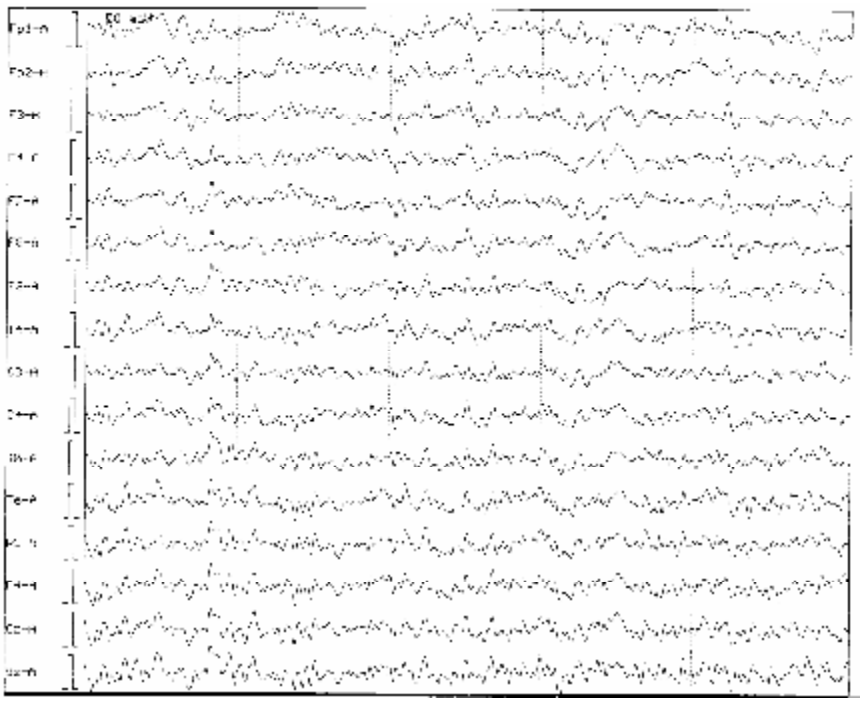


Рис. 4. Приклад ЕЕГ учня O_1 в режимі навчання.

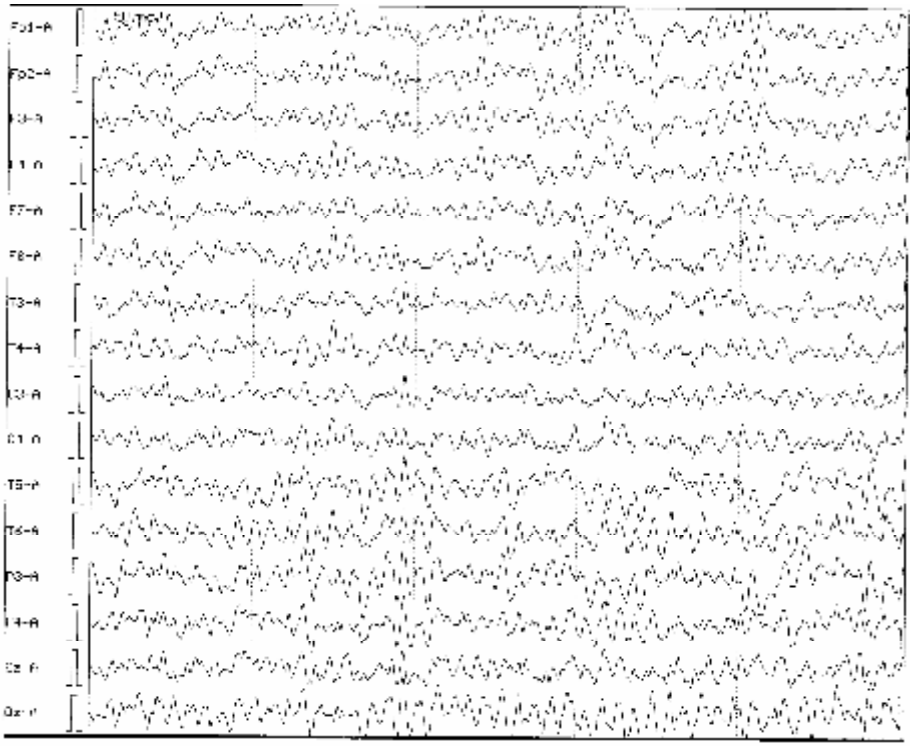


Рис. 5. ЕЕГ учня O_1 при педагогічному впливі PS_ .

Статистична значущість (при $p < 0,05$) виявлена не для всіх ритмів. Так, для стану фону й роботи статистично незалежними є ритми θ, α і β, а для стану робота-педагогічний вплив – ритми δ, θ і α. На рис. 6 подано середні амплітуди δ-, θ-, α- і β-ритмів учня O_1.

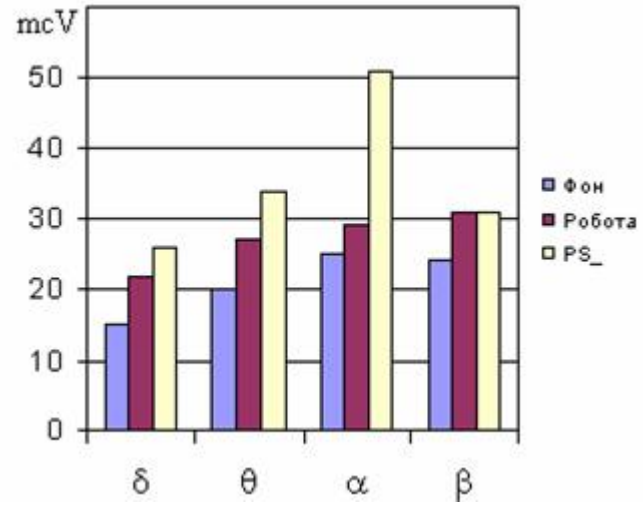


Рис. 6. Середні значення амплітуд δ-, θ-, α- і β-ритмів при навчанні учня O_1.

Домінуючі ритми в учнів змінюються індивідуально й істотно. Наприклад, для учня O_1 їх зміна має характер: α→δ→β→α→δ→α→δ→α→β→δ→β→α→θ, а для O_2 – β→δ→θ→δ→β→δ→θ→β→δ.

На рис. 7. показано картровані зміни активності мозку учня O_7 для домінуючих ритмів у процесі роботи з АПНС, які також свідчать про істотні зміни в активності головного мозку.

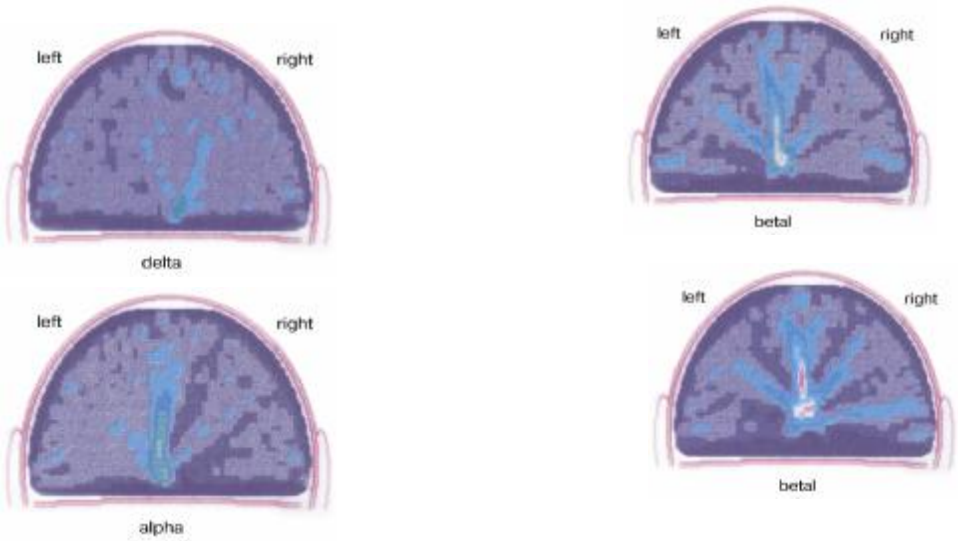
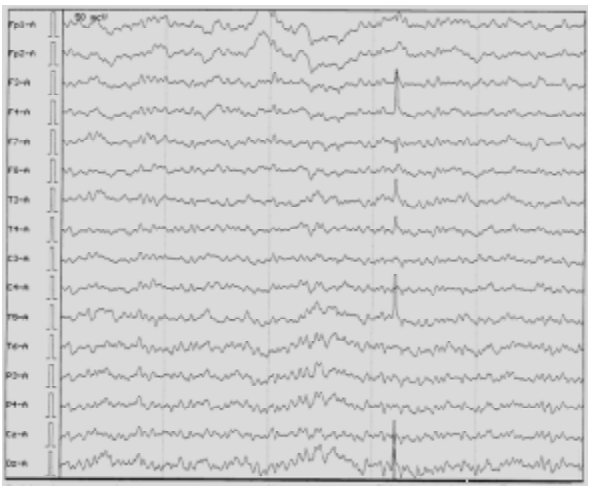
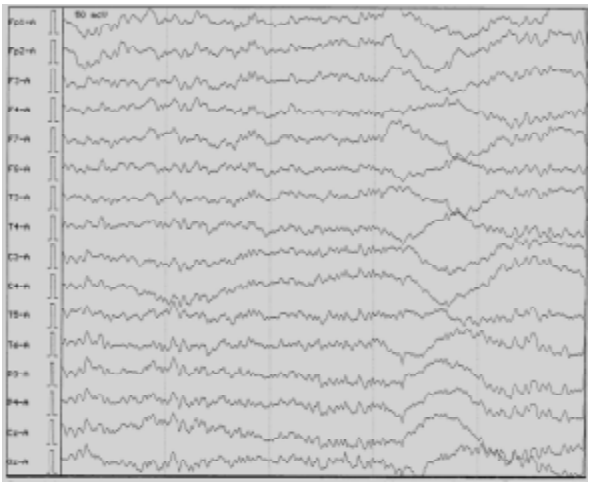


Рис. 7. Картровані зміни активності мозку учня O_7 для домінуючих ритмів у процесі навчання (δ→β→α→β).

У процесі досліджень у ряду учнів виявлено виникнення монофазних і поліфазних спайків при педагогічних впливах (рис. 8).

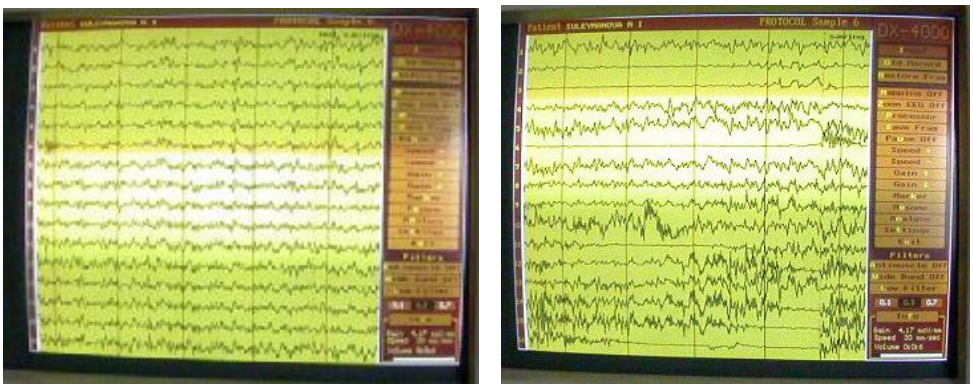


а)



б)

Рис. 8. Приклад: а) монофазних та б) поліфазних спайків в ЕЕГ учнів при педагогічних впливах.



а) б)

Рис. 9. Приклад ЕЕГ учня O_8 при педагогічній стратегії: а) з покаранням PS_-; б) „гуманній" педагогічній стратегії із заохоченням PSg_+.

Також у процесі експериментальних досліджень виявлено ряд учнів з істотними особливостями ЕЕГ при використанні педагогічних стратегій. На рис. 9 показано ЕЕГ та-

кого учня O_8 при використанні педагогічної стратегії з покаранням PS_- (див. рис. 9, а) та „гуманної" стратегії із заохоченням PSg_+ (див. рис. 9, б). Зазначені ЕЕГ вирізняються великою кількістю поліфазних спайків та істотними змінами амплітуди всіх датчиків електроенцефалографа.

При використанні гуманних педагогічних впливів із заохоченням в учня O_8 спостерігається ефект істотної стабілізації параметрів ЕЕГ (рис. 9, б). Це дозволяє стверджувати, що для учнів з указаними особливостями ЕЕГ найбільш доцільним є використання математичних моделей „гуманних" педагогічних стратегій [6].

Виявлений стабілізуючий вплив на учня використання „гуманних" педагогічних дій свідчить про необхідність індивідуального застосування (призначення, вибору) педагогічних впливів (стратегій).

Отримані результати слід розглядати як якісні, попередні, такі, що потребують подальшого розгляду низки досить складних завдань дослідження, пов'язаних з виявленням причин появи моно- і поліфазних спайків, вивчення впливу патологічних факторів в учнів тощо.

Висновки

1. На основі аналізу літературних джерел встановлено відсутність досліджень щодо безперервної об'єктивної функціональної діагностики учнів як у традиційних, так і в інформаційних технологіях навчання; показано, що в ряді випадків це може призводити до вкрай негативних наслідків для учнів [2].
2. Розроблено методику та проведено дослідження з функціональної діагностики педагогічних впливів на учнів засобами комп'ютерної електроенцефалографії в умовах інформаційних технологій навчання.
3. Установлено статистично значущі впливи педагогічних стратегій на учнів, виявлено істотні індивідуальні відмінності зміни домінуючих ритмів в учнів, появу монофазних і поліфазних спайків при педагогічному впливі.
4. Показано необхідність вибору (задання) педагогічних впливів з урахуванням когнітивних індивідуальних властивостей учнів, особливо для випадків, коли треба використовувати моделі „гуманних" педагогічних стратегій (впливів).
5. Перспективним напрямком досліджень є розробка алгоритмів керування педагогічними стратегіями (впливами), які враховують індивідуальні особливості та реакції учнів, а також розробка способів і засобів поточної функціональної діагностики учнів.

Література

1. Державна національна програма „Освіта – Україна XXI століття". – К.: Райдуга, 1994. – 61 с;
2. Дружбинский В. В моей жизни прошу никого не винить // Зеркало недели. – 2003. – № 6(431);
3. Айсмонтас Б.Б. Педагогическая психология: Схемы и тесты. – М.: Изд-во ВЛАДОС-ПРЕС, 2002. – 208 с;
4. Дюк В.А. Компьютерная психодиагностика. – СПб.: Братство, 1994. – 363 с;
5. Ингекамп К. Педагогическая диагностика: Пер. с нем. – М.: Педагогика, 1991. – 240 с;
6. Дружинин В.Н. Психология общих способностей – СПб.: Изд-во „Питер", 2000. – 368 с.: (Серия „Мастера психологи");
7. Меняйленко О.С. Формалізація і класифікація базових педагогічних впливів в адаптивних навчальних системах // Вісн. Східноукр. нац. ун-ту ім. В.Даля. – 2004. – № 5(75). – С. 226–233;
8. Меняйленко О.С. Реалізація педагогічних впливів в автоматизованих навчальних системах – підходи і вирішення // Директор школи, ліцею, гімназії. – 2004. – № 1. – С. 48–52;
9. Меняйленко О.С. Математичні моделі та методи формалізації елементів інформаційних технологій навчання // Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій: Матеріали наук.-практ. конф. Т. 4. – Херсон: Вид-во Херсон. морського ін-ту, 2005. – С. 77–80;
10. Меняйленко О.С. Математичні моделі „гуманних" педагогічних впливів для автоматизованих навчальних систем // Вісн. Східноукр. нац. ун-ту ім. В.Даля. – 2006. – № 1(95). – С. 134–144;

11. Зенков Л.Р. Клиническая электроэнцефалография (с элементами эпилептологии). – Таганрог: Изд-во ТРЕТУ. – 1996. – 358 с.

УДК 538.31

Бранспиз Ю.А.

ТЕОРЕТИЧЕСКАЯ ЭЛЕКТРОТЕХНИКА – КОМПЛЕКСНАЯ ИНФОРМАЦИЯ. ПРОБЛЕМА ПЕРЕДАЧИ И ОСВОЕНИЯ

Дана общая характеристика проблемы передачи и освоения в университетском образовании знаний теоретической электротехники как технической науки.

Введение

Теоретическая электротехника, как и любая другая отрасль знания, немыслима без определенной преемственности в передаче конкретных знаний, позволяющей осваивать эти знания различным их пользователям (инженерно-технические и научные работники, непосредственные пользователи электротехникой). Необходимая преемственность в передаче знаний (с соответствующей *селекцией* тех знаний, которые требуют сохранения и передачи), кроме прочего, осуществляется и в структуре образования. Элементом этой структуры является, в частности, университетское образование – образование, получаемое непосредственно от людей, которые, занимаясь наукой, причастны к получению нового знания (иначе говоря, университетское обучение необходимо осуществляется учеными). Поскольку же имеет место разделение всей совокупности знаний на науки, выделяющее, в частности, технические науки, то является вполне закономерным появление в последнее время в нашей стране и технических университетов, и технических специальностей в рамках классических университетов.

В этой связи преемственность в передаче знаний именно технических наук и, в частности, в теоретической электротехнике требует четкого выделения того знания, которое, собственно, и должно подлежать передаче (с соответствующим освоением). Представляется очевидным, что таким передаваемым знанием должна быть лишь общезначимая составляющая комплекса знаний той или иной отрасли знаний. При этом, если в классических науках (условно говоря, *старых* науках) можно указать какой-то внутренний критерий отбора общезначимой составляющей знаний (например, в виде определенной традиции), то для теоретической электротехники, как *молодой* науки, такой критерий общей значимости того или иного знания непосредственно указать затруднительно (обычно используется критерий практической эффективности, который, однако, не является универсальным). Отсутствие такого критерия общей значимости (хотя бы в виде традиции) вызывает определенные трудности обеспечения преемственности передачи знаний для теоретической электротехники в рамках именно университетского образования. Ведь университетское образование, предусматривающее, вообще-то, преемственность знаний определенной научной школы, характерной для данного университета, соответственно чему знания, которые передаются через университетское образование, имеют существенную личностную составляющую университетских ученых, получивших это знание, что и порождает проблемную ситуацию.

Рассмотрению некоторых аспектов указанной проблемной ситуации передачи и освоения знаний в области теоретической электротехники как технической науки и посвящена данная работа. При этом целью является феноменологическая характеристика этой проблемной ситуации, позволяющая наметить пути ее решения.

1. Знания теоретической электротехники как комплексная информация

Предварительно для более полной характеристики указанной проблеме дадим кратко характеристику тех знаний, которые должны быть освоены (переданы) в процессе университетского обучения. Согласно [1] в теоретической электротехнике имеют место две составляющие: «первичность понимания особенностей электромагнитных процессов в

рассматриваемом конкретном устройстве» и «изучение расчетных методов для их освоения и развития». Наличие этих двух составляющих, как представляется, обусловлено следующим:

- теоретическая электротехника, являясь технической наукой, ищет понимания сути явлений в конкретных электротехнических устройствах, представляющих собой проявления электромагнитного поля, в физике электромагнетизма, изучающей физические явления, которые являются также проявлениями электромагнитного поля;

- теоретическая электротехника, взяв за основу из физики электромагнетизма уравнения электромагнитного поля Максвелла, «работает» только с этими уравнениями, разрабатывая методики решения этих уравнений применительно к конкретным электротехническим устройствам по образцу математики (прикладной математики).

Собственно, на это указывается и в [1], когда отмечается, что развитие теоретической электротехники в прошлом веке осуществлялось путем «… освоения достижений в области, главным образом, физики электромагнитных явлений и прикладной математики».

Причем, если *физическая* составляющая теоретической электротехники представляет собой (и это всегда подчеркивается) результат обобщения (методом индукции) определенных опытных данных, то *математическая* составляющая теоретической электротехники является результатом применения строгих дедуктивных правил получения соответствующих результатов (аналитические или численные решения уравнений электромагнитного поля Максвелла, или тех уравнений, к которым уравнения Максвелла сводятся). При этом, как отмечается в [1]: «Характерным … следует считать практическую неделимость исследований физических явлений, разработки моделей этих явлений и решения прикладных задач, связанных с расчетом исследуемых физических величин».

То есть, теоретическая электротехника представляет собой сложный синтез (комплекс) специфических технических (практических и теоретических) знаний, имеющих индуктивный и дедуктивный характер (по способу получения), что и позволяет характеризовать знания теоретической электротехники понятием «комплексная информация». Именно это и учитывается в дальнейшем.

Хотя, конечно, следует признать, что знания теоретической электротехники как знания конкретной технической науки представляют собой не просто «комплексную информацию» (сумму индуктивных и дедуктивных истин), а – *систему комплексной информации*. Это признание, конечно же, необходимо влечет за собой раскрытие понятия системы в применении к знаниям (с указанием, например, структурообразующих факторов и их взаимодействия, обеспечивающего стабильность системы знаний и ее существование во времени). Но для целей данной работы (феноменологическая характеристика проблемной ситуации передачи и освоения знаний в области теоретической электротехники как технической науки) достаточно и интуитивного понимания названного понятия (*система комплексной информации*).

2. Об обобщенной периодизации процесса передачи и освоения знаний

Прежде всего, следует указать на то, что проблема передачи и освоения знаний в общем случае (а не применительно только к теоретической электротехнике) есть, по сути, проблема превращения *внешнего* знания (знания обучающего) в личностное знание обучаемого. Ясно, что (опять же, в общем случае) это превращение имеет определенные этапы с определенными формами рефлексии над знанием, характеризующие рефлексивно-оценочное отношение субъекта (обучаемого) к объекту (внешнее знание).

Так в [2] в качестве таких форм (этапов) предлагаются: неверие, сомнение, вера, убеждение, что соответствует появлению личностного знания на основе конечного формирования «убежденности» в процессе обучения, когда:

- тот, кто обучается, не имеет вообще никакого знания по данной дисциплине (полное незнание или *неверие* по [2]);

- в процессе начального знакомства с дисциплиной у того, кто обучается, появляется *сомнение* (например, в возможности воспринять внешние знания, в необходимости их практической целесообразности и т. д.);

- в процессе дальнейшего обучения у того, кто обучается, появляется определенная *вера* (доверие к излагаемым *истинам*, когда нет возможности осуществить весь тот путь, по которому прошла конкретная отрасль науки, чтобы получить ту или иную свою истину);

- появление (со временем) у того, кто обучается, убеждений относительно истин данной отрасли знаний.

В [3] автором данной работы предложено видоизменение этой цепочки этапов (неверие – сомнение – вера - убеждение) заменой этапа *неверия* на два последовательных этапа *безразличия* (из-за незнания) и *интереса* (к получению информации) и введением заключительного этапа *практики* (как специфического вида рефлексии над знанием путем непосредственного оперирования им), когда знание становится инструментом деятельности.

Наверно возможна и другая возможность представления этапов рефлективного (оценочного) отношения обучаемого к знаниям. В этой связи отметим, что сама возможность такого различного представления является проявлением сложной и, может быть, неоднозначной структуры самого знания, характер которого определяет, в конечном итоге, и структуру превращения *внешнего* знания (знания обучающего) в личностное знание (знание обучаемого).

Впрочем, несмотря на возможные различия в рассматриваемой периодизации, следует, наверное, признать, что процесс передача и освоение знаний как некоторой формы информации может считаться завершенным, когда у того, кто обучается, сформировалась убежденность в переданных (полученных) знаниях.

То есть следует признать, что образование (по крайней мере, университетское) – это процесс *убеждения*, конечным этапом которого является формирование убежденности в полученных знаниях (не *верования* в них*)*. Как следствие, задача университетского образования состоит не в том, чтобы дать просто определенную сумму информации (знаний), а дать ее, убеждая, и добиваясь убежденности. Если нет этого, то у обучаемого остаются, в лучшем случае, определенные мнения (информация, не представляющая собой определенной системы, несистематическое знание), но нет квалифицированного использования полученных знаний (и нет, в конечном итоге, перехода от незнания к знанию).

3. О рациональном обосновании в теоретической электротехнике

В развитие изложенного выше и для перехода к тому, что излагается дальше, укажем на одну из современных тенденций в теоретической электротехнике, связанную с максимальным использованием теории цепей для решения даже тех задач, которые изначально формулируются как задачи на непосредственное решение полевых уравнений Максвелла. Ведь *убежденность* в этих уравнениях относительно слаба, учитывая необходимость освоения соответствующего сложного математического аппарата, приближающего в этом разделе теоретическую электротехнику к математической физике. Убежденность же в *истинах* теории цепей закладывается еще в школе.

В этой связи большое значение имеет *рациональное* обоснование (доказательство) знания, которое является основным инструментом университетского образования, и от качества которого зависит и качество этого образования. Ведь практикующиеся при любом образовании (в том числе, и университетском) частые ссылки на основу в опыте тех или иных *истин* (знаний) не дают убежденности тому, кто обучается, поскольку непосредственно в процессе образования сами эти опытные факты не воспроизводимы в полной мере (как правило).

Но рациональное доказательство некоторых истин теоретической электротехники обуславливает проблему метода такого доказательства и соответствующего построения теоретической электротехники как науки. В самом деле, ведь знание теоретической электротехники, как указано выше, есть комплексная информация, содержащая определенные

индуктивные и дедуктивные истины при передаче и освоении которых также используется соответствующий арсенал индуктивных или дедуктивных процедур доказательства. Причем такое смешение может приводить на практике к определенным трудностям в понимании.

Так, например, при построении теоретической электротехники по образцу физических наук (соответствующие доказательные процедуры имеют индуктивный характер), векторы напряженности электрического поля и индукции магнитного поля определяются как измерительные процедуры (по силовому воздействию, соответственно, на неподвижный и движущийся электрический заряд) [1]. Если же рассматривать теоретическую электротехнику как дедуктивную науку, то в этом случае указанные векторы представляют собой результат математической процедуры усреднения (методами статистической физики) векторов некоторого микроскопического магнитного поля (см., например, [4]). Очевидно, что такая ситуация затрудняет понимание смысла векторов поля.

В качестве второго примера укажем на закон Ома, для которого, при построении теоретической электротехники по образцу физических наук, обязательно подчеркивается тезис о его опытном характере, и для которого, при построении теоретической электротехники по образцу дедуктивных наук, приводятся доказательные процедуры его аналитического вывода на основе определенных модельных представлений [4, 5].

Вследствие такой двойственности доказательная база для рационального обоснования теоретической электротехники весьма уязвима (можно, конечно, обучать, акцентируя внимание на том, что передаваемые знания, должны рассматриваться лишь как *мнения*, но такой подход не представляется удовлетворительным). В этой связи актуальным представляется анализ доказательной базы теоретической электротехники, учитывающий прикладной характер ее как науки.

4. О научной вере

В результате описанной выше двойственности в рациональном обосновании знаний теоретической электротехники и связанных с этим трудностей в передаче и освоении этих знаний у обучаемых вырабатывается не убежденность, а некоторая компенсирующая форма личностного обоснования знания. При этом тот, кто обучается, приходит к некоторой *уверенности* в знании (на основе доверия к тому, кто обучает), которая является своеобразной научной верой (не основанная на знании убежденность). То есть научная вера компенсирует недостаток средств рационального обоснования.

Здесь важно различать веру (в указанном смысле) и объект веры – знание. Носитель веры – субъект (обучающийся). Носитель знания – наука. Опыт субъекта индивидуален, а потому и ограничен. Опыт науки – неличностен, а потому и не ограничен (ограничением является сама наука). Как следствие, ограниченность индивидуального опыта обучающегося является обусловленным источником веры (уверенности), как своеобразной формы убежденности.

Такая вера (уверенность) является, очевидно, объективной формой сохранения знания. И в этом ее положительная роль. Но такая вера (уверенность) служит и тормозом в развитии знания, поскольку ее носители не воспринимают, как правило, нового знания. И в этом ее отрицательная роль. Ведь вера (уверенность), не может заменить знание, она лишь компенсирует доказательное обоснование.

Все это и надо учитывать, стремясь сформировать последовательно в процессе обучения:

- *уверенность* в определенной информации на основе личного доверия к ней (общезначимые составляющие всей суммы знаний);

- *убежденность* в отдельно выделенных элементах этой информации (знания), в том числе и путем применения доказательных специальных процедур.

Выводы

1. Знания теоретической электротехники как технической науки представляют собой комплексную информацию индуктивного и дедуктивного типа (по способу получе-

ния), передача и освоение которой порождают проблемную ситуацию связанную как с выделением общезначимой составляющей.

2. Формирование убежденности в знаниях теоретической электротехники встречает трудности рационального обоснования этих знаний, что делает объективно необходимым предварительное формирование уверенности в них.

Литература

1. Теоретические основы электротехники: В 3-х т. Т. 1/ К.С. Демирчян, Л.Р. Нейман, Н.В. Коровкин, В.Л. Чечурин. – СПб.: Питер, 2003.– 463 с;
2. Героименко В.И. Личностное знание и научное творчество.– Минск: Наука и техника, 1989.– 208 с;
3. Бранспиз Ю.А. Проблема передачи знания с учетом развития знания // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я. XII міжнародна наук.-практ. конф.: Матеріали. – Харків: НТУ „ХПІ", 2003.– С. 3-6;
4. Поливанов К.М. Теория электромагнитного поля.– М.: Энергия, 1975. – 208 с.– (ТОЭ. В 3-х т. / Под общ. ред. К.М. Поливанова. – Т.3);
5. Тамм И.Е. Основы теории электричества. – М.: Наука, 1989.– 504 с.

УДК 621.4.016.1

Дядичев В.В., Веревка Д.Н., Прилепский К.Ю.

КОМПЛЕКСНЫЙ ПОДХОД К РЕШЕНИЮ ЗАДАЧ АВТОМАТИЗАЦИИ РАБОТЫ И ДОКУМЕНТООБОРОТА В УЧЕБНЫХ ЗАВЕДЕНИЯХ ЛЮБОГО УРОВНЯ АККРЕДИТАЦИИ С ПОМОЩЬЮ СИСТЕМЫ IT - ВУЗ

Проведен анализ задач и состава систем автоматизации учебно-управленческой деятельности ВУЗов. Описаны основные принципы и структуры построения данных систем. Рассмотрена структура, описаны характеристики и функции IT – ВУЗа как способа решения задачи комплексной автоматизации учебно-управленческой деятельности

Постановка проблемы

Современные процессы рыночных преобразований, а также повышение конкуренции на рынке труда требуют постоянного совершенствования процесса подготовки специалистов. Кроме того, современное учебное заведение с территориально распределенной структурой в процессе своего развития постоянно сталкивается с проблемой эффективного управления учебным и контролирующим процессами.

При увеличении объемов образовательных услуг, числа студентов и росте региональной сети ВУЗа все вышеуказанные проблемы проявляются особенно явно. Очевидно, что в условиях ручной обработки управленческой информации невозможно эффективно управлять территориально распределенным вузом, а также поддерживать в нем единый стиль руководства и высокое качество образовательных услуг.

Достижение успеха в решении данных задач во многом зависит от развития автоматизации управленческой деятельности и информационного обеспечения учебного процесса в учебных заведениях, а также от внедрения новых информационных технологий и средств коммуникаций.

Анализ исследований и публикаций. Проблемы автоматизации учебно-управленческой деятельности учебных заведений являются предметом исследования большого числа специалистов. Разработки в этой области ведутся во многих ВУЗах Украины и России: Харьковском техническом университете радиоэлектроники (г. Харьков), Киевском Национальном Университете имени Тараса Шевченко (г. Киев), Институте дистанционного и заочного обучения РосНОУ (г. Москва), Научно-исследовательском институте информационных технологий (г. Санкт-Петербург), Российском государственном институте открытого образования (г. Москва), Красноярском государственном техническом университете, отдел АСУ КГТУ (г. Красноярск) и других ВУЗах [3,43].

Цель статьи. Цель данной статьи состоит в проведении анализа задач и состава систем автоматизации учебно-управленческой деятельности ВУЗов, описании основных принципов и структуры построения данных систем.

Основной материал

На основании анализа развития перспектив IT-образования в развитых странах, можно выделить 4 их основных направления: информатика (computer science), разработка аппаратных платформ (computer engineering), программная инженерия (software engineering) и информационные системы (information systems) [1,85].

Данные направления позволяют выделить круг задач, которые можно решить с помощью системы автоматизации учебно-управленческой деятельности учебных заведений:

- создание материально-технической базы, аппаратного и программного обеспечения научных исследований и учебного процесса, автоматизация управленческих процессов;
- применение информационных технологий в учебном процессе и дистанционном обучении;
- создание электронных образовательных и информационных ресурсов, автоматизация библиотечной деятельности;
- развитие инфраструктуры корпоративной сети университета (увеличение пропускной способности и надежности каналов связи, количества и мощности серверов сети).

Одной из важнейших задач является безусловное обеспечение информатизации учебного процесса в каждом структурном подразделении ВУЗа. В основе информатизации ВУЗа лежит разработка его корпоративной информационной системы и ее внедрение в каждом филиале и представительстве университета.

Техническое и структурное решение задач автоматизации учебно-управленческой деятельности учебных заведений существенно разнятся у разных разработчиков. Единая черта, которая объединяет все известные разработки в этом направлении – это использование технологии «Клиент-сервер». Данная технология является оптимальной для реализации задач автоматизации учебно-управленческой деятельности, поскольку предполагает наличие специальных программ, обрабатывающих запросы клиентов по работе с единой базой данных на сервере. Во время данного взаимодействия клиент не имеет прямого доступа к самим данным и общается только с сервером посредством использования SQL запросов в специальных приложениях.

Выбор программного обеспечения для построения систем автоматизации осуществляется в зависимости от выбора платформы сервера баз данных и приложений.

При выборе платформы и базы данных для подобных систем необходимо учитывать основные требования к их работе:

- возможность достижения высокой скорости разработки;
- простота распространения готового продукта;
- перспективность технологии, уверенность в поддержке и развитии платформы;
- ориентация IT-инфрастуктуры университета и филиалов на данное программное обеспечение;
- наличие кадров, необходимых для внедрения подобных баз данных.

После проведения сопоставительного анализа для реализации системы IT–ВУЗ наиболее перспективной была признана серверная платформа Unix, а языком программирования - PHP. В качестве базы данных информационной системы была выбрана база данных My SQL, которая легко может быть сопряжена с платформой Unix.

Система IT–ВУЗ обладает следующими основными характеристиками, необходимыми для обеспечения необходимой функциональности и возможности дальнейшего развития:

- Модульный принцип построения, основанный на применении WEB – технологий;
- Единая база данных, которая обеспечивает мгновенное получение из нее любой информации;
- Использование дешевого средства передачи данных – Internet / Intranet;

- Единый Web-интерфейс для клиентов системы, отсутствие необходимости установки программного обеспечения на пользовательских машинах;

- Простота внедрения, обновления, изменения, наполнения со стороны разработчиков, возможность удаленной установки и настройки программного обеспечения системы;

- Масштабируемость - легкое подключение новых модулей и пользователей системы;

- Дистанционный контроль за работой системы;

- Работа системы в режиме реального времени.

Основные задачи, которые решает система IT–ВУЗ:

- Автоматизация работы и документооборота учебного заведения;

- Обеспечение инструментами эффективного управления;

- Контроль учебного процесса;

- Поддержка эффективного накопления, хранения и доступа к информации и знаниям;

- Обучение студентов в Интернет / Интранет;

- Легкость внедрения и эксплуатации (легкость интеграции в существующую учебную систему, удаленная настройка и отладка системы разработчиком);

- Высокий показатель возврата инвестиций;

- Получение сводной статистики функционирования учебного заведения.

Структурная схема системы комплексной автоматизации учебно-управленческой деятельности IT–ВУЗ показана на рис. 1.

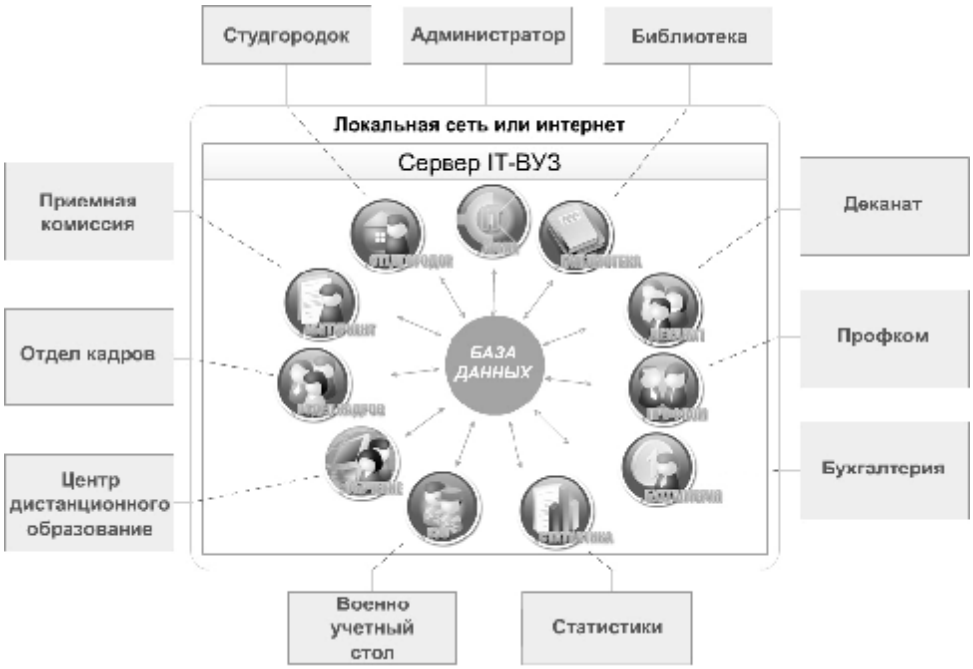


Рис. 1. Структурная схема системы комплексной автоматизации учебно-управленческой деятельности IT–ВУЗ.

Согласно рис. 1, на сервере (1) учебного заведения установлена единая база данных (2) и модули – программы (3) для работы с ней. Подразделения учебного заведения (4), используя локальную сеть или интернет (5), работают с центральной базой данных (2) с помощью своих модулей (3).

Например, подразделение учебного заведения - отдел кадров, работает с общей базой сотрудников и учащихся с помощью модуля «IT-ВУЗ. Отдел кадров», а подразделение приемная комиссия – по средствам модуля «IT-ВУЗ. Абитуриент».

Выводы и перспективы дальнейших исследований

Проведенное исследование позволило определить, что к преимуществам внедрения системы IT-ВУЗ относятся:

- Единая база данных на одной платформе;
- Модульность обучения;
- Использование разнобалльной системы оценки знаний;
- Обеспечения прозрачности обучения;
- Обмен информацией в режиме «on-line»;
- Удаленный контроль работы студентов (возможность обеспечить контроль учебного процесса программно, а не организационно);
- Мгновенное получение любого рода отчетности из базы данных;
- Отсутствие возможности редактирования результатов экзаменов и зачетов;
- Объективный «срез» учебного процесса, проведение промежуточного контроля знаний в разных формах (тесты, упражнения и др.);
- Сбор всевозможной статистической информации о работе учебного заведения (успеваемость, посещаемость и т.д.);
- Конкурентная себестоимость обучения студентов;
- Повышение конкурентоспособности и рейтинга учебного заведения;
- Возможность привлечения дополнительного количества студентов;
- Возможность обеспечения более качественной довузовской подготовки абитуриентов;
- Обеспечение систематизации и структурирования работы учебного заведения;
- Расширение использования новых форм обучения;
- Улучшение качества образования;
- Создание неограниченного доступа к учебной информации.

Необходимо отметить, что внедрение новых информационных технологий и средств коммуникаций является важнейшим условием подготовки будущих специалистов. Использование современных технологий на основе построения системы «IT–ВУЗ», является не только комплексным подходом к решению задач автоматизации работы ВУЗа, но также и важным инструментом для организации работы специалистов по управлению, и кроме того, позволяет добиться более высоких результатов организации процесса учебно-управленческой деятельности ВУЗа и повысить эффективность управления им в целом.

Литература

1. Демкин В.П., Вымятнин В.М., Нежурина М.И. «Информационные технологии в проектировании и производстве» - 1997, с. 85;
2. Ю.В. Карякин. Информатизация лекции. В сб.: Тезисы Российской научно-практической конференции образование в условиях реформ: опыт, проблемы, научные исследования, Кемерово, 1997, с. 60, Изд-во Кемеровского технологического института пищевой промышленности, 1997 г. № 3. - С. 11-15;
3. Н.Г. Созоров. Об опыте создания и использования электронных средств комплексной информационной поддержки учебного процесса. В сб.: Использование новых информационных технологий в учебном процессе, Ульяновск, 2000, с. 43-45. Изд-во Ульяновского государственного технического университета, 2000 г;
4. Институт заочного и дистанционного обучения, www.do.rosnou.ru;
5. Интернет - Университет Информационных Технологий, www.intuit.ru.

УДК 612.68

Поляченко Е.Ю., Ткачук О.А.

КОМПЬЮТЕРНЫЕ ЛАБОРАТОРНЫЕ РАБОТЫ ПО КУРСУ «ПРИКЛАДНАЯ ТЕОРИЯ ЦИФРОВЫХ АВТОМАТОВ» С ИСПОЛЬЗОВАНИЕМ CAD ELECTRONIC WORKBENCH

Предложена структура компьютерных лабораторных работ и приведена одна лабораторная работа с использованием системы электронного моделирования Electronic Workbench.

Повышение требований к умениям и навыкам выпускников технических вузов, усиление роли инженерного образования при одновременном сокращении аудиторного времени, быстром моральном старении оборудования, его дороговизне, с одной стороны, и возрастающие возможности компьютерных технологий с другой стороны – это факторы, свидетельствующие за внедрение в процесс обучения компьютерных лабораторных работ (КЛР).

При проектировании КЛР должны быть особенно тщательно продуманы методические вопросы. Предлагается следующая структура КЛР. Этап подготовки студентов к лабораторным работам – предварительный этап, в компьютерном варианте должен содержать два блока, которые можно условно назвать “Теория” и “Методика”. Каждый из блоков подразделяется на подблоки, например, блок “Теория” – на “Теоретические положения”, “Справочник”, “Новости науки”, а блок “Методика” – на “Описание лабораторной работы”, “Инструкции”, “Задания”. Представленные блоки и подблоки по усмотрению преподавателя могут на какой-то определенный срок быть скрыты от студента, тем самым преподаватель может управлять передвижением студента в “пространстве знаний”.

Второй этап – контроль готовности студентов к выполнению лабораторной работы. Продумывается преподавателем особенно тщательно, необходимо диагностировать готовность студента к проведению эксперимента, а не только выявить его знания теоретических положений.

Третий этап – проведение эксперимента, непосредственного решения экспериментальной задачи.

Четвертый этап – оформление результатов эксперимента и их проверка преподавателем.

Предлагаемая структура была заложена при проектировании цикла КЛР по дисциплине “ Прикладная теория цифровых автоматов ”.

Дисциплина «Прикладная теория цифровых автоматов» читается для студентов второго курса по направлению «Компьютерная инженерия» для специальности «Компьютерные системы и сети». Многие считают данную дисциплину чисто математической. Однако профиль будущих IT-специалистов требует не только качественной математической подготовки, но и достаточно высокого уровеня владения аппаратной частью, а также представления процессов, проходящих в вычислительных элементах. В связи с этим, лабораторный курс был разделен на две логически законченные задачи. Первая – написание двоичного калькулятора для моделирования операций, происходящих в цифровых автоматах (модульный контроль 1 (МК1)), вторая – построение простейших цифровых автоматов из логических элементов (МК2).

Первая задача решалась с помощью любого языка программирования с обязательным описанием алгоритмов и методов их реализации.

Решение второй задачи затруднялось отсутствием достаточной материально-технической базы и отдельной лаборатории данного профиля. Физическое моделирование было заменено компьютерным.

Существует огромное количество программных продуктов (CAM/CAD), основной целью которых является моделирование электронных схем, отвечающих в той или иной степени задачам анализа их работы. Многие из них требуют серьезной предварительной

подготовки конечного пользователя и наличия у него специальных знаний. При этом исключается огромное количество потенциальных пользователей, перед которыми стоят относительно простые задачи, требующие контроля на различных стадиях работ (проектирования новых устройств, модернизации старых, изменения элементной базы и т.д.).

Когда процесс моделирования будет максимально приближен к реальному эксперименту (в этом случае человек, осуществляя естественную последовательность таких операций, как сборка схемы, подключение к ней измерительных приборов, задание исходным параметров, получал бы результаты в привычной для него форме), тогда уровень подготовки конечного пользователя не будет влиять на выбор программного продукта.

Компания Interactive Image Technologies (www.interactiv.com) разработала многофункциональный программный продукт Electronic WorkBench. Богатый выбор профессиональных инструментов и функций, простота и удобство делают этот продукт наилучшим средством для учебных целей. Ее особенностью является наличие контрольно-измерительных приборов, по внешнему виду и характеристикам приближенных к промышленным аналогам.

Студентам предложен лабораторный практикум по цифровым автоматам с памятью (триггеры и счетчики). Практикум разделен на следующие эксперименты (по 1 академическому часу на каждый):

01 эксперимент - исследование RS-триггера;

02 эксперимент - исследование $\overline{RS}$-триггера;

03 эксперимент - исследование JK-триггера;

04 эксперимент - исследование JK-триггера в счетном режиме (T-триггера);

05 эксперимент - исследование JK-триггера, построенного на базе логических элементов и RS-триггеров;

06 эксперимент - исследование D-триггера;

07 эксперимент - исследование D-триггера в счетном режиме;

08 эксперимент - исследование суммирующего счетчика;

09 эксперимент - исследование вычитающего счетчика;

10 эксперимент - исследование счетчика с измененным коэффициентом пересчета;

11 эксперимент - исследование регистра Джонсона;

12 эксперимент - исследование регистра Джонсона, реализованного на JK-триггерах;

Каждый эксперимент является законченной лабораторной работой с обязательным заполнением лабораторной тетради, которая выдается студентам в на МК1 (в электронном виде). По окончанию изучения курса «Прикладная теория цифровых автоматов» и успешной сдачи МК2 лабораторная тетрадь остается у студента. Ее можно использовать при подготовке к сдаче Государственного квалификационного экзамена по курсу бакалавра.

На рис. 1 приведена экспериментальная схема и временная диаграмма восьмого эксперимента.

Использование в эксперименте одновременно светоиндикаторов и семисегментного индикатора с дешифратором позволяет проверять двоичный код, образованный светоиндикаторами, и десятичный – индикатором.

За своевременное выполнение лабораторных работ и их защиту студенты получают баллы, которые по рейтинговой системе оценок дает право им не сдавать МК2 и получить высокую итоговую оценку по дисциплине «Прикладная теория цифровых автоматов».

Выводы

1. Внедрение компьютерных лабораторных работ позволяет строить лабораторные работы на современном уровне и использование новой элементной базы;
2. Использование КЛБ в учебном процессе облегчает усвоение студентами теоретической части и позволяет им овладеть навыками построения цифровых автоматов.

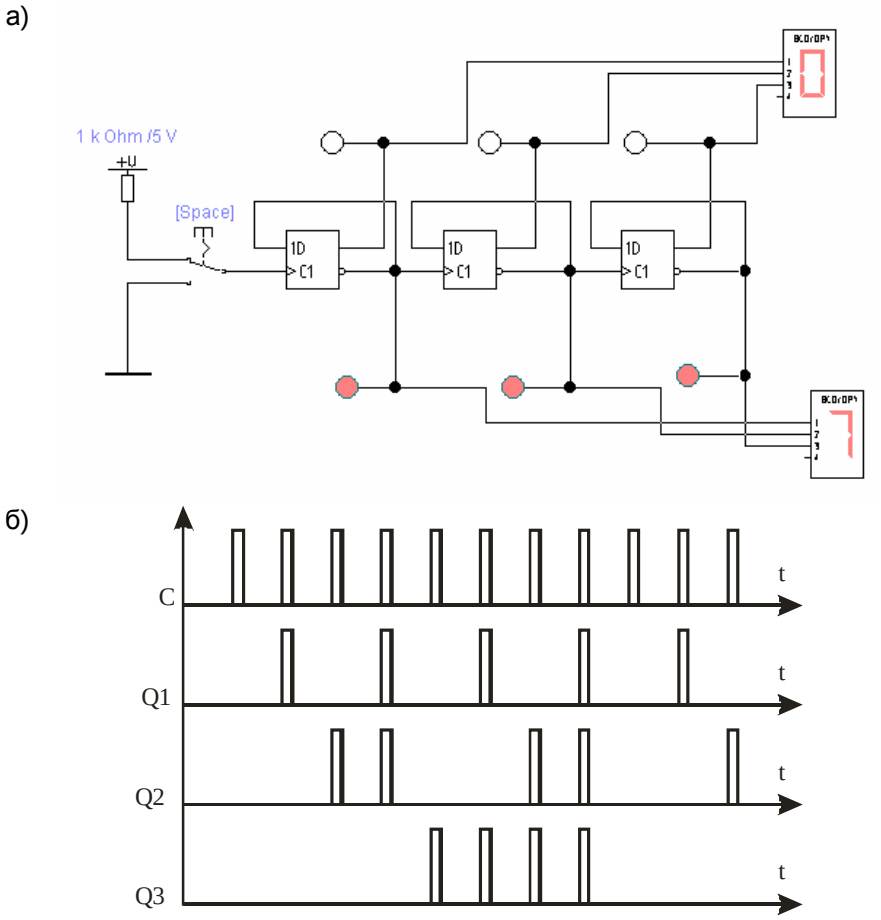


Рис. 1. Исследование суммирующего счетчика: экспериментальная схема (а) и временная диаграмма (б).

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ, ОХРАНЫ И ЗАЩИТЫ ИНФОРМАЦИИ В ЗАКОНОДАТЕЛЬСТВЕ УКРАИНЫ

УДК 004.056

Дригваль Н.П.

ПРОБЛЕМНІ АСПЕКТИ ОХОРОНИ ТА ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ТА НОУ-ХАУ В ЗАКОНОДАВСТВІ УКРАЇНИ

Нетрадиційні об'єкти інформації, які вирізняються серед інших своїм правовим статусом та обмеженим доступом, такі як комерційна таємниця та ноу-хау, досліджуються науковцями різних галузей науки, оскільки питання їх охорони й захисту можливо розглядати з різних позицій: з точки зору вжиття правових, організаційних, технічних, економічних заходів. Тим більше, що володіння й використання зазначених об'єктів забезпечує очевидний пріоритет суб'єкта підприємницької діяльності серед інших та виступає вагомим чинником ефективного економічного розвитку. Саме тому в сучасній юридичній науці є чимало серьозних праць українських і російських учених, які розкривають сутність та правовий статус, висвітлюють напрямки використання розляданих об'єктів. Серед авторів можна назвати: П.П. Крайнєва, В.Г. Зинова, О.А. Підопригору, О.І. Мельниченка, І.І. Дахна, С.І. Карпухіну, Ю.І. Капіцу, М.К. Галянтича та ін. Але, незважаючи на певні позитивні зрушення, питання надійної правової охорони комерційної таємниці та ноу-хау ще потребують подальшого вдосконалення, що й виступає метою написання даної статті.

Звернення до розгляду правових колізій і прогалин охорони й захисту комерційної таємниці та ноу-хау в рамках дослідження проблеми забезпечення охорони й захисту інформації зумовлено тим, що згадані об'єкти є специфічним за своїм правовим статусом видом інформації, що випливає як зі змісту закону, так і з усталеної юридичної термінології, і саме через специфіку свого закріплення і законодавчого регулювання потребують подальшої законодавчої ініціативи для створення надійної та ефективної системи їх охорони й захисту.

Тому в даній статті ми пропонуємо через призму визначення термінів „охорона прав інтелектуальної власності" та „захист прав інтелектуальної власності" простежити, чи можливо здійснювати охорону й захист комерційної таємниці та ноу-хау в традиційному розумінні наведених понять, і саме таким чином визначити найбільш оптимальні правові й організаційні заходи охорони й захисту розгляданих об'єктів.

Відповідно до ст. 505 Цивільного кодексу України „комерційною таємницею є *інформація* (курсив наш – Н.Д.), яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію" [1, 164].

Згідно з п. 2.5 Інструкції Міністерства статистики України № 168 від 06.07.1995 р. „Про порядок заповнення звіту про продаж за кордон ліцензій на об'єкти інтелектуальної власності", „ноу-хау – це конфіденційна *інформація* (курсив наш – Н.Д.) технічного, економічного, адміністративного, фінансового характеру, яка є власністю продавця та не є доступною будь-якій особі при використанні патента або в результаті простого виявлення".

Але на відміну від комерційної таємниці ноу-хау не отримало належного законодавчого закріплення, зокрема воно не визнано об'єктом права інтелектуальної власності в Цивільному кодексі України, хоча надійно закріпилось у діловому вжитку як у світовій, так і в національній практиці. У юридичній літературі ще й досі триває правова дискусія щодо визначення терміна „ноу-хау" і його співвіднесення з терміном

„комерційна таємниця". Не вдаючись до розкриття її змісту, зазначимо лише, що в цілому існує три позиції з цього приводу: 1) наведені категорії тотожні; 2) ноу-хау – особливий вид комерційної таємниці; 3) це не співвідносні категорії.

Разом із тим, відсутні норми про ноу-хау й у світовій практиці, так само як і загальновизнане визначення цього явища. Саме тому доцільно навести думку з цього приводу Р.Л. Наришкіної, яка визначала, що „інформація ноу-хау різноманітна за своїм змістом. Сюди можуть входити винаходи (у тому числі патентноздатні, на які з будь-яких причин не було одержано патент) і науково-технічна інформація, яка не є винаходом, але без володіння якою не може бути налагоджено виробництво. Сюди також відносять інформацію нетехнологічного характеру, яка стосується економіки й організації виробництва, методів реклами, питань фінансування тощо". У зв'язку з цим вона вказувала, що сформулювати точне та вичерпне визначення ноу-хау не тільки важко, а й не потрібно, оскільки „будь-яке визначення тут буде недостатньо, воно неодмінно буде неточним і не відобразить самої суті ноу-хау" [2, 90].

Беручи до уваги роль ноу-хау, яку воно відіграє в торгівлі об'єктами інтелектуальної власності, передачі технологій, воно повинно, на нашу думку, одержати статус об'єкта права інтелектуальної власності і в Цивільному кодексі України доцільно навести найбільш повний перелік відомостей, які становлять ноу-хау, що сприятиме реалізації цілей охорони й захисту даної правової категорії. Оскільки в проекті ЦК вже була спроба визнати ноу-хау об'єктом інтелектуальної власності, для зручності ми будемо його розглядати саме в такому ракурсі.

Так, до ноу-хау можна віднести такі відомості:

1) технологічні секрети**,** які не вдається розкрити аналізом товарів, доступних на вільному ринку, наприклад: критерії вибору найкращої основної (а іноді й допоміжної) сировини; конкретні склади сировини; склади основ купажних вин і багатьох слабо- і безалкогольних напоїв; склади промислових електролітів; оптимальні режими обробки сировини напівфабрикатів; критерії вибору й показники якості найкращих знарядь праці (особливо - інструментів і технологічного оснащення) та оптимальні прийоми їх використання; повна й точна інформація про промислові продукти й технології їх виробництва, прихована в комплектній технічній документації; бази знань, бази даних, логічні та/або математичні алгоритми й складені на їх основі програми для обчислювальних машин, зокрема: алгоритми й програми керування технологічними процесами, бази знань, алгоритми та програмні комплекси автоматизованого проектування об'єктів техніки;

2) особистий професійний досвід працівників промисловості, сільского господарства й охорони здоров'я, який зазвичай передають „із рук у руки" і який все частіше намагаються фіксувати у вигляді так званих „експертних систем", а саме: навички високоефективного виконання будь-яких технологічних операцій у будь-яких галузях народного господарства, досвід діагностики, профілактики та лікування людей і тварин;

3) також до ноу-хау тимчасово можуть бути віднесені відомості про сутність патентоспроможних винаходів, корисних моделей, промислових зразків і топографій інтегральних мікросхем – до першої офіційної публікації; техніко-економічні показники ефективності незапатентованих технологічних процесів – до початку переговорів про продаж ліцензій на ноу-хау.

Беручи до уваги той факт, що в юридичній літературі вже отримали правове визначення такі категорії, як правова охорона та захист прав, ми не будемо зупинятися на розгляді відмінностей цих понять, а лише наведемо їх визначення щодо об'єктів інтелектуальної власності з метою розкриття теми даної статті.

Так, правова охорона об'єктів інтелектуальної власності визначається як діяльність органів державного управління, що врегульована нормами права та спрямована на ідентифікацію, визнання, реєстрацію та видачу охоронного документа на об'єкт інтелектуальної власності, а також на забезпечення організаційно-правового режиму його правомірного використання.

Правова охорона за своєю суттю є системою спеціальних процедур, що спрямовані на дослідження відповідності певного об'єкта його законодавчо закріпленим критеріям та

ознакам, яким повинен відповідати охороноздатний об'єкт інтелектуальної власності. Правова охорона у звичайному розумінні настає після одержання спеціального охоронного документа [2, 24].

Із співвідношення наведеного визначення з комерційною таємницею та ноу-хау стає зрозумілим, що в даному випадку ці об'єкти права інтелектуальної власності не можуть отримати охоронний документ саме через свій секретний характер, тобто охорона даних об'єктів обмежується лише організаційно-правовим режимом їх використання.

У свою чергу, захист прав інтелектуальної власності – це передбачена законодавством діяльність відповідних державних органів із визнання, поновлення прав, а також усунення перешкод, що заважають реалізації прав і законних інтересів суб'єктів права у сфері інтелектуальної власності. Отже, захист прав на об'єкти інтелектуальної власності містить три елементи: 1) визнання оспорюваного права; 2) поновлення порушеного права й охоронюваного інтересу; 3) припинення правопорушень. Поновлення порушеного права та усунення перешкод в реалізації прав інтелектуальної власності передбачає, серед іншого, і застосування до правопорушників передбачених законом заходів юридичної відповідальності [2, 24].

Тому стає очевидною необхідність проаналізувати заходи юридичної відповідальності, які передбачені за порушення прав на комерційну таємницю та ноу-хау.

Адміністративну відповідальність передбачено ст. 164-3 Кодексу України про адміністративні правопорушення (КУпАП) за недобросовісну конкуренцію, зокрема в ч. 3 об'єктивна сторона даного правопорушення полягає в отриманні, використанні, розголошенні комерційної таємниці, а також конфіденціальної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця. Скоєння даного правопорушення тягне за собою накладення штрафу від дев'яти до вісімнадцяти неоподатковуваних мінімумів доходів громадян. Суб'єктом, уповноваженим складати протокол за цією статтею, є органи внутрішніх справ (ст. 255 КУпАП), а розглядати дану категорію справ – суди (ст. 221 КУпАП).

На нашу думку, включення обов'язковою факультативною ознакою мети заподіяння шкоди є не зовсім коректним формулюванням, оскільки найчастіше отримання та використання комерційної інформації відбувається не стільки з метою заподіяння збитків контрагенту, скільки з метою власного збагачення, отримання певних переваг у підприємницькій діяльності, що може призвести до завдання певних збитків конкурентові. Також доцільніше, на нашу думку, вести мову про заподіяння шкоди не майну іншого підприємця, а його майновим інтересам, оскільки це поняття значно ширше й надає можливість включити також і упущену вигоду, що найбільш важливо для кваліфікації дій як недобросовісної конкуренції.

Зміст ст. 164-3 КУпАП, а також Закону України „Про інформацію" не дозволяє віднести ноу-хау до конфіденційної інформації, тобто застосовувати дану статтю можна тільки до відносин із комерційною таємницею.

Ураховуючи наведене, вважаємо за необхідне викласти ч. 3 ст. 164-3 КУпАП у такій редакції: „Отримання, використання, розголошення комерційної таємниці, відомостей, які стосуються ноу-хау, а також конфіденційної інформації, що заподіяло шкоду діловій репутації або майновим інтересам підприємця".

Спеціальним нормативним актом щодо захисту комерційної таємниці виступає Закон України „Про захист від недобросовісної конкуренції" [4], який у главі 4 передбачає відповідальність за такі дії: неправомірне збирання комерційної таємниці, розголошення комерційної таємниці, схилення до розголошення комерційної таємниці, неправомірне використання комерційної таємниці. Незважаючи на положення ст. 2 Закону, де зазначено, що „закон застосовується до відносин, у яких беруть участь господарюючі суб'єкти (підприємці), їх об'єднання, а також органи державної влади, громадяни, юридичні особи та їх об'єднання, що не є господарюючими суб'єктами (підприємцями)", штрафи, передбачені главою 5 Закону, не накладаються на фізичних осіб і фізичних осіб - підприємців, оскільки останні несуть адміністративну відповідальність згідно з положенням Кодексу про адміністративні правопорушення. Вчинення дій, визначених

цим Законом як недобросовісна конкуренція, тягне за собою накладення Антимонопольним комітетом України штрафів, на розмір яких варто звернути увагу, оскільки він перевищує навіть розміри штрафу, передбачені Кримінальним кодексом України за незаконні дії з комерційною таємницею.

Так, ст. 21 Закону „Про захист від недобросовісної конкуренції" передбачено можливість накладення штрафів Антимонопольним комітетом України на господарюючих суб'єктів – юридичних осіб та їх об'єднання до п'яти тисяч неоподатковуваних мінімумів доходів громадян; на юридичних осіб, їх об'єднання та об'єднання громадян, що не є господарюючими суб'єктами, – до двох тисяч неоподатковуваних мінімумів доходів громадян, тимчасом як фізичні особи несуть відповідальність за ст. 164-3 КУпАП, де передбачено відповідальність у вигляді штрафу від дев'яти до вісімнадцяти неоподатковуваних мінімумів доходів громадян.

Аналогічним чином постає питання про відповідність штрафів, що накладаються Антимонопольним комітетом у порядку застосування Закону „Про захист від недобросовісної конкуренції", та судами в результаті притягнення до кримінальної відповідальності, оскільки Кримінальним кодексом України за незаконні дії з комерційною таємницею альтернативним покаранням передбачений штраф у розмірі від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян за ст. 232 КК та в розмірі від двохсот до тисячі неоподатковуваних мінімумів доходів громадян за ст. 231 КК.

Значною перешкодою в належному правовому захисті комерційної таємниці є її визначення, сформульоване в Цивільному кодексу в тій частині, що вимога закону про повну невідомість такої інформації третім особам значно ускладнює процес доказування в справах даної категорії. В цій частині до законодавства України було запозичине визначення нерозкритої інформації, яке міститься в Угоді TRIPS, але внаслідок неточного тлумачення визначення нерозкритої інформації як такої, що не є загальновідомою, було перекладено як „цілком невідома інформація", внаслідок чого потрібно внесення відповідних уточнень до Цивільного кодексу України.

Варто звернути увагу на дослідження, що були проведені за допомогою опитування співробітників найбільших російських компаній про шляхи розголошення комерційної таємниці. Так, серед причин її розголошення були виокремлені такі:

1. Балакучість працівників, особливо пов'язана з уживанням алкоголю і спілкуванням у дружніх компаніях, — 32%.

2. Прагнення працівників заробити гроші в будь-який спосіб за принципом «гроші не пахнуть» — 24%.

3. Відсутність служби безпеки фірми — 14%.

4. «Радянська» звичка персоналу ділитися досвідом, давати поради — 12%.

5. Безконтрольне використання інформаційних і копіювальних засобів на фірмі — 10%.

6. Психологічні конфлікти між працівниками, між працівниками й керівництвом — 8%.

Тобто перше місце посідає так зване ненавмисне розголошення комерційної таємниці, відповідальності за яке не передбачено Кримінальним кодексом України, оскільки суб'єктивна сторона правопорушення передбачає наявність умислу в діях винної особи. Хоча в коментарі до ст. 164-3 КУпАП ідеться про можливість скоєння даного правопорушення у формі необережності, однак це суперечить формулюванню самої статті, оскільки обов'язковою ознакою суб'єктивної сторони правопорушення, як це вже зазначалося раніше, є наявність певної мети – заподіяння шкоди діловій репутації або майну іншого підприємця, яка цілком логічно не може бути досягнена через необережність.

Тобто в законодавстві України не передбачено юридичної відповідальності за розголошення комерційної таємниці внаслідок відсутності в особи здатності „тримати язик за зубами", що вимагає від власників підприємства та заінтересованих осіб ужиття додаткових організаційно-правових заходів щодо збереження комерційної таємниці на підприємстві. Це можливо здійснити шляхом підписання з працівником договору про конфіденцій-

ність, де передбачити можливість накладення певних економічних санкцій, розмір яких установлюється роботодавцем, за невміння зберігати секрети, що послужить певним організуючим чинником у формуванні необхідних професійних якостей у працівників.

Привертає увагу відсутність у Кримінальному кодексі норми, яка б передбачала відповідальність за незаконні дії з ноу-хау, тобто даний специфічний вид інформації захищається тільки нормами цивільного права, а тому також потребує свого вдосконалення.

На нашу думку, доцільно передбачити в ЦК нарівні з ліцензійним договором також вимоги щодо укладення договору **про передачу "ноу-хау"**. Хоча цей вид договорів у цивільному законодавстві не згадується й порядок їх укладання не регулюється, на практиці він використовується доволі часто, що, у свою чергу, підтверджує доцільність його законодавчого врегулювання.

У договорі про передачу „ноу-хау" повинні бути узгоджені умови про предмет (яка інформація передається), строки передачі, розмір винагороди, умови про право на подальшу передачу та збереження конфіденційності, а також заходи відповідальності. Ліцензійний договір про передачу „ноу-хау" відрізняється від патентної ліцензії і за своєю правовою основою, і за об'єктом відчужуваних прав. В основі надання права використання „ноу-хау" лежить не виключне право, а фактична монополія на об'єкт угоди. „Ноу-хау" на відміну від запатентованого винаходу, не можна використовувати, не отримавши його від ліцензіара. Наслідком цього є необхідність не тільки надання за договором права використання, але й передачі самого „ноу-хау" в повному обсязі. „Ноу-хау" можуть бути передані як у матеріальній формі (у вигляді різного роду документації, зразків тощо), так і в нематеріальній формі (у вигляді надання технічної допомоги, навчання, управлінських послуг). Як правило, інформація передається у формі документів (технічні описи, формули, методики тощо). На додаток до них можливою є також передача дослідних зразків виробів. Інколи договори про передачу „ноу-хау" передбачають, що сторона, яка передає, зобов'язана надавати іншій стороні допомогу в налагоджуванні виробництва з використання „ноу-хау". Що ж до розміру і строків виплати винагороди, то тут можуть застосовуватися дві системи – одноразова виплата визначеної договором суми або відсоткові відрахування від обсягів виробленої продукції чи обсягів продажів.

У договорі на передачу „ноу-хау" вкрай важливо вирішити питання, чи зберігає „продавець інформації" право використовувати (продовжувати використовувати) її у власній діяльності або у власному виробництві, а також чи вправі обидві сторони укладати в майбутньому договори на передачу цієї ж інформації іншим особам. Перша умова є цілком допустимою. Друга ж здебільшого забороняється, оскільки, набувши значне поширення, інформація автоматично втрачає статус „ноу-хау". Більше того, учасники договору приймають на себе досить жорсткі зобов'язання зі збереження переданої інформації в таємниці та захисту її від незаконного доступу. Порушення умови про конфіденційність зазвичай дає потерпілій стороні право на одностороннє розірвання договору (це повинно бути прямо передбачено договором) і на відшкодування збитків, включаючи упущену вигоду. У договорі обов'язок відшкодувати збитки може бути замінений обов'язком виплатити компенсацію у фіксованій сумі.

Отже, аналіз наявного стану охорони й захисту комерційної таємниці та ноу-хау виявив такі особливості: 1) даний вид інформації є найбільш уразливим у плані охорони, оскільки неможливо отримати документ, що підтверджує монопольне володіння ним унаслідок об'єктивної природи цих об'єктів, тому їх охорона полягає в прийнятті відповідних організаційно-правових заходів самим власником інформації; 2) чинне законодавство України містить значні прогалини стосовно правового захисту комерційної таємниці за повної відсутності такої для ноу-хау, що дозволяє запропонувати наступні заходи.

1. Доповнити Цивільний кодекс України: віднести до об'єктів інтелектуальної власності ноу-хау, надавши перелік відомостей, які можуть вважатися ноу-хау, законодавчо передбачити такий вид ліцензійного договору, як договор на передачу ноу-хау, установивши вимоги щодо його змісту та порядку укладення.

2. З метою ефективної охорони комерційної таємниці та ноу-хау в адміністративному порядку внести зміни до ч. 3 ст. 164-3 КУпАП, виклавши її в такій редакції: „Отримання, використання, розголошення комерційної таємниці, відомостей, які стосуються ноу-хау, а також конфіденційної інформації, що заподіяло шкоду діловій репутації або майновим інтересам підприємця”.

3. Беручи до уваги, що розголошення комерційної таємниці відбувається працівниками здебільшого ненавмисно, так би мовити, через надмірну балакучість, вважаємо за необхідне керівництву підприємств або інших організацій, де в процесі діяльності використовується комерційна таємниця, запровадити практику підписання з працівниками договору про конфіденційність, де додатковою умовою передбачити можливість накладення економічних санкцій за ненавмисне розголошення комерційної таємниці, яка сталася внаслідок необережних дій працівника.

4. Внести уточнення щодо визначення комерційної таємниці, визначивши останню не як узагалі невідому, а як таку, котра не є загальновідомою, що має принципове значення при доказуванні в справах про порушення прав на комерційну таємницю.

Література

1. Цивільний кодекс України: Офіційне видання. – К.: Атіка, 2003. – 479 с;
2. Нарышкина Р.Л. Договор, патент и деликт в гражданском праве США в условиях государственно-монополистического капитализма: Автореф. дисс. д-ра юрид. наук. – М., 1974. – 382 с;
3. Галянтич М. Актуальні питання охорони та захисту прав на об’єкти промислової власності // Юридична Україна. – 2003. – № 3. – С. 22-33;
4. Закон України № 236/96-ВР від 7 червня 1996 р. „Про захист від недобросовісної конкуренції” // Відомості Верховної Ради України – 1996. – № 36. – Ст. 164.

УДК 004.056

Ахромкин Е.М., Гулик Б.И.

ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ (АВТОРСКОГО ПРАВА) В КОМПЬЮТЕРНЫХ СЕТЯХ

В статье рассмотрены правовые аспекты защиты интеллектуальной собственности (авторского права) в компьютерных сетях в соответствии с законодательством Украины.

Постановка проблемы

В настоящее время активно идет процесс наполнения компьютерных сетей информационными материалами (сайты, Web-страницы и т.п.). Количество объектов интеллектуальной собственности, используемое при этом, очень велико. Отсюда выплывает практическая необходимость уделять значительное внимание вопросам защиты интеллектуальной собственности. Особую актуальность эти вопросы приобретают с учетом присоединения Украины к Всемирной торговой организации и возможного вступления в ЕС.

Анализ последних достижений и публикаций

Интеллектуальная собственность (англ. Intellectual property) - означает закрепленные законом права на результат интеллектуальной деятельности в промышленной, научной, художественной, производственной и других сферах. Различаются следующие объекты интеллектуальной собственности: объекты промышленной собственности; товарные знаки и марки, изобретения, модели, промышленные образцы; объекты авторского права; письменная (рукопись, машинопись, нотная запись и т.д.) и устная (публичное произнесение, публичное исполнение и т.п.), звуко – и видеозапись (механическая, магнитная, цифровая, оптическая и др.), изображение (рисунок, эскиз, картина, план, чертеж, кино-, теле-, видео – или фотокадр и пр.), объемно-пространственная форма произведения (скульптура, модель, макет, сооружение и т.д.), другие формы (программы ЭВМ и базы данных, топологии интегральных микросхем). Для защиты интеллектуальной собственности (информационных ресурсов) в компьютерных сетях можно использовать программные, техниче-

ские, организационные и правовые методы. Вопросы применения и использования таких методов рассмотрены, например, в работах [1-4]. Права интеллектуальной собственности в Украине защищают следующие законы: "Про авторське право і суміжні права"; "Про охорону прав на знаки для товарів і послуг"; "Про охорону прав на промислові зразки"; "Про охорону прав на винаходи і корисні моделі"; "Про охорону прав на зазначення походження товарів"; "Про охорону прав на сорти рослин"; "Про охорону прав на топографії інтегральних мікросхем"; "Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних"; "Про особливості державного регулювання діяльності суб`єктів господарювання, пов'язаної з виробництвом, експортом, імпортом дисків для лазерних систем зчитування"; "Про племінну справу у тваринництві"; "Про науково-технічну інформацію"; "Про лікарські засоби". Следует отметить также Указ Президента Украины от 31.07.2000 г. № 928/2000 “О мероприятиях по развитию национальной составляющей глобальной информационной Сети и обеспечение широкого доступа к этой сети в Украине”. Информация об этих законах и указах расположена на сайте Департамента интеллектуальной собственности www.sdip.gov.ba.

Кроме того, при решении вопросов о защите интеллектуальной собственности в случае необходимости применяются международные договора в сфере интеллектуальной собственности, согласие на обязательность которых предоставлено Украиной. Развитием и защитой интеллектуальной собственности на международном уровне занимается Всемирная организация интеллектуальной собственности (ВОИС), основанная при ООН в 1976 году.

Формулировка целей статьи

Целью данной статьи является знакомство пользователя Сетью с основными положениями защиты интеллектуальной собственности (авторского права).

Изложение основного материала

При размещении материалов в Сети необходимо следить за выполнением двух условий: во-первых, строго контролировать и защищать права своей интеллектуальной собственности; во-вторых, не нарушать авторские права других лиц. Следует иметь в виду, что компьютерные программы (независимо от способа или формы их выражения) охраняются как литературные произведения [5].

Авторское право на материалы, размещенные в Сети, возникает вследствие их создания и не требует дополнительной регистрации. Однако, можно оснастить объекты, требующие защиты, сообщением об авторском праве. Это сообщение должно содержать 3 элемента: символ ©; имя собственника авторского права; год первой публикации. В Сети встречаются и более обширные сообщения об авторском праве [5].

Действует авторское право в течение жизни автора и 70 лет после его смерти, а не имущественное право - бессрочно. Заметим, что статья 51-2 Кодекса об административных правонарушениях и статья 176 Криминального кодекса Украины предусматривают ответственность за нарушение авторского права и смежных прав. Поэтому, если при создании программ вы собираетесь использовать материал, защищенный авторским правом, необходимо получить соответствующее разрешение. Разрешение на использование текста получают у собственника авторского права, разрешение на использование фотографий – у собственника права и, возможно, у всех особ, изображенных на этой фотографии, разрешение на использование кадров из кино- или видеофильма запрашивается не только у собственника, но и у ассоциации актеров, авторов сценария, режиссеров, продюсера, а также у всех особ, чей голос или изображение присутствует на данных кадрах.

В некоторых случаях Законом предусмотрено использование объектов интеллектуальной собственности без согласия автора. Допускается (с обязательным указанием имени автора и источника заимствования): 1) использование цитат в объеме, оправданном поставленной целью, в том числе цитат в форме коротких отрывков из выступлений и произведений, включенных в фонограммы (видеограммы) или программы вещания; 2) использование литературных и художественных произведений в объеме, оправданном поставленной целью, как иллюстраций в материалах учебного характера; 3) публичное оглашение

предварительно опубликованных в газетах или журналах статей из текущих экономических, политических, религиозных и социальных вопросов или публично извещенных произведений такого же самого характера в случаях, когда право на такое воссоздание, публичное оглашение или другое публичное сообщение специально не запрещено автором; 4) воссоздание в каталогах произведений, выставленных на доступных публике выставках, аукционах, ярмарках или в коллекциях для освещения отмеченных мероприятий, без использования этих каталогов в коммерческих целях; 5) воссоздание произведений для судебного и административного осуществления в объеме, оправданном этой целью; 6) воссоздание с информационной целью публично произнесенных речей, обращений, докладов и других подобных произведений в объеме, оправданном поставленной целью;

Без согласия автора, лицо, правомерно владеющее компьютерной программой, может: внести в программу изменения (модификации) с целью обеспечения ее функционирования на технических средствах лица, а также исправить явные ошибки; изготовить одну копию компьютерной программы при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра; декомпилировать компьютерную программу с целью получения информации, необходимой для достижения ее взаимодействия с независимо разработанной компьютерной программой.

Законом определено понятие "служебное произведение" - произведение, созданное автором в порядке выполнения служебных обязанностей соответственно служебному заданию или трудовому договору (контракту) между ним и работодателем. В этом случае (если не оговорено иное в договоре), личное неимущественное право остается за автором, а имущественное право на служебное произведение принадлежит работодателю. То есть работодатель имеет исключительное право на использование служебного произведения (копирование, распространение, перевод и т.п.).

В заключение отметим, что объектом авторского права не являются: 1) сообщения о новостях дня или текущих событиях; 2) произведения народного творчества (фольклор); 3) официальные документы политического, законодательного, административного характера (законы, указы, постановления, судебные решения, государственные стандарты и тому подобное) и их официальные переводы; 4) государственные символы Украины, государственные награды; символы и знаки органов государственной власти, Вооруженных Сил Украины и других военных формирований; 5) символика территориальных общин; символы и знаки предприятий, учреждений и организаций; 6) денежные знаки; 7) расписания движения транспортных средств, расписания телерадиопередач, телефонные справочники и другие аналогичные базы данных.

Литература

1. Конахович Г.Ф. и др. Защита информации в телекоммункационных системах - К.: "МК-Пресс", 2005. – 288 с;
2. Хорошко В.А., Чекатов А.А. Методы и средства защиты информации - К.: Юниор, 2003 – 504 с;
3. За ред. М.Я. Швеця, Р.А. Калюжного. Інформатизація управління соціальними системами (організаційно-правові питання теорії і практики). Навч.посіб. - К.: МАУП, 2003 – 250 с;
4. Задірака В.К, О.С. Олексюк. Методи захисту фінансової інформації – К.: Вища школа, 2000 – 460 с;
5. Закон України "Про авторське право і суміжні права", №2627-III від 11 липня 2001 року.

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ЭНЕРГЕТИКИ, ПРОМЫШЛЕННОСТИ, ТРАНСПОРТА

УДК 676.163.022

Нечаев Г.И., Камель Г.И., Яковлева А.Г.

АВТОМАТИЗАЦИЯ КОНТРОЛЯ И РЕГУЛИРОВАНИЯ ПРОЦЕССА ЗАГРУЗКИ И ВАРКИ В УСТАНОВКАХ СИСТЕМЫ КАМЮР

В работе приведена схема автоматизации контроля процессом варки целлюлозы на установке типа Камюр. Приведены элементы управления процессом непрерывной варки с помощью ЭВМ. Рис. 1. Ист. 1.

Автоматизация контроля и регулирования процесса непрерывной варки целлюлозы в установках Камюр на разных стадиях эксплуатации влияет на надежность, срок службы оборудования и качество получаемой целлюлозы. Анализ литературных источников показал, что на разных предприятиях эти проблемы решаются по-разному.

Целью данной статьи является решение следующих задач: описать схему автоматизации и управления процессом варки целлюлозы, привести перечень конкретных технологических схем контроля, которые используются в установках; конкретно назвать приборы и оснастку, которая используется при автоматизации контроля и регулирования процесса варки: описать управления и регулирования процесса варки; описать управления процессом варки в варочном котле, которые обеспечивают поддержание заданных условий и необходимых температурных графиков.

Установка непрерывной варки оснащена контрольно-измерительными и регулирующими приборами, позволяющими вести управление технологическим процессом варки автоматически. Для контроля варочного процесса на щите пульта управления, находящегося в варочном цехе, нанесена мнемосхема и смонтированы все основные контрольно-измерительные и регулирующие приборы, технологическая и аварийная сигнализация, ключи дистанционного управления, пусковые кнопки и амперметры электродвигателей.

Постоянство дозирования щепы регулируется частотой вращения ротора дозатора через вариатор, приводимый в движение от электродвигателя. Давление в пропарочной камере измеряется манометром. Необходимое давление в камере поддерживается с помощью регулятора, который открывает доступ в камеру свежего пара низкого давления в тех случаях, когда паров вскипания оказывается недостаточно. Уровень щепы в питательной трубе измеряется уровнемером. Положение регулирующего вентиля может переключаться с одного положения в другое с помощью автоматического или ручного управления. Объем белого щелока измеряется магнитным расходомером. Замер преобразуется в пневматическое давление 0,02-0,1 МПа и регистрируется самописцем с редукционным клапаном и переключателем для регулятора. Ручное регулирование на автоматическое и обратно переключается по специальной инструкции. Объем щелока в линии циркуляции высокого давления измеряется трубкой Вентури. На щите управления устанавливают показывающий расходомер.

Объем варочного циркулирующего щелока измеряется трубкой Вентури. На щите находится только показывающий расходомер. Объем щелока, подаваемого в варочный котел, измеряют ручным регулированием вентилей, расположенных на установке. Объем черного щелока измеряют трубкой Вентури. Поступление черного щелока регулируется находящимися на щите пульта управления измерительными приборами, редукционным клапаном с пневматическим переключателем. Управляют регулятором в соответствии с инструкцией.

Выдувным вентилем управляют при помощи редукционного клапана, установленного на щите пульта управления. Там же расположен и прибор, показывающий положение вентиля.

Температура щелока в варочной циркуляции измеряется при помощи передатчика температуры, имеющего капиллярный датчик, заполненный ртутью. Регулятор температуры и самопишущий регистрирующий прибор расположены на щите пульта управления. Управление регулятором и переключение с ручного на автоматическое управление и обратно осуществляется в соответствии со специальной инструкцией. Прибор на щите пульта управления регистрирует замеренное значение и показывает установочное значение и положение вентиля.

Давление в варочном котле измеряется автоматическим передатчиком давления и записывается на самописце, расположенном на щите пульта управления. Установленный на щите регулятор управляет объемом подаваемого черного щелока в нижнюю часть котла. Концентрация массы в концентраторе измеряется по мощности, расходуемой смесительным насосом. В качестве передатчика применяется преобразователь электрического тока, выходное напряжение его преобразуется в пневматический сигнал давления.

Управление всеми электродвигателями сосредоточено на щите пульта управления. На мнемонической схеме технологического процесса каждый электродвигатель условно обозначается двумя сигнальными лампочками: зеленый зажигается, когда двигатель в работе; красный - когда он не работает. Кроме того, электродвигатели и пускатели на мнемосхеме обозначены порядковыми номерами.

На щите пульта управления под защитным стеклом расположена кнопка аварийного останова оборудования, а также система аварийной сигнализации от винта пропарочной камеры, питателя высокого давления, винта загрузочного устройства, выдувных трубопроводов, трубопровода белого щелока, уровнемера черного щелока, а также сигнализации уровня щепы в котле, давления в котле, давления пара высокого и низкого давления на трубопроводе и давления сжатого воздуха. При включении аварийной сигнализации подается звуковой сигнал и зажигается мигающая желтая лампочка, которая горит до ликвидации аварийного состояния. На щите пульта управления располагаются также блокировочные переключатели, предупреждающие возможность включения в работу насосов варочного цеха в неправильном порядке. Предусмотрены две самостоятельные блокировочные системы: первая для блокирования работы питателя низкого давления и дозатора щепы, вторая синхронизирует работу винта загрузочного устройства, насоса питательной циркуляции высокого давления, винта пропарочной камеры и дозатора щепы. Когда переключатели блокировочной системы находятся в положении "сблокировано", пуск электродвигателей возможен только в указанном порядке.

На рис. 1. показана схема расположения измерительных и регулирующих приборов в однопоточной установке непрерывной варки типа Камюр.

- Давление пара в пропарочной камере поддерживается регулятором Р1, регулирующим выпуск парогазовой смеси из камеры воздействием на регулирующий клапан 7, расположенный на трубопроводе для отвода парогазовой смеси, и регулятором давления, воздействующим на регулирующий клапан 2 в том случае, если давление сдувочных газов недостаточно для осуществления процесса пропарки.

- Уровень варочного щелока в питательной трубе регулируется уровнемером У2, воздействующим на регулирующий клапан 3.

- Температура в верхней части котла регистрируется термометром Т1, установленным на линии верхней питательной циркуляции, подающей в варочный аппарат смесь щелока со щепой.

- Уровень щелока в резервуаре постоянного уровня поддерживается регулятором У2, воздействующим на регулирующий клапан 4.

- Расходомер Q1 указывает на расход щелока в верхней питательной циркуляции, а также на состояние чистоты сит загрузочного устройства варочного котла.

- Терморегуляторы ТР1 и ТР2 регулируют температуру варочного щелока, циркулирующего в двух зонах варки, воздействуя на регулирующие клапаны 5 и 6.

- Температура варочного щелока в соответствующей зоне варки регистрируется термометрами Т1 и Т3. Объем циркулирующего щелока замеряется расходомерами Q1 и Q2.

- Уровень жидкости в конденсационных горшках поддерживается регуляторами уровнями У3 и У4, воздействующими на регулирующие клапаны 7 и 8.

- Необходимое давление в варочном котле поддерживается регулятором давления Рз, регулирующим подачу черного щелока воздействием на регулирующий клапан 9. Объем подаваемого в котел черного щелока регулируется расходомером Q4, воздействующими на регулирующий клапан 10.

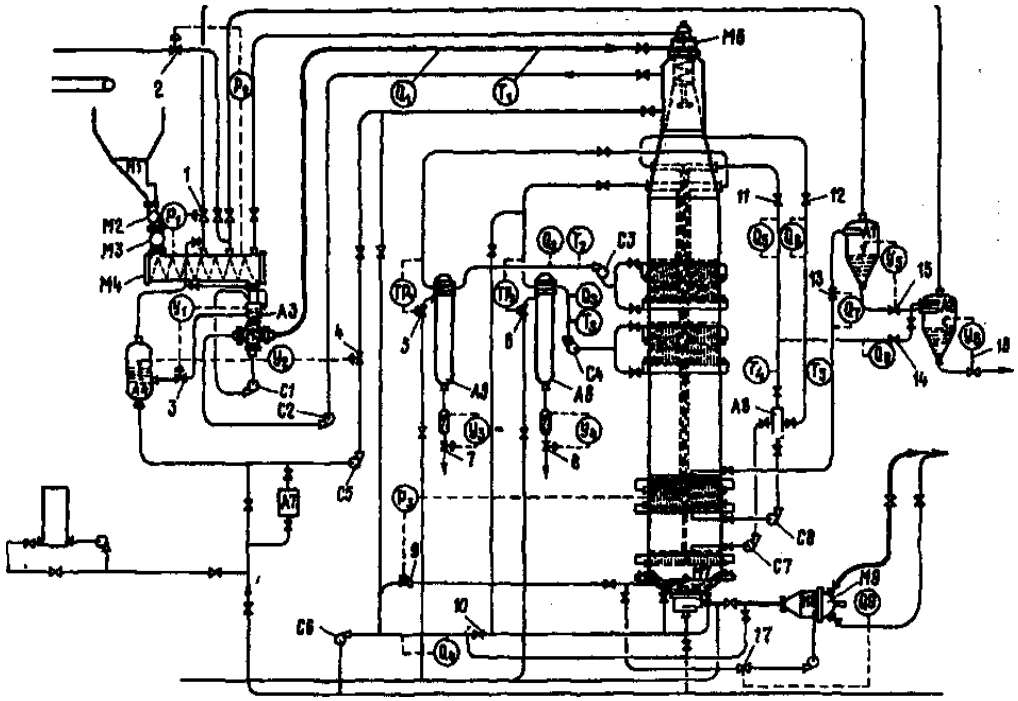


Рис. 1. Схема автоматизации контроля и управления процессом варки на установке типа Камюр.

- Объем циркулирующего варочного щелока в зоне диффузионной промывки регулируется расходомерами Q5 и Q6, воздействующими на регулирующие клапаны 11 и 12. Температура щелока регистрируется термометрами Т4 и Т5.

- Объем щелока, отбираемого из варочного котла в расширительный резервуар (циклоны-испарители), регулируется расходомерами Q? и Qs, воздействующими на регулирующие клапаны 13 и 14.

- Уровень щелока в расширительном резервуаре (циклонах-испарителях) поддерживается регуляторами У5 и У6, воздействующими на регулирующие клапаны 15 и 16.

- Концентрация массы в концентраторе регулируется объемом отбираемого черного щелока через расходомер Q9 при воздействии на регулирующий клапан 17.

Процессом варки управляет оператор (старший варщик), который включает и выключает кнопки на щите пульта управления.

Управление процессом непрерывной варки при помощи ЭВМ.

В режимах изменения производительности установки и вида вырабатываемой продукции очень сложно обеспечивать стабильность технологического процесса, минимальное снижение качественных показателей конечного продукта, особенно степени его делигнификации, а также увеличение выхода продукции, получение оптимальной крепости черного щелока, отбираемого на регенерацию химикатом, и другие параметры, независимо от субъективных особенностей оператора (старшего варщика), осуществляющего контроль и регулирование варочного процесса. Сейчас широко используются автоматизированные системы управления процессом варки с применением электронно-вычислительных

машин, исключающих субъективное влияние оператора (старшего варщика) на ход процесса.

Система регулирования подачи щепы в установку измеряет частоту вращения ротора дозатора и настраивает ее таким образом, чтобы была обеспечена заданная производительность установки и установленная продолжительность нахождения щепы в котле. Нагрузка на привод питателя низкого давления служит индикатором объема подаваемой в котел щепы. Другая система регулирует расход варочного щелока в зависимости от объема подаваемой щепы, поддерживая заданное соотношение активной щелочи и загруженной щепы. Эта система стабилизирует процесс варки и способствует достижению требуемой степени делигнификации при минимальном избытке щелочи.

Температура и скорость прохождения промывного щелока зависят от расхода отбираемого щелока. Для того, чтобы управлять этими параметрами раздельно, применяют дополнительную линию циркуляции массы из выдувной линии обратно в зону охлаждения. Система управления выдувкой массы обеспечивает постоянство ее концентрации в выдувной линии. Расход в этой линии задается в зависимости от требуемой производительности установки. Оператор (старший варщик) вводит в ЭВМ значения отношения объемного расхода массы в минуту к суточной производительности установки.

Система регулирования уровня щепы в верхней части варочного котла поддерживает постоянный уровень щепы, чтобы обеспечить стабильную скорость ее продвижения в нижнюю часть котла и, следовательно, требуемую длительность пребывания щепы в варочной зоне. Уровень щепы в котле вычисляется по нагрузке на привод винта сепаратора загрузочного устройства и показателям сигнализирующей аппаратуры. Частота вращения винта используется в качестве первичного регулируемого параметра, воздействующего на уровень концентрации массы в выдувной линии.

Плавное изменение производительности установки осуществляется таким образом, чтобы в переходном режиме степень делигнификации целлюлозы не изменилась.

В соответствии с уравнениями математической модели вначале находятся и задаются изменения в зонах варки, определяющих завершение процесса варки при изменении ее продолжительности, а затем изменения в объемах подаваемой щепы, варочного щелока и других составляющих. В случае необходимости немедленного изменения производительности установки все указанные выше параметры изменяются одновременно, но в таком соотношении, чтобы отклонение степени делигнификации в переходном режиме было минимальным. Аналогичным способом осуществляется переход выработки с одного вида продукции на другой или при изменении породного состава древесины.

Выводы

1. Современные варочные котлы оснащены контрольно-измерительными и регулировочными приборами, которые позволяют вести управление технологическими процессами варки автоматически.

2. Из анализа схемы автоматизации контроля и управления процессом варки целлюлозы видно, что роль роторных питателей чрезвычайно велика, так как они обеспечивают автоматическую подачу в варочный котел технологической щепы.

3. Управление всеми двигателями сконцентрировано на щите пульта управления. На кинематической схеме все двигатели имеют свое обозначение в виде сигнальных лампочек, и по их загоранию судят о рабочем состоянии того или иного двигателя.

4. Процесс управления варкой целлюлозы можно вести как в автоматическом, так и в ручном режиме. При ручном режиме происходит снижение качественных показателей целлюлозы.

5. В перспективе необходимо будет более подробно установить комплекс факторов, выполняемых роторным питателем по подаче шеллы в варочный котел.

Литература

1. Камель Г.И. Повышение надежности и производительности роторных питателей непрерывной варки на базе системного анализа их функционирования. // Дисс. док. тех. наук, - Санкт-Петербург: СПбГТУРП.-386 с.

ВІСНИК

Східноукраїнського національного університету

імені Володимира Даля

№ 9 (103) 2006
науковий журнал

Відповідальний секретар випуску	*Петров О.С.*
Літературний редактор:	*Андронова З.І.*
Технічний редактор	*Дроговоз Т.М.*
Коректор	*Подова С.В.*
Розробка оригінал-макету	*Полупан Ю.В.*

Здано до набору 26.08.2006. Підписано до друку 03.09.2006.
Формат 70x108 1/16. Папір офсетний. Гарнітура Arial
Умов. друк. арк. Обл. друк. Арк. Наклад 300 прим.
Видавничий № 891. Замовлення №_____. Ціна вільна

Видавництво
Східноукраїнського національного
університету імені Володимира Даля
91034, м. Луганськ, кв. Молодіжний, 20а

Свідоство про реєстрацію серія ДК №1620 від 18.12.2003

Адреса редакції: 91034, м. Луганськ, кв. Молодіжний, 20а
Телефон 8(0642) 46-13-04. Факс 8(0642) 46-13-64
E-mail: uni@snu.edu.ua