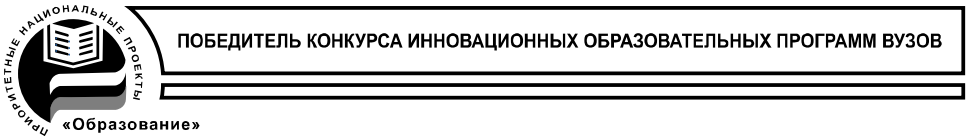
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ



НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК

Выпуск 52

ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

САНКТ-ПЕТЕРБУРГ
2008

В научно-техническом вестнике СПбГУ ИТМО, Выпуск 52 «ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ» представлены работы, выполненные в рамках:

– инновационной образовательной программы «Инновационная система подготовки специалистов нового поколения в области информационных и оптических технологий» вузов России на 2007–2008 гг.;
– аналитической ведомственной целевой программы «Развитие научного потенциала высшей школы (2006–2008 гг.) (Федеральное агентство по образованию);
– Федеральной целевой программы развития образования на 2006–2010 гг. (Федеральное агентство по образованию);
– Федеральной целевой программы развития научно-технологического комплекса России на 2007–2012 гг. (Федеральное агентство по науке и инновациям);
– Российского фонда фундаментальных исследований, а также инициативные разработки.

В 2007 году СПбГУ ИТМО стал победителем конкурса инновационных образовательных программ вузов России на 2007–2008 годы. Реализация инновационной образовательной программы «Инновационная система подготовки специалистов нового поколения в области информационных и оптических технологий» позволит выйти на качественно новый уровень подготовки выпускников и удовлетворить возрастающий спрос на специалистов в информационной, оптической и других высокотехнологичных отраслях экономики.

ISSN 1819-222X

1 ФОТОНИКА И ОПТОИНФОРМАТИКА

ИНТЕРФЕРЕНЦИЯ ФЕМТОСЕКУНДНЫХ СПЕКТРАЛЬНЫХ СУПЕРКОНТИНУУМОВ С ЛИНЕЙНОЙ ФАЗОВОЙ МОДУЛЯЦИЕЙ

А.А. Дроздов, А.Н. Цыпкин
Научный руководитель – д.ф.-м.н., профессор С.А. Козлов

Проанализирована интерференция фемтосекундных световых импульсов с сильной линейной фазовой модуляцией. Показано, что при такой интерференции формируется квазидискретный спектральный суперконтинуум, которому соответствует терагерцовая последовательность импульсов из малого числа колебаний светового поля. Показано, что данная последовательность может быть использована для передачи информации со скоростями более 50 Тбт/сек.

Введение

Фемтосекундные световые импульсы могут распространяться в диэлектрических средах без оптического пробоя вещества при интенсивностях излучения, превышающих 10^{13} Вт/см^2 [1]. Это позволяет наблюдать такое красивое нелинейное явление, как генерация спектрального суперконтинуума, в поле фемтосекундных импульсов практически во всех прозрачных средах [2].

В области нормальной групповой дисперсии диэлектрика сверхуширение спектра фемтосекундного светового импульса реализуется за счет фазовой самомодуляции, которая на выходе из среды может оказаться близкой к линейной [3]. Гладкость фазовой модуляции излучения в этом спектральном диапазоне вещества позволяет путем сфазирования спектрального суперконтинуума получать импульсы, содержащие лишь несколько колебаний светового поля [4]. Отметим, что структура спектрального суперконтинуума, генерируемого в области аномальной групповой дисперсии диэлектрической среды, более сложная. Она может быть порождена обрушением волнового фронта, возникновением солитонов [5] и т.п.

В работах [6, 7] было показано, что при распространении в нелинейной диэлектрической среде с нормальной групповой дисперсией двух импульсов при их взаимодействии может формироваться квазидискретный спектральный суперконтинуум, который можно использовать в оптических системах сверхбыстрой передачи информации. В настоящей работе показано, что такой квазидискретный суперконтинуум, которому соответствует последовательность сверхкоротких оптических сигналов, удобно получать при интерференции излучения на выходе нелинейной среды (смотри также [8]). Показано, что при интерференции образуется последовательность сверхкоротких импульсов с квазидискретным континуумным спектром. Определена зависимость частоты повторения импульсов в этой последовательности от параметров фазовой модуляции. Продемонстрированы принципы кодирования информации, передаваемой в последовательности световых сигналов.

Иллюстрация фемтосекундного фазомодулированного импульса

Пусть на выходе оптической системы (например, нелинейного волновода [3]) имеем импульс, колебания электрического поля E которого имеют линейную фазовую модуляцию:

$$E = E_0 \cdot e^{-\left(\frac{t}{\tau}\right)^2} \cdot \sin(\omega_0 t + \alpha\omega_0 t^2), \qquad (1)$$

где E_0 – амплитуда импульса, ω_0 – его центральная частота, τ – длительность, α – коэффициент фазовой модуляции, t – время. Соответственно спектр G такого излучения имеет вид

$$G(\omega) = G_0 \cdot e^{-\left(\frac{(\omega-\omega_0)^2}{\left((\alpha\omega_0)^2+\frac{1}{\tau^4}\right)\tau^4}\right)}, \qquad (2)$$

где амплитуда спектра $G_0 = \dfrac{\pi}{\sqrt{\left(\alpha^2\omega_0^2 + \dfrac{1}{\tau^4}\right)}}$.

На рис. 1 иллюстрированы зависимости (1) и (2) при $\lambda = \dfrac{2\pi c}{\omega_0} = 0.78$ мкм, $\tau = 20$ фс, $\alpha = 0.05 \cdot \omega_0 \, c^{-1}$, характерных для интенсивных импульсов титан-сапфирового лазера на выходе из кварцевого волокна [3].

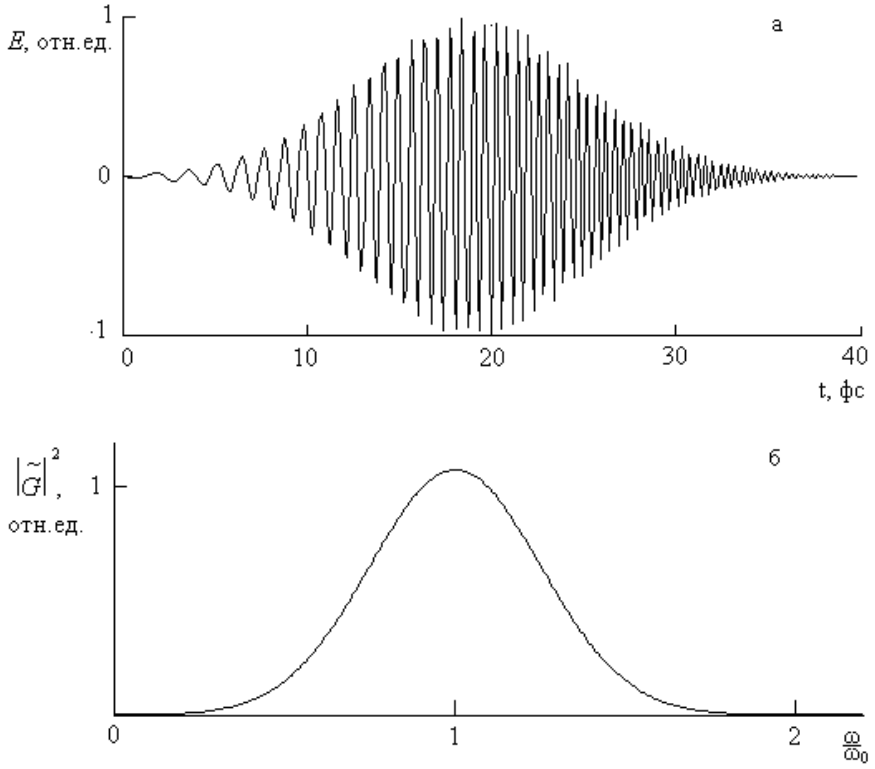


Рис. 1. Динамика поля $E(t)$ (а) и модуля спектра $|G|^2$ (б) фемтосекундного импульса с фазовой модуляцией, нормированных на максимумы амплитуды E_0 и спектра G_0

Интерференция фемтосекундных импульсов с линейной фазовой модуляцией

Интерференция двух одинаковых фемтосекундных фазомодулированных импульсов вида (1) с взаимной задержкой $\Delta\tau$ описывается соотношением для суммарного поля

$$E = E_1 + E_2 = E_{01} \cdot e^{-\left(\frac{t}{\tau}\right)^2} \cdot \sin(\omega_0 t + \alpha\omega_0 t^2) + \\ + E_{02} \cdot e^{-\left(\frac{t+\Delta\tau}{\tau}\right)^2} \cdot \sin(\omega_0 \left(t + \Delta\tau\right) + \alpha\omega_0 \left(t + \Delta\tau\right)^2), \quad (3)$$

где E_1 и E_2 – электрическое поле первого и второго (задержанного) импульсов.

Будем рассматривать интерференцию импульсов с $E_{02} = E_{01} = E_0$. Тогда соотношение (3) удобно записать в виде:

$$E = E_0 \mathrm{e}^{-\left(\frac{t}{\tau}\right)^2} (2\cos((\omega_0 + \omega_{\mathrm{mod}})t + \alpha\omega_0 t^2 + \varphi_0) \cdot \cos((\omega_{\mathrm{mod}})t + \varphi_0) + \\ + (\exp(\frac{-2\tau t - \tau^2}{\tau^2}) - 1) \cdot (\cos(\omega_0 (t + \tau)) + \alpha\omega_0 (t + \tau)^2), \quad (4)$$

где $\varphi_0 = \frac{\omega_0 \tau}{2} \cdot (1 + \alpha\tau)$ – начальная фаза, $\omega_{\mathrm{mod}} = \alpha\omega_0\tau$ – частота модуляции интерференционного поля.

При $\Delta\tau << \tau$ последним слагаемым в (4) можно пренебречь, и выражение для суперпозиций световых полей двух импульсов примет простой вид:

$$E = 2 \cdot E_0 \cdot e^{-\left(\frac{t}{\tau}\right)^2} \cdot \cos((\omega_0 + \omega_{\mathrm{mod}})t + \alpha\omega_0 t^2 + \varphi_0) \cdot \cos(\omega_{\mathrm{mod}} t + \varphi_0), \quad (5)$$

Спектр зависимости (5) имеет вид:

$$G(\omega) = 2 \cdot A(\omega) \cdot (1 + \cos(\gamma + \psi\omega)), \quad (6)$$

где $A(\omega) = \frac{E_0}{\sqrt{\alpha\omega_0}} \cdot e^{-\left(\frac{i \cdot (\omega - \omega_0)^2}{4 \cdot \alpha\omega_0}\right)}$ – амплитуда спектра, $\gamma = 8 \cdot \omega_{\mathrm{mod}}{}^3 + 8 \cdot \omega_{\mathrm{mod}}{}^2 \cdot \omega_0$, $\psi = 4 \cdot \omega_{\mathrm{mod}} \cdot \omega_0$

На рис. 2 иллюстрирована интерференция полей одинаковых фемтосекундных импульсов, вид которых представлен на рис. 1, задержанных друг относительно друга на временной интервал $\Delta\tau = 12$ фс.

Как видно из рис. 2, а, результатом интерференции является регулярная последовательность световых импульсов, содержащих лишь несколько оптических колебаний, которой соответствует квазидискретный спектральный суперконтинуум, приведенный на рис. 2, б.

Из выражения (5) следует, что частота повторения импульсов имеет вид ω_{mod}, которая линейно зависит от временной задержки импульсов и от коэффициента их фазовой модуляции. На рис. 3 представлена зависимость частоты повторения сверхкоротких сигналов в последовательности для интерферирующих импульсов с длительностью $\tau = 40$ фс, с коэффициентом фазовой модуляции $\alpha = 0.04 \cdot \omega_0\, \mathrm{c}^{-1}$, в зависимости от временной задержки $\Delta\tau$ без использования приближения (5). Рис. 3 подтверждает практически линейную зависимость частоты повторения сигналов в интерференционной последовательности от временной задержки исходных импульсов и вне применимости неравенства $\Delta\tau \square\ \tau$.

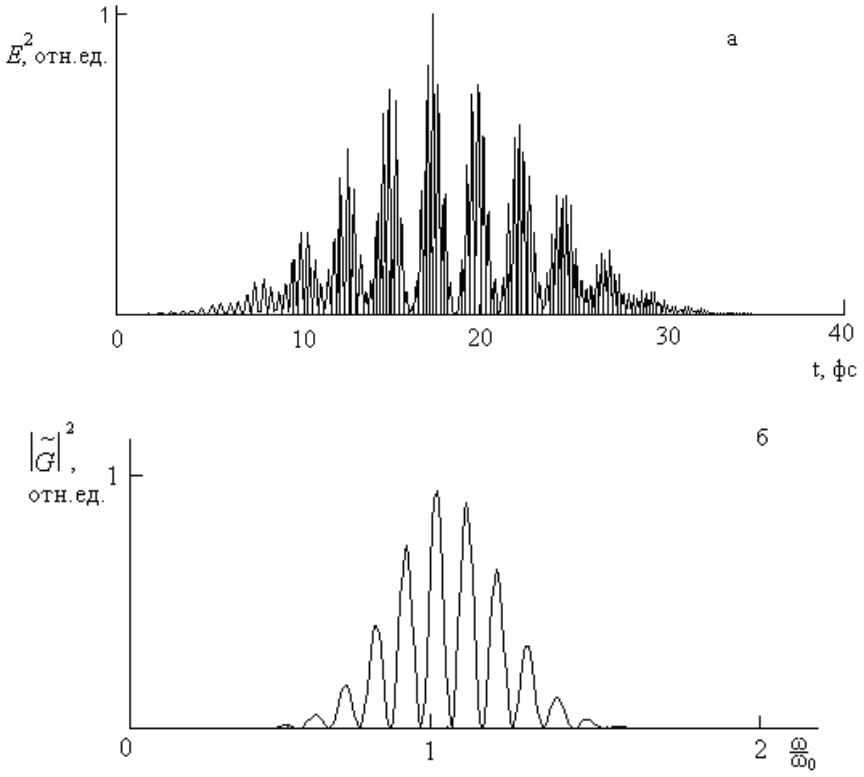


Рис. 2. Нормированные квадрат результирующего поля $E^2(t)$ (а) и квадрат модуля спектра $|G|^2$ (б) двух сдвинутых по времени друг относительно друга интерферирующих фазомодулированных фемтосекундных импульсов

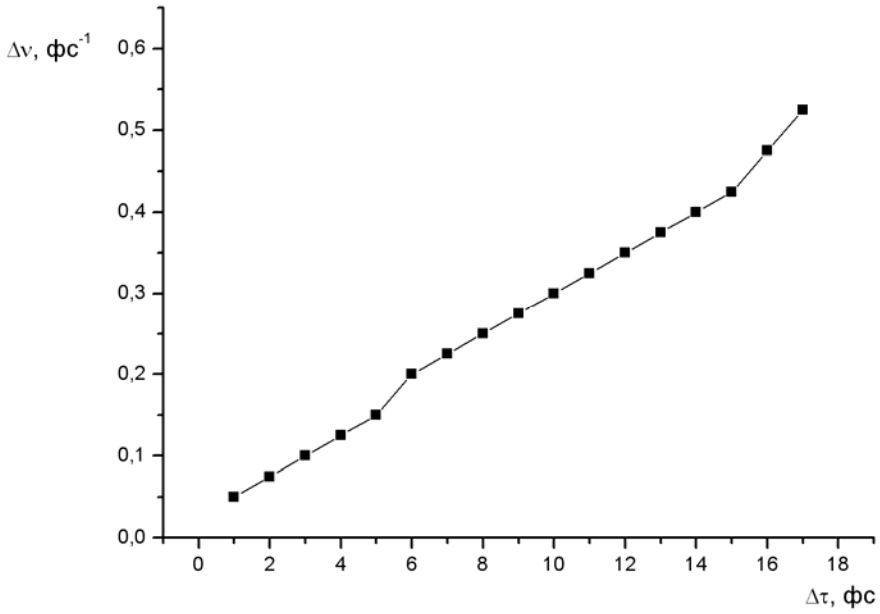


Рис. 3. Зависимость частоты повторения сверхкоротких импульсов от временной задержки

Структура временной последовательности и спектрального суперконтинуума, представлены на рис. 2, аналогичны тем, которые были получены в работах [5, 6] при анализе взаимодействия разночастотных фемтосекундных импульсов в нелинейных средах. Однако рис. 2 показывает, что для создания последовательности световых им-

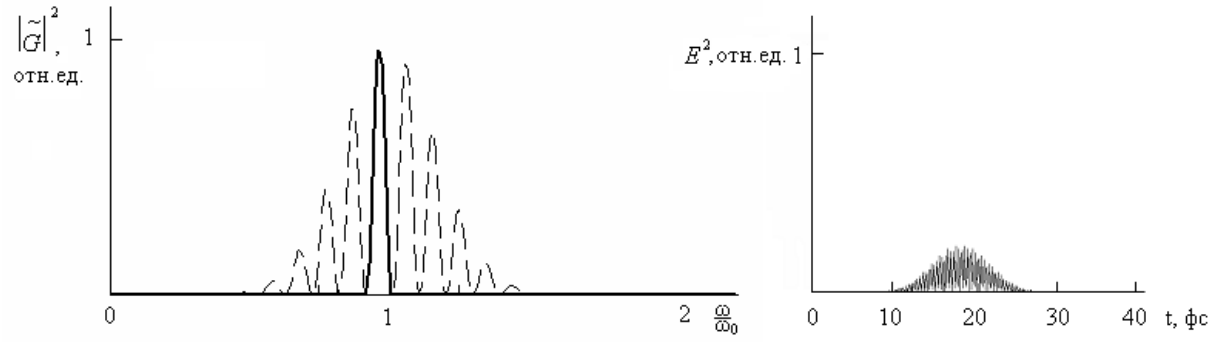
пульсов с частотой следования около 100 ТГц организовывать в нелинейной среде взаимодействие импульсов, к тому же имеющих разный спектральный состав на входе в среду, не обязательно. Достаточно получить интерференцию двух задержанных друг относительно друга импульсов со сверхуширенными спектрами. Экспериментальная возможность получения таким образом квазидискретного суперконтинуума продемонстрирована и в работе [8], но в этой работе, в отличие от настоящей, не обсуждается временная структура поля излучения, соответствующая сверхуширенному спектру.

Кодирование последовательности сверхкоротких оптических сигналов

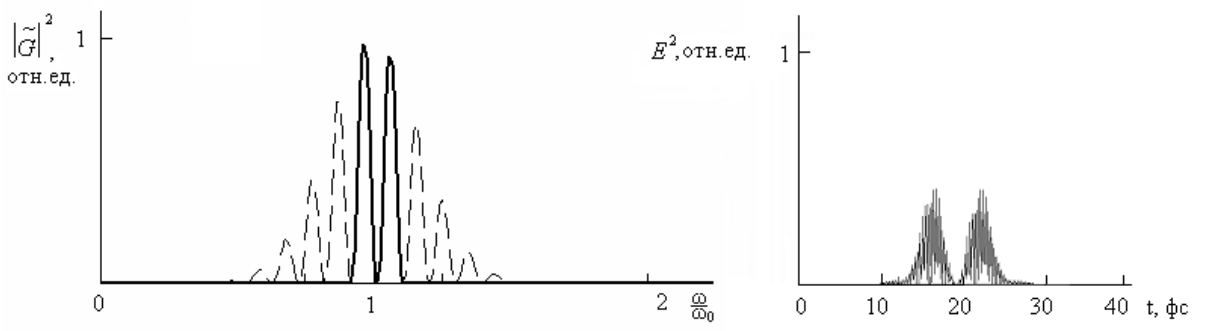
Из соотношения (5) и рис. 2, а, видно, что каждый последующий импульс во временной последовательности интерференционной структуры несколько отличается от предыдущего центральной частотой. Это позволяет осуществлять кодирование информации с использованием такой последовательности подобно тому, как было показано в [7], удалением соответствующего выбранному импульсу пичка в квазидискретном спектре излучения подобранным спектральным фильтром.

Проведем анализ возможности кодирования информации с помощью интерференционного квазидискретного спектра. На рис. 4 представлены возможные варианты «вырезаний» спектральных пичков и полученные в результате этой процедуры временные структуры. Из рис. 4, а–г, видно, что каждая компонента спектра коррелирует со «своим» импульсом во временной структуре. Но, несмотря на очевидную связь сигналов во временной последовательности и спектральных пичков, отдельный пичок, как видно из рисунка, – это не спектр отдельного сигнала. Действительно, его «вырезание» в качестве основного следствия имеет удаление определенного светового сигнала, но при этом искажается и вся последовательность. Эти искажения тем меньше, чем больше импульсов в последовательности.

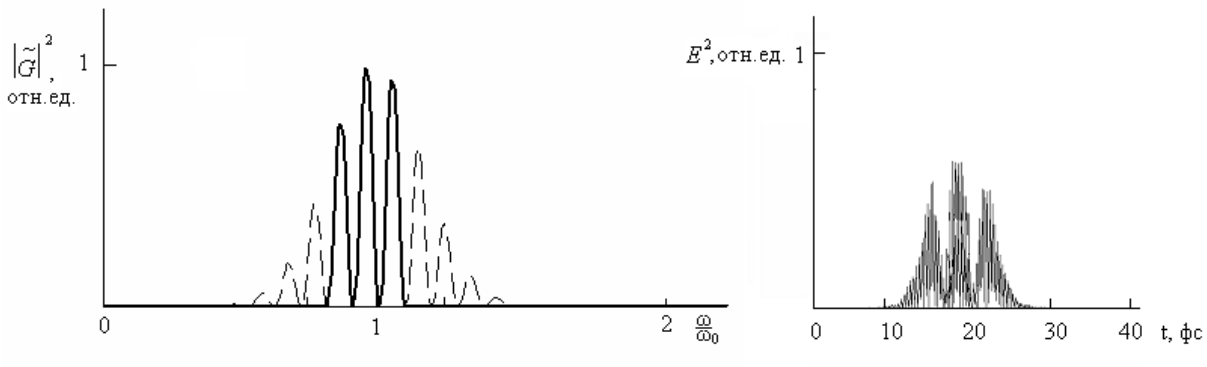
а)



б)



в)



г)

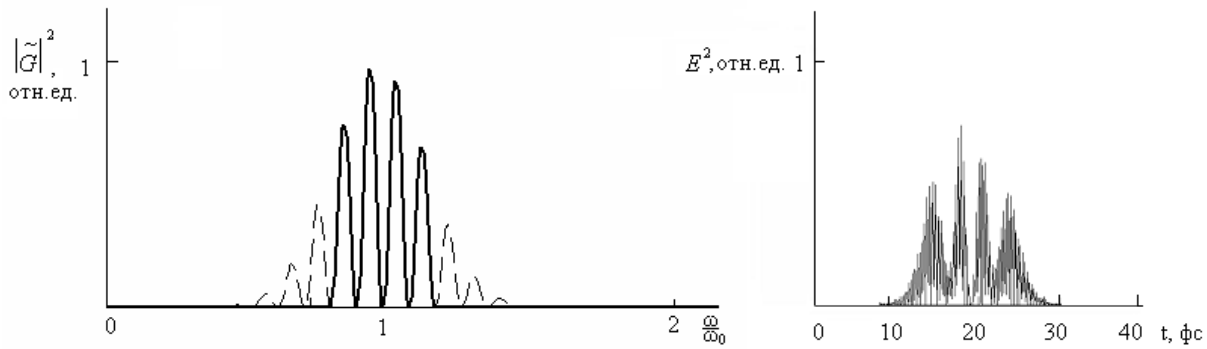


Рис. 4. Анализ кодирования информации на основе квазидискретного спектрального суперконтинуума путем оставления одного (а), двух (б), трех (в) и четырех (г) пичков в спектральной структуре, а также соответствующие им временные последовательности сигналов

На рис. 5, а, приведена временная последовательность сигналов с двумя удаленными импульсами при «вырезании» соответствующих спектральных компоненты из общего спектра выходного излучения, представленного на рис. 2б.

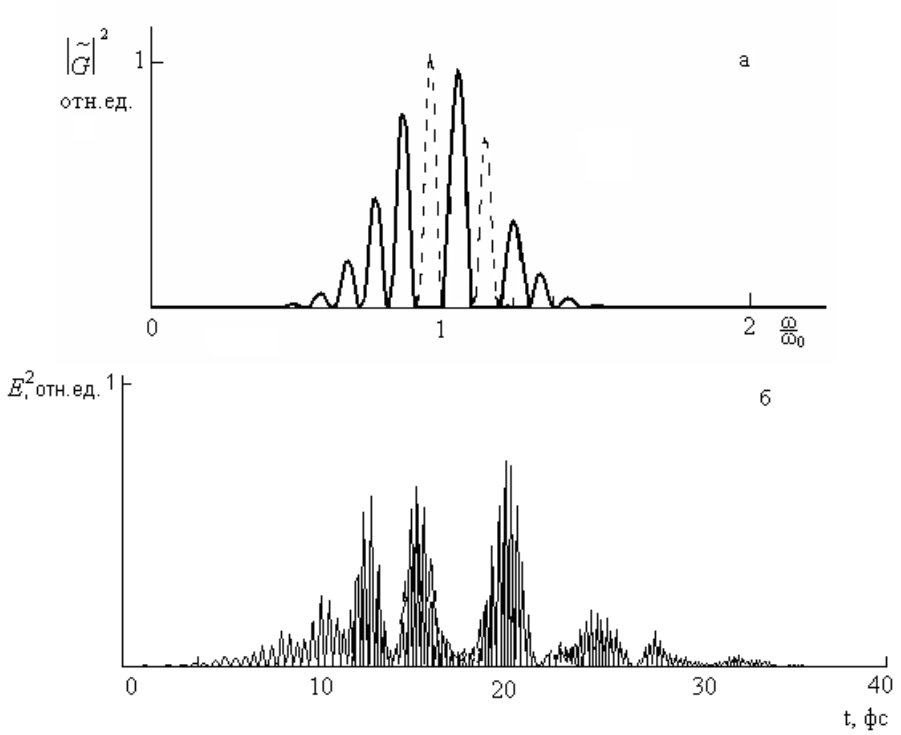


Рис. 5: а – спектр излучения с «вырезанными» пичками, б – временная последовательность сигналов с удаленными двумя импульсами

На рис. 6 представлен более сложный пример кодирования битовой последовательности (1000001100111010101001001111001110) путем удаления соответствующих комонент в спектре, на примере слова «ANTON».

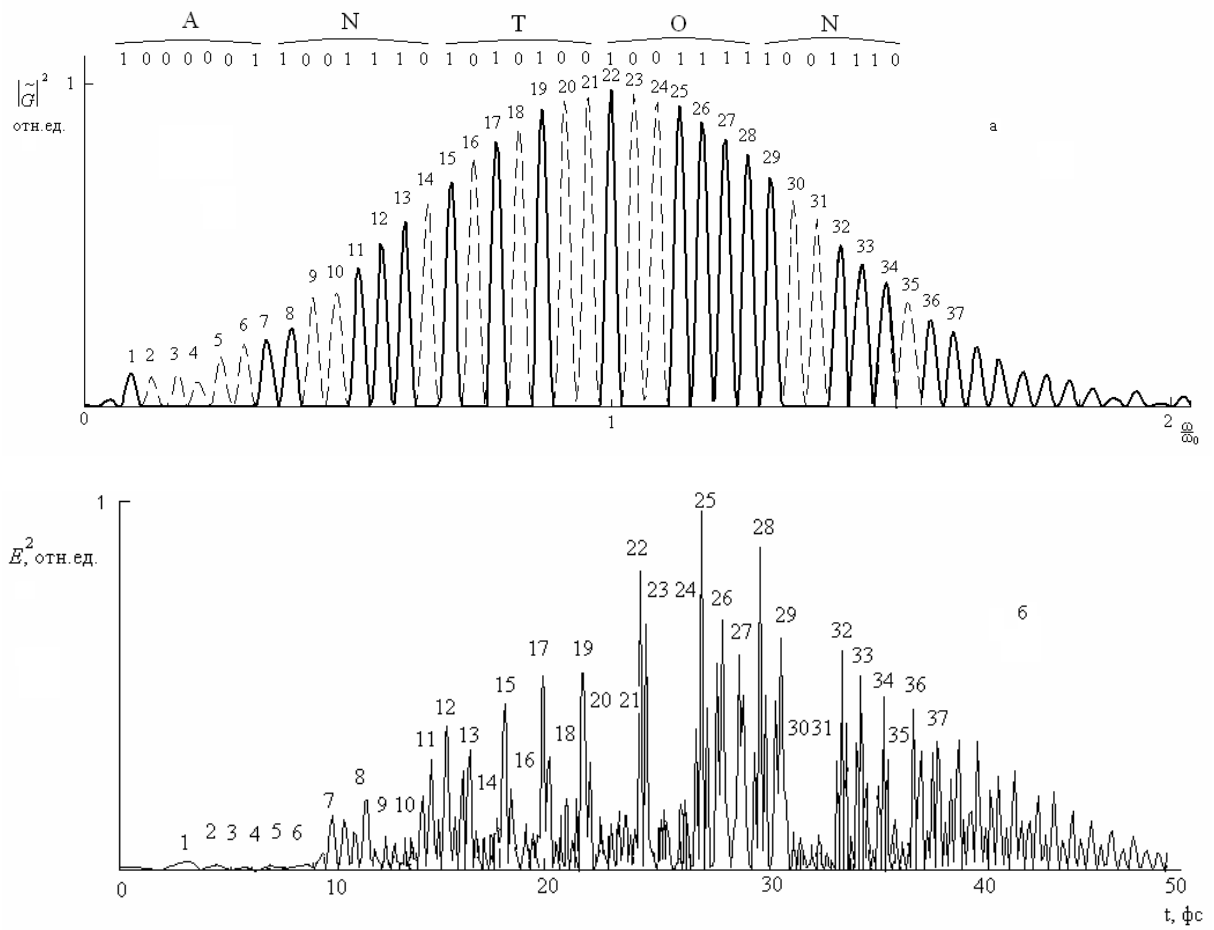


Рис. 6: а – кодирования битовой последовательности путем «вырезания» нескольких спектральных компонент в квазидисктретном спектре выходной последовательности, кодирующих слово «ANTON», б – временная последовательность сигналов с соответствующими удаленными импульсами

Заключение

Таким образом, в работе показано, что в результате интерференции двух фемтосекундных импульсов из малого числа колебаний светового поля с сильной линейной фазовой модуляцией может образовываться последовательность сверхкоротких импульсов, центральная частота каждого из которых несколько отличается от частоты предыдущего. Последовательность имеет квазидискретный спектр, при этом каждой компоненте спектра выходного излучения соответствует «свой» импульс в последовательности. Это свойство может быть использовано для кодирования информации, передаваемой приблизительно 100 ТГц последовательностью световых импульсов, состоящих лишь из нескольких оптических колебаний. При этом показано, что, несмотря на связь сигналов во временной последовательности и спектральных пичков, отдельный пичок – это не спектр отдельного сигнала. «Вырезание» спектрального пичка в качестве основного следствия имеет удаление определенного светового сигнала, но при этом несколько искажается и вся последовательность. Эти искажения тем меньше, чем больше импульсов в последовательности.

Литература

1. Sudrie L., Couairon A., Franko M. Femtosecond Laser-Induced Damage and Filamentary Propagation in Fused Silica // Phys. Rev. Lett. – 2002. – V.89. – №18. – P.1–4.
2. Brodeur A., Chin S.L. Ultrafast white-light continuum generation and self-focusing in transparent condensed media // J. Opt. Soc. Am. B. – 1999. – V.16. – №4. – P.637–650.
3. Беспалов В.Г., Козлов С.А., Сутягин А.Н., Шполянский Ю.А.. Сверхуширение спектра интенсивных фемтосекундных лазерных импульсов и их временное сжатие до одного колебания светового поля // Оптический журнал. – 1998. – Т. 65. – №10. – С. 85–88.
4. Nisovi M., De Silvestri S., Svelto O., Szipocs R., FerenczK., Spielmann Ch., S artania S., Krausz F. Compression of high-energy laser pulses below 5 fs // Opt. Lett. – 1997. – V.22. – № 8. – P.522–524.
5. Husakou A.V., Herrmann J. Supercontinuum generation, four-wave mixing, and fission of higher-order solitons in photonic-crystal fibers // J. Opt. Soc. Am. B. – 2002. – V.19. – №9. – P.2171–2182.
6. Бахтин М.А., Козлов С.А. Формирование последовательности сверхкоротких сигналов при столкновении импульсов из малого числа колебаний светового поля в нелинейных оптических средах // Оптика и спектроскопия. – 2005. – Т. 98. – №3. – С.425–430.
7. Bakhtin M.A., Kozlov S.A. Generation of the discrete spectral supercontinuum in two intensive ultrashort pulses interaction // Optical Memory and Neural Network. 2006. V.15. №1. P.1–10.
8. Corsi C., Tortora A., Bellini M. Mutual coherence of supercontinuum pulses collinearly generated in bulk media // Appl. Phys. B. – 2003. – V.77. – № 2–3. – P. 255–290.

ОБЪЕМНЫЕ ФАЗОВЫЕ ГОЛОГРАММЫ НА ОСНОВЕ СИЛИКАТНОГО ФОТО-ТЕРМО-РЕФРАКТИВНОГО СТЕКЛА, АКТИВИРОВАННОГО РЕДКОЗЕМЕЛЬНЫМИ ИОНАМИ

А.С. Златов

Научный руководитель – д.ф.-м.н., ст.н.с. Н.В. Никоноров

Проведены исследования свойств объемных фазовых голограмм на силикатном фото-термо-рефрактивном стекле, легированном ионами лантана и эрбия. Проведено сравнение исходного ФТР-стекла с лантановым и эрбиевым ФТР-стеклами. Установлено, что введение ионов лантана приводит к снижению фоточувствительности ФТР-стекла, а также уменьшению динамического диапазона показателя преломления, а введение ионов эрбия практически не изменяет фоточувствительность и динамический диапазон показателя преломления по сравнению с исходным ФТР-стеклом.

Введение

К настоящему времени объемные фазовые голограммы на основе фото-термо-рефрактивных (ФТР) стекол [1] находят все более широкое применение в лазерной технике. Так, например, на их основе возможно создание брэгговских сверхузкополосных спектральных селекторов, фильтров и внутрирезонаторных зеркал для мощных твердотельных и полупроводниковых лазеров и т.д. [2, 3]. Голограммы на ФТР-стеклах обладают высокой дифракционной эффективностью и спектрально-угловой селективностью. Также у них отсутствует стирание изображения в процессе считывания и нет ограничений на время их жизни. ФТР-стекла обладают высокой химической устойчивостью и механической прочностью, они выдерживают воздействие мощного непрерывного и импульсного лазерного излучения. Однако наличие полосы поглощения коллоидного серебра, а также рассеяние на микрокристаллической фазе ограничивают применения этого материала в видимом диапазоне спектра. Таким образом, ФТР-стекла наиболее привлекательны для создания голограммных оптических элементов, работающих в ИК-диапазоне спектра.

В настоящей работе были проведены исследования свойств объемных фазовых голограмм на силикатном ФТР-стекле, легированном ионами лантана и эрбия. Определен динамический диапазон изменения амплитуды модуляции первой гармоники показателя преломления в ФТР-стеклах с добавлением ионов эрбия, с добавлением ионов лантана и без них, установлены оптимальные времена термообработки. Также проведено сравнение исходного ФТР-стекла с лантановым и эрбиевым ФТР-стеклами.

Объект исследования и эксперимент

В работе были исследованы цинковоалюмосиликатные стекла с большим содержанием фтора, активированные ионами церия, серебра и сурьмы. Стекла были синтезированы в кварцевых тиглях при температуре 1500°С из реактивов марки ОСЧ. Запись голограмм производилась He-Cd-лазером на длине волны 325 нм по симметричной двулучевой схеме. Термообработка образцов проводилась при Т=520–530°С.

Обычно измерение контура угловой селективности проводятся на длине волны λ=633 нм He-Ne-лазером. Однако поглощение коллоидного серебра в видимом диапазоне приводит к потерям и уменьшению дифракционной эффективности. Кроме этого, голограмма становится амплитудно-фазовой, контур селективности приобретает специфическую форму, которую трудно интерпретировать. Поэтому измерения контура угловой селективности проводились в ИК-области с помощью полупроводникового лазера, работающего на длине волны λ = 850 нм.

Схема установки представлена на рис. 1. В качестве источника излучения использовался полупроводниковый лазер с коллимирующей оптической системой. Исследуе-

мый образец с голограммой находился на поворотном столике, управляемом с компьютера и обеспечивающем шаг разворота 10^{-5} рад. Измерялась зависимость интенсивности прошедшего и дифрагированного пучка от угла поворота столика. Полученные данные обрабатывались и захватывались с помощью программного пакета LabView 5.

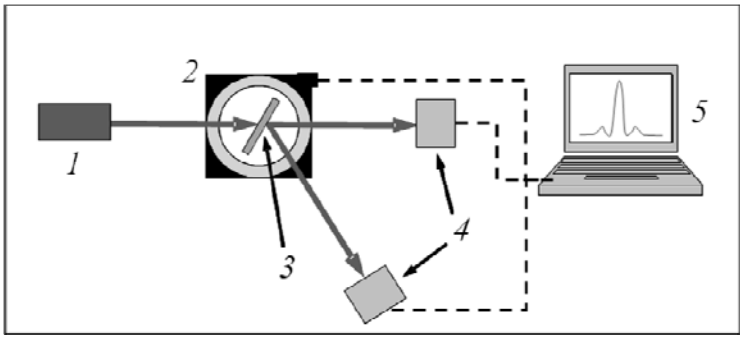


Рис. 1. Схема экспериментальной установки для тестирования голограмм:
1 – полупроводниковый лазер, 2 – поворотный столик, 3 – исследуемый образец с голограммой, 4 – фотоприемники, 5 – компьютер

Как известно [4], зависимость дифракционной эффективности (ДЭ) пропускающих трехмерных фазовых голограмм от амплитуды модуляции показателя преломления носит осциллирующий характер – $\eta = \sin^2\varphi_1$, где $\varphi_1 = \pi n_1 T/(\lambda\cos\theta_0)$, n_1 – амплитуда модуляции показателя преломления, T – толщина среды, λ – длина волны восстанавливающего излучения в воздухе, θ_0 – угол падения восстанавливающего пучка на голограмму в среде. При этом при $\varphi_1 = k\pi \pm \arcsin\sqrt{\eta}$ (где k = 1, 2, 3, …) в условиях Брэгга достигаются одинаковые ДЭ, и для выбора k, т.е. однозначного определения φ_1, использовалось сопоставление формы расчетного контура угловой селективности с экспериментально измеренной [5].

Результаты и обсуждения

Рассчитанные экспозиционные зависимости амплитуд модуляции показателя преломления при оптимальных временах термообработки представлены на рис. 2.

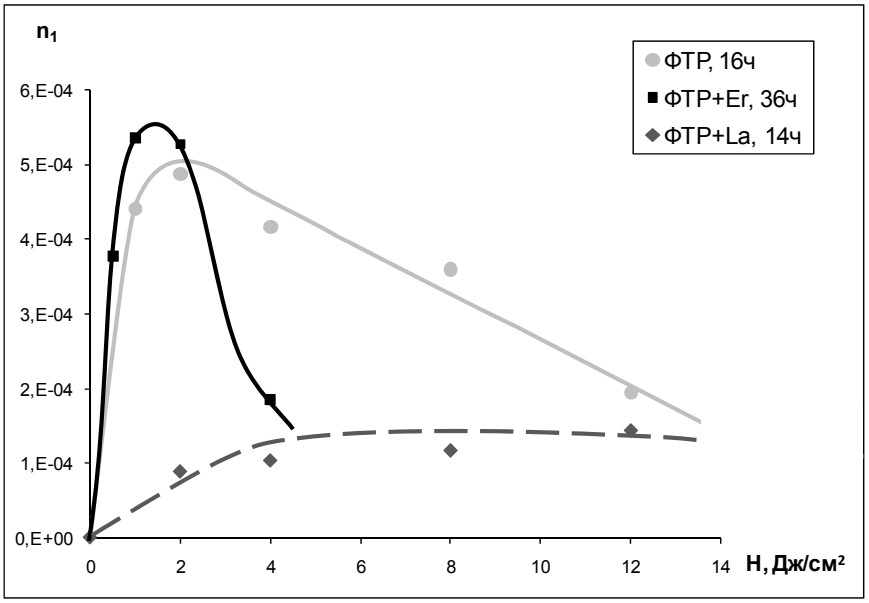


Рис. 2. Зависимости амплитуд модуляции первой гармоники показателя преломления от экспозиции при оптимальных временах термообработки

Из рис. 2 видно, что при оптимальных временах термообработки динамические диапазоны изменения показателя преломления ФТР-стекла, активированного ионами Er^{3+} и ФТР-стекла, не содержащего ионы редкой земли, практически совпадают и составляют величину порядка $5 \cdot 10^{-4}$, а для ФТР-стекол, содержащих ионы La^{3+} – $1{,}5 \cdot 10^{-4}$. Также из рисунка видно, что для образцов ФТР-стекла, содержащих ионы эрбия, максимальное значение амплитуды модуляции первой гармоники показателя преломления достигается при меньшей дозе облучения, чем для ФТР-стекол, не содержащих ионы редкой земли, а для образцов, содержащих ионы лантана – при значительно большей дозе. Таким образом, введение ионов эрбия практически не изменяет фоточувствительность, когда введение ионов лантана приводит к ее снижению. Установлено, что введение ионов эрбия приводит к изменению кинетики кристаллизации стекла, что ведет к увеличению времени термообработки. Также установлено, что введение ионов редкой земли в ФТР-стекло приводит к увеличению оптимальной температуры термообработки.

Выводы

Получена зависимость амплитуды модуляции первой гармоники показателя преломления от экспозиции для ФТР-стекол, активированных эрбием и лантаном, а также не активированных. Установлено, что введение ионов эрбия в ФТР-стекло не приводит к уменьшению максимального значения амплитуды модуляции первой гармоники показателя преломления, когда введение ионов лантана приводит к его уменьшению. Максимальное значение амплитуды модуляции первой гармоники показателя преломления для ФТР-стекол с эрбием составило $5{,}5 \cdot 10^{-4}$, для ФТР-стекол с лантаном $-1{,}5 \cdot 10^{-4}$, для неактивированых ФТР-стекол – $5 \cdot 10^{-4}$. Полученные данные необходимо учитывать при разработке сверхузкополосных селекторов света и лазеров с распределенной обратной связью на основе активированных ФТР-стеклол.

Литература

1. Кучинский С.А., Никоноров Н.В., Панышева Е.И., Савин В.В., Туниманова И.В. Свойства объемных фазовых голограмм на мультихромных стеклах // Оптика и спектроскопия. – 1991. – Т. 70. – № 6. – С.1296.
2. Venus G., Sevian A., Glebov L. Stable coherent coupling of laser diodes by a volume Bragg grating in PTR glass // High-Power Diode Laser Technology and Applications IV. Ed.: M. Zediker. – Proceedings of SPIE. – 6104 (2006). – 61040S.
3. Venus G., Sevian A., Glebov L. Spectral Stabilization of High Efficiency Diode Bars by External Bragg Resonator // 18th Annual Solid State and Diode Laser Technology Review, SSDLTR-2005 Technical Digest, Poster-1, Los Angeles, CA, June 2005.
4. Kogelnik H. Coupled wave theory for thick hologram grating // Bell Syst. Techn. J. – 1969. – Vol. 48. – №9. – P. 2909–2947.
5. Андреева О.В., Корзинин Ю.Л., Назаров В.Н., Гаврилюк Е.Р., Курсакова А.М. Дифракционная эффективность серебросодержащих голограмм на пористых стеклах в красной и ИК-областях спектра // Оптический журнал. – 1997. – Т. 64. – №4. – С.142.

ОПТИМИЗАЦИЯ СОСТАВА ФТР-СТЕКЛА ДЛЯ ЗАПИСИ ОБЪЕМНЫХ ФАЗОВЫХ ГОЛОГРАММ ДЛЯ ВИДИМОГО ДИАПАЗОНА

А.С. Златов

Научный руководитель – д.ф.-м.н., ст.н.с. Н.В. Никоноров

Проведены исследования свойств объемных фазовых голограмм на силикатном фото-термо-рефрактивном стекле, оптимизированном для видимого диапазона спектра. Проведено сравнение исходного ФТР-стекла с оптимизированным. Установлено, что уменьшение содержания активирующих добавок приводит к снижению фоточувствительности ФТР-стекла, уменьшению динамического диапазона показателя преломления и значительному увеличению пропускания в видимом диапазоне.

Введение

Одним из перспективных материалов для создания эффективных голограммных объемных элементов являются фото-термо-рефрактивные (ФТР) стекла [1]. Голограммы на этих стеклах обладают высокой дифракционной эффективностью и спектрально-угловой селективностью. Высокая термическая и оптическая прочность фото-термо-рефрактивных стекол позволяет использовать такие голограммные оптические элементы в мощных лазерных системах. Кроме этого, голограммы, зарегистрированные в ФТР-стекле, обладают высокой химической устойчивостью и механической прочностью и в этом отношении практически не отличаются от коммерческого оптического стекла К8.

В основе записи голограмм на фото-термо-рефрактивных стеклах лежит фото-термо-индуцированная кристаллизация стекла (рис. 1). Суть процесса заключается в следующем. Облучение стекла УФ-излучением приводит к фотоионизации Ce^{3+}, освободившийся электрон посредством сурьмы захватывается ионом серебра с образованием нейтрального атома серебра. На этой стадии показатель преломления еще не изменен, и эффективность голограммы составляет менее 0.01%. Последующая термическая обработка приводит к росту коллоидного серебра и выделению в объеме стекла микрокристаллов *NaF* и *NaBr*. В результате фото-термо-индуцированной кристаллизации происходит изменение показателя преломления на величину $\sim 10^{-4}$, что достаточно для получения 100% дифракционной эффективности в образце с толщиной порядка 1 мм. Благодаря тому, что этот процесс является необратимым, отсутствует стирание изображения в процессе считывания, а также нет ограничений на время жизни объемной фазовой голограммы. Однако наличие широкой полосы поглощения коллоидного серебра в районе 410–450 нм, а также рассеяние на микрокристаллической фазе ограничивают применения этого материала в видимом диапазоне спектра. Кроме этого, из-за сильной полосы поглощения ионов Ce^{3+} нет возможности записывать голограммы на толстых (3–5 мм) образцах. Эти факторы существенно ограничивают применение голограмм в видимом диапазоне спектра.

В настоящей работе была предпринята попытка оптимизации состава ФТР-стекла для использования голограммных элементов увеличенной толщины в видимом диапазоне. Для этой цели в ФТР-стекле было в 2–3 раза уменьшено содержание активирующих добавок – ионов серебра, церия и сурьмы. В работе были проведены исследования свойств объемных фазовых голограмм, записанных на оптимизированном и исходном стеклах, установлены оптимальные времена термообработки. Также проведено сравнение исходного ФТР-стекла с оптимизированным.

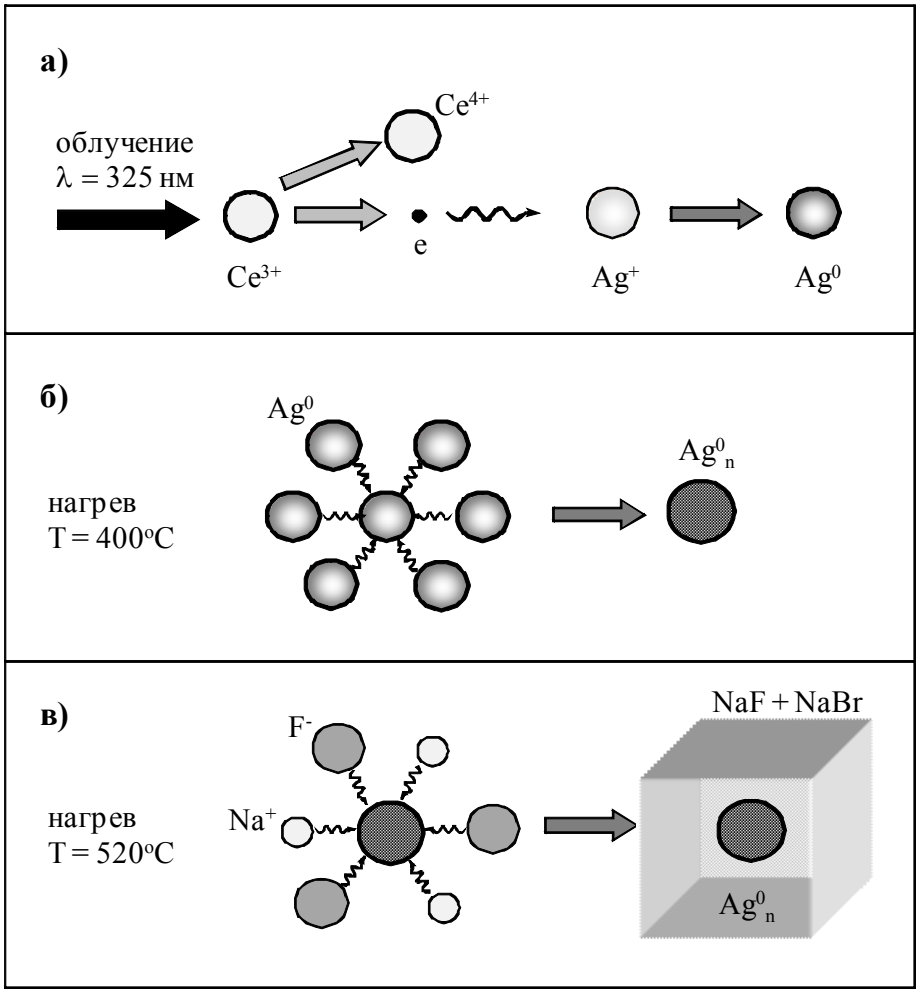


Рис. 1. Фото-термо-индуцированная кристаллизация стекла: а) фотоионизация церия УФ-излучением с образованием свободных электронов, захват электронов ионами серебра и образование атомарного серебра; б) образование коллоидного серебра при нагревании облученного стекла (480ºС); в) рост микрокристаллов NaF на коллоидных центрах при 520ºС

Объект исследования и эксперимент

В работе были исследованы цинк-алюмосиликатные стекла с большим содержанием фтора, активированные ионами церия, серебра и сурьмы. Стекла были синтезированы в кварцевых тиглях при температуре 1500°С из реактивов марки ОСЧ.

Запись голограмм производилась He-Cd лазером на длине волны 325 нм по симметричной двулучевой схеме. Термообработка образцов проводилась при Т=520°С.

Схема установки представлена на рис. 2. В качестве источника излучения использовался полупроводниковый лазер с коллимирующей оптической системой. Исследуемый образец с голограммой находился на поворотном столике, управляемом с компьютера и обеспечивающего шаг разворота 10^{-5} рад. Измерялась зависимость интенсивности прошедшего и дифрагированного пучка в зависимости от угла поворота столика. Полученные данные обрабатывались и захватывались с помощью программного пакета LabView 5.

Как известно [2], зависимость дифракционной эффективности (ДЭ) пропускающих трехмерных фазовых голограмм от амплитуды модуляции показателя преломления носит осциллирующий характер – $\eta = \sin^2\varphi_1$, где $\varphi_1 = \pi n_1 T/(\lambda\cos\theta_0)$, n_1 – амплитуда модуляции показателя преломления, T – толщина среды, λ – длина волны восстанавли-

вающего излучения в воздухе, θ_0 – угол падения восстанавливающего пучка на голограмму в среде. При этом при $\varphi_1 = k\pi \pm \arcsin\sqrt{\eta}$ (где k = 1, 2, 3, …) в условиях Брэгга достигаются одинаковые ДЭ, и для выбора «k», т.е. однозначного определения φ_1, использовалось сопоставление формы расчетного контура угловой селективности с экспериментально измеренной [3].

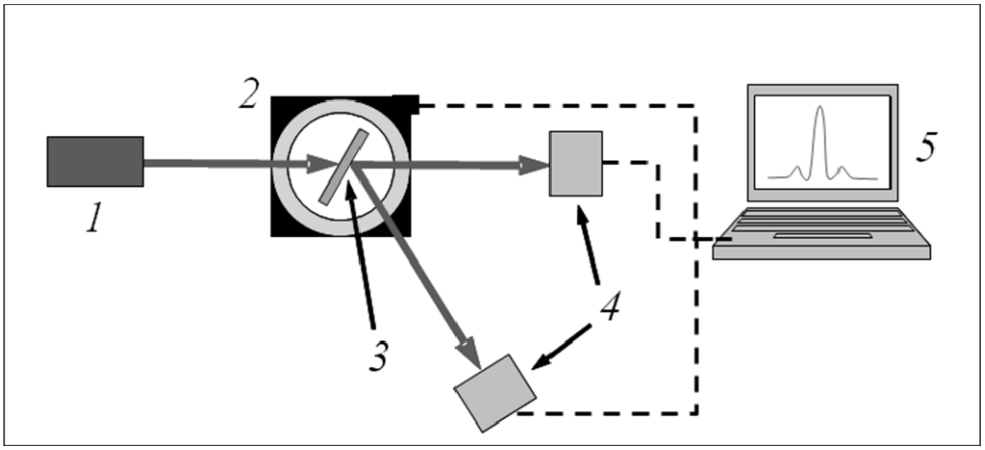


Рис. 2. Схема экспериментальной установки для тестирования голограмм:
1 – полупроводниковый лазер, 2 – поворотный столик, 3 – исследуемый образец с голограммой, 4 – фотоприемники, 5 – компьютер

Результаты и обсуждения

Рассчитанные экспозиционные зависимости амплитуд модуляции показателя преломления при оптимальных временах термообработки представлены на рис. 3.

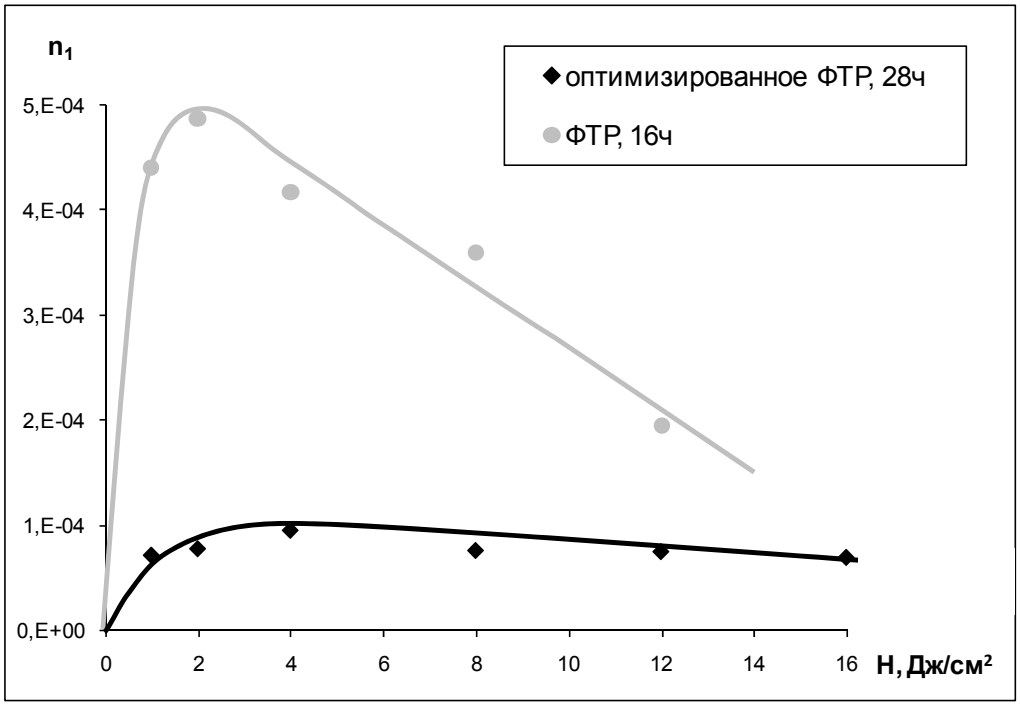


Рис. 3. Зависимости амплитуд модуляции первой гармоники показателя преломления от экспозиции при оптимальных временах термообработки

Видно, что уменьшение содержания активирующих добавок приводит к уменьшению динамического диапазона изменения показателя преломления ФТР-стекла. Также из рисунка видно, что для оптимизированного ФТР-стекла максимальное значение амплитуды модуляции первой гармоники показателя преломления достигается при большей дозе облучения, чем у исходного ФТР-стекла, кроме этого, оптимизация состава приводит к изменению кинетики кристаллизации стекла, что ведет к значительному увеличению времени термообработки. Максимальное значение амплитуды модуляции первой гармоники показателя преломления для оптимизированного ФТР-стекла составило $1 \cdot 10^{-4}$, а для исходного ФТР-стекла – $5 \cdot 10^{-4}$. Установлено, что коэффициент поглощения голограмм, записанных на оптимизированном ФТР-стекле, уменьшился в 5 раз. Этот результат достигнут за счет уменьшения поглощения на коллоидном серебре и снижения рассеяния на границе кристаллической фазы и матрицы стекла.

Выводы

Получена зависимость амплитуды модуляции первой гармоники показателя преломления от экспозиции исходного и оптимизированного ФТР-стекла. Установлено, что значительное уменьшение содержания активирующих добавок (церия, серебра и сурьмы) приводит к снижению фоточувствительности, уменьшению динамического диапазона и увеличению времени термообработки. В то же время пропускание голограмм в видимом диапазоне увеличивается в 5 раз. Это позволяет получать толстые (3–5 мм) голограммы на ФТР-стекле для видимого диапазона спектра.

Литература

1. Кучинский С.А., Никоноров Н.В., Панышева Е.И., Савин В.В., Туниманова И.В. Свойства объемных фазовых голограмм на мультихромных стеклах // Оптика и спектроскопия. – 1991. – Т. 70. – № 6. – С. 1296.
2. Kogelnik H. Coupled wave theory for thick hologram grating // Bell Syst. Techn. J. – 1969. – Vol. 48. – №9. – P. 2909-2947.
3. Андреева О.В., Корзинин Ю.Л., Назаров В.Н., Гаврилюк Е.Р., Курсакова А.М. Дифракционная эффективность серебросодержащих голограмм на пористых стеклах в красной и ИК-областях спектра // Оптический журнал. – 1997. – Т. 64. – №4. – С. 142.

ПОЛУЧЕНИЕ ВТОРОЙ СТОКСОВОЙ КОМПОНЕНТЫ ВКР(Λ~1,3152 МКМ) В КРИСТАЛЛАХ $KY(WO_4)_2$ ПРИ НАКАЧКЕ $GD_3GA_5O_{12}$:ND-ЛАЗЕРОМ

О.Н. Антонов, Я.С. Пантась, А.В. Сандуленко, М.Г. Сугракшиева
Научный руководитель – д.ф.-м.н., профессор И.В. Мочалов

Статья содержит описание принципов работы и особенностей генерации моноимпульсного твердотельного ВКР лазера, генерирующего на длине волны 1,3152 мкм. Излучение на длине волны 1,3152 мкм генерировалось путем преобразования излучения неодима в кристалле $Gd_3Ga_5O_{12}$:Nd на основном переходе во вторую стоксову компоненту ВКР кристаллом $KY(WO_4)_2$.

Введение

Для инициирования работы мощных каскадов лазерных усилителей на парах йода используется задающий генератор с управляемыми спектральными, временными и пространственными характеристиками излучения. Обычно в качестве такого задающего генератора используется генератор на парах йода, но его использование осложняется необходимостью после каждого использования удалять из рабочей камеры продукты реакции (кристаллический йод, углерод и пр.). Поэтому представляется актуальной задача разработки лишенного этого недостатка твердотельного генератора. При создании такого излучателя необходимо учитывать все предъявляемые к нему требования по спектральным, пространственным и временным характеристикам.

Одним из основных требований, предъявляемых к задающему генератору, является точное соответствие длины волны генерируемого излучения линии усиления йода (λ=1,3152 мкм). Возможным решением этой задачи могло бы быть создание лазера на твердотельной активной среде, генерирующей непосредственно на 1,3152 мкм. Известно, что в области 1,3 мкм ионы трехвалентного неодима могут излучать на дополнительном переходе $^4F_{3/2} \rightarrow {}^4I_{13/2}$. Однако поперечное сечение вынужденного излучения на этом переходе в 3–3,5 раза меньше, чем на более сильном основном $^4F_{3/2} \rightarrow {}^4I_{11/2}$, поэтому одна из основных трудностей получения эффективной генерации на данном переходе связана со сбросом инверсии населенности через канал суперлюминесценции, протекающей на более сильном основном переходе. При работе с небольшими выходными энергиями генерации такой лазер мог бы надежно работать, но при необходимости достижения более высоких выходных энергий эта трудность становится непреодолимой. Кроме того, ни одна из известных неодим-содержащих лазерных сред [1] не обеспечивает длину волны генерации, равную 1,315 мкм, а поиск новых активных сред (не обозначенных в справочниках), генерирующих на заданной длине волны, является дорогостоящей исследовательской работой.

Другой возможностью получения генерации на необходимой длине волны могла бы явиться разработка параметрического генератора света, однако при этом существенным недостатком является высокая чувствительность установки к изменению внешних параметров, особенно к температуре. Специфика задачи требует высокой стабильности длины волны задающего излучателя, что усложняет и увеличивает стоимость реализации этого метода.

В качестве одной из возможных схем задающего лазера, удовлетворяющей всем поставленным условиям, предлагается использовать генератор, в котором излучение на требуемой длине волны получается как вторая стоксова компонента, генерируемая при накачке твердотельной ВКР-активной (ВКР – вынужденное комбинационное рассеяние) среды неодимовым лазером. Особенностью схемы является внутрирезонаторное расположение ВКР-активного элемента [2].

Постановка задачи

Задачей настоящей работы являлось исследование возможности получения генерации на длине волны λ=1,3152 мкм с использованием преобразования излучения на основном переходе $^4F_{3/2} \rightarrow {}^4I_{11/2}$ иона неодима в кристалле $Gd_3Ga_5O_{12}$:Nd во вторую стоксову компоненту ВКР в кристалле $KY(WO_4)_2$. Для этого необходимо было разработать лазер, отвечающий следующим требованиям:

(а) длина волны генерации λ=(1,3152±0,00005) мкм;
(б) полуширина линии генерации ≤ 0,5 $см^{-1}$;
(в) длительность импульса ≤ 1 нс;
(г) энергия импульса > 1 мДж.

Требования к точности длины волны генерации обусловлены необходимостью попадания в узкую спектральную линию усиления паров йода.

Выбор пары активная среда – ВКР кристалл

Для выбора твердотельной активной среды задающего лазера и ВКР-активной среды, обеспечивающих возможность получения генерации на длине волны λ=1,3152 мкм, требовалось осуществить расчет необходимой длины волны лазера накачки, чтобы вторая стоксова компонента, генерируемая одной из известных ВКР-активных сред [3], обеспечила получения необходимой длины волны. Расчет производился по формуле

$$\lambda = . \frac{10^4}{\left(10^4 \Big/ \lambda_{зад} + 2\Omega_R \right)}, \qquad (1)$$

где $\lambda_{зад}$ – требуемая длина волны 1,3152 мкм; λ – искомая длина волны накачки (мкм); Ω_R – величина стоксова сдвига ($см^{-1}$).

В табл. 1 приведены величины стоксова сдвига некоторых ВКР-активных кристаллов и рассчитанные по формуле (1) требуемые длины волн генерации.

Наименование кристалла	Величина стоксова сдвига ($см^{-1}$)	Требуемая длина волны генерации (мкм)
$KGd(WO_4)_2$	767,4	1,0943
$KGd(WO_4)_2$	901,0	1,0631
$KY(WO_4)_2$	905,6	1,0621
$KYb(WO_4)_2$	908,0	1,0616
$Na_2\ WO_4$	929,2	1,0569
$Ba(NO_3)_2$	1048,6	1,0309

Таблица 1. Величины Стоксовых сдвигов ВКР-активных кристаллов и требуемые длины волн генерации твердотельной активной среды задающего лазера

В табл. 2 приведены длины волн генерации некоторых неодим-содержащих кристаллов [1]. Данные приведены для матриц, обеспечивающих генерацию на длинах волн, близких к требуемым при комнатной температуре.

Наименование кристалла	Длина волны генерации (мкм) при T=300K
$Gd_3Sc_2Al_3O_{12}$:Nd	1,0620
$Lu_3Sc_2Al_3O_{12}$:Nd	1,0620
$Gd_3Ga_5O_{12}$:Nd	1,0621
$Y_3Sc_2Al_3O_{12}$:Nd	1,0622
$Ca_5(PO_4)_3F$:Nd	1,0630
LaF_3:Nd	1,0632
CaF_2-YF_3:Nd	1,0632

Таблица 2. Длины волн генерации некоторых неодим-содержащих кристаллов при 300K

В результате анализа данных, приведенных в табл. 1 и 2, были выбраны 2 пары кристаллов, позволяющие получить генерацию на требуемой длине волны:

- LaF_3:Nd (фтористый лантан, активированный неодимом) и $KGd(WO_4)_2$(КГВ – калий–гадолиниевый вольфрамат);
- $Gd_3Ga_5O_{12}$:Nd (ГГГ – галлий–гадолиниевый гранат, активированный неодимом) и $KY(WO_4)_2$ (КИВ – калий-иттриевый вольфрамат).

Использование в качестве ВКР-активных сред кристаллов двойных вольфраматов предоставляло возможность замены редкоземельных ионов основы (иттрия или гадолиния) на ионы других спектрально-нейтральных редкоземельных металлов (лантана, иттербия или лютеция), что, в конечном итоге, позволяло плавно изменять значение стоксова сдвига и настраивать излучение на нужную длину волны. Используемая в работе в качестве модельной схема генерации с ламповой накачкой и длиной резонатора в несколько десятков сантиметров заведомо не могла обеспечить требуемых длительностей импульса. Для достижения длительности импульсов ~1 нс необходимо использование коротких (~1 см) резонаторов, реализуемых в схемах лазеров с диодной накачкой.

Экспериментальная установка

Эксперименты проводились на макете лазера, оптическая схема которого приведена на рис. 1.

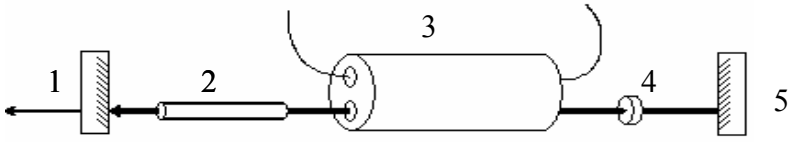


Рис. 1. Оптическая схема ВКР лазера: 1 – выходное зеркало; 2 – ВКР-активная среда; 3 – квантрон с лампой накачки и активным элементом; 4 – пассивный затвор; 5 – глухое зеркало

В резонаторе использовалось плоское глухое зеркало, имеющее R~100% на длинах волн 1,06 мкм, 1,17 мкм и 1,31 мкм, что соответствует излучению неодимового лазера, первой и второй стоксовой компоненты. В качестве выходного использовалось сферическое зеркало с радиусом кривизны 1,5 м, R>99% на длинах волн 1,06 мкм, 1,17 мкм и R~50% на длине волны 1,31 мкм. Для обеспечения моноимпульсной генерации использовался пассивный кристаллический затвор (Q-switch).

Спектральные исследования

Измерение максимума длины волны генерации лазера на кристалле ГГГ:Nd (переход $^4F_{3/2}$-$^4I_{1/2}$ λ~1,06 мкм)

В литературных источниках [1, 3] приводятся отличные друг от друга значения максимумов длин волн генерации иона неодима в кристаллах ГГГ на переходе $^4F_{3/2} \rightarrow {}^4I_{11/2}$. Поэтому вопрос уточнения значения максимума длины волны генерации кристаллов ГГГ на переходе $^4F_{3/2} \rightarrow {}^4I_{11/2}$ представлялся достаточно важным при выполнении настоящей работы.

Для проведения спектральных исследований на активном элементе из кристалла ГГГ был собран лазер с торцевой диодной накачкой, имеющий следующие параметры:

(а) длина резонатора 18 мм;
(б) зеркала плоские;
(в) коэффициент отражения выходного зеркала на длине волны λ~1,06 мкм R=85 %;
(г) начальное пропускание пассивного кристаллического затвора YAG:Cr^{3+} T_0=75 %;
(д) режим работы – импульсный частота 500 Гц;
(е) ток лазерного диода накачки (LDD-9) – 3,2 А.

Проведенные измерения показали, что длина волны генерации кристаллов ГГГ:Nd составляла λ=(1,0621±0,00005) мкм. Это значение с хорошей точностью совпало с длиной волны задающего генератора, которую мы использовали в наших расчетах, для получения генерации на длине волны λ=1,3152 мкм, считая, что стоксов сдвиг в ВКР-активной среде (кристалле КИВ) составляет 905,6 $см^{-1}$.

Измерение максимума длины волны генерации второй стоксовой компоненты ВКР лазера на основе пары ГГГ:Nd – КИВ (λ~ 1.315)

Было проведено измерение длины волны генерации второй стоксовой компоненты ВКР лазера на основе пары ГГГ:Nd – КИВ с ламповой накачкой (рис. 1). Для проведения измерений был собран лазер, резонатор которого имел следующие параметры:

(а) «глухое» зеркало – плоское, коэффициент отражения *R*>99%, λ~1,06, 1,18 и 1,32 мкм;
(б) выходное зеркало – сферическое, с радиусом кривизны r=1,5 м и коэффициентами отражения *R*>99%, λ~1,06 и 1,18 мкм, и *R*~65%, λ~1,32 мкм;
(в) длина резонатора 0,4 м;
(г) активный элемент находился в трубке из кварца марки КЛЖ толщиной 1 мм;
(д) в качестве пассивного кристаллического затвора использовалась просветленная на рабочих длинах волн пластина из кристалла ГСГГ:Cr^{4+} толщиной ~1,5 мм, с начальным пропусканием *R*=18%;
(е) энергия накачки составляла 20 Дж;

Было установлено, что максимум длины волны второй стоксовой компоненты ВКР лазера на основе пары ГГГ – КИВ соответствовал длине волны λ=(1,3152±0,00005) мкм. Это подтвердило правильность выбранной концепции построения задающего генератора для каскада усилителей на парах йода с использованием твердотельного лазера, преобразующего излучение неодима в кристалле ГГГ на основном переходе во вторую стоксову компоненту ВКР в кристалле КИВ.

Исследование контура спектральной линии второй стоксовой компоненты ВКР лазера ГГГ:Nd – КИВ

Для оценки полуширины линии излучения были проведены исследования контура спектральной линии второй стоксовой компоненты описываемого ВКР лазера.

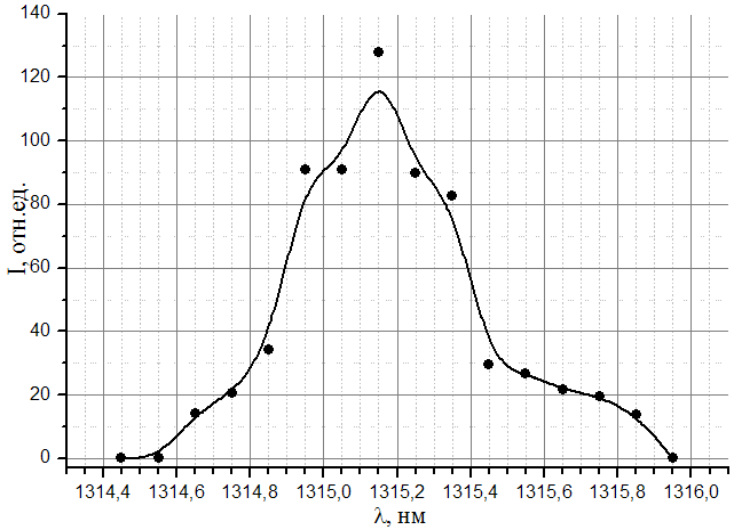


Рис. 2. Форма спектральной линии второй стоксовой компоненты ВКР лазера

Измеренная полуширина линии (рис. 2) соответствовала значению ~2,4 см$^{-1}$. Такая полуширина свидетельствует о наличии нескольких продольных мод в излучении лазера и может быть уменьшена переходом к одномодовому режиму, например, путем введения внутрь резонатора интерферометра Фабри-Перо или трехмерной брегговской структуры для узкополосной фильтрации задающего излучения.

Исследования динамики и формы импульса

Исследования временной формы импульса проводились с использованием быстродействующего фотоприемника ЛФД2 и осциллографа LeCroy LC-534. Собранная установка позволяла измерять длительность импульсов с точностью не хуже 1 нс. Параметры резонатора аналогичны указанным при описании измерения длины волны ВКР лазера. На рис. 3 приведена временная форма импульса второй стоксовой компоненты ВКР лазера (λ=1,3152 мкм), преобразующего излучение неодима в кристалле ГГГ на основном переходе во вторую стоксову компоненту ВКР в кристалле КИВ.

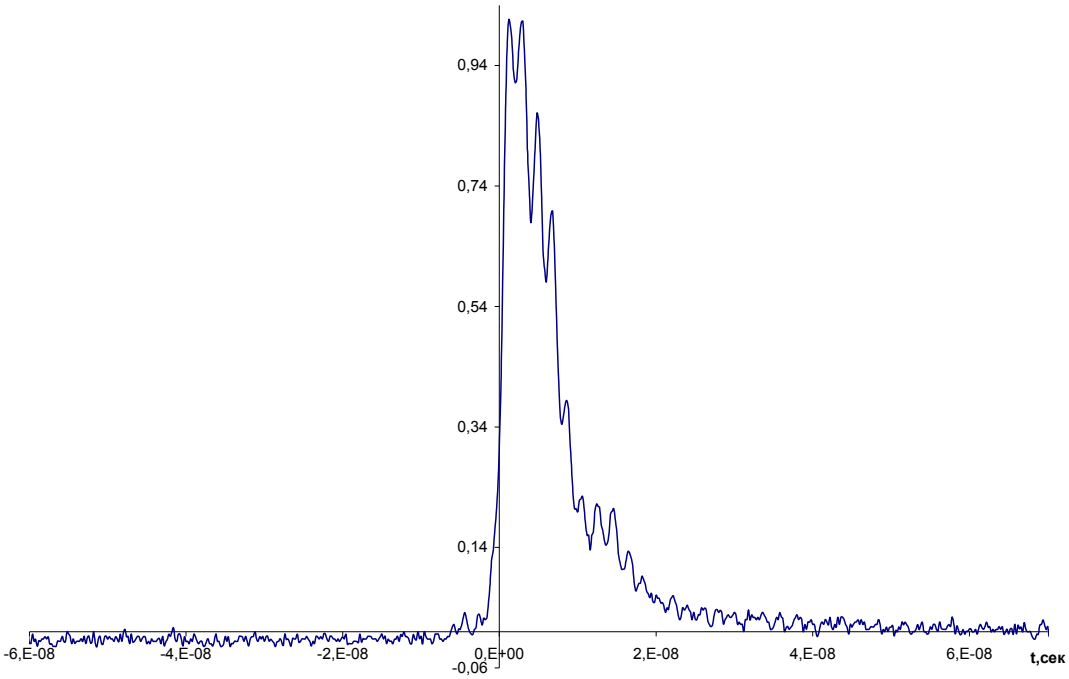


Рис. 3. Осциллограмма импульса второй стоксовой компоненты ВКР лазера

Длительность импульса составила ~7 нс. Подобная длительность импульса характерна для схемы с ламповой накачкой. В схеме с диодной накачкой за счет уменьшения длины резонатора до нескольких миллиметров эта величина может быть доведена до ~1 нс.

Заключение

В работе описана схема лазера, в котором излучение на длине волны 1,3152 мкм получается преобразованием излучения на основном переходе иона неодима в кристалле $Gd_3Ga_5O_{12}$:Nd во вторую стоксову компоненту в кристалле $KY(WO_4)_2$.

ВКР лазер, собранный по предложенной схеме, обеспечил получение генерации на длине волны 1,3152 мкм с полушириной спектральной линии ~1,4 $см^{-1}$ и длительностью импульса ~7 нс. Для получения более коротких длительностей импульса необходим переход к резонатору длиной не более 15–20 мм и использование диодной накачки вместо ламповой.

В результате проведенных экспериментов показана принципиальная возможность использования в качестве задающего генератора для каскада усилителей на парах йода твердотельного ВКР лазера, генерирующего излучение на длине волны λ=1,3152 мкм при преобразовании генерации на основном переходе неодима в кристалле $Gd_3Ga_5O_{12}$ (λ=1,0621 мкм) во вторую стоксову компоненту ВКР в кристалле $KY(WO_4)_2$.

Литература

1. Weber, M. J. Handbook of Laser Wavelengths. – CRC Press LLC, 1999. – 777 p.
2. Webb C.E., Jones J.D. Handbook of Laser Technology and Applications. 3 Volumes. – IoP, 2004. – 2725 p.
3. Basiev T.T., Sobol A.A., Zverev P.G., Osiko V.V. Comparative spontaneous Raman spectroscopy of crystals for Raman lasers. // Sov. J. Quantum Electron. – 17. – 1999. – 1560–1563.
4. Справочник по лазерам. Т.1. / Под ред. Прохорова А.М. – М.: Советское радио, 1978. – 504 с.

ДИСПЕРСИЯ ПАРАМЕТРОВ ГОЛОГРАММ-РЕШЕТОК В ПОЛИМЕРНОЙ СРЕДЕ С ФЕНАНТРЕНХИНОНОМ

А.А. Кулешов, В.В. Лесничий
Научный руководитель – к.ф.-м.н., ст.н.с. О.В. Андреева

Рассмотрена дисперсия амплитуды фазовой модуляции голограмм-решеток, предназначенных для использования в качестве голограммных оптических элементов. Экспериментальные данные получены на основании измерения дифракционной эффективности и контуров угловой селективности голограмм при различных длинах волн видимого излучения. Получены зависимости амплитуды модуляции показателя преломления в исследуемых образцах от длины волны излучения.

Введение

Объемные голограммы представляют большой интерес с точки зрения создания на их основе голограммных оптических элементов для практического использования в ряде научно-технических приложений. В ходе работы был проанализирован ряд зарубежных [1] и отечественных работ в данной области.

В данной работе проведено исследование малоизученной характеристики полимерных регистрирующих сред на основе фенантренхинона (ФХ) – дисперсии зарегистрированных голограмм-решеток в видимой области спектра. Данная характеристика определяет возможности использования оптических элементов, созданных на основе объемных голограмм, в различных областях спектра.

Объект исследования

Объектом исследования являлись пропускающие объемные голограммы-решетки на полимерном регистрирующем материале «Диффен». Данный материал представляет собой твердый раствор ФХ в полиметилметакрилате (ПММА). При облучении светом определенной длины волны (спектр поглощения ФХ и фотопродукта представлен на рис. 1) ФХ переходит в фотопродукт (ФП), прикрепляясь к твердому каркасу из ПММА [4–6].

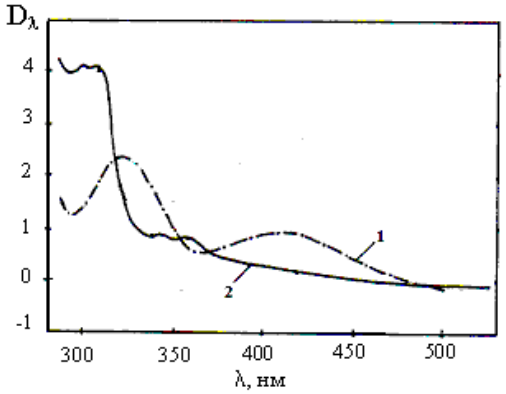


Рис. 1. Спектры поглощения фенантренхинона (кривая 1) и фотопродукта (кривая 2) в полимерной матрице

Зарегистрированная голограмма проходит стадию постэкспозиционного диффузного усиления и стадию фиксирования. Готовая голограмма представляет собой модуляцию концентрации молекул фотопродукта в полимерной матрице. Дисперсия параметров голограммы определяется дисперсией оптических параметров среды, обусловленной наличием молекул фотопродукта.

Теоретическая часть

Среди параметров объемных голограмм в работе основное внимание уделялось дифракционной эффективности (ДЭ) и контуру угловой селективности голограммы. Объемные пропускающие голограммы имеют только два порядка дифракции – нулевой и первый. Дифракционная эффективность η определяется отношением интенсивности дифрагированного пучка к сумме интенсивностей пучков за голограммой:

$$\eta = \frac{I_д}{I_д + I_0}, \qquad (1)$$

где $I_д$ – интенсивность пучка первого (единственного) порядка дифракции; I_0 – интенсивность пучка нулевого порядка дифракции. По этой формуле ДЭ легко вычислить при проведении эксперимента.

Для аналитического описания параметров пропускающих голограмм с учетом оптических характеристик регистрирующей среды используют формулу теории связанных волн Когельника [7]:

$$\eta = \sin^2\sqrt{\xi^2 + \varphi_1^2} \Big/ \left(\frac{\xi^2}{\varphi_1^2} + 1\right), \qquad (2)$$

где параметр ξ определяет отклонение от условий Брэгга при освещении голограммы, а φ_1 – амплитуда фазовой модуляции – определяется формулой:

$$\varphi_1 = \frac{\pi n_0 n_1 T}{\lambda_в \cos\theta_0}, \qquad (3)$$

n_1 – амплитуда первой гармоники изменения показателя преломления среды; T – толщина голограммы; $\lambda_в$ – длина волны падающего излучения в воздухе; $2\theta_0$ – угол между пучками $I_д$ и I_0, n_0 – показатель преломления среды.

Для фазовых пропускающих голограмм при выполнении условий Брэгга зависимость (2) принимает вид

$$\eta = \sin^2 \varphi_1. \qquad (4)$$

Формула (4) связывает измеряемые параметры голограммы (ДЭ) с параметрами регистрирующей среды (n_1, T) и условиями эксперимента (λ, $\cos\theta$).

Экспериментальная часть

Данные экспериментальных измерений и расчетов для одной из исследуемых голограмм приведены в таблице для различных длин волн (λ – столбец 1), ДЭ (столбец 2) – экспериментальный параметр, определяемый по данным измерений $I_д$ и I_0 по формуле (1). Амплитуда фазовой модуляции (φ_1 – столбец 3) определялась по формуле (4) на основании измерений ДЭ и контура угловой селективности. Необходимые для проведения расчетов данные $n_0(\lambda)$ – столбец 4 – взяты из справочной литературы [8].

Угол между пучками, соответствующий выполнению условия Брэгга внутри среды для данной длины волны (θ_0 – столбец 5) для исследуемой решетки определялся расчетным путем по известной пространственной частоте голограммы. Толщина исследуемых голограмм (T) известна, что позволяло произвести расчеты по формуле (3) амплитуды модуляции показателя преломления (n_1 – столбец 6).

В ходе экспериментов было проведено шесть серий измерений на разных длинах волн, при использовании ионного аргонового лазера (458 и 488 нм), неодимового твердотельного лазера с диодной накачкой (532 нм), гелий-неонового лазера (633 нм), полупроводникового лазера на основе модуля KLM-650 (654 нм), титан-сапфирового лазера в непрерывном режиме (808 нм).

График зависимости фазовой модуляции от длины волны для двух исследованных голограмм приведен на рис. 3.

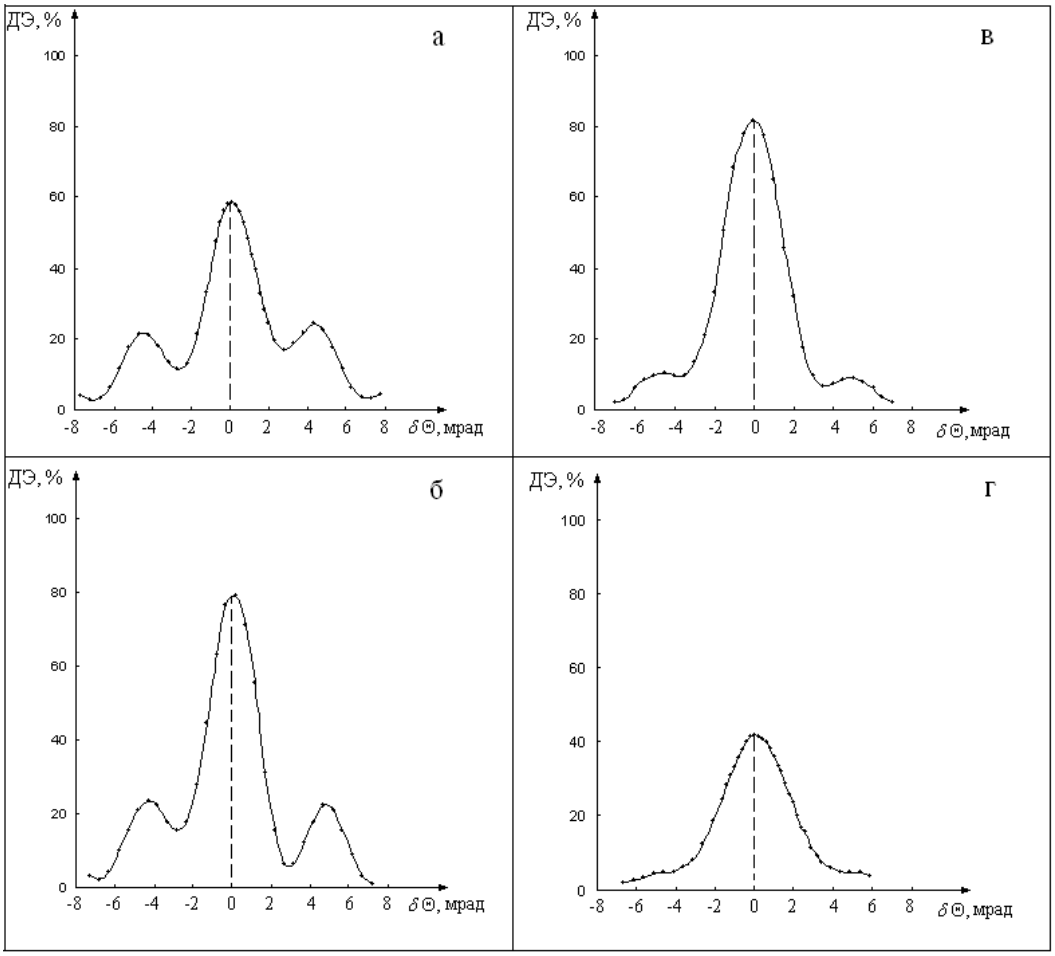


Рис. 2. Контуры угловой селективности голограммы №1 при измерении с различными источниками излучения: а – λ = 458 нм; б – λ = 532 нм; в – λ = 654 нм; г – λ = 808 нм, $\delta\,\Theta$ – отклонение от угла Брэгга, ДЭ – дифракционная эффективность

λ,нм	ДЭ	φ_1	n_0	θo	n_1
1	2	3	4	5	6
458	0,59	0,72π	1,4990	$2{,}89^o$	$2{,}20\cdot10^{-4}$
488	0,54	0,72π	1,4960	$3{,}43^o$	$2{,}34\cdot10^{-4}$
532	0,79	0,68π	1,4933	$3{,}74^o$	$2{,}42\cdot10^{-4}$
633	0,84	0,55π	1,4886	$4{,}47^o$	$2{,}33\cdot10^{-4}$
654	0,82	0,53π	1,4880	$4{,}62^o$	$2{,}32\cdot10^{-4}$
808	0,42	0,23π	1,4846	$5{,}72^o$	$1{,}25\cdot10^{-4}$

Таблица. Результаты измерений и расчетов

В соответствии с тем, что молекулы фотопродукта, образующие голограмму-решетку имеют полосу поглощения в коротковолновой области спектра (рис. 1, кривая 2), наблюдается снижение величины φ_1 при увеличении длины волны.

Значительный интерес представляет спектральная зависимость амплитуды модуляции показателя преломления среды, которая представлена на рис. 4. Следует отметить, что изменение показателя преломления среды, обусловленное наличием фотопро-

дукта, также имеет устойчивую тенденцию к падению при увеличении длины волны для всех исследованных голограмм.

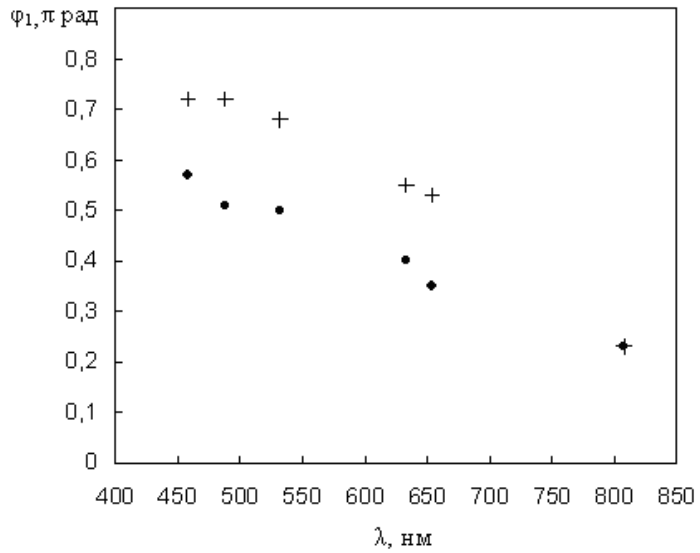


Рис. 3. Зависимость фазовой модуляции (φ_1) от длины волны падающего излучения (λ) для двух образцов: + – голограмма 1; ● – голограмма 2

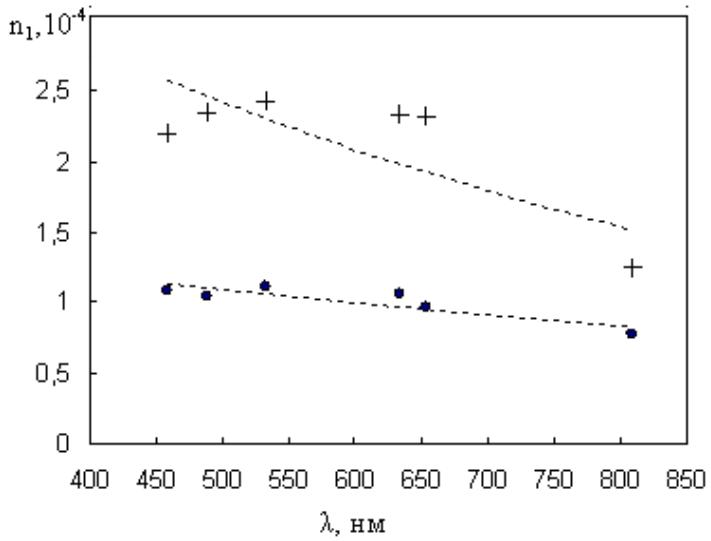


Рис. 4. Дисперсия амплитуды модуляции показателя преломления среды, обусловленная наличием молекул фотопродукта для голограмм: + – голограмма 1; ● – голограмма 2. Пунктир – аппроксимация экспоненциальной зависимостью

Выводы

Представлены результаты экспериментов по определению дисперсии параметров голограмм, полученных в регистрирующей среде на основе фенантренхинона.

Продемонстрирован нормальных характер дисперсии амплитуды фазовой модуляции голограмм и амплитуды модуляции показателя преломления среды.

Результаты работы могут быть использованы при оценке параметров голограммных оптических элементов при различных длинах волн и при изучении оптических параметров регистрирующей среды при ее засветке и постэкспозиционной обработке.

Авторы статьи выражают особую благодарность О.В. Бандюк и А.А. Парамонову за совместную работу.

Литература

1. Lawrence J.R., O'Neill F.T., Sheridan J.T. Photopolymer holographic recording material // International Journal for Light and Electron Optics. – 2001. – №10. – P. 449–463.
2. Вениаминов А.В., Гончаров В.Ф., Попов А.П. Усиление голограмм за счет диффузионной деструкции противофазных периодических структур // Оптика и спектроскопия. – 1991. – Т.70. – В.4. – С. 864–869.
3. Андреева О.В., Бандюк О.В., Парамонов А.А. и др. Объемные пропускающие голограммы в полимерной среде с фенантренхиноном // Оптический журнал. – 2000. – №12. – С. 27–33.
4. Андреева О.В., Бандюк О.В., Парамонов А.А., Кушнаренко А.П., Лесничий В.В., Начаров А.П., Андреева Н.В. Высокоэффективные мультиплексные голограммы на полимерном материале «Диффен» // Оптический журнал. – 2006. – №9. – С. 60–64.
5. H. Kogelnik. Coupled wave theory for thick hologram gratings//The bell system technical journal. – 1969. – №9. – P. 2909–2947.
6. R.M. Waxler, D. Horowitz & A. Feldman. Optical and physical parameters of Plexiglas 55 and Lexan // Applied Optics. – 1979. – №18. – P. 101–104.

ПОЛУЧЕНИЕ ПОЛИМЕРНЫХ МАТРИЦ МИКРОЛИНЗ МЕТОДОМ ГОРЯЧЕГО ТИСНЕНИЯ

Ю.А. Громова
Научный руководитель – М.И. Фокина

Рассматривается возможность реализации процесса получения матриц микролинз (для размера линз порядка 10 мкм) методом горячего тиснения на пленках полиметилметакрилата.

Введение

В последние годы стала интенсивно развиваться оптическая связь, интегральная и волоконная оптика, происходит внедрение оптоэлектроники в аппаратуру широкого применения, где требуются рельефные выпуклые микроструктуры на поверхности оптических материалов. Чаще всего используются микролинзы. Как следует из названия, микролинзы – это миниатюрные линзы размером от единиц до сотен микрон, которые могут быть объединены в двумерную решетку.

Области применения микролинз напрямую связаны с развитием микроэлектроники и оптоэлектроники. Микролинзы и решетки микролинз применяются во многих областях техники: в фотолитографии для копирования матриц микроэлементов; для улучшения параметров фотоприемных матриц, для связи оптических волноводов, в том числе и разных диаметров [1– 3].

Общим для всех областей применения является необходимость максимального удешевления как материалов, так и используемых технологических процессов, что делает использование классического оптического стекла в этой области весьма проблематичным. Одним из выходов в данной ситуации является использование альтернативных материалов (например, полимеров) и методов формообразования оптических деталей, исключающих сложные технологические операции, такие как шлифовка и полировка.

Технические требования к параметрам микролинз разнообразны соответственно областям их применения. На сегодняшний день известны различные технологий изготовления полимерных микрооптических элементов (в основном микролинз): электроосаждение [4], метод, основанный на деформации под действием импульса лазера [5], метод ультрафиолетового отверждения [6, 7], также используются свойства усадки полимеров. Еще один способ получения микролинз – горячее тиснение [8] – выдавливание полимера через жесткую маску при высоких температурах. Этот метод позволяет получить матрицы необходимого размера из одинаковых элементов с хорошей сферической поверхностью, которая определяется силами поверхностного натяжения. Также есть возможность необходимым образом варьировать упаковку и размеры микролинз. Горячее тиснение является технологически простым и незатратным способом производства, что крайне привлекательно для его практического применения. В свете этих причин этот способ и был выбран для более детального изучения.

Эксперимент

Для проведения опыта была изготовлена пленка из ПММА (полиметилметакрилат) двух типов ATONAS V5 и CO-120. Такие материалы были выбраны из-за их доступности, также важны их оптические свойства. Конечно, по пропусканию света полимеры во много раз уступают стеклу (стандартное рассеяние оптических полимеров порядка единиц процентов, а рассеивание стекла порядка 10^{-5}%). Но для областей, где применяются микролинзы, а основной их задачей является концентрация света, получаемого оптического качества вполне достаточно. Еще одним плюсом использованных материалов является невысокая температура размягчения (около 100°C), пластичность,

а, следовательно, технологические операции не требуют сложной технологической базы, также эти материалы устойчивы к повреждениям.

Пленки получались методом полива из раствора ПММА в дихлорэтане. Пленка высыхает несколько дней, после чего помещается на сутки в печь при температуре t=50°С для удаления возможных остатков растворителя. Полученные образцы обладают коэффициентами рассеиванья порядка 15% , в то время как стандартные показатели для полимеров равны 0,2% для поликарбоната и полиэстера 0,5–1%, а для акрилатов 1–2%. Такие данные объясняются неидеальными условиями эксперимента и неотработанной на данный момент технологией.

Установка для получения микролинз представлена на рис. 1.

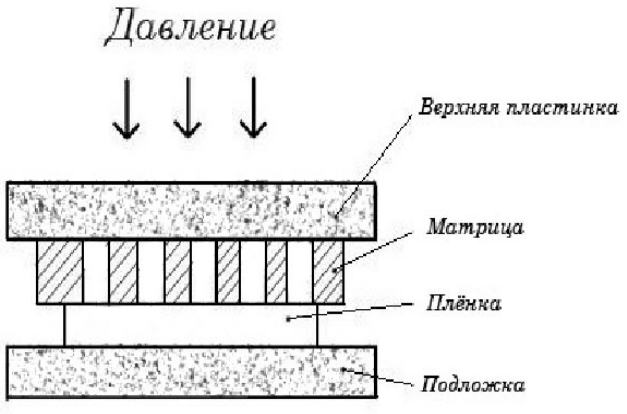


Рис. 1. Схема получения микролинз методом горячего тиснения

В качестве матрицы использовалась микроячеистая кварцевая пластина с плотной упаковкой (рис. 2). Давление обеспечивалось грузом порядка 1 кг. Наиболее оптимальная для проведения эксперимента температура – 100–105°С, время давления от 30 до 40 мин. Под действием давление происходит затекание размягченного полимера в микропоры матрицы, благодаря плохой смачиваемости стенок отверстий и силам поверхностного натяжения образуется поверхность микролинзы, близкая к сферической.

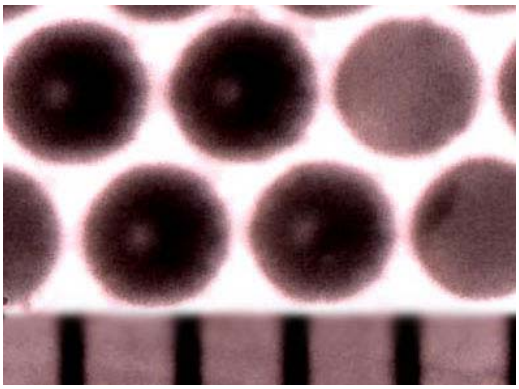
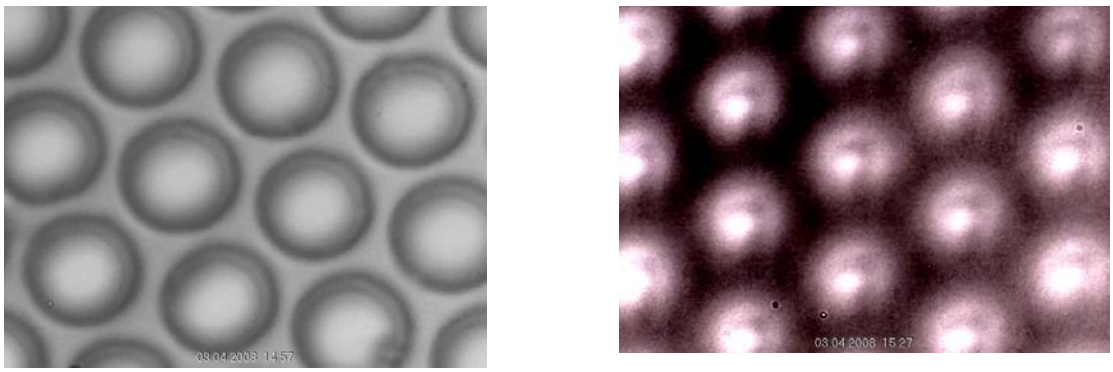


Рис. 2. Микроячеистая пластина. Объект-микрометр. 1 деление – 10 мкм

В результате были получены решетки микролинз (рис. 3, а), состоящие из идентичных элементов, способных фокусировать изображение (рис.3, б). Изображение цифры 7, построенное микролинзами, подтверждает их оптическое качество.



а) б)

Рис. 3: а – матрица микролинз; б – изображение цифры 7, построенное в микролинзах

Заключение

Горячие тиснение является экономически выгодным и технологически простым способом получения решеток микролинз довольно высокого качества. Этот новый способ еще недостаточно изучен, но уже на данном этапе понятно, что он чрезвычайно интересен для применения на практике.

Литература

1. Wu M.-H. and Whitesides G. M. Fabrication of two – dimensional arrays of microlenses and their applications in photolithography // J. Micromech. Microeng. – 2002. – V.12. – P. 747–758.
2. Berkel C., McGarvey B.P. and Clarke J.A. Microlens arrays for 2D large area image sensors // Pure Appl. Opt – 1994. – V. 3. – P. 177–182.
3. Richard R., Syms A., Refractive Collimating Microlens Arrays by Surface Tension Self-Assembly // IEEE Photonics Technology Lett. – 2000. – V.12. – P. 1507–1509.
4. Sakurai Y., Okuda S., Nishiguchi H., Nagayama N. and Yokoyama M. Microlens array fabrication based on polymer electrodeposition // J. Mater. Chem. – 2003. – V. 13. – P. 1862–1864.
5. Hessler Th., Rossi M., Pedersen J., Gale M.T., Wegner M., Steudle D. and Tiziani H.J. Microlens arrays with spatial variation of the optical function // Pure Appl. Opt. – 1997. – V. 6. – P. 673–681.
6. Madanagopal V. Kunnavakkam, Houlihan F M., Schlax M., Liddle J.A., Kolodner P., Nalamasu O. and Rogers J.A. Low-cost, low-loss microlens arrays fabricated by soft – litography replication process // Appl. Phys. Lett. – 2003. – V. 8. – P. 1152–1154.
7. Chan-Park M.B., Neo W.K. Ultraviolet embossing for patterning high aspect ratio polymeric microstructures // Microsystem Technologies. – 2003. – V. 9. – P. 501–506.
8. Pantelis P., McCartney D.J. Polymer microlens arrays // Pure Appl. Opt. – 1994. – V. 3. – P. 103–108.

ОСОБЕННОСТИ ФОРМИРОВАНИЯ МИКРОСТРУКТУР С ВЫСОКИМ ФОРМАТНЫМ ОТНОШЕНИЕМ ПРИ ФОТООТВЕРЖДЕНИИ ПОЛИМЕРА

В.Г. Булгакова

Научные руководители – Ю.Э. Бурункова; к.т.н., доцент Н.Д. Ворзобова

Приведены результаты исследований процесса формирования микроструктур в УФ-отверждаемых нанокомпозиционных материалах методом глубокой литографии (deep lithography). Исследован эффект расширения области фотополимаризации за пределы точки экспонирования при уменьшении относительного расстояния между формируемыми элементами.

Введение

Методы формирования микроэлементов и микроструктур представляют интерес для различных направлений науки и техники. Полимерные микроструктуры в настоящее время востребованы в качестве структур, составляющих основу технологий получения интегральных микросхем, элементов MEMS и MOEMS, а также элементов управления световыми пучками в системах телекоммуникаций, в том числе в волоконных линиях связи, информационных системах. Микрорельефные структуры получаются в настоящее время методами литографии. Существующие технологии литографии позволяют получать преимущественно тонкие планарные структуры. Перспективным направлением литографии является получение объемных микроструктур [1, 2]. Современный уровень исследований в данном направлении характеризуется поиском возможных методов формирования структур нужной формы, уменьшением характеристического размера элементов, увеличением форматного отношения.

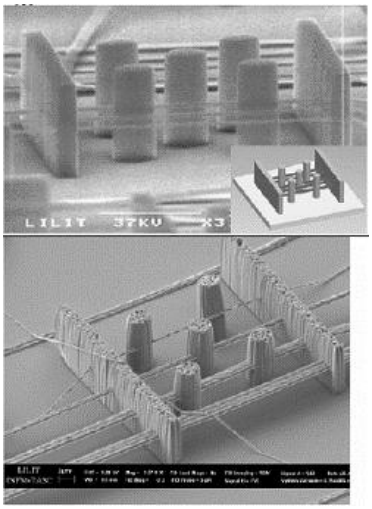


Рис. 1. Пример современной реализации MEMC элемента

Пример двух элементов интегральной микроэлектромеханической структуры, сформированной на базе полимера по технологии рентгеновской литографии, представлен на рис. 1 [3]. Приведенный рисунок показывает, что для реализации MEMC элементов необходимы технологии, обеспечивающие формирование 3-мерных структур микронных размеров сложной формы. Реализация этих структур обычными методами литографии невозможна, и необходима разработка новых технологий.

В настоящее время большая часть полимерных MEMC структур формируется с использованием рентгеновской литографии, однако данный метод требует применения дорогостоящего оборудования, и поэтому продолжаются исследования, направленные

на поиск альтернативных методов, основанных на оптической фотолитографии и специальных полимерных материалах. В данной работе исследовался метод фотолитографии, основанный на эффекте самофокусировки света в фотополимере с положительным знаком изменения показателя преломления при фотополимеризации, описанный в работе [4]. Исследовались эффекты, наблюдаемые при получении структур высотой в несколько сотен микрон с малым относительным расстоянием между элементами, сравнимым с их размером, и их связь с составом материала.

Традиционные полимерные фоторезисты не позволяют получить высокие микроструктуры, например высотой 300 мкм – 1 мм, поскольку при нанесении полимерного слоя соответствующей толщины на подложку из раствора растворитель очень медленно выходит из полимера. Так, все полимерные слои, нанесенные из раствора, содержат некоторое количество растворителя. При увеличении толщины слоя полимера содержание остаточного растворителя увеличивается, так что максимальная толщина слоя полимера, нанесенного методом полива из раствора, составляет 20–50 мкм. Это не позволяет применять для данной цели традиционные полимерные фоторезисты.

По указанным причинам зарубежные исследования высоких структур [1, 2] базируются на использовании специальных фоторезистов, например SU8, которые представляют собой олигомер с низкой молекулярной массой, нанесение которого возможно также из раствора, однако при последующем нагревании происходит его плавление и полное удаление растворителя. Однако даже при применении SU8 остается проблема получения толстых, более 200 мкм толщиной, слоев, поскольку удаление растворителя из толстого слоя затруднено и приводит к получению рыхлой структуры.

По вышеуказанным причинам мы исследовали способы получения высоких структур с применение процессов нанесения слоя, исключающих растворитель. Были использованы жидкие мономерные композиции, основанные на смеси жидких мономеров, описанные в работе [5]. Состав наносился не из раствора, как это обычно имеет место при нанесении полимерных пленок, а в виде капли жидкого вещества (при его нагреве до температуры плавления), нанесенного между подложкой и фотошаблоном. Отсутствие растворителей и полное превращение мономера в полимер приводило к отсутствию эффектов, связанных с выходом растворителей из структуры.

Впервые данный подход был исследован в работе [4], была показана возможность получения структур на базе мономерных композиций и получены структуры с высоким отношением высота/ширина и вертикальными боковыми поверхностями. В данной работе было продолжено исследование эффектов, проявляющихся при уменьшении расстояния между элементами структуры.

Методика эксперимента

В экспериментах в качестве фотополимеризующегося состава использована смесь мономеров моно- и диакрилатов, которая полимеризовалась под действием УФ света длиной волны 365 нм, в соответствии со спектром поглощения введенного фотоинициатора, того же, как и в работе [4]. Использованные вещества приведены в табл. 1.

На базе вышеуказанных веществ (табл. 1) были составлены композиции из смеси акрилатов (табл. 2). Компонент №1 вводился в оба состава для улучшения адгезии формируемых микроструктур к стеклянной подложке. Инициатор вводился во все композиции в концентрации 0,2%, поэтому в таблице не приведен. По сравнению с составом №1 состав №2 имеет большую вязкость. Влияние вязкости состава на процесс формирования структур будет рассмотрен далее.

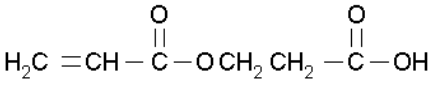
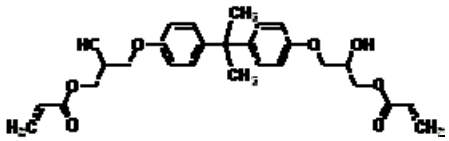
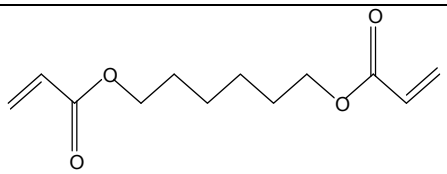
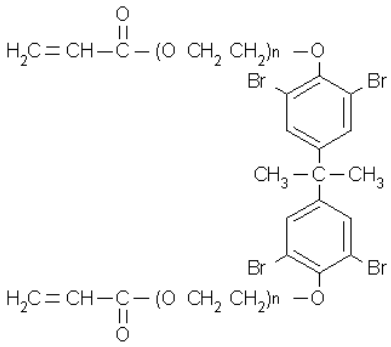
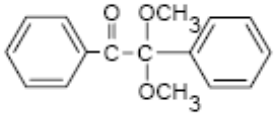
№	Название	Производитель	Показатель преломления	Химическая формула	Назначение
1	2-carboxyethyl acrylate	Aldrich, № 552348	1,4570		моноакрилат
2	Bisphenol A glycerolate	Aldrich, № 41,116-7	1,557		жидкий диакрилат
3	1,6-hexanediol diacrylate	Aldrich № 24,681-6	1,456		жидкий диакрилат
4	RDX 51027	USB	1,585		твердый диакрилат
5	Диметоксифенилацетофенон (фотоинициатор)	Aldrich			Фотоинициирующая система

Таблица 1. Использованные УФ-отверждаемые мономеры и олигомеры

№	акрилаты	вес %	свойства*
1	№1 №2 №3	60 30 10	жидкая
2	№1 №4	30 70	вязкая

* - агрегатное состояние при температуре экспонирования.
твердые композиции плавятся при 30–50^{0}C.

Таблица 2. Состав композиций (номера компонентов по табл. 1)

В отвержденном состоянии полимер имеет хорошие оптические свойства (отсутствие окраски, незначительное светорассеяние), что позволяет использовать его как альтернативу стекла. Более подробно составы и их характеристики рассмотрены в работе [5]. Процесс получения микроэлементов и микроструктур состоял из трех этапов: 1 – изготовление амплитудного фотошаблона, 2 – фотополимеризация слоя мономерной композиции УФ излучением, прошедшим через фотошаблон, 3 – удаление неотвержденного материала при обработке в изопропиловом спирте

Фотошаблоны изготавливались методом оптического уменьшения изображения исходного рисунка (трафарета), полученного методом компьютерной графики, с использованием фотопроекционной установки. Для получения шаблонов использовалась высокочувствительная фотопленка Kodak EL Camera. Обработка проводилась в проявителе Accumax Rapid Access.

Для исследования процессов светоотверждения использовалась лабораторная установка с источником УФ излучения. Схема установки показана на рис. 2.

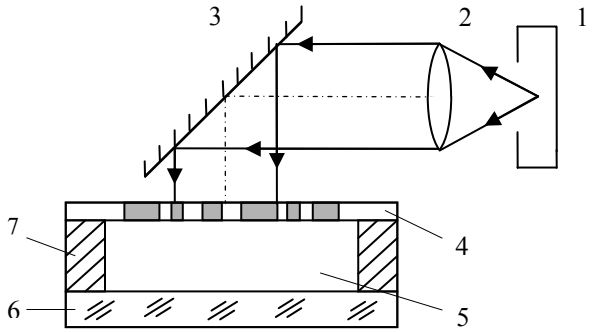


Рис. 2. Схема установки фотополимеризации

Капля нагретой УФ-отверждаемой мономерной композиции 5 наносится на стеклянную подложку 6, затем на нее накладывается фотошаблон 4 с антиадгезионным покрытием. Антиадгезионное покрытие, с одной стороны, препятствует прилипанию фотошаблона к полимеризованной структуре, а с другой стороны – создает условия для начала полимеризации со стороны стеклянной подложки и, в результате, направленную полимеризацию структуры от подложки вверх. Толщина полимерного слоя регулируется толщиной прокладок 7 между шаблоном и подложкой и определяет высоту формируемых микроэлементов или микроструктур. Далее композиция экспонируется параллельным пучком УФ излучения ртутной лампы 1 с длиной волны 365 нм, сформированным линзой 2 и зеркалом 3, после чего фотошаблон снимается, а неполимеризованный материал удаляется при промывке в изопропиловом спирте.

Результаты

Известны жидкие фотополимеризующиеся мономерные композиции. Они успешно применяются при получении крупных изделий и пленок методом фотополимеризации в форме. В то же время практически нет исследований процессов фотополимеризации в микрообъеме, в которых фотополимеризация проходит в точке экспонирования, окруженной неполимеризованным жидким мономером.

Нами были выполнены эксперименты по экспонированию слоя жидкой мономерной композиции под фотошаблоном по методу, приведенному в предыдущем разделе. При этом использовался фотошаблон, имеющий периодические прозрачные линии, расстояние между которыми прогрессивно уменьшается.

Вначале, при больших относительных расстояниях между линиями, они формируются правильно, с четкими боковыми поверхностями, что подтверждает отсутствие

паразитной подсветки вне линии. Разница в вязкости составов не играет значительной роли в формировании микроэлементов (рис. 3).

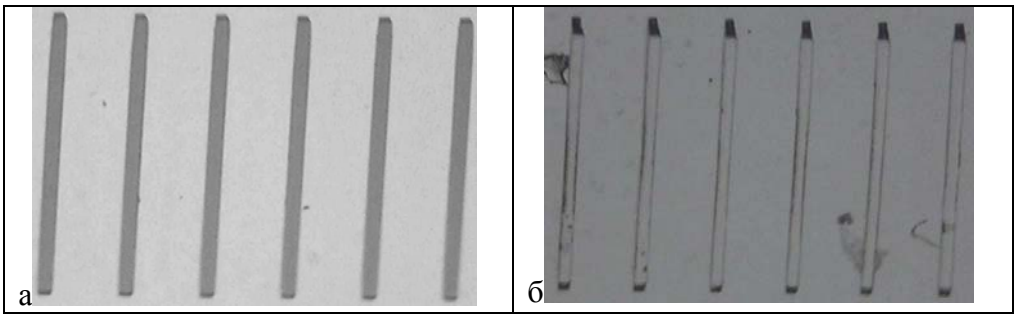


Рис. 3. Микроструктуры, расположенные на относительно большом расстоянии друг от друга: а – состав №1; б – состав №2 (высота структур 300 мкм, ширина 100 мкм, расстояние между ними 400 мкм)

В случае жидкой композиции при приближении линий друг к другу на расстояние, близкое к их ширине, между областями экспонирования начинают образовываться мостики (рис. 4, а), в результате при дальнейшем сближении отдельные полимеризованные столбики сливаются в один полимеризованный элемент (рис. 5, а) (композиция №1, табл. 2). При проведении экспериментов с различными по составу композициями было обнаружено, что использование более вязкой композиции (композиция №2, табл. 2) приводит к уменьшению и даже полному исчезновению вышеуказанного эффекта – в этом случае даже при максимальном сближении областей экспонирования мостики между ними не образуются и четко обозначены отдельные, близко расположенные полоски полимера (рис. 5, б).

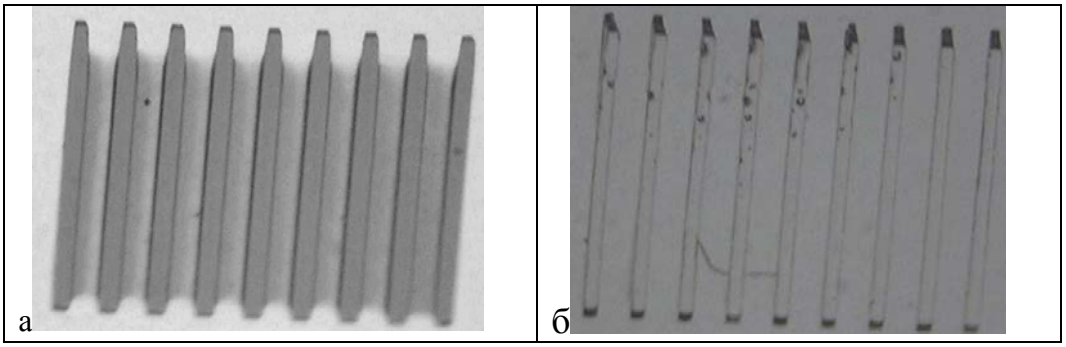


Рис. 4. Уменьшение расстояния между микроструктурами: а – состав №1; б – состав №2 (ширина структур 100 мкм, расстояние между ними 200 мкм)

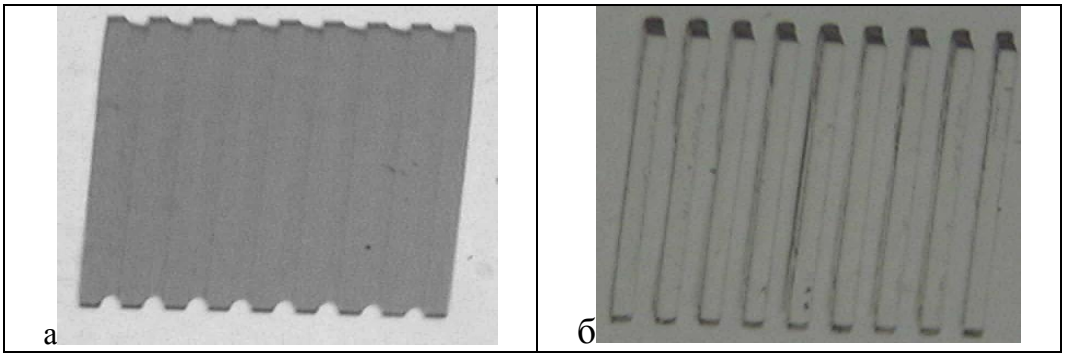


Рис. 5. Близко расположенные микроэлементы: а – состав №1; б – состав №2 (ширина структур 100 мкм, расстояние между ними 100 мкм)

Мы предполагаем, что данный эффект можно объяснить следующим образом: при экспонировании и полимеризации вещества в освещенной области объем материала уменьшается на 5–15% в зависимости от типа полимера, за счет усадки [5]. Вследствие разряжения, возникающего при уменьшении объема, окружающий жидкий полимер перетекает в зону освещения, где также полимеризуется. Поэтому в освещенных областях оказывается больше полимера, чем в неосвещенных. Соответственно, повышение вязкости композиции (переход от композиции №1 к №2, табл. 2) препятствует перетеканию полимера из неосвещенной области в освещенную, следовательно, боковая граница структуры остается более ровной. При сравнении рис. 4, а, и 4, б (более жидкая и более вязкая композиции соответственно) заметно, что более четкой границей обладают микроструктуры, полученные из состава №2.

Заключение

Отмечен эффект формирования полимеризованного слоя вне областей экспонирования фотополимера при сближении областей экспонирования на малые расстояния. Данный эффект оказывает негативное влияние на возможность получения трехмерных элементов сложной формы на жидких фотополимеризующихся композициях.

Обнаружено, что при повышении вязкости композиции данный эффект минимизируется, что позволяет эффективно формировать микроструктуры с высокой плотностью заполнения площади подложки.

Работа выполнена при поддержке по гранту Рособразования РНП.2.1.1.1403 «Исследование процессов формирования микрооптических поверхностей в поле световой волны при фотоотверждении мономерных композиций».

Литература

1. Kondo T., Juodkazis S., Mizeikis V., Matsuo S., Mizawa H. Fabrication of three-dimensional periodic microstructures in photoresist SU-8 by phase-controlled holographic lithography // New Journal of Physics. – 2006. – V.8. – P. 250.
2. Liu G., Tian Y., Kan Y. Fabrication of high-aspect-ratio microstructures using SU8 photoresist. // Microsystem Technologies, Springer-Verlag. – 2005. – P. 343–346.
3. Romanato F., Businaro1 L., M. Tormen, Perennes F., Matteucci M., Marmiroli B., Balslev S. and Di Fabrizio E. Fabrication of 3D micro and nanostructures for MEMS and MOEMS: an approach based on combined lithographies. // International MEMS Conference 2006. – Journal of Physics: Conference Series 34, 200. – P. 904–911.
4. Фокина М.И., Денисюк И.Ю. Формирование решеток микролинз методом дозированной фотополимеризации УФ-отверждаемых оптических композитов. // Оптический журнал. – 2006. – № 11.– С. 90–96.
5. Смирнова Т.В., Бурункова Ю.Э., Денисюк И.Ю. Измерение усадок УФ-отверждаемых композиций на основе акрилатов и диакрилатов // Оптический журнал. – 2006. – №5. – С. 57–61.

ОПТИМИЗАЦИЯ УСЛОВИЙ ПОЛУЧЕНИЯ ГОЛОГРАФИЧЕСКОГО ЗАЩИТНОГО ЭЛЕМЕНТА

Е.В. Степанова
Научный руководитель – к.т.н., доцент Н.Д. Ворзобова

Приведены характеристики отражательных голограмм при записи в красной, зеленой и синей областях спектра на промышленных материалах применительно к технологии получения голографических защитных элементов.

Введение

Интенсивное развитие науки и техники определяет новые виды информации, продукции, услуг, повышая требования к их защите. Одним из широко применяемых способов защиты является голографический способ. В настоящее время применяется технология, основанная на получении радужных голограмм. Однако за рубежом уже много лет существует оборудование для производства радужных голограмм. Оборудование является легкодоступным, что увеличивает риск подделки защитных элементов. В связи с этим актуальной является задача разработки новых технологий и реализации новых защитных признаков.

Общей целью работы является разработка технологии получения голографических защитных элементов, обеспечивающих новый защитный признак – направленное отражение и изменение спектрального состава отраженного излучения при изменении угла наблюдения. К разрабатываемой технологии и элементу предъявляется комплекс требований, среди которых – отечественное производство используемых материалов, высокая визуальная яркость и возможность реализации процесса в условиях серийного производства. Обеспечение данных требований предполагает проведение исследований, направленных на определение оптимального материала, источников записывающего излучения, условий записи и химико-фотографической обработки.

Задачи исследований

Основными требованиями к разрабатываемой технологии и элементу являются: доступность материалов, высокая дифракционная эффективность, чувствительность, наибольший динамический диапазон экспозиций, наименьшее влияние наложенной записи, наименьшая усадка фотослоя, химическая безопасность и безвредность используемых химических реактивов, стабильность характеристик элементов. Наиболее важным требованием является высокая дифракционная эффективность, определяющая визуальную яркость разрабатываемого элемента.

Задачей работы являлось обоснование оптимального регистрирующего материала, условий записи (длины волны записывающего излучения) и величины экспозиции, условий химико-фотографической обработки, обеспечивающих наибольшие значения дифракционной эффективности. Получение высоких значений дифракционной эффективности при записи на различных длинах волн видимой области спектра является актуальным как для решения поставленной задачи, так и с точки зрения использования промышленных материалов для решения других практических задач.

Методика эксперимента

Регистрирующие среды

Основным требованием к регистрирующим средам является доступность и отечественное производство материалов. В связи с этим объектом исследования являлись отечественные промышленные материалы ПФГ-03М, ПФГ-03Ц, ПФГ-01, ВРП. Сведе-

ния о характеристиках данных материалов в информационных материалах производителя (ОАО Компания «Славич») ограничены. Так, материалы ПФГ-03М рекомендованы для записи отражательных голограмм в красной области спектра (0,63 мкм) при дифракционной эффективности (ДЭ) 40%. Для материалов ПФГ-03Ц приведены характеристики ДЭ для записи в красной и зеленой областях (0,63 и 0,51 мкм) – 40%. Материалы ПФГ-01 рекомендованы для записи пропускающих голограмм в красной области с ДЭ 35%. Материалы ВРП рекомендованы для записи пропускающих голограмм в зеленой области спектра (характеристики не приведены).

Решение задачи получения цветоизменяющего элемента требует одновременной записи на двух длинах волн. В качестве источников излучения могут быть использованы источники в красной, зеленой и синей областях. Перечисленные материалы не сенсибилизированы к синей области спектра, и информации об их характеристиках в синей области не приводится. Таким образом, имеющаяся информация является недостаточной для решения поставленной задачи.

Источники излучения

Основным требованием к источникам излучения является когерентность, высокая выходная мощность, надежность, доступность, простота в эксплуатации и спектральные характеристики, согласованные с чувствительностью регистрирующих сред. В данной работе использовались источники излучения, в значительной степени удовлетворяющие данным требованиям: гелий-неоновый лазер ГИ-15Р (0,63 мкм), гелий-кадмиевый лазер (0,43 мкм), DPSS-лазер KLM-532 (0,53 мкм). Следует отметить, что DPSS-лазер является новой разработкой, и достаточной информации о возможности его использования для голографической записи не имеется. Обоснование оптимальных источников излучения для записи голограмм на двух длинах волн являлось задачей исследований.

Экспериментальные установки

В основе разрабатываемого защитного элемента лежит отражательная голограмма. Исследование характеристик отражательных голограмм при различных условиях записи и обработки проводилось с использованием установки, схема которой приведена на рис. 1.

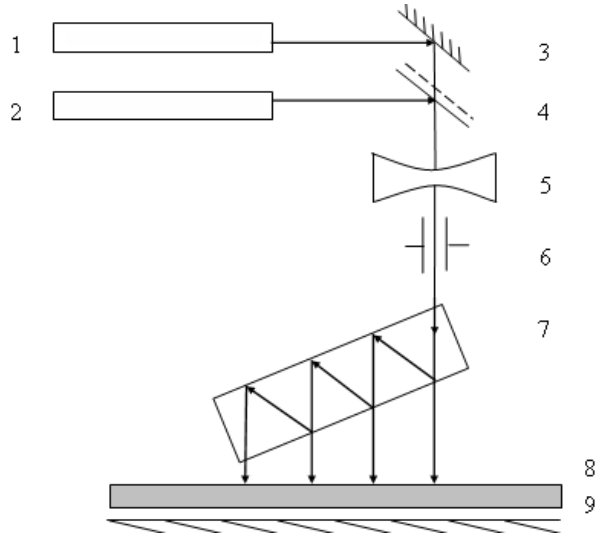


Рис. 1. Схема установки для записи отражательных голограмм: 1, 2 – лазеры, 3 – зеркало, 4 – полупрозрачное зеркало, 4 – линза, 5 – диафрагма, 6 – диафрагма, 7 – множительный элемент, 8 – голографическая пластинка, 9 – зеркало

Установка позволяет исследовать характеристики отражательных голограмм при записи как на одной длине волны (0,43; 0,53; 0,63 мкм), так и при одновременной записи на двух длинах волн.

Для измерения дифракционной эффективности использовалась установка, схема которой приведена на рис. 2.

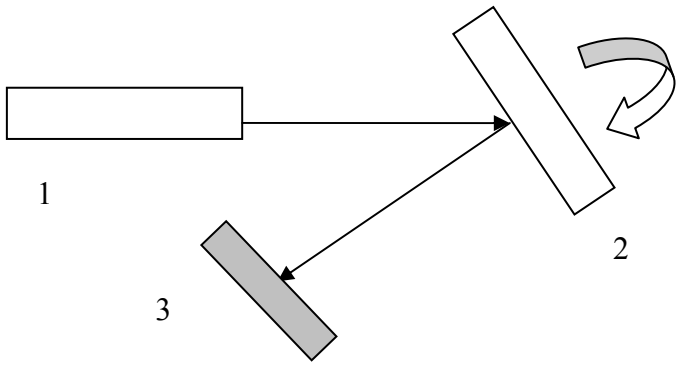


Рис. 2. Схема установки для измерения дифракционной эффективности:
1 – лазер, 2 – голограмма, 3 – фотоэлемент

Определение максимальных значений дифракционной эффективности было основано на обеспечении условия Брэгга, что достигалось поворотом голограммы или расширением эмульсионного слоя.

Процессы обработки

Процессы обработки исследуемых материалов были основаны на переводе фотолитического серебра в коллоидное серебро при использовании составов типа ГП при изменении концентрации роданистого аммония и едкого калия, а так же концентрации рабочего раствора (процесс 1). Кроме того, использовались процессы с отбеливанием, основанные на преобразовании остаточного галоидного серебра (процесс 2) и на переводе металлического серебра в прозрачные соли (процесс 3). Так как для записи отражательных голограмм, кроме мелкозернистых слоев ПФГ-03М и ПФГ-03Ц (с размерами микрокристаллов менее 30 нм), использовались более чувствительные крупнозернистые слои ПФГ-01 и ВРП (с размерами микрокристаллов более 40 нм), для их проявления использовались составы, не приводящие к ухудшению разрешающей способности [1]. Длительность проявления изменялась в широких пределах с целью определения оптимального значения для каждого материала.

Полученные результаты

Кривые зависимости дифракционной эффективности от величины экспозиции при записи отражательных голограмм в красной (0.63 мкм), зеленой (0.53 мкм) и синей (0.43 мкм) областях спектра для материалов ПФГ-03М, ПФГ-03Ц, ПФГ-01 и ВРП приведены на рис. 3–5.

Результаты исследования влияния совместной записи на двух длинах волн 0,63 и 0,43 мкм, 0,63 и 0,53 мкм показали, что наибольшее влияние наблюдается при обработке в составах типа ГП (процесс 1). При использовании обработки с отбеливанием (процесс 2) дифракционная эффективность каждой из монохромных составляющих уменьшается до двух раз, что меньше теоретически ожидаемого уменьшения (пропорционального квадрату числа наложений).

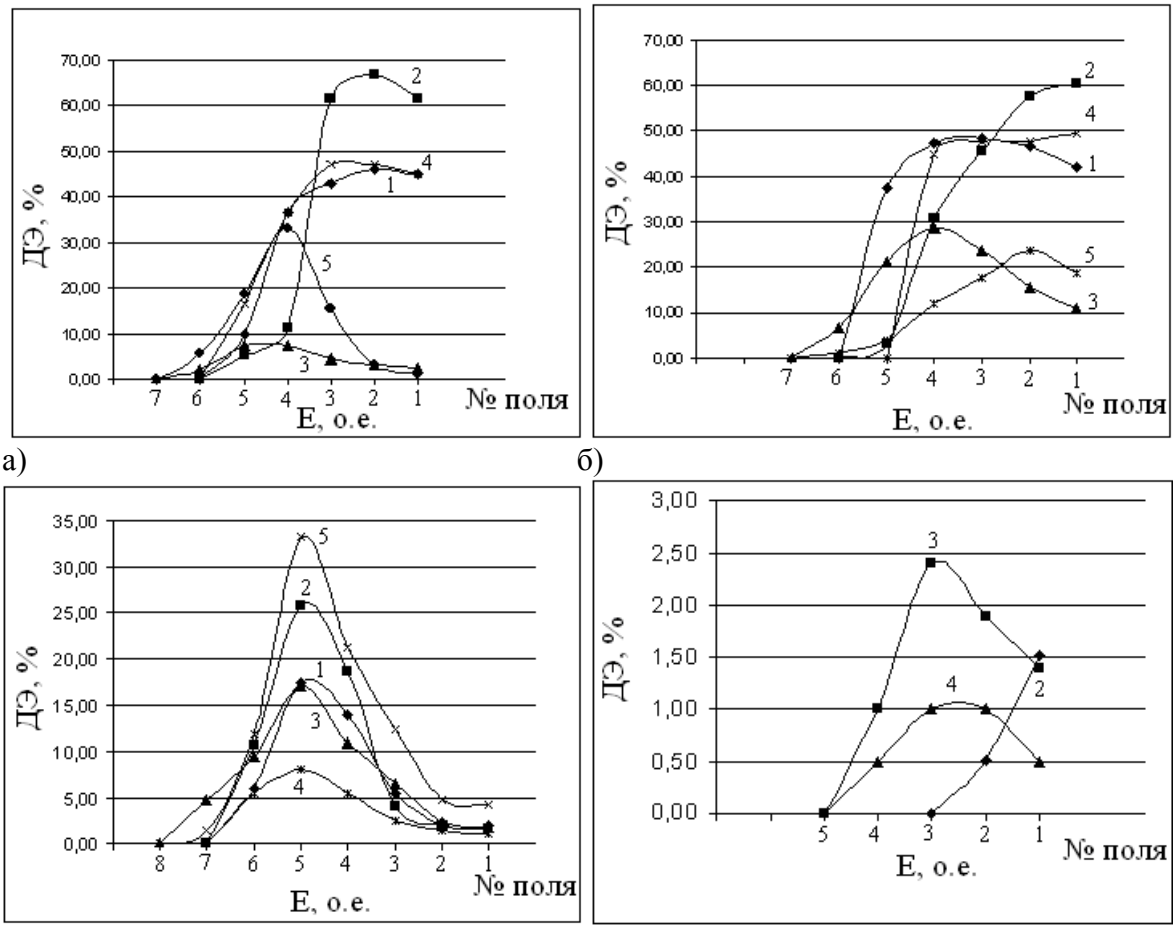
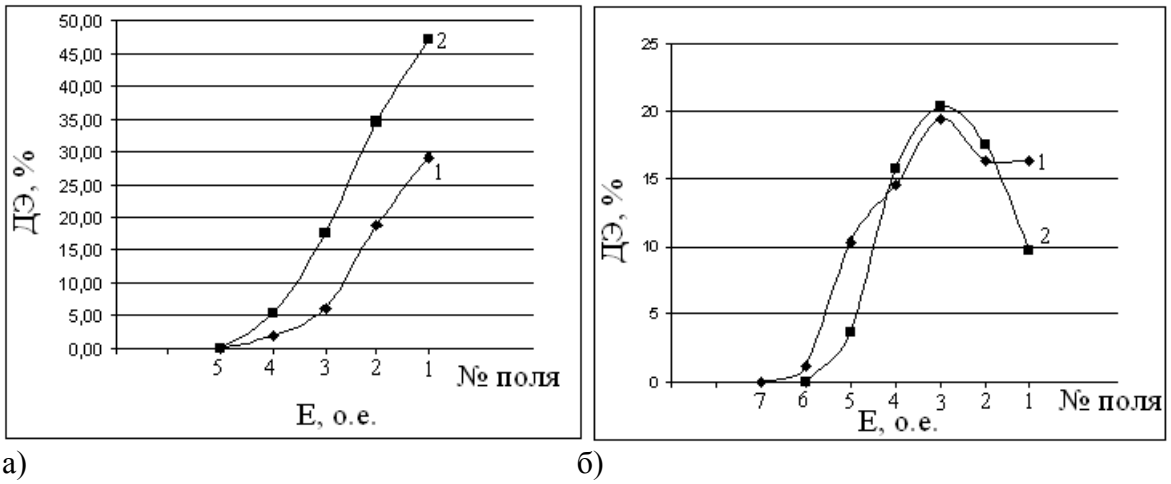
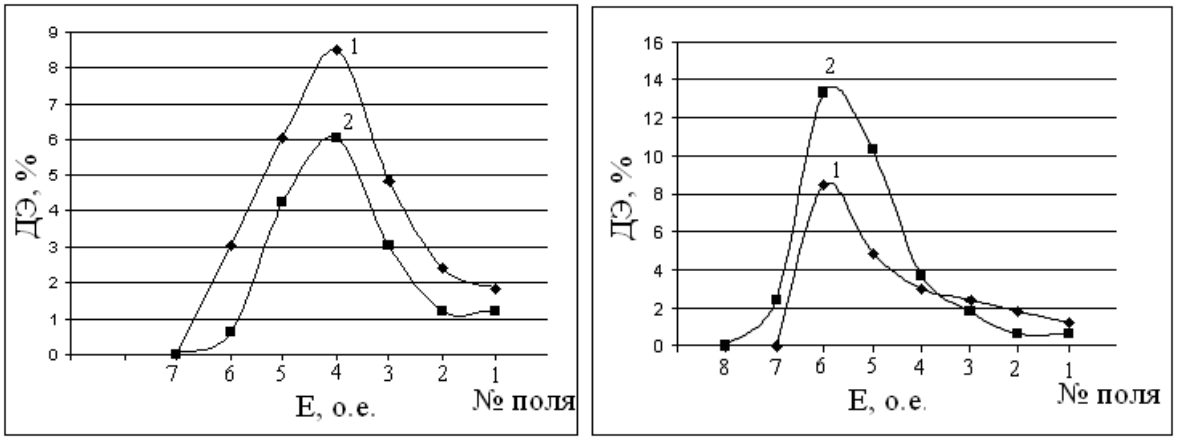


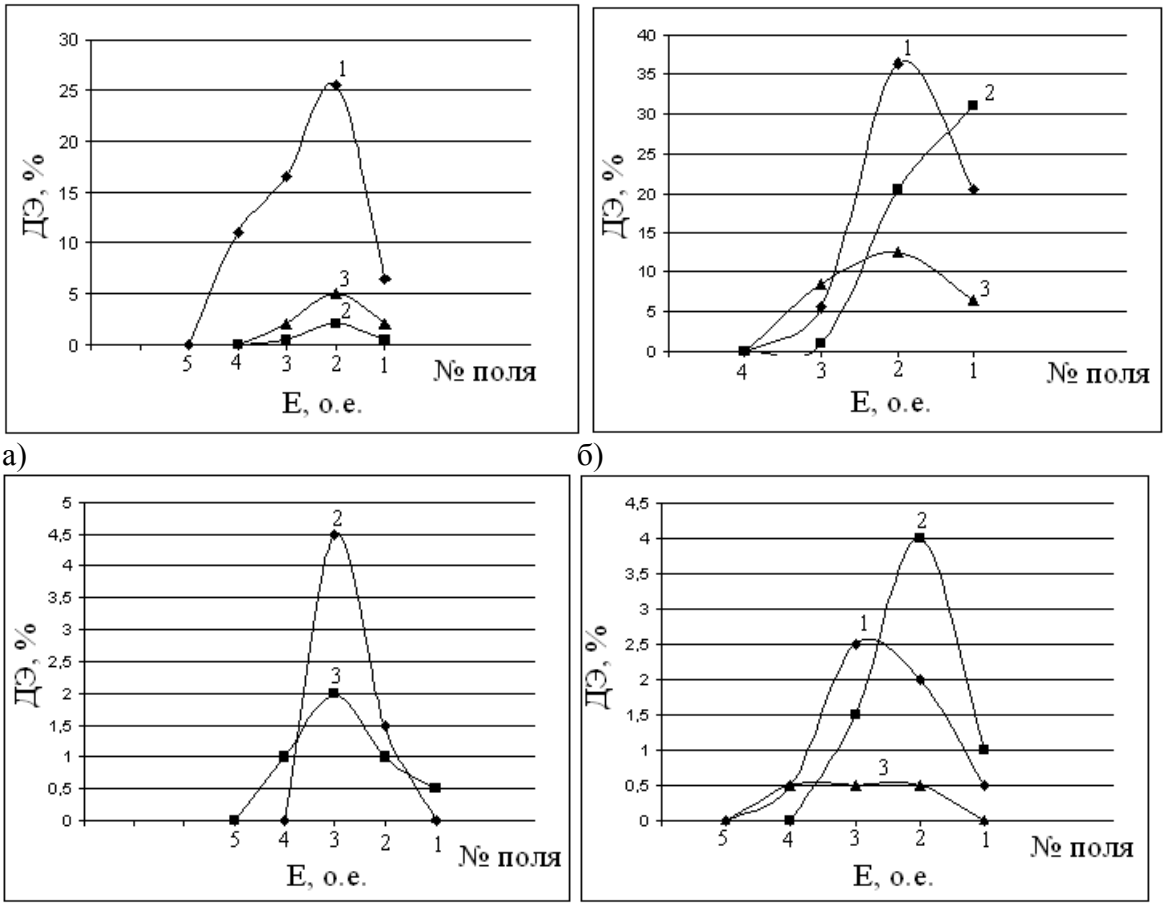
Рис. 3. Экспозиционные кривые дифракционной эффективности отражательных голограмм при записи в красной области спектра. Обработка: 1 – процесс 1 (с увеличенной концентрацией роданистого аммония и едкого калия), 2 – процесс 2, 3 – процесс 3, 4 – процесс 1 (с увеличенной концентрацией рабочего раствора), 5 – процесс, рекомендованный в информационных материалах производителя. а – ПФГ-03М, б – ПФГ-03Ц, в – ПФГ-01, г – ВРП





в) г)

Рис. 4. Экспозиционные кривые дифракционной эффективности отражательных голограмм при записи в зеленой области спектра. Обработка: 1 – процесс 1 (с увеличенной концентрацией роданистого аммония и едкого калия), 2 – процесс 2. а – ПФГ-03М, б – ПФГ-03Ц, в – ПФГ-01, г – ВРП



а) б)

в) г)

Рис. 5. Экспозиционные кривые дифракционной эффективности отражательных голограмм при записи в синей области спектра. Обработка: 1 – процесс 1 (с увеличенной концентрацией роданистого аммония и едкого калия), 2 – процесс 2, 3 – процесс 3. а – ПФГ-03М, б – ПФГ-03Ц, в – ПФГ-01, г – ВРП

Обсуждение результатов и выводы

Исследование характеристик отражательных голограмм при записи на длинах волн 0,63 и 0,53 мкм в промышленных материалах установило возможность получения значений дифракционной эффективности более 60%, что превышает значения, приведенные в информационных материалах производителя (40%). Для промышленных мелкозернистых материалов, не сенсибилизированных к синей области спектра, при записи на длине волны 0,43 мкм и обработке в составах типа ГП получены значения дифракционной эффективности более 30% (восстановление на длине волны 0,63 мкм). Однако при восстановлении в синей области дифракционная эффективность может уменьшаться вследствие увеличения поглощения в синей области спектра. Значения дифракционной эффективности до 40% получены при использовании обработки с отбеливанием, основанной на преобразовании остаточного галоидного серебра (процесс 2), что является достаточным для решения поставленной задачи, а также ряда других задач, которые требуют записи в синей области спектра. Достаточно высокие значения дифракционной эффективности при увеличении чувствительности получены в крупнозернистых слоях (с размерами микрокристаллов более 40 нм), разработанных и рекомендованных для записи в попутных пучках.

Для получения защитных элементов с наибольшей дифракционной эффективностью при записи на двух длинах волн могут быть рекомендованы материалы ПФГ-03М и ПФГ-03Ц при обработке с отбеливанием (процесс 2). Для обработки возможно также использование составов на основе ГП с увеличенной концентрацией роданистого аммония и едкого калия (процесс 1), однако в этом случае увеличивается влияние наложенной записи. Возможно также использование сочетания материалов ПФГ-01 и ВРП, обеспечивающих большую чувствительность, что может позволить увеличить размеры формируемых элементов.

Заключение

Исследована зависимость дифракционной эффективности отражательных голограмм (определяющая визуальную яркость разрабатываемого защитного элемента) от типа материала, длины волны записывающего излучения, величины экспозиции, условий химико-фотографической обработки при раздельной и совестной записи на различных длинах волн видимой области спектра. Обоснованы оптимальные материалы, источники излучения, процессы обработки, величины экспозиции, составляющие основу технологии получения голографических защитных элементов. Полученные результаты использованы для получения первых образцов цветоизменяющих защитных элементов.

Литература

1. Vorzobova N.D., Ryabova R.V. Pulsed holographic recording on silver halide emulsions // Sci. Appl. Photo. 2000.

ПРИМЕНЕНИЕ МЕТОДА НАНОИМПРИНТА ДЛЯ ФОРМИРОВАНИЯ ПЛЕНОЧНЫХ РЕТРОРЕФЛЕКТОРОВ

Е.Б. Шекланова

Научный руководитель – д.ф.-м.н., ст.н.с. И.Ю. Денисюк

Рассматривается возможность формирования пленочных ретрорефлекторов в объеме гибкой полимерной пленки толщиной не более 100 мкм методом наноимпринта.

Введение

На сегодняшний день, пожалуй, единственным материалом для изготовления оптических микроструктур являются полимеры. Они делают возможным получение структур микро- и наноразмеров, а также позволяют подбирать физические и оптические свойства, такие как показатель преломления, жесткость и т.д., в зависимости от конкретной задачи.

Существует несколько способов получения различных полимерных микроструктур. В основном их изготовление сводится к различным способам копирования на полимер схемы с уже готовой структуры, которая в большинстве случаев не является полимерной. Как правило, это литографический шаблон, с которого впоследствии выполняется обратная копия – штамп, а затем с его помощью изготавливаются полимерные структуры. Существуют и способы «прямой записи» оптических интегральных схем – полутоновая литография, запись лазерным лучом. Эти методы позволяют создавать практически любые конфигурации электрооптических схем, но их недостатком является не слишком хорошая воспроизводимость формы поверхности. Методом, позволяющим воспроизводить формы с точностью до 1,5 нм, является метод наноимпринта.

Целью данной работы является формирование пленочных ретрорефлекторов в объеме гибкой полимерной пленки толщиной не более 100 мкм, обеспечивающих отражение света в направлении источника не зависимо от угла падения на него света (до 60°).

Метод наноимпринта

В настоящее время одним из наиболее перспективных методов в области изготовления различных микрооптических элементов является метод наноимпринта. Но сам по себе метод наноимпринта имеет ряд недостатков, например для увеличения сроков эксплуатации требуется подбирать полимеры с как можно более высокими температурами плавления, что нежелательно. Для решения этой и ряда других проблем была разработана технология soft lithography (буквальный перевод – гибкая литография), в которой используется гибкий штамп из полидиметилсилоксана и УФ-отверждаемая композиция мономеров, жидкая при комнатной температуре. В этом случае жидкая композиция затекает в штамп при комнатной температуре, а затем проводится ее УФ полимеризация с получением твердого термостойкого материала.

Технология основана и была бы невозможна без полидиметилсилоксана. Полидиметилсилоксан (ПДМС) – новый полимерный материал, имеющий ряд необычных свойств. Он прозрачен до 250 нм, следовательно, возможно проведение УФ-полимеризации жидкой композиции при освещении ее через готовый ПДМС штамп. Основная особенность полимера ПДМС, на которой и основано его применение – изменение адгезии при полимеризации. Исходный мономер имеет высокую адгезию к большинству материалов. Этим обеспечивается смачивание и его затекание в мельчайшие элементы формы. Малые размеры молекулы мономера обеспечивают затекание в объемы размером более 1,5 нм [1]. После полимеризации свободные связи исходного мономера замыкаются и его адгезия уменьшается почти до нуля.

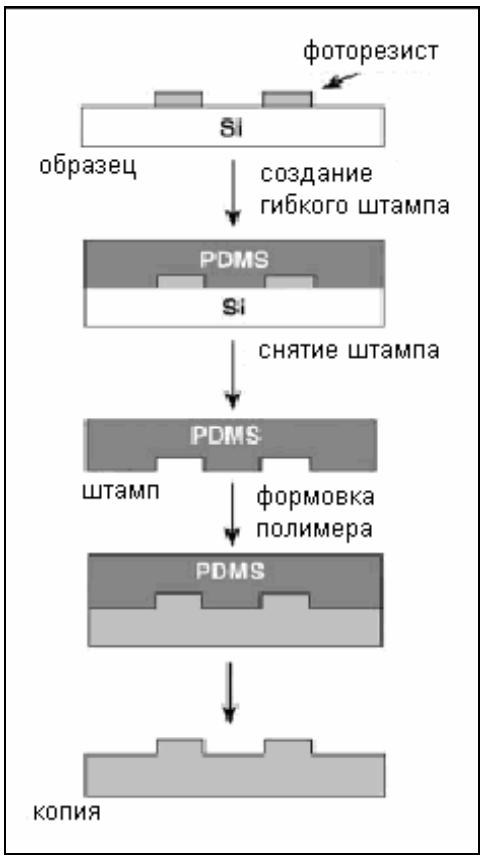
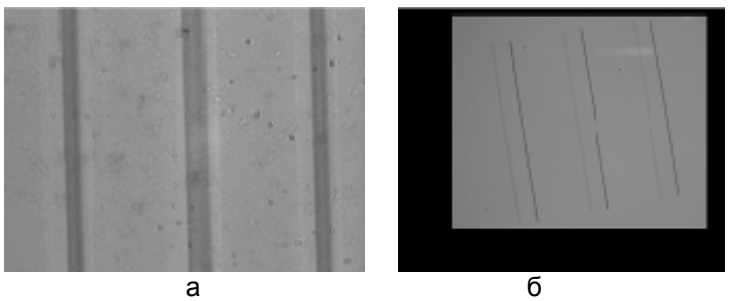


Рис. 1. Последовательность стадий процесса Soft lithography

Реализация копирования различных структур включает следующие стадии (рис. 1).

1. Нанесение жидкого ПДМС с введенным инициатором на поверхность копируемого элемента – шаблона. Для изготовления гибкого штампа необходим фотолитографический шаблон определенной формы (для конкретной задачи). Поверхность шаблона должна быть чистой и свободной от загрязнений. Для этого необходимо провести предварительное очищение шаблона, поместив его в состав растворителя на несколько минут.
2. Полимеризация ПДМС в контакте с поверхностью элемента, разъединение ПДМС и элемента.
3. В полученную матрицу из ПДМС заливается жидкая УФ-полимеризуемая композиция с необходимыми оптическими свойствами.
4. УФ полимеризация жидкой композиции в матрице ПДМС. Штамп ПДМС оптически прозрачен на длине волны более 280 нм, поэтому возможно полимеризация при УФ-облучении через ПДМС на непрозрачной подложке. Затем штамп отделяют. Отделение происходит достаточно просто, так как силоксан не имеет адгезии к подложкам и является гибким и прочным. Под микроскопом видно, что силоксан полностью затекает во все мелкие элементы оригинала, и форма получаемого штампа передается с хорошей точностью (рис. 2) [1–3].

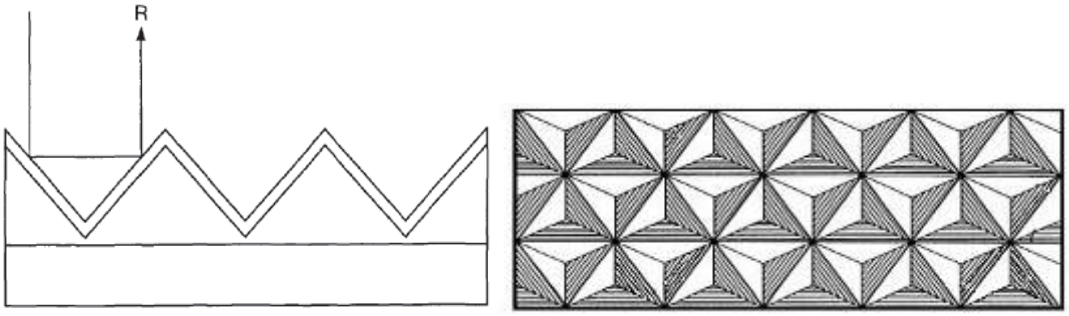


а б

Рис. 2. Получение гибкого штампа: а – шаблон; б – гибкий штамп

Уголковый отражатель, ретрорефлектор

Призменные отражатели – они же катафоты – несложны в изготовлении, способны работать при угле отклонения падающего излучения до 60° [4]. Первоначально уголковые отражатели были разработаны для радиолокационной техники. Поэтому в видимом диапазоне используется принцип работы отражателя, и теория его разработана для РЛС с учетом соответствующей длины волны света. Уголковый отражатель (УО) представляет собой пирамиду, три грани которой являются взаимно перпендикулярными зеркалами, а четвертая грань прозрачна и обращена к наблюдателю (рис. 3) [4].



а б

Рис. 3. Принцип работы призменного отражателя (а) и сам уголковый отражатель (б)

Оптические УО получили распространение после появления лазеров. У них эффективная площадь рассеяния, представляющая себой площадь гипотетической плоской цели, имеющей коэффициент отражения в заданном направлении, что и данная цель, довольно велика за счет отношения a/λ, где λ – длина волны излучения, a – размер грани. При этом величина эффективной площади рассеяния слабо зависит от угла падения на нее электромагнитных волн. Рассчитать ее можно по формуле [5]:

$$S_{эф} = 4\pi a^4/3\lambda. \quad (1)$$

Для сравнения рассчитаем эффективную площадь рассеивания для уголкового отражателя с гранью порядка 3–5 мм и точно такого же микропризменного элемента с гранью порядка 20–100 мкм при длине волны λ=650 нм.

Катафот: $S_{эф} = 4\pi\cdot(3\cdot10^{-3})^4/3\cdot650\cdot10^{-9}$, $S_{эф}= 1{,}94\cdot10^{-5}$(м^2), a/λ=4615,4

Микропризменный УО: $4\pi\cdot(30\cdot10^{-6})^4/3\cdot650\cdot10^{-9}$, $S_{эф}= 5{,}12\cdot10^{-13}$(м^2), a/λ=46,154

Для классических катафотов соотношение размер/длина волны очень велико, поэтому в данной работе по исследованию микрооптических элементов их не принимают во внимание. При размере микропризмы 50–100 мкм это соотношение уже является существенным и лимитирует минимальный размер микропризмы на уровне 20–30 мкм, ниже которого не выполняются законы геометрической оптики.

Пленочные ретрорефлекторы в объеме гибкой полимерной пленки

Были изготовлены пленочные ретрорефлекторы с микропризменным рельефом при использовании двух типов штампов, которые определяли форму структур. В работе исследованы оптические характеристики как копий, так и образцов ретрорефлекторных пленок зарубежных фирм. На рис. 4 и 5 показаны графики зависимости интенсивности отраженного луча от угла падения света. Хорошо видно, что наиболее благоприятными углами являются 0° и 30°.

На рис. 6 изображена исходная пленка фирмы 3М, размер элемента составляет порядка 20 мкм, элементы ретрорефлектора являются зеркальными поверхностями, поэтому при использовании высокоапертурных объективов не удается наблюдать форму

ретрорефлектора [6]. На рис. 7 изображена другая пленка, с гораздо более крупным размером элементов, что позволяет их рассмотреть.

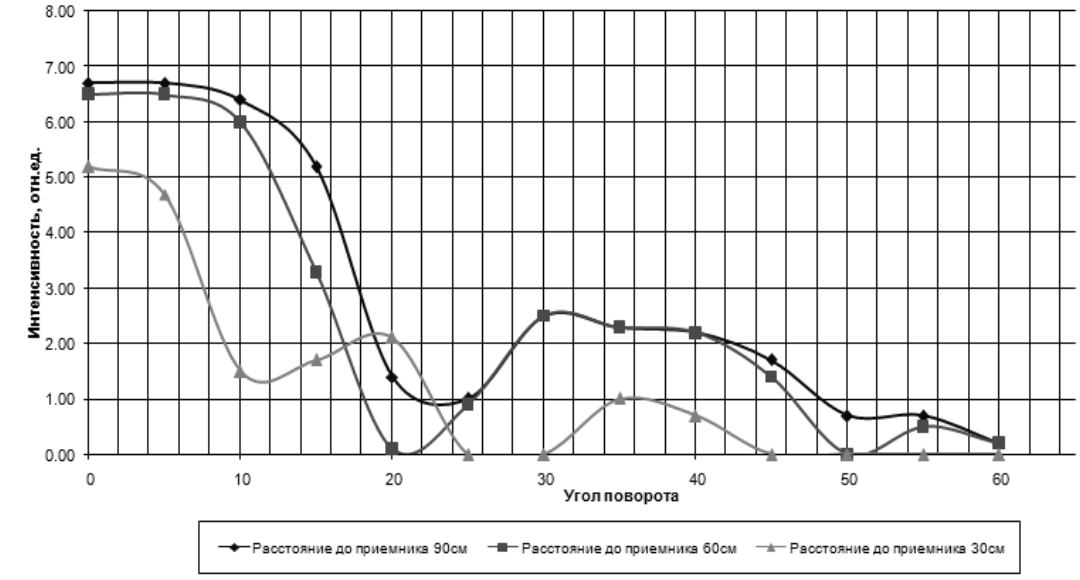


Рис. 4. Интенсивность отраженного излучения в зависимости от расстояния до приемника и угла падения света на ретрорефлектор (угол поворота ретрорефлектора отсчитывается от нормали). Пленка фирмы 3М США, оригинал

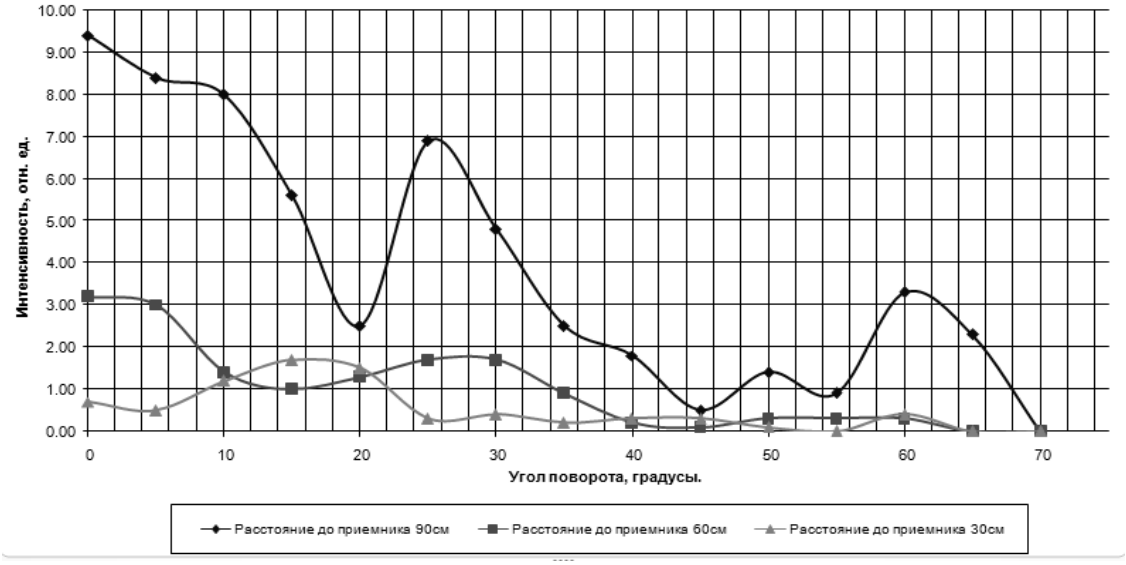
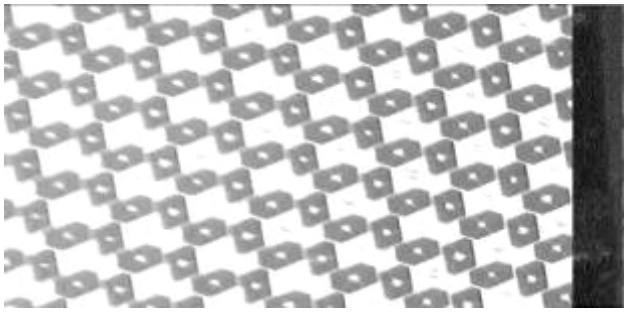
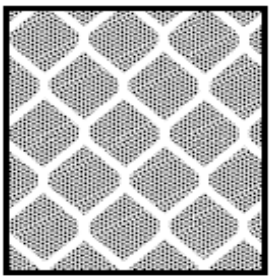


Рис. 5. Интенсивность отраженного излучения в зависимости от расстояния до приемника и угла падения света на ретрорефлектор (угол поворота ретрорефлектора отсчитывается от нормали). Пленка, произведенная в Китае, оригинал



а



б

Рис. 6. Пленка фирмы 3М, США. Фотография, сделанная при помощи микроскопа (а); внешний вид (б)

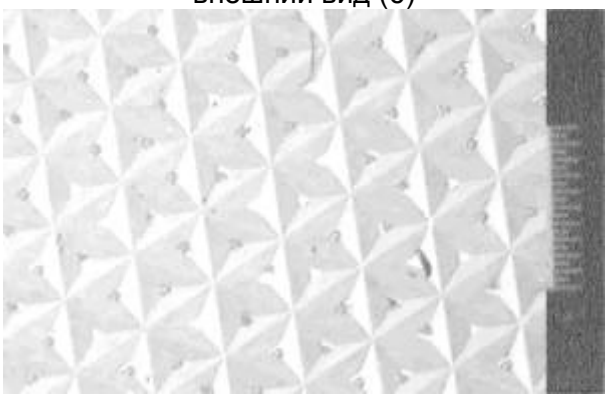


Рис. 7. Форма элементов

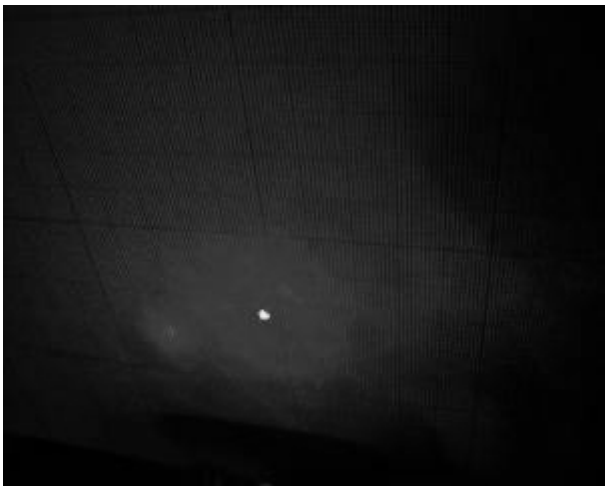


Рис. 8. Копия пленки китайского производства. Свет падает под углом 0˚ к нормали

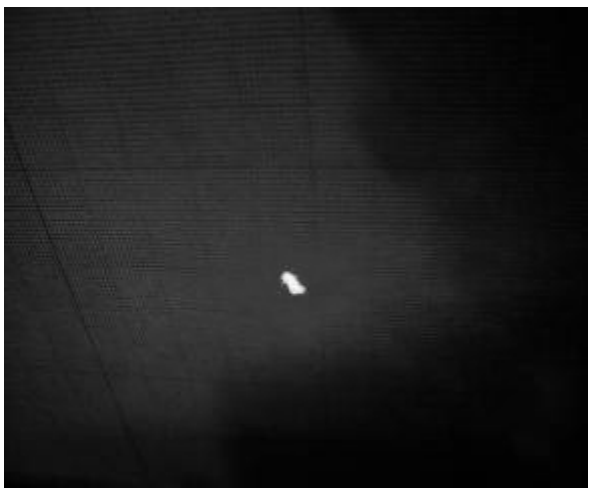


Рис. 9. Копия, снятая с пленки китайского производства.
Свет падает под углом 30° к нормали

Как видно из рис. 8 и 9, отраженный луч после прохождения через скопированный пленочный ретрорефлектор довольно сильно рассеивается. Но при сравнении с ис-

ходными образцами видно, что рассеивание света на копии практически соответствует рассеянию света на оригинале.

Заключение

В ходе работы была исследована возможность применения метода наноимпринта, а именно технологии гибкой литографии, с использованием гибкого штампа для формирования пленочных ретрорефлекторов в объеме гибкой полимерной пленки толщиной не более 100 мкм методом наноимпринта. Были получены структуры с размером элемента порядка 20–30 мкм. Как видно, уголковые отражатели в виде микроструктуры в полимерной пленке толщиной 100 мкм легко выполнимы и имеют хорошие характеристики по отражению, близкие к оригиналу.

Литература

1. Byron D. Gates Nanofabrication with molds & stamps // Materialstoday. – Feb. 2005. – P. 45–49.
2. L. Jay Guo Recent progress in nanoimprint technology and its applications // Jornal of Physics D: Applied Phisics. – 2004. – № 37. – P. 123–141.
3. A. Rogers and Ralph G. Nuzzo Recent progress in soft lithography // Materialstoday. – Feb. 2005. – P. 50–56.
4. Patent No.: US 6967053 B1. Durable, open-faced retroreflective prismatic construction.
5. БСЭ, Уголковый отражатель [Электронный ресурс]; – Режим доступа: http://bse.chemport.ru, свободный. – Загл. с экрана. – Яз. рус.
6. MSDS, Diamond Grade™ LDP Reflective Sheeting [Электронный ресурс]; – Режим доступа: http://www.mmm.com, свободный. – Загл. с экрана. – Яз. анг.

СОЗДАНИЕ ГРАДИЕНТНЫХ ВОЛНОВОДОВ НА ФОТО-ТЕРМО-РЕФРАКТИВНОМ СТЕКЛЕ И ИЗМЕРЕНИЕ ИХ ПРОФИЛЯ ПОКАЗАТЕЛЯ ПРЕЛОМЛЕНИЯ

С.С. Киселев

Научный руководитель – д.ф.-м.н., профессор Н.В. Никоноров

В работе исследовались возможности фото-термо-рефрактивного стекла как материала для создания градиентных волноводов. Методом низкотемпературной ионообменной диффузии и методом термической эффузии на ФТР-стекле были созданы многомодовые градиентные волноводы, изучены их оптические параметры и построены профили показателя преломления.

Введение

На сегодняшний день перспективным направлением является изучение свойств фото-термо-рефрактивных (ФТР) стекол, используемых как эффективный фоторегистрирующий материал для записи объемных фазовых голограмм. ФТР-стекла обладают высокой химической устойчивостью и механической прочностью, выдерживают воздействие мощного непрерывного и импульсного лазерного излучения, а их спектральные характеристики остаются неизменными при многократном нагреве до высоких температур (490°C). Кроме того, фото-термо-рефрактивные стекла могут сочетать в себе одновременно лазерные и волноводные свойства. Таким образом, открывается возможность создания на основе ФТР-стекла полифункциональных устройств для интегральной оптики.

В настоящей работе исследовались возможности ФТР-стекла как материала для создания градиентных волноводов. Исходя из химического состава стекла (Na_2O- ZnO- Al_2O_3- F- Br- SiO_2), можно заключить о возможности создания на его основе градиентных волноводов двумя наиболее простыми методами – методом низкотемпературной ионообменной диффузии и методом термической эффузии. Целью данной работы являлось создание градиентных волноводов на основе ФТР-стекла двумя методами, а также измерение их профиля показателя преломления, дающего информацию о глубине волноводного слоя, количестве волноводных мод и величине двулучепреломления.

Методы создания волноводов

Среди известных методов создания градиентных волноводов (ионная имплантация, эффузия, твердотельная диффузия, электростимулированная диффузия) особое место занимает метод ионообменной диффузии [1–3]. Этот метод обладает рядом преимуществ: простота, технологичность, воспроизводимость. Диффузионные волноводы могут быть получены с разнообразными параметрами на широком наборе силикатных стекол при использовании различных ионов-диффузантов с хорошим качеством поверхности и однородностью, с низким затуханием и повышенной механической прочностью. Суть метода заключается в обмене ионов щелочных металлов, содержащихся в стекле, на ионы других одновалентных металлов из расплавов солей вследствие различия их химических потенциалов. Как правило, диффундирующие из расплава в стекло ионы имеют большую удельную рефракцию, чем ионы, диффундирующие из стекла в расплав, например **Ag^+, Li^+, Tl^+, Rb^+, Cs^+ (расплав) ↔ Na^+ (стекло)**. В результате такой замены происходит увеличение показателя преломления в поверхностном слое стекла, что приводит к образованию волновода. Кроме того, в случае обмена ионов различных радиусов изменение показателя преломления и формирование волновода в поверхностном слое стекла обусловливается возникающими механическими напряжениями. Например, при ионном обмене **K^+ (расплав) ↔ Na^+ (стекло)**, так как коэффициенты реф-

ракции ионов $\mathbf{K}^+$ и $\mathbf{Na}^+$ близки, изменение показателя преломления и формирование волновода полностью определяется возникающими сжимающими механическими напряжениями [4–6]. Обычно ионный обмен проводят при температурах ниже T_g стекла.

Создание волновода методом эффузии заключается в уменьшении концентрации фторид-ионов в поверхностных слоях ФТР-стекла за счет улетучивания фторидных компонентов стекла, что приводит к увеличению показателя преломления [7, 8].

Методика измерения профиля показателя преломления волноводов

Экспериментальное исследование полученных на ФТР-стекле волноводов в данной работе заключалось в измерении эффективных показателей преломления волноводных мод методом их селективного резонансного возбуждения при помощи призменных устройств ввода/вывода лазерного излучения в волноводный слой [9, 10]. Схема экспериментальной установки представлена на рис. 1.

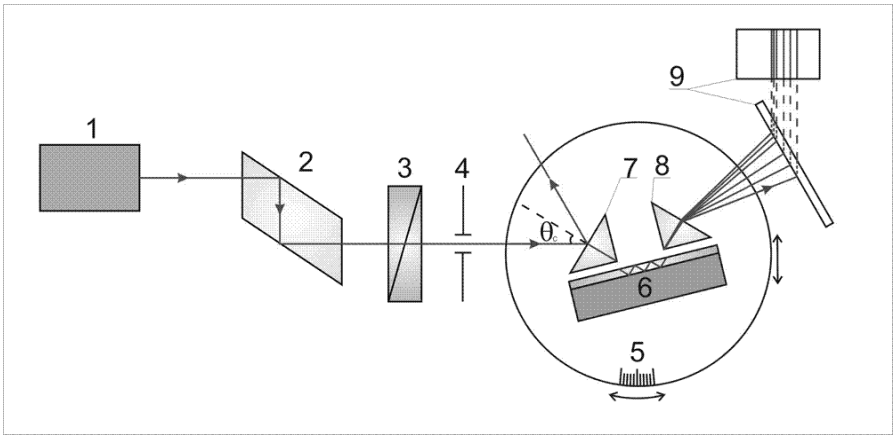


Рис. 1. Схема экспериментальной установки для измерения параметров волноводов. На схеме: 1. одномодовый He-Ne-лазер (λ = 0,6328мкм), 2. ромб Френеля, 3. поляризатор, 4. диафрагма, 5. поворотный столик с лимбом (стрелками показаны возможные перемещения поворотного столика), 6. исследуемый волновод, 7,8. призмы ввода и вывода, 9. экран

В качестве источника излучения использовался одномодовый He-Ne-лазер (λ=632,8 нм). Перемещением поворотного столика с лимбом падающий лазерный луч направляется на призму, плотно прижатую к волноводу, под такими углами, чтобы свет внутри призмы испытывал полное внутреннее отражение. Если зазор между призмой и волноводом составляет порядка 1/4 λ, то, благодаря эффекту оптического туннелирования, излучение проникает в волноводный слой и при углах, соответствующих условию фазового синхронизма, резонансно возбуждает волноводные моды. Изменением направления поляризации излучения можно возбуждать TE и TM моды одновременно или поочередно. Второй призмой возбужденные волноводные моды выводятся из волновода на экран, что позволяет зафиксировать и записать резонансные углы возбуждения мод θ_c, по которым, зная показатель преломления призмы n_p и преломляющий угол призмы P, определяются эффективные показатели преломления мод n_m:

$$n_m = n_p \sin\left[P \pm \arcsin \frac{\sin \theta_c}{n_p} \right]. \qquad (1)$$

Кроме того, фиксируя угол θ_c, при котором наступает полное внутреннее отражение, по формуле (1) можно определить показатель преломления подложки волновода

(метод Аббе с обратным ходом лучей), что очень важно, так как его значение может изменяться в процессе создания волновода.

По измеренным данным с помощью метода ВКБ с использованием кусочно-линейной аппроксимации [11], реализованном в среде MathCad, восстанавливается профиль показателя преломления волновода, т.е. зависимость значения показателя преломления от глубины волноводного слоя.

Эксперимент и обработка результатов

При создании градиентного волновода методом низкотемпературной ионообменной диффузии на натриево-цинко-алюмо-фтор-силикатном ФТР-стекле предварительно разогретый образец помещался в расплав KNO_3 и выдерживался внутри печи при температуре 370°С в течение 5 часов. Точность измерения и поддержания температуры составляла ±1°С. Описанной выше методикой были измерены эффективные показатели преломления мод полученного волновода, а также значение показателя преломления подложки. Измерения проводились с помощью призмы с преломляющим углом 59,93°, сделанной из промышленного стекла марки ТБФ3 (показатель преломления для λ=632,8 нм равен n_p =1,75207). Точность измерений составляет ±0,0002. Результаты измерений представлены в табл. 1.

Номер моды	Значения эффективного показателя преломления мод ТЕ-поляризации	Значения эффективного показателя преломления мод ТМ-поляризации	Значение показателя преломления подложки до ионного обмена	Значение показателя преломления подложки после ионного обмена
0	1,4998	1,5010	1,4939	1,4939
1	1,4978	1,4987		
2	*1,4963*	1,4973		
3	1,4951	1,4960		
4	1,4940	1,4949		
5		1,4940		

Таблица 1. Результаты измерений оптических параметров K^+- ионообменного волновода, созданного на ФТР-стекле при $T=370^0$С в течение 5 часов

В среде MathCad с помощью метода ВКБ был построен профиль показателя преломления полученного волновода (рис. 2).

Создание градиентного волновода методом термической эффузии проводилось на образце из того же стекла, что и при ионном обмене. Образец выдерживался в печи при температуре 370°С в течение 21 часа. В результате такой термообработки волноводного слоя на поверхностном слое образца не обнаружено. В то же время было зафиксировано уменьшение значения показателя преломления стекла на 0,0007, что, возможно, связано с процессами отжига стекла и релаксацией напряжений.

Следующий эксперимент по созданию волновода методом эффузии из того же ФТР-стекла проводился при температуре 512°С в течение 12 часов. В результате измерений было обнаружено возникновение четырехмодового волновода, а уменьшение значения показателя преломления подложки составило 0,0025, что, вероятно, обусловлено паразитной кристаллизацией в объеме стекла. Результаты приведены в табл. 2.

С помощью метода ВКБ в среде MathCad был получен профиль показателя преломления волновода, представленный на рис. 3.

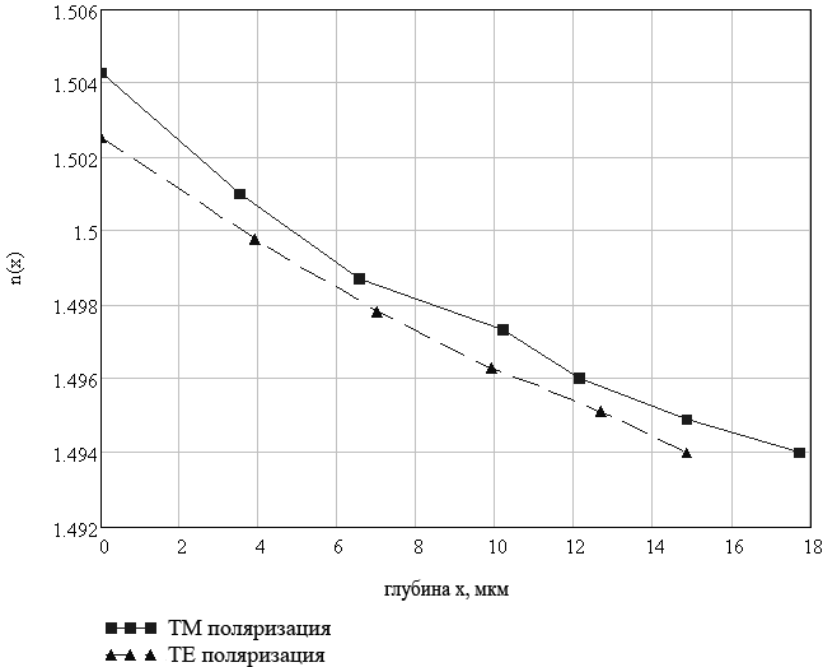


Рис. 2. Профиль показателя преломления K^+-ионообменного волновода, созданного на ФТР-стекле при Т=370°С в течение 5 часов

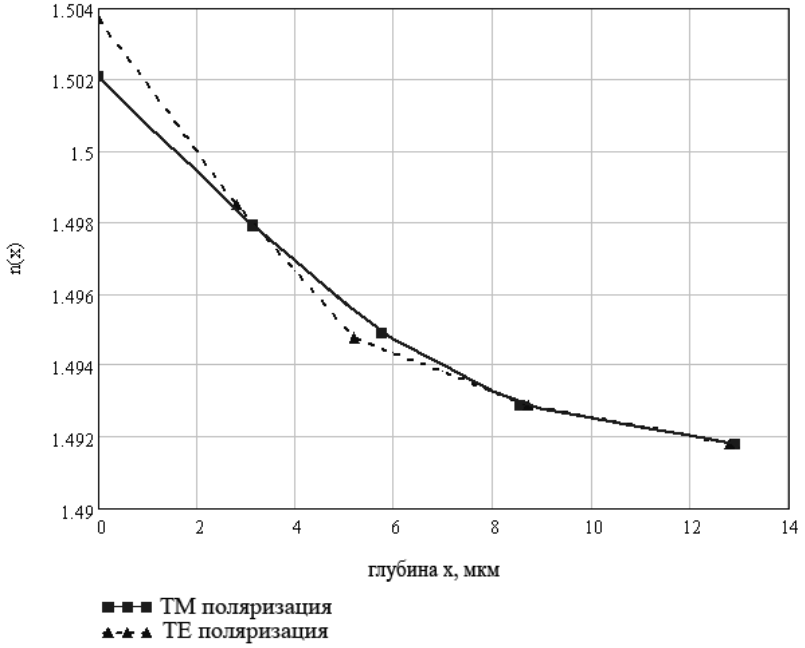


Рис. 3. Профиль показателя преломления эффузионного волновода, созданного на ФТР-стекле при Т=512°С в течение 12 часов

Номер моды	Значения эффективного показателя преломления мод ТЕ-поляризации	Значения эффективного показателя преломления мод ТМ-поляризации	Значение показателя преломления подложки до эффузии	Значение показателя преломления подложки после эффузии
0	1,4985	1,4979	1,4939	1,4914
1	1,4948	1,4949		
2	1,4929	1,4929		
3	1,4918	1,4918		

Таблица 2. Результаты измерений оптических параметров эффузионного волновода, созданного на ФТР стекле при Т=512^{0}С в течение 12 часов

Обсуждение результатов

Полученная методом низкотемпературного ионного обмена многомодовая волноводная структура (рис. 2) подтверждает применимость к ФТР-стеклу ионообменной технологии. Кроме того, из табл. 1 видно, что в результате ионного обмена оптические свойства (а именно показатель преломления) самого стекла не изменились, а значит, стекло не должно ухудшить свои фоточувствительные и лазерные свойства. Характерная для K^+-ионообменных волноводов напряжений анизотропия и глубина волноводного слоя (~18 мкм), полученные при данных условиях, характеризуют ФТР-стекло как близкое по ионообменным свойствам к коммерческому стеклу К-8 [12].

В работе было также доказана возможность создания многомодового волновода на ФТР-стекле методом термической эффузии (рис. 3), однако данный метод не представляется на данный момент перспективным с точки зрения волноводной технологии, так как требует длительных термообработок при высоких температурах, которые приводят к изменению оптических и ухудшению физико-химических свойств стекла [13]. Уменьшение концентрации фторидных соединений в процессе эффузии, вероятно, может отрицательно влиять на фото-рефрактивные свойства ФТР-стекла. Кроме того, проявление записанных на ФТР-стекле голограмм происходит, как правило, при температурах 512–520°С, поэтому представляет интерес более подробное изучение влияние эффузии на процесс записи фазовых голограмм.

Заключение

В работе исследовались возможности ФТР-стекла как материала для создания градиентных волноводов. Методом низкотемпературной ионообменной диффузии и методом термической эффузии на ФТР-стекле были созданы многомодовые градиентные волноводы. По описанной в работе схеме, методом резонансного возбуждения волноводных мод, были изучены оптические параметры полученных волноводов и построены зависимости значения показателя преломления от глубины волноводного слоя. По полученным результатам можно сделать вывод, что ФТР-стекло близко по ионообменным свойствам к коммерческому стеклу К-8, а процесс эффузии требует более подробного изучения с точки зрения влияния улета фторид-ионов на фото-рефрактивные свойства стекла.

Литература

1. Петровский Г.Т., Агафонова К.А., Мишин А.В., Никоноров Н.В. Волноводный эффект в оптических стеклах, модифицированных методом ионообменной диффузии из расплавов $AgNO_3$-$NaNO_3$ // Физ. и хим. стекла. – 1981. – Т.7. – № 1. – С. 98–102.
2. Аксенов Е.Т., Липовский А.А., Павленко А.В. Формирование маломодовых оптических волноводов в стекле, образованных диффузией ионов K^+ // Ж. техн. физ. – 1981. – Т.51. – № 1. – С. 222–224.
3. Евстропьев К.К. Диффузионные процессы в стекле. – Л., Стройиздат, 1970. – 168 с.
4. Глебов Л.Б., Никоноров Н.В., Петровский Г.Т., Филиппова М.Н. Влияние напряжений на показатель преломления градиентных слоев стекла, полученных методом ионообменной диффузии // Физ. и хим. стекла. – 1983. – Т. 9. – № 2. – С. 683–688.
5. Глебов Л.Б., Морозова И.С., Петровский Г.Т. Роль напряжений в формировании спектра мод в плоском диффузионном волноводе // Физ. и хим. стекла. – 1984. – Т.10. – № 2. – С. 194–198.

6. Глебов Л.Б., Никоноров Н.В., Петровский Г.Т. О возникновении напряжений в стекле в процессе низкотемпературного ионного обмена // Физ. и хим. стекла. – 1988. – Т.14. – № 6. – С. 904–906.
7. Редько В.П., Шляхтичев О.Д. Получение оптических волноводов методом эффузии // Письма в ЖТФ. – 1978. – Т.4. – № 23. – С. 1414–1416.
8. Петровский Г.Т., Редько В.П., Шляхтичев О.Д. Неоднородные планарные оптические волноводы на основе фторсодержащих стекол // Докл. АН БССР. – 1982. – Т.26. – № 3. – С. 222–224.
9. Интегральная оптика. / Под ред. Т. Тамира. – М.: Мир, 1978. – 344 с.
10. Tien P.K., Ulrich R., Martin R.J. Modes of propagating light waves in thin deposited semiconductor films // Appl. Phys. Lett. – 1969. – V.14. – № 9. – P. 261–294.
11. White J.M., Heidrick P.F. Optical waveguide refractive index profiles determined from measurements of mode indices: a simple analysis //Appl. Opt. – 1976. – V.15. – № 1. – P. 151–155.
12. Никоноров Н.В. Механизм формирования планарных диффузионных оптических волноводов на стеклах и образование в них центров окраски. Дис. ... д.т.н. – Л., 1985, С.36–43.
13. Никоноров Н.В. Влияние ионообменной обработки на физико-химические свойства поверхности стекол и волноводов // Физ. и хим. стекла. – 1999. – Т.25. – № 3. – С. 271–308.

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК СПЕКЛ-ИНТЕРФЕРЕНЦИОННЫХ ПОЛЕЙ В ДВУХ ДЛИНАХ ВОЛН

Т.Ф. Дудина
Научный руководитель – д.т.н., профессор И.П. Гуров

Рассмотрены особенности методов формирования и обработки спекл-интерференционных полей в двух длинах волн при нормальном перемещении объекта с шероховатой поверхностью. Приведены результаты исследования точности и помехоустойчивости метода двухволновой спекл-интерферометрии с использованием компьютерной обработки спекл-интерференционных полей.

Введение

Спекл-картина формируется при освещении шероховатой поверхности когерентным излучением [1] и содержит полезную информацию, которая используется, в частности, для бесконтактного интерферометрического контроля объектов с оптически грубыми поверхностями. Метод спекл-интерферометрии в двух длинах волн позволяет измерять смещения и исследовать форму объектов при расширенном диапазоне однозначности. Помимо «тонкой» шкалы для одной длины волны, появляется шкала биений интенсивности, по которой можно измерять «грубо». Это повышает помехоустойчивость и быстродействие метода, поскольку для выделения сигнала биений можно использовать меньшее число отсчетов.

В статье представлены результаты исследований точности и помехоустойчивости метода двухволновой спекл-интерферометрии, особенностей формирования и регистрации спекл-полей в двух длинах волн.

Особенности метода двухволновой спекл-интерферометрии

Спекл-интерференционная картина в двух длинах волн [2] представляет собой сумму двух взаимно некогерентных спекл-картин. Результирующая интенсивность равна

$$I = I_{\lambda_1} + I_{\lambda_2}. \qquad (1)$$

При интерференции плоских волн выражение (1) можно интерпретировать как суперпозицию двух гармонических функций с близкими периодами. При этом, как известно, возникают периодические изменения амплитуды – «биения», период которых в случае двух периодических картин интерференционных полос определяется значением синтезированной длины волны:

$$\lambda_S = \frac{\lambda_1 \lambda_2}{\lambda_1 - \lambda_2}. \qquad (2)$$

Из выражения (2) видно, что $\lambda_S >> \lambda_1, \lambda_2$. Соответственно этому, фаза огибающей двухволнового интерферометрического сигнала определена в расширенном диапазоне однозначности λ_S. Таким образом, в двухволновой интерферометрии значения фазы дают полезную информацию подобно двум отчетным шкалам: «грубой», с периодом λ_S, и «тонкой», с периодом $\lambda_{\text{ср}} = \frac{\lambda_1 \lambda_2}{\lambda_1 + \lambda_2}$.

Выбирая источники с различными длинами волн, можно устанавливать шаг биений интенсивности двухволновой картины полос. Существует широкий выбор источников с различными длинами волн, поэтому чувствительность метода может варьироваться в зависимости от конкретного применения. Известно, что для восстановления фазы интерферометрического сигнала требуется не менее двух отсчетов на периоде сигнала, полученных при изменении оптической разности хода. Огибающая двухвол-

нового интерферометрического сигнала изменяется медленно, поэтому число отсчетов может быть соответственно уменьшено, что повышает быстродействие метода с использованием двух длин волн по сравнению с одноволновым вариантом.

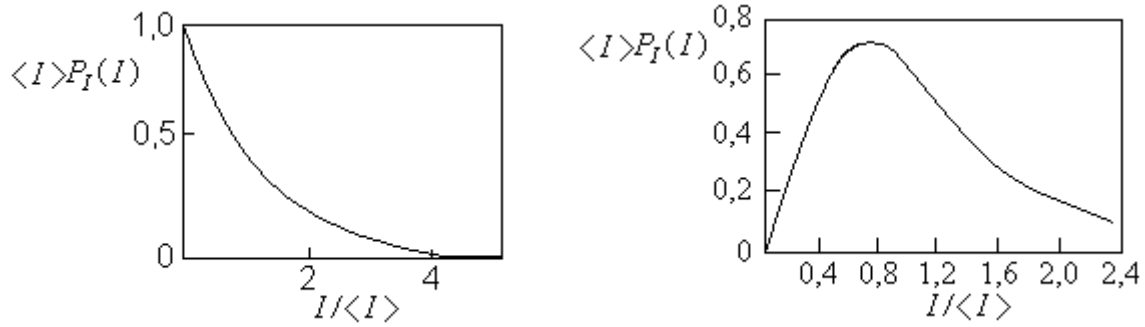
Важно отметить, что при отражении от шероховатой поверхности огибающая сигнала носит случайный характер. Целесообразно обратиться к статистическим характеристикам спекл-картин для случаев одной и двух длин волн.

Если поверхность освещать источником только с одной длиной волны, то распределение плотности вероятности значений интенсивности будет равно [3]

$$P_I(I) = \frac{1}{\langle I \rangle} \exp\left(-\frac{1}{\langle I \rangle}\right). \qquad (3)$$

Таким образом, распределение интенсивности в картине спеклов подчиняется отрицательно-экспоненциальному статистическому закону.

На рис. 1, *а* показан график функции $P_I(I)$. Как видно из графика, наиболее вероятное значение яркости спеклов – нулевое, что соответствует черным спеклам.



а *б*

Рис. 1. Распределение плотности вероятности интенсивности в картине спеклов: *а* – в одной длине волны; б – для некогерентной суммы двух спекл-картин, имеющих одинаковые средние интенсивности ½ <*I*> [3]

Если некогерентно складываются две статистически одинаковые, но некоррелированные спекл-картины, имеющие равную среднюю интенсивность, то распределение плотности вероятности интенсивности в результирующей спекл-картине описывается следующим выражением [3]:

$$P_I(I) = \frac{4I}{\langle I \rangle^2} \exp\left(-\frac{2I}{\langle I \rangle}\right). \qquad (4)$$

Вид функции (4) изображен на рис. 1, *б*. Из графика видно, что в некогерентной сумме двух некоррелированных спекл-картин мало темных спеклов, яркость принимает некоторое ненулевое значение.

Из изложенного видно, что статистические параметры спекл–интерференционных полей, формируемых излучением на двух длинах волн существенно отличаются от статистических параметров спекл-интерференционных полей в одной длине волны. При этом регистрация и обработка сигналов имеют особенности, которые рассмотрены в следующем разделе.

Экспериментальные исследования

Для получения спекл-интерференционных картин использовался спекл-интерферометр с двумя длинами волн, схема которого показана на рис. 2. Линейно поляризованное излучение от источников 1 и 2 (гелий-неоновые стабилизированные лазеры с длинами волн $\lambda_1 = 632$ нм и $\lambda_2 = 612$ нм и нестабильностью частоты

$\delta\lambda_1/\lambda_1 = \pm 1\times 10^{-7}$ и $\delta\lambda_2/\lambda_2 = \pm 2\times 10^{-7}$) после анализаторов 3 и 3' и четвертьволновых пластинок 4 и 4' преобразуются в излучение с круговой поляризацией. После зеркала 5 и светоделителя 6 двухволновое излучение попадает в объектив 7. После объектива 7 двухволновое излучение проходит через светоделитель 8. Затем часть пучка попадает на опорную поверхность 9, а часть пучка, прошедшая через светоделитель 8, попадает на исследуемую поверхность 11. Отраженные волны складываются и с помощью объектива 14 попадают на матрицу светочувствительных элементов видеокамеры 15. Видеокамера 15 подключена к компьютеру 16.

При подаче напряжения от источника питания 13 на пьезопривод 12 происходит смещение исследуемой поверхности 11 и производится регистрация видеокадра. При изменении напряжения на заданную величину происходит следующий шаг смещения исследуемой поверхности с регистрацией видеокадра, и т.д. в пределах заданного полного диапазона смещения.

Объектив 7 предназначен для выделения малого участка на исследуемой поверхности с целью увеличения размера спеклов, так как из формулы (9) следует, что чем меньше размер пятна освещаемой поверхности, тем больше размер спеклов, а именно

$$b = 1{,}5\lambda z / H, \qquad (9)$$

где H – размер участка освещаемой поверхности.

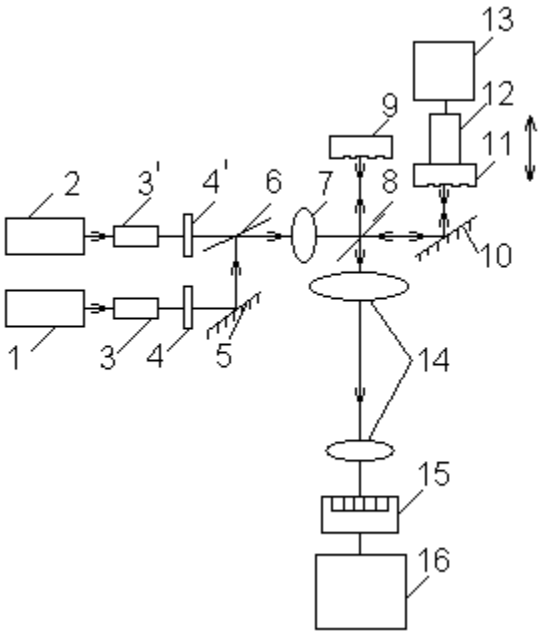


Рис. 2. Схема двухволнового спекл-интерферометра: 1, 2 – лазеры; 3, 3' – анализаторы; 4, 4' – четвертьволновые пластинки; 5, 10 – зеркала; 6, 8 – светоделители; 7 – объектив; 9 – опорная шероховатая поверхность; 11 – исследуемая шероховатая поверхность; 12 – пьезопривод; 13 – блок питания с регулируемым выходным напряжением; 14 – объектив; 15 – видеокамера; 16 – ПК

Анализаторы 3 и 3' и четвертьволновые пластинки 4 и 4' в схеме рис. 2 являются оптическими изоляторами от обратно отраженных пучков, так как стабилизированные лазеры чувствительны к обратным пучкам.

Регистрация спекл-интерференционных полей производится при помощи видеокамеры. Следует отметить, что линейный размер пикселя фоточувствительной матрицы не должен превышать оценочный размер спекла, иначе при усреднении снизится контраст спекл-интерференционной картины. Необходимо наложить ограничения на вы-

ходную апертуру, так как чем меньше диаметр выходной апертуры, тем больше размер спекла, что видно из следующей формулы:

$$b = 1{,}5\lambda z / D, \qquad (10)$$

где b – размер спекла; D – диаметр выходной апертуры; λ – длина волны; z – расстояние от выходной апертуры до изображения.

Для юстировки в схеме спекл-интерферометра опорная и исследуемая шероховатые поверхности заменялись на зеркала. Специфика юстировки двухволнового спекл-интерферометра заключается в том, что необходимо получить интерференционные картины от лазерных источников и свести лазерные пучки таким образом, чтобы полученные некогерентные спекл-картины от двух источников по возможности параллельно накладывались друг на друга. В этом заключается сложность юстировки по сравнению с одноволновым интерферометром.

Видность V интерференционной картины зависит от соотношения интенсивностей I_1 и I_2 интерферирующих пучков:

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}},$$

$$I_{\max} = (\sqrt{I_1} + \sqrt{I_2})^2,$$

$$I_{\min} = (\sqrt{I_1} - \sqrt{I_2})^2.$$

Для регистрации спекл-картины измерительное зеркало заменялось на исследуемую шероховатую поверхность. Как видно из формул, контраст интерференционной картины максимален при равенстве интенсивностей $I_1 = I_2$. Для выравнивания интенсивностей опорной и измерительной волн целесообразно использовать шероховатую опорную поверхность 9. Помимо этого, для наилучшей видности интерференционной картины требуется, чтобы мощности источников излучения 1 и 2 были приблизительно одинаковыми.

Пример одной из зарегистрированных спекл-картин в двух длинах волн показан на рис. 3. На рис. 4 для сравнения показана спекл-картина в одной длине волны. Визуально две спекл-картины подобны, но гистограммы распределения плотности вероятности интенсивности, полученные экспериментальным путем, показывают, что в спекл-картине, полученной в двух длинах волн, мало темных спеклов, а в спекл-картине, полученной в одной длине волны, меньше светлых.

Объектив проецирует спекл-картину на чувствительную площадку видеокамеры KPC-S190(H) с форматом кадра 500×582 пикселя. Оценочный размер спекла составляет 19 мкм (по формуле (9)), линейный размер элемента фоточувствительной матрицы равен 12 мкм. Зарегистрированную спекл-картину можно считать достоверной, так как на один спекл приходится 1,6 пикселя.

По теореме Х. Найквиста, для однозначного определения интерференционной полосы необходимо не менее двух отсчетов на полосу, т.е. частота дискретизации должна быть не меньше, чем удвоенная наибольшая частота в спектре сигнала. При этом исходный сигнал может быть восстановлен без искажений по дискретной выборке отсчетов. Однако когда имеется сигнал с узкополосным спектром, можно применять метод субдискретизации [4], который позволяет значительно уменьшить частоту дискретизации по отношению к значению, определяемому критерием Найквиста.

При проведении эксперимента была получена серия из 83 видеокадров и зафиксирована на компьютере. Диапазон перемещения объекта составлял 32 мкм. Период биений интерференционной картины определяется синтезированной длиной волны, которая равна $\lambda_S = \frac{\lambda_1\lambda_2}{\lambda_1 - \lambda_2} = \frac{0{,}632 \times 0{,}612}{0{,}02} = 19$ мкм, $\frac{\lambda_S}{2} = 9{,}5$ мкм, поэтому число полос

муара составило $M = \frac{32}{9,5} = 3,4$, что было подтверждено в ходе эксперимента, когда наблюдалось три целых периода муара и дробная часть. Была проведена обработка данных с помощью специального программного обеспечения. Компьютерная программа позволила выделить огибающую сигнала в одной и той же точке по последовательности видеокадров.

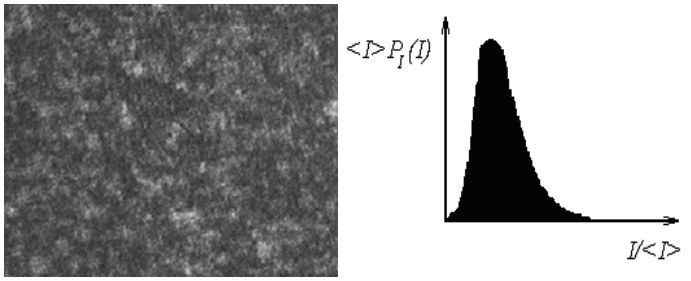


Рис. 3. Спекл-картина в двух длинах волн и гистограмма значений интенсивности

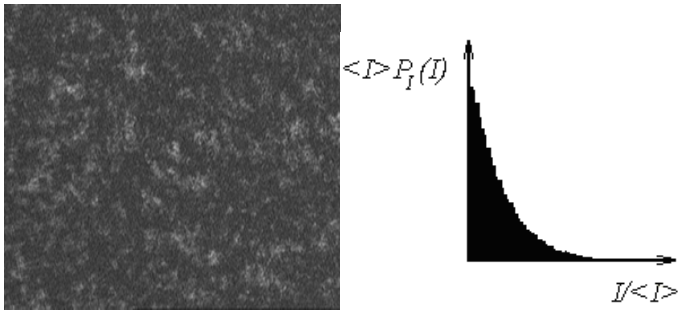


Рис. 4. Спекл-картина в одной длине волны и гистограмма значений интенсивности

Отметим, что при регистрации использованы 4 отсчета в пределах пяти интерференционных полос, т. е. объем обрабатываемой информации снижен в 2,5 раза по сравнением с определяемым по критерию Найквиста.

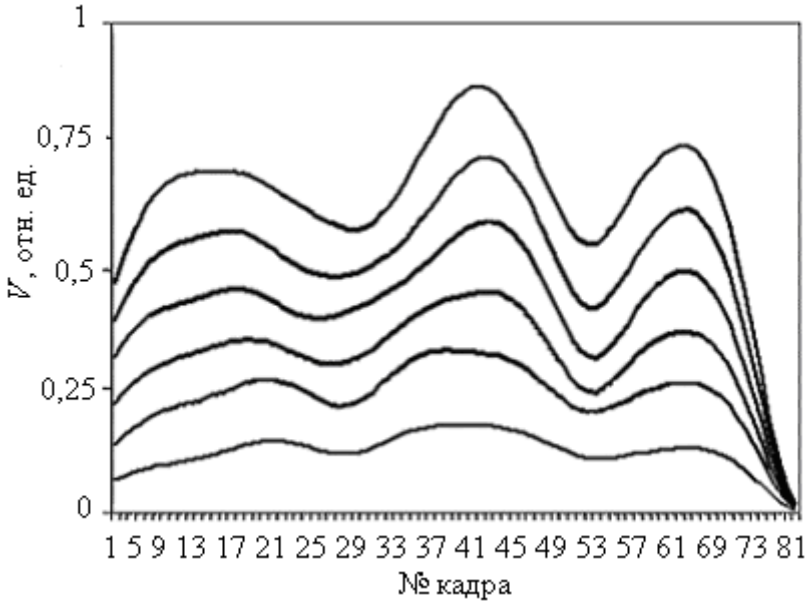


Рис. 5. Покадровая зависимость видности муара последовательности пикселов

На рис. 5 представлены экспериментальные зависимости изменения оценок огибающих сигналов для нескольких соседних пикселов. Каждой кривой соответствует отдельный пиксель. Для наглядности кривые смещены по вертикальной координате относительно друг друга. Совокупность кривых показывает локальные свойства сечения спекл-картины. Видно, что амплитуды спеклов различны. Внутри одного спекла амплитуды и фазы примерно одинаковы, следовательно, если кривые последовательности пикселов подобны друг другу, то можно сделать вывод, что они принадлежат одному спеклу. Если кривые в группе заметно отличаются, это свидетельствует о том, что захватываются соседние спеклы.

Вследствие статистического характера спеклов некоторые сигналы могут быть малыми по сравнению с шумом, поэтому была проведена многоканальная обработка полученных данных, и набор огибающих последовательности пикселов усреднялся. Результат усреднения показан на рис. 6.

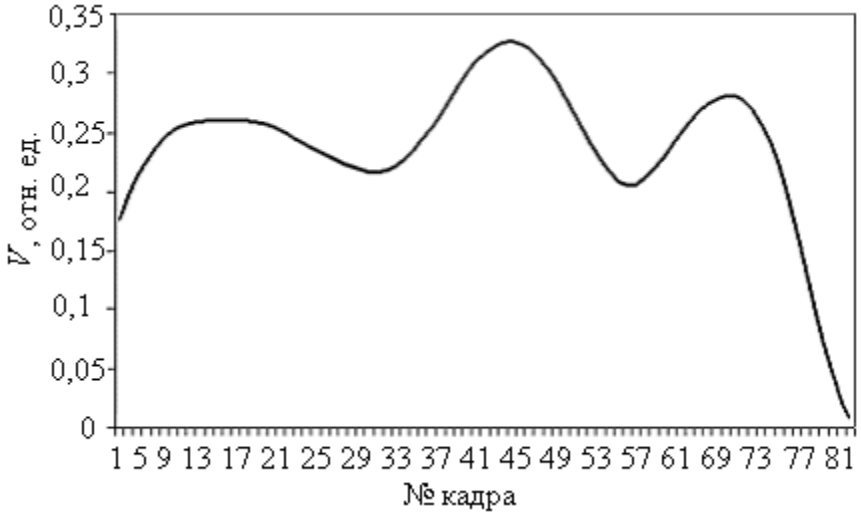


Рис. 6. Покадровая зависимость средней видности муара последовательности пикселов

Из рис. 6 видно, что форма огибающей после усреднения соответствует теоретической оценке числа периодов муара M=3,4. Вместе с тем заметно влияние краевых эффектов при фильтрации.

Заключение

Двухволновая спекл-интерферометрия применима для контроля нормального смещения шероховатых поверхностей при условии многоканальной обработки, когда суммируются огибающие, а не сами сигналы. Можно повысить быстродействие метода путем уменьшения количества видеокадров при регистрации, что, в свою очередь, достигается за счет шага перемещений, величина которого больше одной интерференционной полосы (достаточно грубых измерений), при использовании метода субдискретизации. Разработанные методики и технические средства могут быть использованы для бесконтактного контроля различных объектов со значительными отклонениями рельефа при погрешности измерения менее 5 мкм.

Литература

1. Франсон М. Оптика спеклов. – М.: Мир, 1980.
2. Polhemus C. Two-Wavelength Interferometry // Applied Optics. – 1973. – V. 12. – № 9. P. 2071–2074.

3. Вест Ч. Голографическая интерферометрия. – М.: Мир, 1982.
4. Васильев В.Н., Гуров И.П., Захаров А.С., Таратин М.А. Обработка сигналов с узкополосным спектром на основе метода субдискретизации и нелинейной фильтрации Калмана // Изв. вузов. Приборостроение. – 2006. – Т.49. – № 8. – С. 47–54.
5. Рябухо В.П. Спекл-интерферометрия // Соросовский Образовательный журнал. – 2001. – № 5. – С. 102–109.
6. Deng Luogen. Analysis on the requirement of the intensity equalization of dual spectrum lines in beatwave length interferometry // Metrology & Measurement Technique. – 1991. – № 5. – P. 1–4.
7. Джоунс Р., Уайкс К. Голографическая и спекл-интерферометрия. – М.: Мир, 1986.
8. Iizuka K. Elements of photonics. Vol. I. // Free space and special media. – New York: John Wiley & Sons, 2002.

МЕТОД УПРАВЛЕНИЯ ВИДНОСТЬЮ ИНТЕРФЕРЕНЦИОНЫХ ПОЛОС ПРИ ИЗМЕНЕНИЯХ КОЭФФИЦИЕНТА ОТРАЖЕНИЯ ИЗМЕРИТЕЛЬНОЙ ВОЛНЫ

М.А. Волынский
Научный руководитель – д.т.н., профессор И.П. Гуров

В ряде интерференционных экспериментов исследуемые объекты имеют различные коэффициенты отражения. Различие интенсивностей опорной и измерительных волн вызывает уменьшение видности интерференционных полос. В работе показана возможность управления видностью полос при использовании двух опорных волн с управляемым взаимным фазовым сдвигом.

Введение

Исследование характеристик различных объектов оптическими методами является важной задачей неразрушающего контроля. Оптические схемы, основанные на использовании двухлучевого интерферометра, в котором роль отражателя в измерительном плече играет исследуемый образец, получили широкое распространение [1]. Общим недостатком подобных систем является влияние возможного изменения коэффициента отражения измерительной волны при исследовании различных образцов, которое приводит к снижению видности интерференционной картины [2, 3]. В частности, при исследовании образцов с рассеивающей поверхностью или случайно-неоднородных сред заметно усложняется решение обратной задачи [4], необходимое для реконструкции микроструктуры исследуемого объекта.

Видность интерференционных полос, как известно, определяется соотношением интенсивностей измерительной и опорной волн. При контролируемом изменении интенсивности опорной волны с обеспечением примерно равной интенсивности с опорной волной можно повысить видность интерференционных полос и точность интерферометрической системы. В работе показана возможность управления видностью полос при использовании двух опорных волн с управляемым взаимным фазовым сдвигом.

Формирование интерференционных полос

Рассмотрим схему интерферометра Майкельсона (рис. 1).

Обозначим через E_0 модуль комплексной амплитуды источника излучения с длиной волны λ. Введем коэффициент $\alpha \in [0, 1]$, характеризующий светоделитель. При этом амплитуда измерительной волны определяется как $E_{изм.} = \alpha E_0$, амплитуда опорной волны составит $E_{оп.} = (1–\alpha)E_0$. Ввиду частичного рассеяния излучения измерительной волны при отражении от неидеально зеркальной поверхности образца необходимо ввести коэффициент $\gamma \in [0, 1]$, показывающий долю отраженного образцом излучения. Комплексная амплитуда измерительной волны в плоскости фотодетектора с учетом повторного прохождения через светоделитель определяется выражением

$$\mathbf{E}_1 = \gamma\alpha(1-\alpha)E_0 \exp(i\phi), \qquad (1)$$

где ϕ – фаза волны. Аналогичным образом можно представить комплексную амплитуду опорной волны:

$$\mathbf{E}_2 = \alpha(1-\alpha)E_0 \exp[i(\phi + \Delta\phi)], \qquad (2)$$

где $\Delta\phi$ – разность фаз интерферирующих волн.

Комплексная амплитуда результирующего светового колебания будет иметь вид

$$\mathbf{E} = \mathbf{E}_1 + \mathbf{E}_2 = \alpha(1-\alpha)E_0 \exp(i\phi)[\gamma + \exp(i\Delta\phi)]. \qquad (3)$$

Соответствующее выражение для интенсивности результирующей волны найдем, умножив **E** на комплексно-сопряженную величину:

$$I = \mathbf{E}\mathbf{E}^{*}. \qquad (4)$$

Видность полос определяется как

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}}. \qquad (5)$$

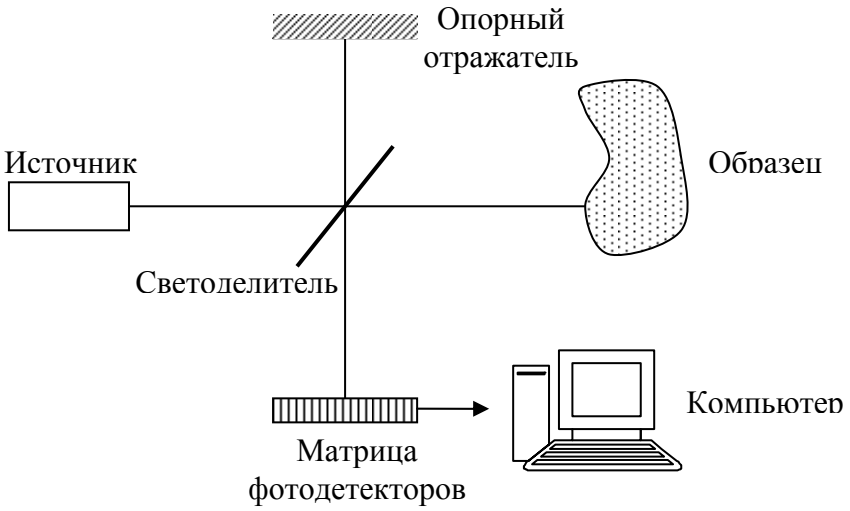


Рис. 1. Схема интерферометра Майкельсона

Введем в опорное плечо интерферометра тонкую непоглощающую пластинку с коэффициентом пропускания β (и коэффициентом отражения (1– β), соответственно) на некотором расстоянии d от опорного зеркала и обеспечим возможность управления этим расстоянием. Введенная пластинка делит излучение, идущее в направлении опорного зеркала, на две части. Одна часть отражается от пластинки, а другая проходит через нее и отражается от опорного зеркала. При этом волна (1) представляет собой сумму двух опорных волн, идущих от пластинки и опорного зеркала, а именно

$$\mathbf{E}_{21} = (1-\beta)\mathbf{E}_2 \qquad (6)$$

и

$$\mathbf{E}_{22} = \beta^2 \mathbf{E}_2 \exp[i\delta(d)], \qquad (7)$$

где набег фаз, вносимый зазором между пластинкой и опорным зеркалом составляет

$$\delta(d) = 4\pi d / \lambda. \qquad (8)$$

С полученными двумя опорными волнами складывается волна, отраженная от образца, и имеет место трехлучевая интерференция. С учетом (6) и (7), формула (3) примет вид

$$\mathbf{E} = \mathbf{E}_1 + \mathbf{E}_{21} + \mathbf{E}_{22} = \alpha(1-\alpha)E_0 e^{i\phi}[\gamma + e^{i\Delta\phi}(1-\beta+\beta^2 e^{i\delta(d)})]. \qquad (9)$$

Следует отметить, что $\delta(d)$ зависит от показателя преломления материала пластинки и от длины волны, следовательно, необходим дисперсионный элемент, который обеспечивал бы один и тот же набег фаз (при фиксированной геометрической толщине) для всех длин волн. Будем считать, что ширина спектра излучения $\Delta\lambda << \lambda$, и необходимые требования обеспечиваются воздушным промежутком между пластинкой и опорным зеркалом (при фиксированном δ), поэтому показатель преломления внутри зазора принимаем равным единице.

Можно показать, что видность полос при трехлучевой интерференции обратно пропорциональна $\cos(\delta/2)$, откуда следуют ограничения на область определения функции видности:

$$\delta \neq \frac{\pi}{2} + \pi n\,,\ n = 0, \pm 1, \ldots\,. \qquad (10)$$

Из рис. 2 видно, что за «рабочий» участок целесообразно выбрать интервал $\delta/2 \in [0, \pi/2)$.

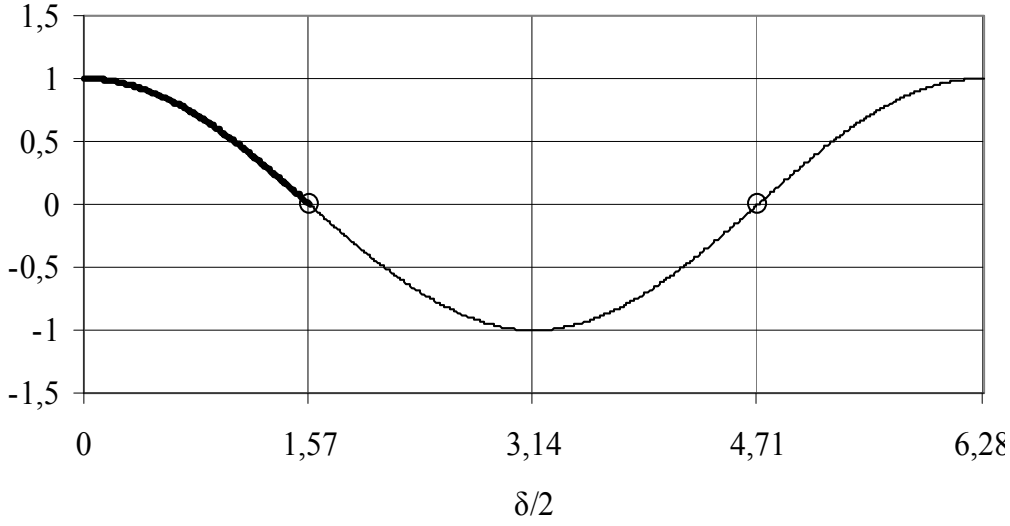


Рис. 2. Интервал управляемого изменения разности фаз двух опорных волн

Моделирование изменений функции видности

Будем считать, что в качестве источника излучения используется гелий-неоновый лазер с длиной волны λ = 632 нм. Примем величину $E_0 = 1$ и долю отраженного образцом изучения γ = 0,1.

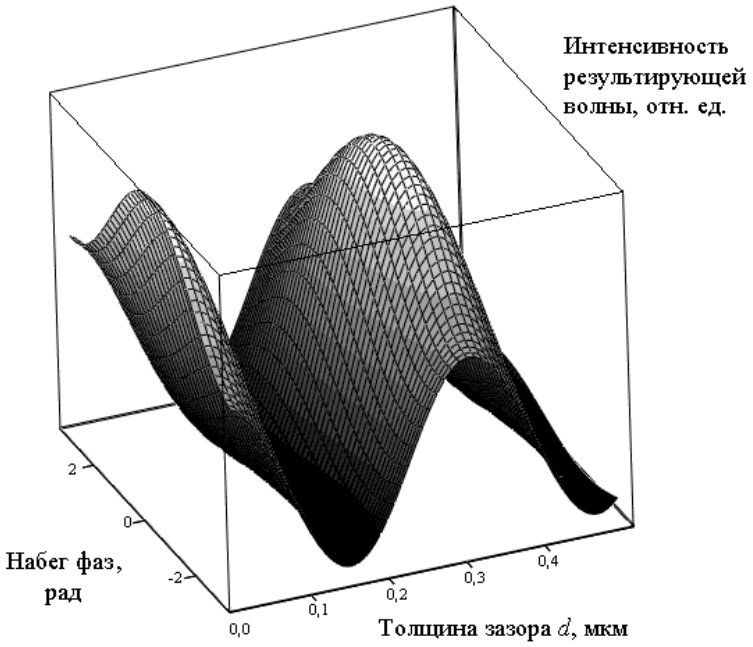


Рис. 3. Интенсивности результирующего излучения при α = 0,5

Как известно, интерференционный эффект максимален, когда амплитуды интерферирующих волн равны. Приравнивая амплитуды из (6) и (7) можно получить, что наилучшее значение $\beta = \dfrac{3+\sqrt{5}}{2} \approx 0{,}38$ (с учетом того, что $\beta \in [0, 1]$).

На рис. 3 показан график зависимости результирующей интенсивности в точке с фиксированным значением фазы ϕ (без потери общности рассмотрения можно принять $\phi = 0$) от значений $\Delta\phi$ и d. Видно, что модуляция излучения происходит по обеим осям. Модуляция по оси фазовой расстройки $\Delta\phi$ вызвана вкладом волны, отраженной от образца, а модуляция по второй оси d обусловлена действием пластины, введенной в опорное плечо интерферометра, т.е. интерференцией волн (6) и (7).

На рис. 4 представлен график видности интерференционных полос как функции от величины зазора d.

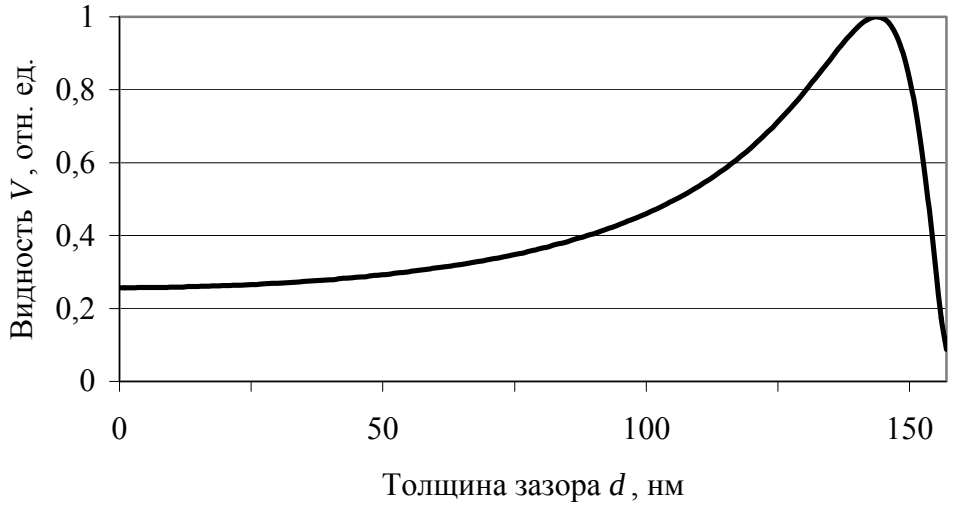


Рис. 4. Видность интерференционных полос при α = 0,5

На рис. 5 представлено множество кривых видности для различных значений коэффициента β.

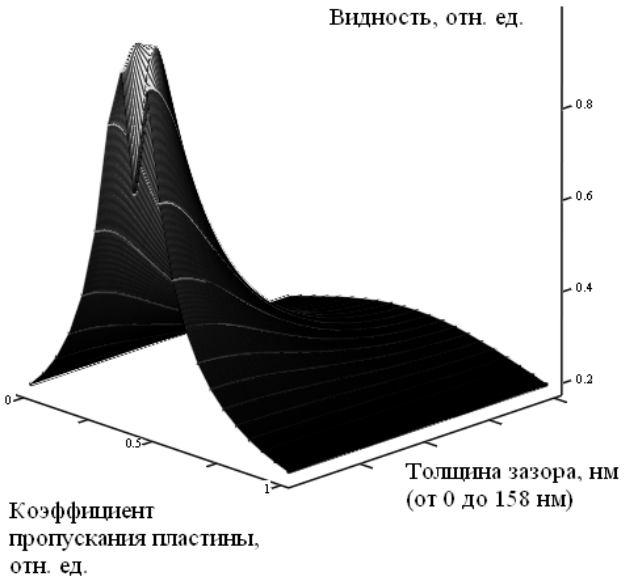


Рис. 5. График видности интерференционных полос (диапазон изменения толщины зазора соответствует области определения функции видности)

Используя (1), (4)–(9), несложно показать, что видность интерференционных полос не зависит от выбора коэффициента α. Таким образом, зная коэффициент γ, можно выбрать оптимальное значение коэффициента β, позволяющее наилучшим образом управлять видностью интерференционных полос. Из рис. 5 видно, что изменение толщины зазора при фиксированном пропускании пластины можно заменить на изменение пропускания пластины при фиксированной толщине зазора.

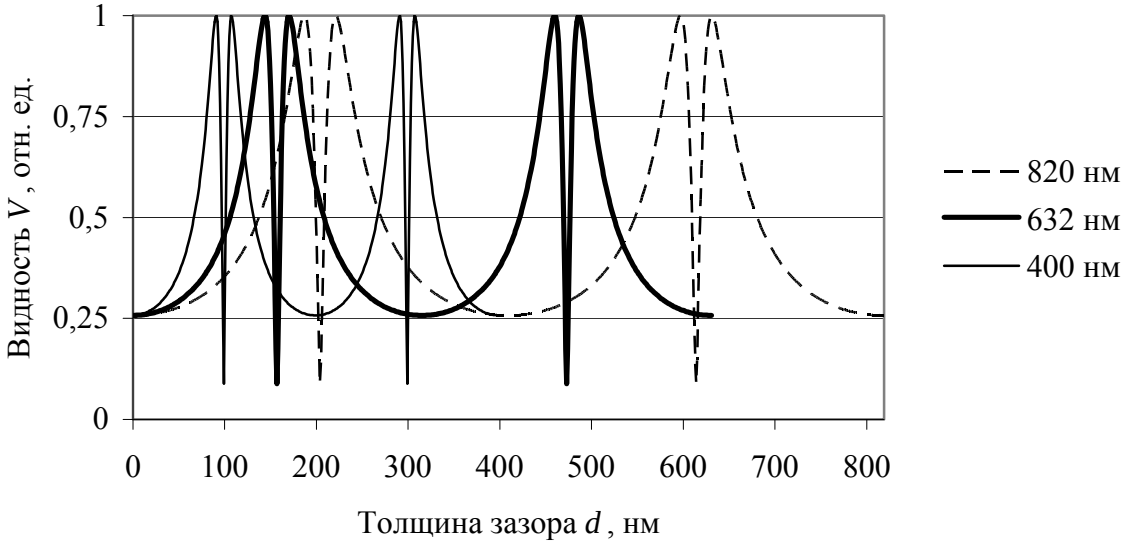


Рис. 6. Видность интерференционных полос при α = 0,5 для различных длин волн

Следует отметить, что диапазон, в котором целесообразно варьировать величину зазора, определяется длиной волны излучения источника. На рис. 6 представлены кривые видности интерференционных полос для различных длин волн из видимого диапазона спектра. Из рис. 6 видно, что в случае использования источника малой когерентности вследствие дисперсии происходит ухудшение видности ввиду вкладов различных длин волн. На рис. 7. представлено интегральная функция видности интерференционных полос при использовании источника с гауссовым спектром в диапазоне от 400 до 820 нм с центральной длиной волны λ_0 = 600 нм и полушириной $\Delta\lambda$ = 200 нм.

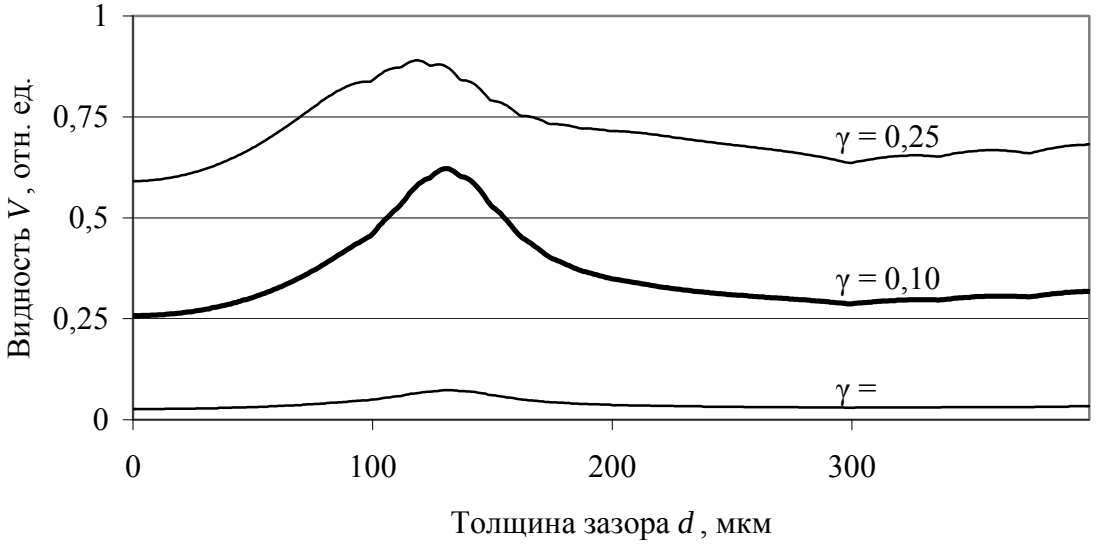


Рис. 7. Видность интерференционных полос малой когеретности при различных значениях коэффициента отражения от образца (α = 0,5)

Из рис. 7 видно, что при использовании некогерентных источников рабочий диапазон управления значением видности ограничивается минимальной длиной волны в спектре. Однако возможно управление правой границей рабочей области, например, с использованием нейтрального светофильтра. Видно, что при увеличении отражения от образца видность интерференционных полос повышается при сохранении качественного характера зависимости.

При уменьшении ширины спектра излучения происходит увеличение видности и расширение диапазона изменения ширины зазора (рис. 8).

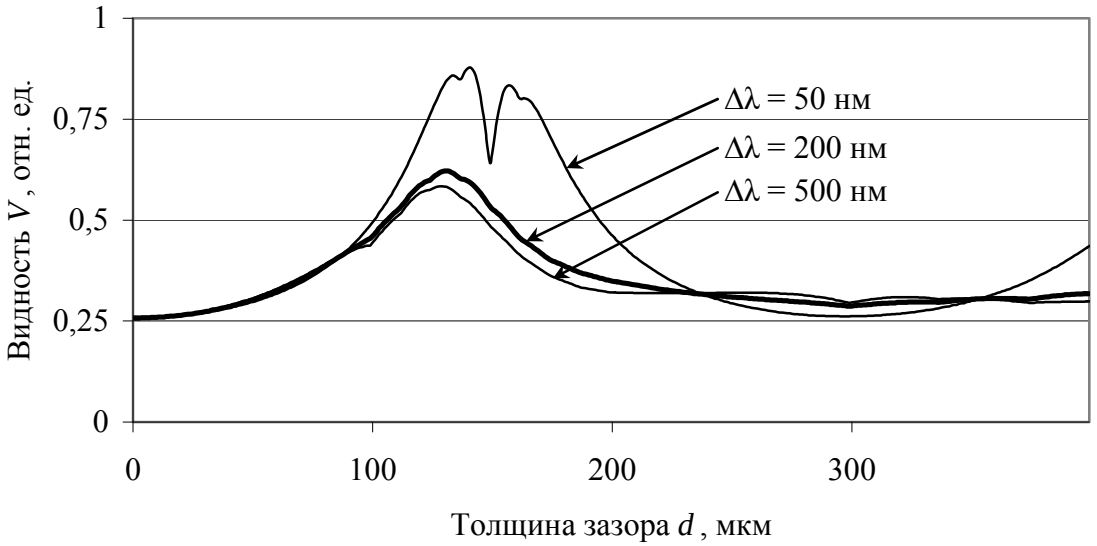


Рис. 8. Видность интерференционных полос малой когеретности при различной ширине спектра излучения (α = 0,5)

Заключение

При обеспечении управляемого и стабильного изменения толщины зазора между пластиной и опорным отражателем существует возможность управления видностью интерференционных полос в интерферометре Майкельсона со значительны рассеянием измерительной волны или при обеспечении управления пропусканием пластинки в опорном плече. Имея информацию о величине коэффициента отражения образца, можно получить зависимость видности интерференционных полос от величины зазора между пластинкой и опорным отражателем и, установив пластинку в необходимое положение, обеспечить максимальную видность полос. При применении немонохроматических источников излучения видность полос уменьшается с уменьшением степени когерентности излучения.

Литература

1. Laude B., De Matrino A., Drevillov B., Benattar L., Schwartz L. Full-field optical coherence tomography with thermal light //Applied Optics. – 2002. – V. 41. – № 31. – P. 6637–6645.
2. Коломийцов Ю.В. Интерферометры: основы инженерной теории, применение. – Л.: Машиностроение, 1976. – 296 с.
3. Борн М., Вольф Э. Основы оптики. – М.: Наука, 1970. – 856 с.
4. Гуров И.П. Оптическая когерентная томография: принципы, проблемы и перспективы. В кн.: Проблемы когерентной и нелинейной оптики / Под ред. И.П. Гурова и С.А. Козлова, СПб: СПбГУ ИТМО, 2004. – С. 6–30.

КАЧЕСТВО ЭЛЕКТРОННЫХ КОПИЙ ФИЗИЧЕСКИХ ОБЪЕКТОВ

В.О. Тишкин
Научный руководитель – к.т.н., доцент А.Н. Вершинин

Технология бесконтактного лазерного 3D-сканирования позволяет получать точные электронные копии реальных объектов в виде объемных компьютерных моделей. С помощью специализированных программных пакетов полученные модели могут подвергаться обработке, анализу, модификации, а также воспроизведены физически на специальном оборудовании (станки с ЧПУ). Качество электронных копий, с точки зрения расхождения с оригиналом, особенно важно при изготовлении, поэтому анализ электронных моделей является важной задачей при моделировании.

3D-сканирование – это систематический процесс определения координат точек, принадлежащих поверхностям физических объектов, с целью последующего получения их пространственных компьютерных моделей, которые могут модифицироваться с помощью различных программных пакетов. Устройства, с помощью которых осуществляется сканирование объектов, называют 3D-сканерами. Эти устройства не только упрощают процесс создания 3D-моделей, но и позволяют решать эту задачу с максимальной степенью достоверности по отношению к исходному оригиналу.

В настоящее время существует целый ряд технологий, позволяющих создавать трехмерные образы аппаратными методами, т.е. без привычного 3D-моделирования в специализированных программных пакетах. Условно технологии трехмерного сканирования разделяются на два типа: контактные и бесконтактные.

Первые подразумевают наличие механического устройства – «щупа», при помощи которого в компьютер передаются координаты выбранных оператором точек. Система позиционирования и координатоисчисления таких приборов построена на основе работы механических датчиков, аналогичных тем, что используются в оптико-механических манипуляторах «мышь». Последние закреплены в каждом шарнире крепления «щупа», и именно от точности этих датчиков и зависит точность работы прибора пространственного сканирования в целом.

Более перспективными, но и более сложными приборами являются бесконтактные 3D-сканеры, в которых заложены весьма изощренные алгоритмы создания пространственных каркасов. Так, во многих из них используется двойная (дополняющая основную) система ввода координат тела. Многие устройства совмещают лазерные датчики (заменяющие механический «щуп» контактных 3D-сканеров) и цифровой фотоаппарат, который используют для большей точности сканирования, что позволяет получить модели объектов с наложенными текстурами.

Большинство из существующих сейчас бесконтактных сканеров так или иначе являются стационарными: либо это специальные машины наподобие станков с ЧПУ, либо сканер закрепляется на штативе, и во время регистрации поверхности остаются неподвижными как он сам, так и объект.

Поясним работу таких сканеров на примере сканеров японской корпорации Konica Minolta (рис. 1).

Принцип, используемый в таких приборах, достаточно прост: луч, испускаемый источником, после прохождения через оптическую систему отражается от поверхности объекта и регистрируется матрицей-приемником. При этом регистрируемая часть объекта позиционируется в электронном пространстве относительно сканера, т.е. прибор является нулем координат (рис. 2).

Рис. 1. Сканеры Konica Minolta

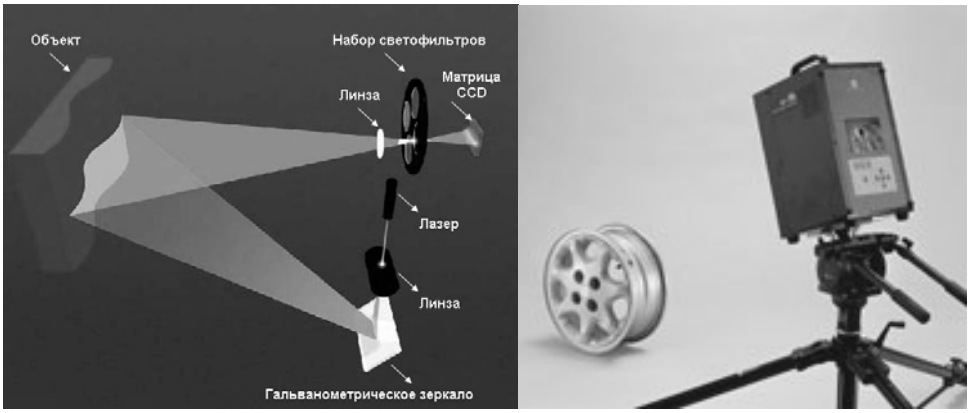


Рис. 2. Принцип сканирования

При таком подходе объект необходимо последовательно снимать с разных ракурсов и далее собирать в специальных программных пакетах для получения полной 3-х мерной копии.

Совершенно иной принцип сканирования у появившихся в недавнее время ручных сканеров, наиболее яркими представителями которых являются REV и EXAscan канадской фирмы Creaform (рис. 3).

Рис. 3. Сканеры Creaform

Такие сканеры работают по принципу размещения на поверхности модели специальных светоотражающих маркеров, регистрируя которые, прибор может производить считывание поверхности или, проще говоря, сканирует ее (рис. 4). Одним из существенных плюсов такого вида приборов является возможность получения полных 3-х мерных моделей без дополнительной сборки-сшивки.

Теперь о качестве электронных копий. Здесь один из важнейших факторов – это плотность полигональной сетки или, иначе говоря, размер одного полигона. Конечно, в зависимости от настроек на одном и том же приборе можно получить разное качество

регистрируемой поверхности. Например, если говорить о приборах типа японских, то всегда имеются несколько сменных линз (как правило, широкоугольная, средняя и телескопическая), которые захватывают разные площади поверхности и дают, соответственно, большую плотность при меньших площадях захвата и меньшую при больших площадях. Кроме того, есть возможность программной настройки фокусного расстояния каждой линзы, что, естественно, отражается на захватываемой площади.

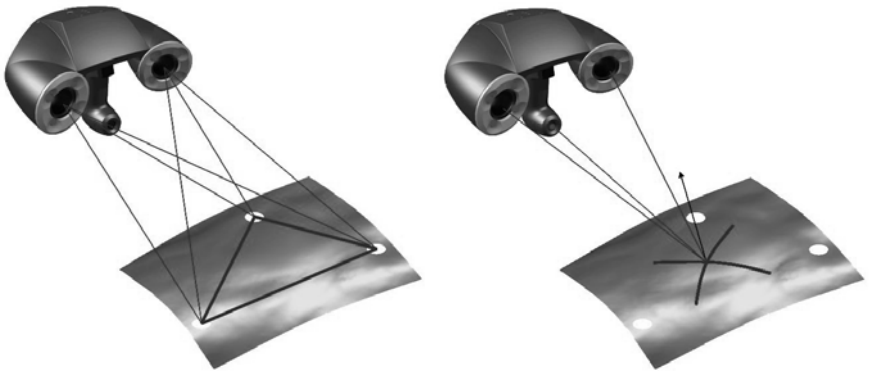


Рис. 4. Принцип сканирования приборами Creaform

Такие приборы, соответственно из-за мощной оптики (не последнюю роль играет, конечно, и стационарность), целесообразно использовать при сканировании детализированных поверхностей, например, художественные изделия (рис. 5), а также если требуется высокоточная копия технического объекта.

Рис. 5. Сканирование художественных изделий

С другой стороны, ручные приборы выигрывают при сканировании однородных поверхностей (например, корпуса у автомобилей), так как дают хорошее качество сетки для таких видов объектов. Естественно у таких сканеров также есть возможность различной настройки, но только программной, так как нет сменной оптики, позволяющей контролировать качество. Причем за счет достаточно необычного принципа сканирования настройка также интересна. Она производится за счет изменения объема виртуального куба, в котором происходит регистрация (рис. 6). Чем больше куб, тем больше размер полигона и тем ниже качество копии, тем не менее, при таком подходе важнейший из факторов – скорость сканирования, а, значит, и получения 3-х мерной модели. Не говоря уже и о том, что ручные приборы дают возможность получения целиком всей модели, с одной стороны, а с другой – упрощают сборку цельной модели: если качество модели при цельном сканировании неудовлетворительно, за счет маркеров, которые создают единую систему координат.

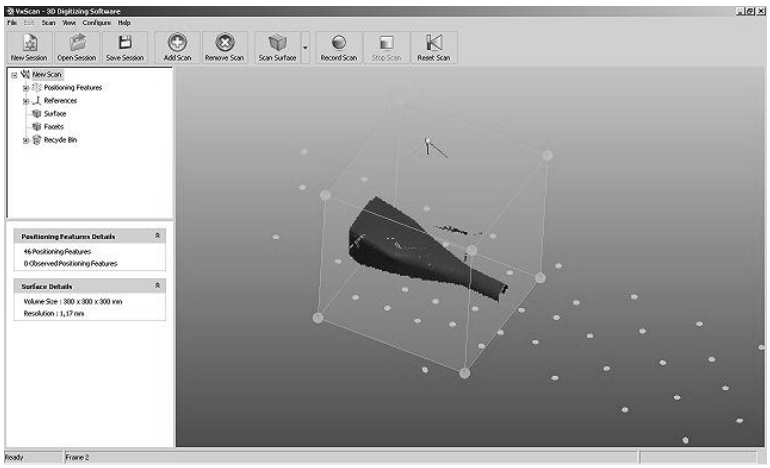


Рис. 6. Виртуальный куб

Заключение

Обозначим области применения 3D-сканеров.

Техническое проектирование:

- индустриальный дизайн, создание вручную 3D-моделей и их оцифровка с последующей доработкой методами машинной графики;
- создание 3D-моделей имеющихся штампов, пресс-форм и других изделий сложной формы, например, уникальных, в случае необходимости их изменения, ремонта или повторного воспроизведения;
- инженерный 3D-анализ, измерение геометрических параметров изделий, которые не могут быть измерены стандартными методами;
- On-Line контроль качества (проверка точности изготовления) (CAI, CAT).

Архитектура:

- в ходе реставрации, путем создания банка электронных копий (виртуального архива) и последующего изготовления или восстановления (промышленного воспроизведения) оригиналов скульптур и других рельефных изделий (сувениров, украшений, барельефов, горельефов и т.д.);
- создание виртуальных архитектурных музеев.

Медицина:

- хирургическое планирование, ортопедия, протезирование, пластическая хирургия, косметология, стоматология.

Дизайн, компьютерная графика, анимация.

Археология:

- виртуальное охранение произведений искусства;
- создание 3D-документации;
- виртуальная реставрация, а также копирование для последующей репликации;
- создание виртуальных музеев.

Каждый из пунктов подразумевает возможность использования как ручных, так и стационарных сканеров. Использование того или иного устройства обусловлено, естественно, лишь необходимым качеством электронной копии.

Литература

1. Кривобок А.С. 3D сканирование и моделирование. – СПб: ООО «Оптика-сканер», 2007.
2. Аметист-оптика. Сайт компании. – Режим доступа: www.ametist.com/3d
3. Сайт cybercon.ru. – Режим доступа: www.cybercon.ru

МОДЕЛЬ КЛЕТОК ЗРИТЕЛЬНОЙ КОРЫ, СЕЛЕКТИВНЫХ К ПРОСТРАНСТВЕННО-ПЕРИОДИЧЕСКИМ СТРУКТУРАМИ, НА ОСНОВЕ СЕТИ ХОПФИЛДА-ТАНКА

А.С. Потапов, А.Н. Аверкин
Научный руководитель – д.т.н., профессор И.П. Гуров

Построена модель клеток зрительного тракта, селективных к пространственно-периодическим структурами и участвующих в текстурной сегментации изображений. Модель представляет собой искусственную нейронную сеть типа Хопфилда-Танка, в которой рецептивные поля нейронов заданы функциями Габора, а латеральные связи обеспечивают выделение групп нейронов, дающих отклики на одинаковые структуры.

Введение

В настоящее время в области компьютерного зрения разработано большое количество методов, реализующих различные аспекты анализа изображений, однако до сих пор возможности систем компьютерного зрения далеки от возможностей соответствующих биологических систем. Таким образом, остается актуальной проблема повышения эффективности методов автоматического анализа изображений, и одним из перспективных направлений здесь является построение моделей биологических систем зрительного восприятия на основе нейрофизиологических данных [1].

Построение моделей клеток зрительного тракта позволяет как прояснить принципы функционирования биологических систем, так и использовать полученные сведенья при проектировании систем компьютерного зрения. Недавно открытыми являются несколько типов клеток зрительной коры, селективных к пространственно-периодическим структурам [2]. Эти клетки участвуют в текстурном анализе, относящимся также к фундаментальным и не вполне решенным проблемам компьютерного зрения.

Принято считать [3], что селективность к пространственно-периодическим структурам обеспечивается за счет того, что клетки обладают рецептивными полями, позволяющими им выполнять вейвлет-подобные преобразования. В частности, работа простых клеток зрительной коры хорошо моделируется с помощью функций Габора [4]. Однако подобные модели не описывают процесс сегментации изображений, для которого необходимо учитывать не только рецептивные поля отдельных клеток, но и систему связей между ними, которая бы обеспечивала совместную активацию групп клеток внутри однородных текстурных областей.

В работе производится построение и исследование модели клеток зрительной коры указанного типа. Модель представляет собой трехуровневую искусственную нейронную сеть (ИНС). Первый уровень ИНС имитирует работу простых клеток зрительной коры, рецептивные поля которых описываются функциями Габора. На втором уровне имитируются сложные клетки, отклики которых соответствуют габоровской энергии. Третий уровень представляет собой рекуррентную нейронную сеть Хопфилда-Танка (см., напр., [5]), выделяющую группы нейронов, дающие отклики на одинаковые структуры. На основе экспериментальных исследований показывается правдоподобность, но недостаточность модели для объяснения механизмов текстурного анализа.

Нейросетевая модель

Построенная нейросетевая модель клеток зрительной коры, участвующих в текстурном анализе изображений, имеет структуру, представленную на рис. 1.

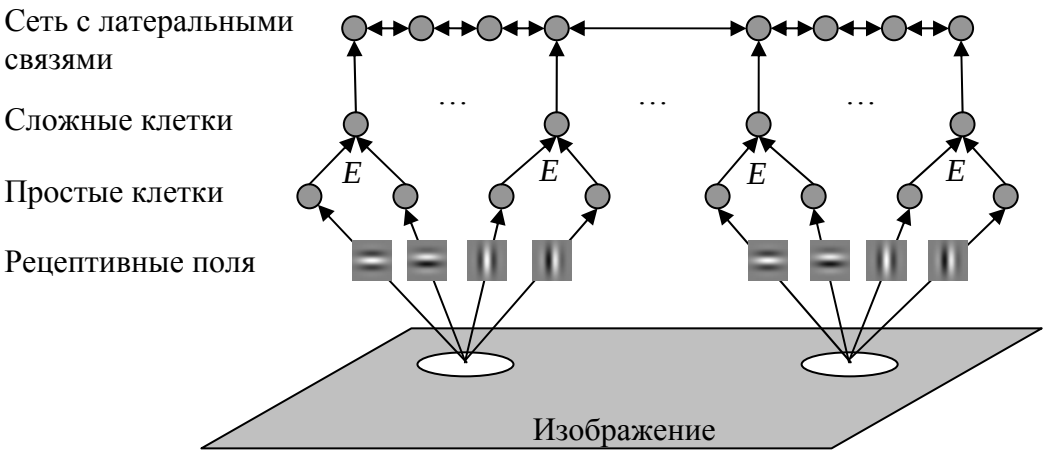


Рис. 1. Общая структура искусственной нейронной сети для моделирования клеток, селективных к пространственно-периодическим структурам

Построенная ИНС состоит из трех уровней. На первом уровне моделируется работа простых клеток зрительной коры, рецептивные поля которых задаются в виде габоровских функций:

$$g_{\xi,\eta,\theta,\sigma,\gamma,\lambda,\varphi}(x,y) = e^{-\frac{\tilde{x}^2+\gamma^2\tilde{y}^2}{2\sigma^2}} \cos\left(2\pi\frac{\tilde{x}}{\lambda}+\varphi\right),$$

где $\tilde{x} = (x-\xi)\cos\theta - (y-\eta)\sin\theta$ и $\tilde{y} = (x-\xi)\sin\theta + (y-\eta)\cos\theta$ – преобразованные координаты.

Параметры функций Габора имеют следующий смысл. Величины ξ и η определяют координаты центра рецептивного поля клетки на изображении, θ, σ и γ – угол ориентации, размер и вытянутость этого поля, а λ и φ – длину волны и фазу периодической компоненты.

В построенной ИНС каждой точке на изображении соответствует большое число простых клеток с разными значениями параметров функций Габора. Все простые клетки разделены на слои; в каждом слое значения параметров постоянны, за исключением значений ξ и η. Таким образом, в каждом слое нейроны селективны по отношению к одинаковым структурам, но помещенным в разные точки изображения. Количество слоев определялось как количество комбинаций допустимых значений различных параметров (всего использовалось порядка пятидесяти слоев). Варьировались параметры λ, θ и γ. Значение параметра σ определялось, исходя из следующего соотношения $\sigma/\lambda = 0.56$, принятого в моделях простых клеток [2]. Параметр φ принимал значения 0 и $-\pi/2$ и участвовал не в разделении простых клеток на слои, а в формировании отклика клеток следующего уровня. Этот отклик определялся по формуле

$$E_{\xi,\eta,\theta,\sigma,\gamma,\lambda}(x,y) = \sqrt{r^2_{\xi,\eta,\theta,\sigma,\gamma,\lambda,\varphi=0}(x,y) + r^2_{\xi,\eta,\theta,\sigma,\gamma,\lambda,\varphi=-\pi/2}(x,y)},$$

где r – отклик простой клетки как свертка $r_{\xi,\eta,\theta,\sigma,\gamma,\lambda,\varphi}(x,y) = (f \otimes g_{\xi,\eta,\theta,\sigma,\gamma,\lambda,\varphi})(x,y)$ рецептивного поля g и изображением f. Отклик сложной клетки E представляет собой габоровскую энергию и не зависит от значения фазы φ. На рис. 2 представлено текстурированное изображение и примеры откликов сложных клеток в двух слоях (темным цветом обозначены более сильные отклики). Как видно из рисунка, характер откликов сильно отличается в разных областях изображения в зависимости от параметров рецептивных полей.

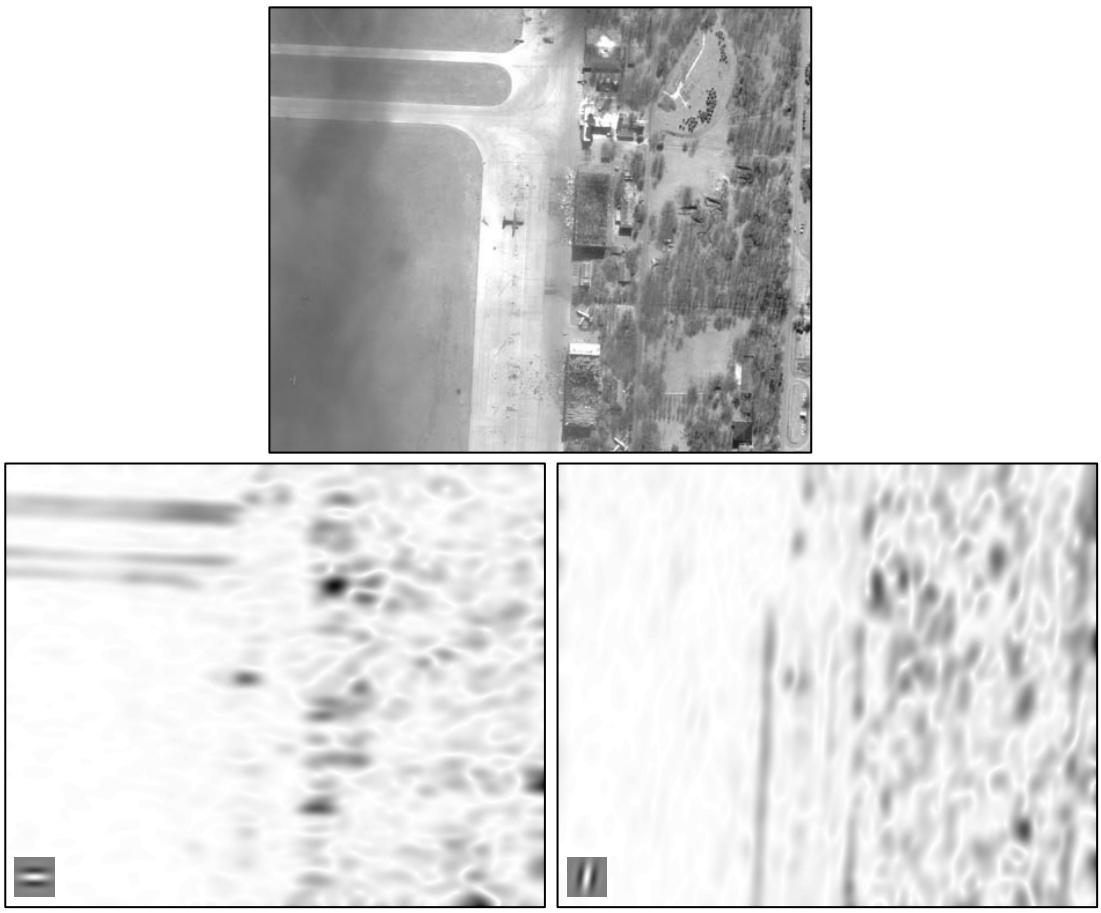


Рис. 2. Пример изображения и соответствующих откликов сложных клеток в двух слоях с приведенными рецептивными полями

Следующий уровень нейронной сети представлял собой рекуррентную нейронную сеть, топологически эквивалентную уровню сложных клеток, но включающую набор латеральных связей между нейронами. Пусть нейроны этого слоя пронумерованы от 1 до *N*. Обозначим через $U_i(t)$ уровень возбуждения *i*-го нейрона в момент времени t. Выход от *i*-го нейрона $V_i(t)$ определяется его уровнем возбуждения $U_i(t)$ и некоторой нелинейной передаточной функцией ψ, в качестве которой может быть взята линейная передаточная функция с насыщением

$$V_i(t) = \psi\big(U_i(t)\big) = \begin{cases} 0, & U_i(t) \le 0 \\ U_i(t), & 0 < U_i(t) < 1 \\ 1, & U_i(t) \ge 1 \end{cases}.$$

Обозначим через $W_{i,j}$ вес связи, идущей от *i*-го нейрона к *j*-му нейрону. Тогда изменение уровня возбуждения *i*-го нейрона в следующий такт времени задается следующей формулой:

$$U_i(t+1) = U_i(t) + \sum_{j=1}^{N} W_{j,i} V_j(t).$$

Исходно каждый нейрон данного уровня получал сигнал от соответствующего ему нейрона предыдущего уровня для установления начальных значений $U_i(0)$.

Веса связей $W_{i,j}$ должны быть организованы таким образом, чтобы в результате релаксации сети в каждом слое оставались только нейроны, чьи характеристики рецеп-

тивных полей и координаты на изображении соответствуют областям однородной текстуры. Остальные нейроны при этом должны подавляться. Таким образом, близко расположенные (в системе координат изображения) нейроны одного слоя должны поддерживать друг друга, а разных слоев – подавлять. В результате для каждой точки на изображении останется активным нейрон только в одном слое, характеристики которого наиболее соответствуют характеристикам текстуры в данной точке.

Для реализации связей между нейронами с указанными свойствами веса были заданы на основе функции вида

$$\Omega(d) = \frac{1}{\sqrt{2\pi}\sigma^3}\left(\frac{d^2}{\sigma^2} - 1\right)\exp\left(-\frac{d^2}{2\sigma^2}\right),$$

где $d = \sqrt{(\xi_1 - \xi_2)^2 + (\eta_1 - \eta_2)^2}$ – расстояние в плоскости изображения между нейронами с координатами (ξ_1, η_1) и (ξ_2, η_2), а σ – параметр функции Габора, определяющий размер рецептивного поля. Эта функция, имеющая форму «мексиканской шляпы», выделяет вокруг нейрона две области (см. рис. 3) – круг и кольцо, в одном из которых влияние нейронов друг на друга положительное, а в другом – отрицательное. Знак влияния зависит от удаленности слоев (по прочим параметрам функций Габора), к которым относятся связанные нейроны.

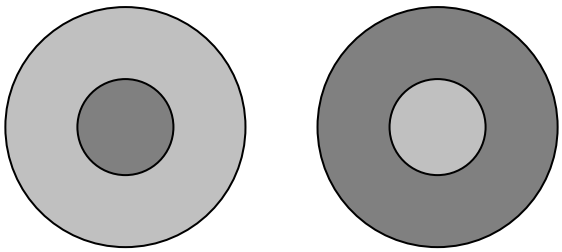


Рис. 3. Смена подкрепления и торможения пары нейронов в зависимости от расстояния между ними и удаленности соответствующих слоев

В частности, подкрепление нейронов в одном слое осуществляется в кольце, в то время как для нейронов удаленных слоев в кольце осуществляется торможение. Степень близости двух слоев определяется в пространстве параметров $(\lambda, \theta, \gamma)$, которые для каждого слоя имеют индивидуальные значения. Конкретные значения параметров латеральных связей и параметров релаксации ИНС были подобраны эмпирически, после чего было произведено экспериментальное изучение функционирования данной модели.

Экспериментальное исследование модели

Было произведено экспериментальное исследование разработанной ИНС. Как показали эксперименты, слои, исходно содержащие малоактивные нейроны, после релаксации сети полностью подавлялись. При этом в других слоях рекуррентной сети происходило подавление лишь части нейронов, в то время как остававшиеся активные нейроны соответствовали определенным текстурным областям. На рис. 4 представлены типичные примеры слоев нейронной сети, в которых произошло выделение групп активных нейронов, соответствующих какой-либо области. После релаксации ИНС в слоях остаются активные группы нейронов, располагающихся в узлах текселов и находящихся на удалении, в среднем равном размеру рецептивного поля. Как видно из рис. 4, в слое остаются активными нейроны, соответствующие одной определенной текстуре.

Эксперименты показывают адекватность модели клеток и возможность использования данного подхода для решения задач текстурного анализа. Однако для автомати-

ческого решения прикладных задач на основе результатов работы построенной ИНС требуется их дополнительная обработка. Также на основе текущей модели невозможно количественно оценить эффективность выполняемой ею текстурной сегментации.

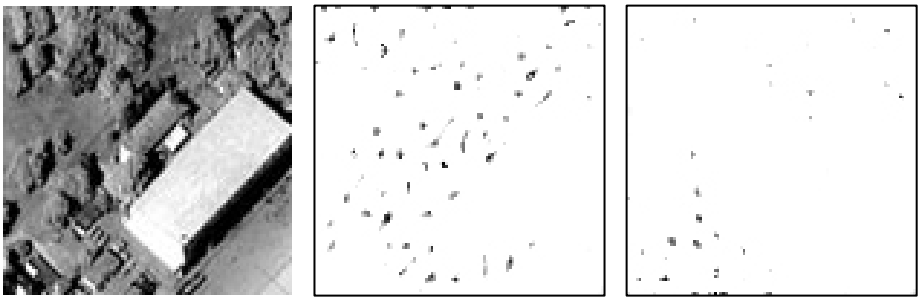


Рис. 4. Фрагмент исходного изображения и активность двух слоев нейронов после релаксации ИНС

Заключение

Нами была разработана и протестирована нейросетевая модель клеток зрительной коры, селективных к пространственно-периодическим структурам. Данная модель представляет собой трехуровневую искусственную нейронную сеть, в которой рецептивные поля нейронов нижнего уровня описываются функциями Габора, выход нейронов второго уровня соответствует габоровской энергии, а третий уровень является рекуррентной нейронной сетью, латеральные связи в которой обеспечивают выделение групп клеток, отвечающих определенным текстурным областям.

Экспериментальная проверка показала, что с помощью данной ИНС в определенной степени возможно выделение областей с постоянной текстурой, т.е. модель в целом является адекватным описанием нейрофизиологических данных, которые могут быть перенесены в область компьютерного зрения. Однако результат работы данной модели не пригоден для автоматического использования без дополнительной обработки. Помимо этого, одним из существенных недостатков разработанной ИНС в плане практического использования является низкая скорость работы. Таким образом, обнаруженные принципы организации естественных нейронных сетей требуют либо аппаратной реализации, либо поиска такой программной реализации, которая бы воспроизводила основные идеи, но в адаптированной к возможностям последовательных цифровых машин форме, что и является предметом наших последующих исследований.

Литература

1. Kruizinga P., Petkov N. Nonlinear operator for oriented texture // IEEE Tran. on image processing. – 1999. – Vol. 8. – No. 10. – P. 1395–1407.
2. Grigorescu C., Petkov N., Westenberg M.A. Contour detection based on nonclassical receptive field inhibition // IEEE Trans. on image processing. – 2003. – Vol. 12. – No. 7. – P. 729–738.
3. Field D.J. Wavelets, vision and the statistics of natural scenes // Phil. Trans. R. Soc. Lond. A. – 1999. – Vol. 357. – P. 2527–2542.
4. Daugman J.G. Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters // J. Opt. Soc. Amer. A. – 1985. – Vol. 2. – No. 7. – P. 1160–1169.
5. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. – 2-е изд. – М.: Горячая линия-Телеком, 2002. – 382 с.

ПРЕДСТАВЛЕНИЕ МНОГОКАНАЛЬНЫХ ИЗОБРАЖЕНИЙ В ПСЕВДОЦВЕТЕ ПО ПРИНЦИПУ СХОДСТВА С ОБРАЗЦОМ

А.М. Малов
(ФГУП НИИ комплексных испытаний оптико-электронных приборов и систем)
Научный руководитель – д.т.н., профессор И.П. Гуров

Представлен способ визуализации многоканальных изображений в псевдоцвете. Синтез итогового изображения проводится интерактивно с применением преобразования изображений по принципу сходства с образцом под визуальным контролем пользователя. Способ может быть использован для обработки многоканальных изображений медико-биологических микропрепаратов, в материаловедении, а также – для обработки многоспектральных данных дистанционного зондирования, полученных с помощью аэрокосмической съемки. Работоспособность способа продемонстрирована на примерах обработки нескольких гиперспектральных изображений.

Введение

Из множества задач, решаемых в рамках компьютерной обработки изображений, можно выделить задачу визуализации – представления данных в наглядной форме и в виде, удобном для их дальнейшего использования. Эта задача наиболее актуальна при обработке многоканальных изображений.

В связи с трудностями наглядного представления многомерных данных известные методы визуализации многоканальных изображений либо используют представление лишь части этих данных – цветовой синтез трех выборочных спектральных зон (выбирают эти зоны различными способами) [1], либо предлагают отображение трехмерных данных в виде так называемого «многоспектрального куба» [2]. При таком подходе к визуализации многоканальных изображений пытаются сохранить все исходные данные и представить все отображаемые объекты. При этом визуальное восприятие затруднено – приходится «рассматривать» различные варианты представления.

Однако при решении конкретной задачи не все объекты представляют одинаковый интерес. Очевидно, что производить визуализацию целесообразно таким образом, чтобы для выделения объектов использовалась вся относящаяся к ним информация, и при этом на итоговом изображении объекты, представляющие интерес, отображались наилучшим образом с сохранением, по возможности, контекстной информации.

Для визуализации многоканальных изображений в работе предлагается использовать метод преобразования изображений по принципу сходства с образцом [3, 4].

Синтез итогового изображения в псевдоцвете

При обработке многоканальных изображений часто возникает необходимость выделить и отобразить на одном изображении сразу несколько групп разнотипных объектов, представляющих интерес для исследователя. Наиболее наглядного представления имеющейся информации можно достичь, если каждой группе объектов сопоставить свой цвет, синтезировав, таким образом, изображение в псевдоцвете.

Для решения данной задачи предлагается использовать метод преобразования изображений по принципу сходства с образцом [3, 4].

Процесс представления многоканальных изображений в псевдоцвете состоит из нескольких этапов. Сначала выбирают образцы (эталоны), представляющие интерес. Затем для каждого из образцов синтезируют монохроматическое изображение, представляющее собой визуализацию меры сходства с этим эталоном. Итоговое изображение получается путем слияния всех изображений, полученных для выбранных образцов, каждому из которых присвоен свой цвет.

При слиянии всех монохроматических изображений цвет каждого пикселя на итоговом изображении определяется следующим правилом:

$$Ixy_{итоговое} = \max\{Ixy_k \mid k = 1,2,..,N\}, \quad (1)$$

где $Ixy_{итоговое}$ – интенсивность пикселя с пространственными координатами x и y на итоговом изображении, Ixy_k – интенсивность пикселя с теми же пространственными координатами на k-м монохроматическом изображении, а N определяет количество выбранных образцов.

Продемонстрируем результат синтеза итогового изображения в псевдоцвете на примере обработки 50 гиперспектральных изображений поперечного среза корневища ландыша с концентрическими васкулярными узелками. Изображения получены с помощью автофлюоресцентной микроскопии в спектральном диапазоне от 420 до 750 нм с интервалом 6 нм. На рис. 1 в качестве примера исходных данных приведены 6 из 50 изображений препарата.

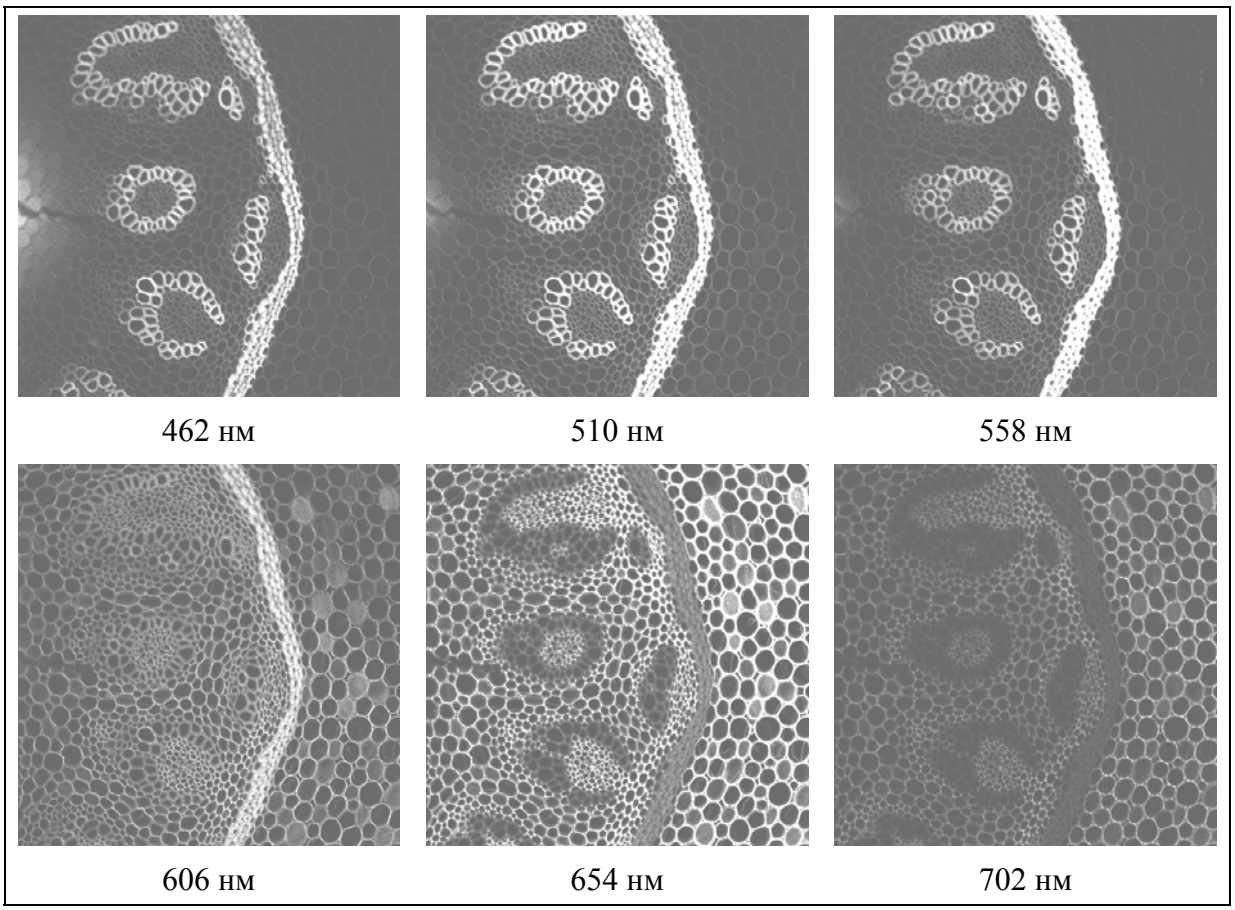
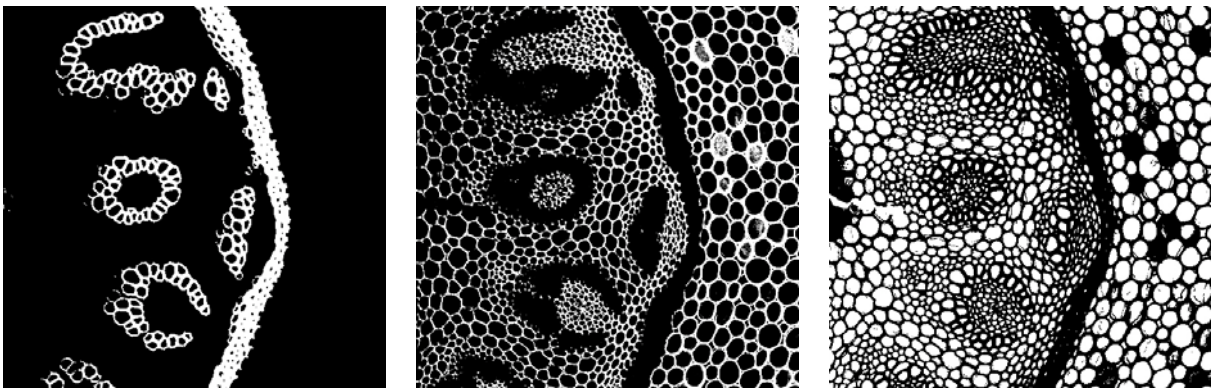


Рис. 1. Некоторые из 50 использованных для обработки исходных гиперспектральных изображений микропрепарата

После обработки всех 50 исходных гиперспектральных изображений были получены монохроматические изображения, которые представляют собой визуализацию меры сходства с каждым из трех выбранных нами эталонов. Результаты обработки приведены на рис. 2.



Эталон 1 Эталон 2 Эталон 3

Рис. 2. Монохроматические изображения. Визуализация меры сходства с каждым из трех выбранных эталонов

Из-за сложности представления цветного изображения в тонах серого для демонстрации синтеза изображения в псевдоцвете мы выбрали лишь три эталона. В реальной практике, при работе с полноцветной RGB палитрой, количество выбранных эталонов (следовательно, количество выделяемых объектов интереса) может быть больше. В нашем примере с первым эталоном был сопоставлен зеленый цвет, со вторым – желтый, а с третьим – белый. Осуществив по правилу (1) слияние трех монохроматических изображений, представленных на рис. 2, мы синтезировали итоговое изображение в псевдоцвете. Результат синтеза показан на рис. 3.

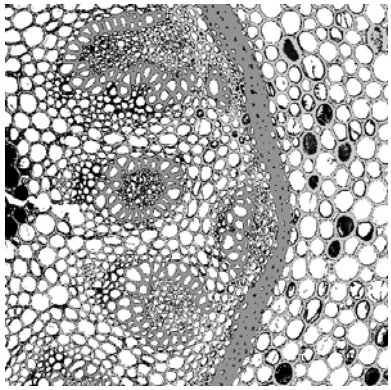


Рис. 3. Результат синтеза итогового изображения в псевдоцвете с выделением объектов трех типов

Отметим, что этот метод позволяет включать в процесс визуализации, кроме спектральных, и другие признаки отображаемых объектов, например, текстурные, путем добавления преобразованных исходных изображений.

При обработке данных дистанционного зондирования, полученных с помощью аэрокосмической съемки, часто также возникает необходимость в визуализации многоканальных изображений в псевдоцвете, например, для создания различных тематических карт. Синтез итогового цветного изображения в данном случае производится по тому же принципу, который описан нами выше. При интерактивном создании промежуточных монохроматических изображений пользователь идентифицирует определенный эталон с конкретным объектом, руководствуясь контекстной информацией, основанной на его собственном опыте, и данными, полученными с помощью наземных измерений.

Метод не чувствителен к изменениям условий съемки. Действительно, если использовать значения спектральных признаков для эталонов, которые получены при съемке (а не из спектральной библиотеки), то при визуализации данным методом условия съемки не окажут влияния на результат, так как используемые значения признаков изображений визуализируемой сцены получены при тех же условиях и имеют те же искажения. Кроме того, в этом случае метод менее чувствителен к погрешностям попиксельного совмещения исходных каналов по сравнению с методами, использующими базы спектральных данных, так как если спектр эталона, выбранного на изображении, искажен из-за смещения, то он также искажен и у других пикселей, сходных с эталоном.

В качестве примера мы выполнили синтез гиперспектральных снимков городского ландшафта в псевдоцвете с использованием 330 спектральных каналов. Некоторые из использованных гиперспектральных снимков приведены на рис. 4. Результат визуализации всех 330 гиперспектральных снимков, среди которых были и зашумленные с помехами различной величины (около 20 снимков очень сильно зашумлены, 54 имеют частичные искажения), представлен на рис. 5.

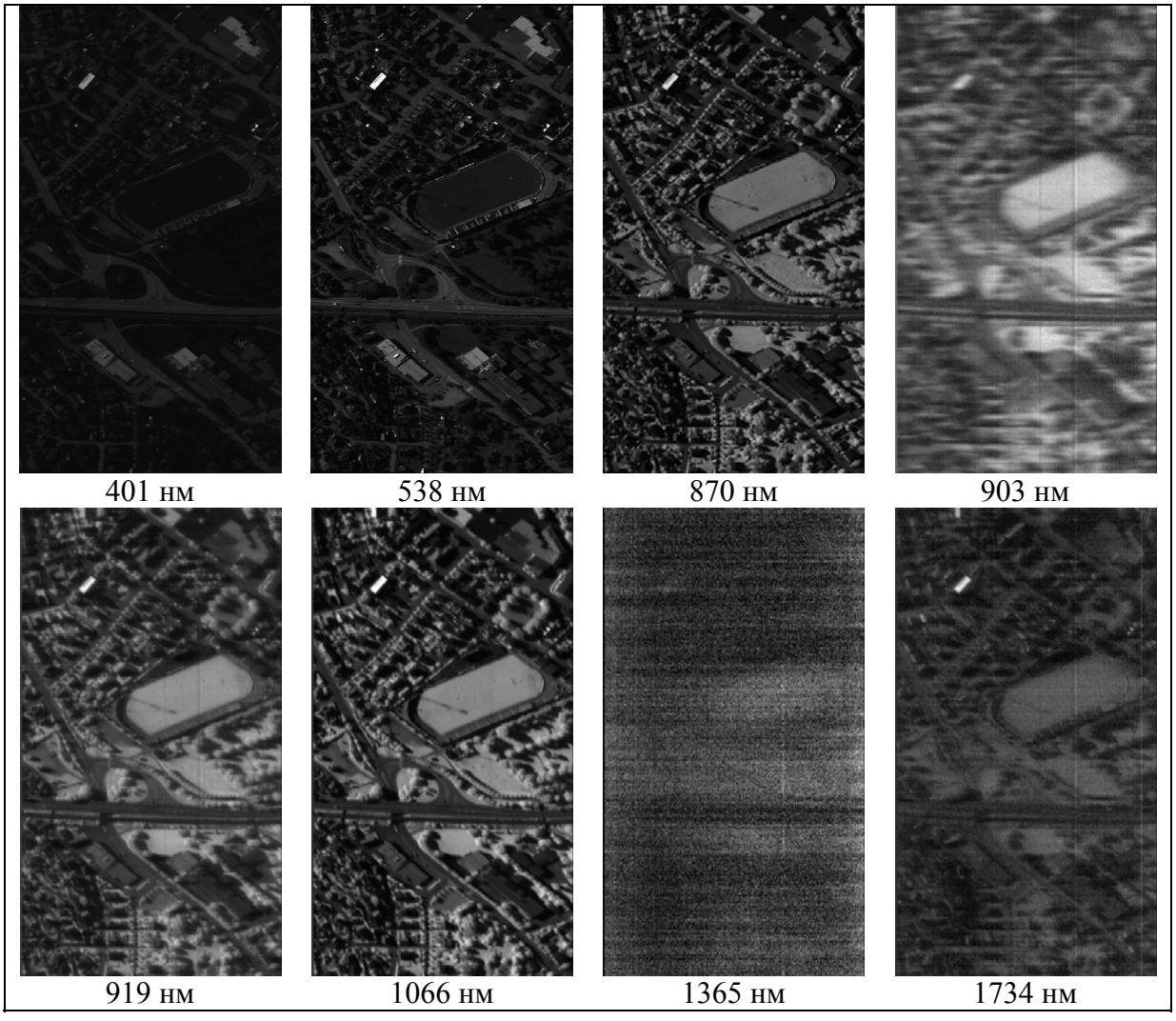


Рис. 4. Примеры некоторых из 330 гиперспектральных снимков, участвовавших при синтезе цветного изображения

Рис. 5. Итоговое цветное изображение,
синтезированное с использованием 330 гиперспектральных снимков

Заключение

Предложенный подход к решению задачи представления многоканальных изображений в псевдоцвете имеет ряд положительных свойств:

- синтез итогового изображения осуществляется интерактивно, под визуальным контролем пользователя;
- для такой визуализации не требуется проведения предварительной классификации: напротив, визуализированное изображение способствует проведению классификации с меньшей погрешностью;
- в процессе получения промежуточных монохроматических изображений для достижения лучшего качества выделения объектов интереса может быть привлечена дополнительная информация (текстурные, градиентные и другие признаки).

Рассмотренный способ представления многоканальных изображений в псевдоцвете реализован в специализированном программном обеспечении.

В статье использованы гиперспектральные снимки, любезно предоставленные Convallaria section, acquisition with Leica TCS SP5, data received from Biotechnologisches Zentrum der TU Dresden (объекты автофлюоресцентной микроскопии) и компанией “Norsk Elektro Optikk AS” (данные дистанционного зондирования земной поверхности).

Литература

1. Know H., Der S.Z., Nasrabadi N.M., Adaptive multisensor target detection using feature-based fusion. // Optical Engineering. – 2002. – V. 41(1). – 69–80.
2. Hyperspectral Image Analysis. Geomatica 10. – Режим доступа: www.pcigeomatics.com
3. Sheremetyeva T.A., Filippov G.N., Malov A.M. Visualization of multispectral images. / International Symposium OPTRO 2005, Paris, France.
4. Шереметьева Т.А., Филиппов Г.Н. Способ преобразования изображений. Патент РФ № 2267232. // Бюллетень изобретений. – 2005. – №36. – С. 265.

СМЕЩЕНИЕ ОСИ СВЕТОВОГО ПУЧКА, НАКЛОННО ПАДАЮЩЕГО НА ГРАНИЦУ АНИЗОТРОПНО РАССЕИВАЮЩЕЙ СРЕДЫ

Е.И. Задорожная, М.Е. Кононенко
Научный руководитель – к.ф.-м.н., доцент Ю.И. Копилевич

В приближении малоуглового рассеяния для уравнения переноса излучения в поглощающей и рассеивающей среде исследовано распределение освещенности в поперечном сечении светового пучка, наклонно падающего на границу заполненного средой полупространства. Показано, что несимметричность ослабления относительно геометрической оси пучка в среде приводит к смещению энергетического центра пучка. Изучено изменение величины смещения с глубиной, проанализирована зависимость эффекта от оптических характеристик среды, угла падения и параметров исходного пучка.

Введение

С наклонным падением светового пучка на границу поглощающей и/или рассеивающей среды приходится сталкиваться в различных областях применения лазеров – от лазерной обработки материалов до дистанционного зондирования океана, причем зачастую важно учитывать изменение распределения освещенности по поперечному сечению пучка с глубиной проникновения в среду [1, 2]. Сущность рассматриваемого здесь явления состоит в смещении максимума поперечного распределения освещенности в пучке относительно его геометрической оси, соответствующей закону преломления на границе среды.

Проведенный теоретический анализ основывается на применении уравнения переноса излучения (УПИ) [3, 4]. Предполагается, что падающий пучок имеет достаточно малую расходимость, а индикатриса рассеяния в среде является сильно вытянутой вперед, что позволяет использовать малоугловое диффузионное приближение для решения УПИ [4, 5].

Формулировка задачи

Пусть в декартовых координатах $\{z, \mathbf{x}\}$, $\mathbf{x} = \{x, y\}$ плоскость $z = 0$ является границей поглощающей и рассеивающей среды с показателем преломления n_2, заполняющей полупространство $z > 0$; контактирующая среда с показателем преломления n_1 в области $z < 0$ предполагается прозрачной. Ось монохроматического светового пучка ($O\zeta$ на рис. 1), падающего на границу раздела из прозрачной среды, составляет угол ϑ_1 с осью Oz.

В декартовых координатах $\{\zeta, \boldsymbol{\xi}\} = \{\zeta, \xi_{//}, \xi_{\perp}\}$ обозначим через $I(\zeta, \boldsymbol{\xi}, \boldsymbol{\kappa}) \equiv I(\zeta, \xi_{//}, \xi_{\perp}, \boldsymbol{\kappa})$ лучевую яркость падающего пучка в направлении $\{1, \boldsymbol{\kappa}\} = \{1, \kappa_{//}, \kappa_{\perp}\}$, причем предполагается, что $\kappa^2 << 1$.

Ограничимся для простоты рассмотрением двумерной задачи; начальное распределение яркости на плоскости $\zeta = 0$ зададим в виде

$$I(0, \boldsymbol{\xi}, \boldsymbol{\kappa}) \equiv I(0, \xi_{//}, \xi_{\perp}, \boldsymbol{\kappa}) = \frac{1}{\pi R div} \exp\left(-\frac{\xi_{//}^2}{R^2}\right) \exp\left(-\frac{\kappa_{//}^2}{div^2}\right) \delta(\kappa_{\perp}), \qquad (1)$$

где R – начальный радиус пучка, div – его расходимость ($div << 1$) в плоскости падения, $\delta(\kappa)$ – дельта-функция Дирака.

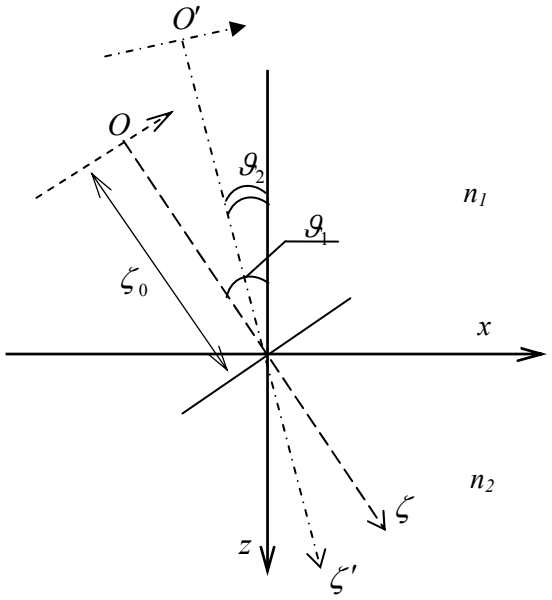


Рис. 1. Геометрия задачи: плоскость $z = 0$ является границей раздела прозрачной (при $z < 0$) и рассеивающей (при $z > 0$) сред; $O\zeta$ – ось падающего пучка, $O\zeta'$ – ось преломленного пучка

Решение задачи распространения пучка в прозрачной среде и преломления на границе раздела

Решение УПИ в однородной среде имеет вид

$$I(\zeta,\boldsymbol{\xi},\boldsymbol{\kappa}) = I(0,\boldsymbol{\xi}-\boldsymbol{\kappa}\zeta,\boldsymbol{\kappa}). \qquad (2)$$

Используя (2), для распределения яркости $I_+(z=0,\mathbf{x},\boldsymbol{\kappa})$ пучка вида (1) на плоскости $z=0$ находим:

$$\begin{aligned} I_+(0,\mathbf{x},\boldsymbol{\kappa}) &= I(\zeta_0 + x\sin\vartheta_1, x\cos\vartheta_1, y, \boldsymbol{\kappa}) = \\ &= I(0, x\cos\vartheta_1 - \kappa_{//}(\zeta_0 + x\sin\vartheta_1), y, \boldsymbol{\kappa}) = \\ &= \frac{1}{\pi R div}\exp\left\{-\frac{1}{R^2}\left[x\cos\vartheta_1 - \kappa_{//}(\zeta_0 + x\sin\vartheta_1)\right]^2\right\}\times\exp\left\{-\frac{\kappa_{//}^{\,2}}{div^2}\right\}\delta(\kappa_\perp) \end{aligned}, \qquad (3)$$

где ζ_0 – расстояние вдоль оси пучка, проходимое светом в прозрачной среде.

Найдем теперь распределение яркости преломленного пучка $I_-(z,x,y,\boldsymbol{\kappa}')$ на границе раздела *(z = 0 + 0)*. Учитывая предположение о малости отклонения вектора направления $\{1,\kappa_{//},\kappa_\perp\}$ для яркости падающего пучка от оси $O\zeta$, закон преломления Снеллиуса приводит к равенствам:

$$\sin\vartheta_1 = n\sin\vartheta_2,\ \kappa_\perp = n\kappa'_\perp,\ \cos\vartheta_1\kappa_{//} = n\cos\vartheta_2\kappa'_{//}, \qquad (4)$$

причем $n = n_2/n_1$.

Из (3), с учетом (4), получаем:

$$\begin{aligned} I_-(0,x,y,\boldsymbol{\kappa}') &= \frac{T}{\pi R div}\exp\left\{-\frac{1}{R^2}\left[x\cos\vartheta_1 - \kappa'_{//}n\frac{\cos\vartheta_2}{\cos\vartheta_1}\left(\zeta_0 + x\sin\vartheta_1\right)\right]^2\right\}\times \\ &\times\exp\left\{-\frac{\kappa'^{\,2}_{//}}{div^2}n^2\left(\frac{\cos\vartheta_2}{\cos\vartheta_1}\right)^2\right\}\delta(\kappa'_\perp n) \end{aligned}, \qquad (5)$$

где T – коэффициент пропускания границы раздела для светового пучка:

$$T = n^2(1-|\rho|^2), \tag{6}$$

ρ – френелевский коэффициент отражения [3].

Эквивалентная задача для пучка в рассеивающей среде

Введем обозначения

$$R' = R\frac{\cos\vartheta_2}{\cos\vartheta_1},\ div' = div\frac{\cos\vartheta_1}{n\cos\vartheta_2},\ \zeta_0' = \zeta_0 n\left(\frac{\cos\vartheta_2}{\cos\vartheta_1}\right)^2, \tag{7}$$

перепишем (5) в виде:

$$I_-(0,x,y,\boldsymbol{\kappa}') = \frac{Tn}{\pi R' div'}\times$$

$$\times\exp\left\{-\frac{1}{R'^2}\left[x\cos\vartheta_2 - \kappa_{//}'\left(\zeta_0' + x\sin\vartheta_1 n\left(\frac{\cos\vartheta_2}{\cos\vartheta_1}\right)^2\right)\right]^2\right\}\exp\left\{-\frac{\kappa_{//}'^2}{div'^2}\right\}\delta(\kappa_\perp' n).$$

Используя равенство $\alpha\,\delta(\alpha x) = \delta(x)\,(\alpha > 0)$ и условие $div\cdot\operatorname{tg}\vartheta_1 << 1$, последнее выражение можно упростить:

$$I_-(0,x,y,\boldsymbol{\kappa}') \approx \frac{T}{\pi R' div'}\exp\left\{-\frac{1}{R'^2}\left[x\cos\vartheta_2 - \kappa_{//}'(\zeta_0' + x\sin\vartheta_2)\right]^2\right\}\times$$

$$\times\exp\left\{-\frac{\kappa_{//}'^2}{div'^2}\right\}\delta(\kappa_\perp'). \tag{8}$$

Из сравнения полученной формулы с выражением (3) видно, что распределение яркости (8) совпадает в плоскости $z = 0$ с решением «эквивалентной задачи» в среде с постоянным показателем преломления для пучка, ось $O\zeta'$ которого составляет угол ϑ_2 с осью Oz (см. рис. 1). В декартовых координатах $\{\zeta',\boldsymbol{\xi}'\} = \{\zeta',\xi_{//}',\xi_\perp'\}$ исходное распределение яркости «эквивалентного» пучка в плоскости $\zeta' = 0$ имеет вид

$$I'(0,\xi_{//}',\xi_\perp',\boldsymbol{\kappa}') = \frac{T}{\pi R' div'}\exp\left(-\frac{1}{R'^2}\xi_{//}'^2\right)\exp\left(-\frac{\kappa_{//}'^2}{div'^2}\right)\delta(\kappa_\perp'), \tag{9}$$

а длина пути вдоль оси пучка до пересечения с плоскостью $z = 0$ равна величине ζ_0', определяемой формулой (7).

Теперь задача сводится к решению эквивалентной задачи о распространении светового пучка с начальным распределением яркости вида (9) в двухслойной среде с постоянным показателем преломления n_2 (рис. 2), причем в координатах $\{\zeta',\xi_{//}',\xi_\perp'\}$ плоскость $\zeta' = \zeta_0' + \xi_{//}'\operatorname{tg}\vartheta_2$ является границей раздела прозрачной (в полупространстве $\zeta' < \zeta_0' + \xi_{//}'\operatorname{tg}\vartheta_2$) и мутной сред.

Пусть a и b – показатели поглощения и рассеяния света мутной средой, соответственно. Индикатриса рассеяния $X(\gamma)$, где γ – угол рассеяния, $0 \le \gamma \le \pi$, подчиняется условию нормировки $\frac{1}{2}\int_0^\pi X(\gamma)\sin\gamma\,d\gamma = 1$ и определяет вероятность обратного рассея-

ния $\widetilde{b}_b = \frac{1}{2}\int_{\pi/2}^{\pi} X(\gamma)\sin\gamma\, d\gamma$, так что показатель обратного рассеяния есть $b_b = b\widetilde{b}_b$. Предполагая выраженную анизотропию рассеяния, индикатрису зададим в виде

$$X(\gamma) = (1-2\widetilde{b}_b)x(\gamma) + 2\widetilde{b}_b, \tag{10}$$

где $x(\gamma)$ определяет рассеяние на малые углы, причем

$$\tfrac{1}{2}\int_0^{\pi} x(\gamma)\sin\gamma\, d\gamma \approx \tfrac{1}{2}\int_0^{\infty} x(\gamma)\gamma\, d\gamma = 1; \quad \tfrac{1}{2}\int_{\pi/2}^{\pi} x(\gamma)\sin\gamma\, d\gamma << \widetilde{b}_b. \tag{11}$$

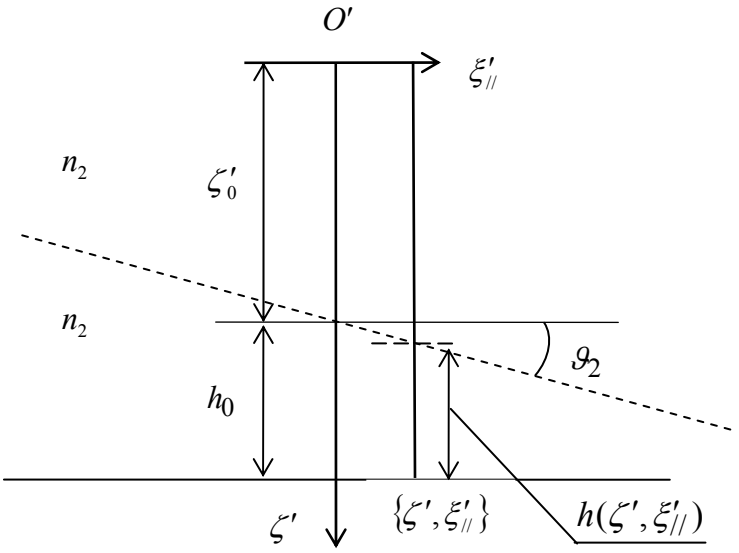


Рис. 2. Геометрия эквивалентной задачи в среде с постоянным показателем преломления. Наклонная пунктирная линия соответствует реальной границе раздела прозрачной и рассеивающей сред, горизонтальная – заданию локального положения границы для приближенного нахождения решении в точке $\{\zeta', \xi'_{//}\}$

В силу малости углов рассеяния и исходной расходимости пучка, яркость пучка $I'(\zeta', \xi'_{//}, \xi'_{\perp}, \boldsymbol{\kappa}')$ в произвольной точке $\{\zeta', \xi'_{//}, \xi'_{\perp}\}$ рассеивающей среды ($\zeta' > \zeta'_0 + \xi'_{//}\operatorname{tg}\vartheta_2$) приближенно совпадает с решением задачи распространения пучка с граничным условием (9) в стратифицированной среде с зависящими от ζ' показателями поглощения $a(\zeta')$ и рассеяния $b(\zeta')$ вида

$$a(\zeta') = \begin{cases} 0, & \zeta' < \zeta'_0 + \xi'_{//}\operatorname{tg}\vartheta_2 \\ a, & \zeta' \ge \zeta'_0 + \xi'_{//}\operatorname{tg}\vartheta_2 \end{cases}; \; b(\zeta') = \begin{cases} 0, & \zeta' < \zeta'_0 + \xi'_{//}\operatorname{tg}\vartheta_2 \\ b, & \zeta' \ge \zeta'_0 + \xi'_{//}\operatorname{tg}\vartheta_2 \end{cases}.$$

Используя аналитическое решение уравнения переноса излучения в малоугловом приближении для пучка света в стратифицированной рассеивающей среде [6], яркость $I'(\zeta', \xi'_{//}, \xi'_{\perp}, \boldsymbol{\kappa}')$ находим из соотношений:

$$I'(\zeta', \boldsymbol{\xi}', \boldsymbol{\kappa}') = \int_{\infty}^{\infty}\int\int \widetilde{I}'(\zeta', \mathbf{k}, \mathbf{p}; \boldsymbol{\xi}')\exp\left(i\mathbf{k}\boldsymbol{\xi}' + i\mathbf{p}\boldsymbol{\kappa}'\right) d^2\mathbf{k}\, d^2\mathbf{p}; \tag{12}$$

$$\widetilde{I}'(\zeta', \mathbf{k}, \mathbf{p}; \boldsymbol{\xi}') = \widetilde{I}'(0, \mathbf{k}, \mathbf{p} + \mathbf{k}\zeta') \times$$

$$\times \exp\left\{-(a+b_b)\left[\zeta' - \zeta'_0(\boldsymbol{\xi}')\right] + (b-2b_b)\int_0^{\zeta'-\zeta'_0(\boldsymbol{\xi}')} \varkappa\left(|\mathbf{p} + \mathbf{k}\zeta|\right) d\zeta\right\}, \; \zeta' \ge \zeta'_0(\boldsymbol{\xi}'), \tag{13}$$

где $\widetilde{I}'(0, \mathbf{k}, \mathbf{p}) = (2\pi)^{-4}\int_{\infty}^{\infty}\int\int I'(0, \boldsymbol{\xi}', \boldsymbol{\kappa}')\exp\left(-i\mathbf{k}\boldsymbol{\xi}' - i\mathbf{p}\boldsymbol{\kappa}'\right) d^2\boldsymbol{\xi}'\, d^2\boldsymbol{\kappa}'$, (14)

– преобразование Фурье исходного распределения яркости (9) по поперечным координатам и углам,

$$\zeta'_0(\boldsymbol{\xi}') = \zeta'_0 + \xi'_{//} \operatorname{tg} \vartheta_2 \tag{15}$$

– длина пути луча в прозрачной среде для точки наблюдения $\{\zeta', \xi'_{//}, \xi'_{\perp}\}$,

$$\tilde{x}(p) = \frac{1}{2}\int_0^{\infty} x(\gamma) J_0(p\gamma)\gamma \, d\gamma \tag{16}$$

– преобразование Фурье-Бесселя малоугловой части индикатрисы рассеяния из (10).

Получим теперь формулу для распределения освещенности $E'(\zeta', \xi'_{//}, \xi'_{\perp})$ по поперечному сечению пучка $\zeta' = \text{const}$ в рассеивающей среде,

$$E'(\zeta', \xi'_{//}, \xi'_{\perp}) = \iint_{\infty} I'(\zeta', \xi'_{//}, \xi'_{\perp}, \boldsymbol{\kappa}') \, d^2\boldsymbol{\kappa} \, ; \tag{17}$$

заметим, что в рассматриваемом «малоугловом» случае освещенность совпадает с облученностью [3, 4]. Из (13)–(15) следует выражение

$$E'(\zeta', \xi'_{//}, \xi'_{\perp}) = (2\pi)^2 \times$$
$$\times \iint_{\infty} \tilde{I}'(0, \mathbf{k}, \mathbf{k}\zeta') \exp\left\{ i\mathbf{k}\boldsymbol{\xi}' - (a+b)\left[\zeta' - \zeta'_0(\boldsymbol{\xi}')\right] + (b - 2b_b) \int_0^{\zeta' - \zeta'_0(\boldsymbol{\xi}')} \tilde{\varkappa}\,(|\mathbf{k}\zeta|)\, d\zeta \right\} d^2\mathbf{k} \, , \tag{18}$$
$$\zeta' \geq \zeta'_0(\boldsymbol{\xi}') = \zeta'_0 + \xi'_{//} \operatorname{tg} \vartheta_2 \, ,$$

в котором $\tilde{I}'(0, \mathbf{k}, \mathbf{p})$ по-прежнему дается формулой (14).

Полученный результат существенно упрощается в малоугловом диффузионном приближении, которое эквивалентно замене в (18) Фурье-образа $\tilde{\varkappa}$ малоугловой части индикатрисы двумя первыми членами его разложения в ряд Тейлора:

$$\tilde{x}(p) = \frac{1}{2}\int_0^{\infty} x(\gamma) J_0(p\gamma)\gamma \, d\gamma \approx \frac{1}{2}\int_0^{\infty} x(\gamma)\left[1 - \frac{(p\gamma)^2}{2}\right]\gamma \, d\gamma = 1 - p^2 \frac{\left\langle \gamma^2 \right\rangle}{2}, \tag{19}$$

причем параметр $\left\langle \gamma^2 \right\rangle$ равен среднему квадрату угла рассеяния на малые углы. С учетом (19) из (18) получаем:

$$E'(\zeta', \xi'_{//}, \xi'_{\perp}) = (2\pi)^2 \times$$
$$\times \iint_{\infty} \tilde{I}'(0, \mathbf{k}, \mathbf{k}\zeta') \exp\left\{ i\mathbf{k}\boldsymbol{\xi}' - a_e\left[\zeta' - \zeta'_0(\boldsymbol{\xi}')\right] + b_f \frac{\mathbf{k}^2}{6}\left\langle \gamma^2 \right\rangle \left[\zeta' - \zeta'_0(\boldsymbol{\xi}')\right]^3 \right\} d^2\mathbf{k} \, , \tag{20}$$
$$\zeta' \geq \zeta'_0(\boldsymbol{\xi}') = \zeta'_0 + \xi'_{//} \operatorname{tg} \vartheta_2 \, ,$$

где введены обозначения $a_e = a + 2b_b$ для эффективного показателя поглощения (учитывающего ослабление пучка за счет поглощения и рассеяния света на большие углы) и $b_f = b - 2b_b$ для показателя рассеяния на малые углы [5, 6].

Подстановка начального распределения (9) в (14) дает

$$\tilde{I}'(0, \mathbf{k}, \mathbf{k}\zeta') = (2\pi)^{-3} T \, \delta(k_{\perp}) \exp\left[-\frac{k_{//}^2}{4}\left(R'^2 + \zeta'^2 div'^2 \right) \right],$$

и из (20) получаем окончательный результат:

$$E'(\zeta', \xi'_{//}, \xi'_{\perp}) = \frac{T}{\sqrt{\pi} R_{eff}(\zeta', \xi'_{//})} \exp\left\{ -a_e\left[\zeta' - \zeta'_0(\boldsymbol{\xi}')\right] \right\} \times$$
$$\times \exp\left[-\frac{{\xi'_{//}}^2}{R_{eff}^2(\zeta', \xi'_{//})} \right], \tag{21}$$

$$\zeta' \geq \zeta'_0(\xi') = \zeta'_0 + \xi'_{//} \operatorname{tg} \vartheta_2, \tag{22}$$

где $h(\xi'_{//}) = \zeta' - \zeta'_0(\xi'_{//})$, (23)

– длина трассы распространения в рассеивающей среде для луча, приходящего в точку наблюдения $\{\zeta', \xi'_{//}, \xi'_{\perp}\}$ (см. рис. 2), и

$$R^2_{eff}(\zeta', \xi'_{//}) = R'^2 + \zeta'^2 div'^2 + \frac{2}{3} b_f \left\langle \gamma^2 \right\rangle h^3(\xi'_{//}). \tag{24}$$

Анализ результатов

Ограничимся здесь рассмотрением случая, когда вкладом малоугловой части рассеяния, определяемым параметром b_f, в распределение яркости можно пренебречь. Тогда

$$R^2_{eff}(\zeta', \xi'_{//}) \approx R^2_{eff}(\zeta') = R'^2 + \zeta'^2 div'^2,$$

причем R_{eff} является эффективным радиусом пучка в плоскости $\zeta' = \text{const}$, и выражение (21) можно переписать в виде

$$E'(\zeta', \xi'_{//}, \xi'_{\perp}) = \frac{\exp\left[-a_e(\zeta' - \zeta'_0)\right]}{\sqrt{\pi} R_{eff}(\zeta')} \times \\ \times \exp\left[\frac{a_e^2 R^2_{eff}(\zeta') \operatorname{tg}^2 \vartheta_2}{4}\right] \exp\left\{-\frac{\left[\xi'_{//} - S(\zeta')\right]^2}{R^2_{eff}(\zeta')}\right\}, \tag{25}$$

где $S(\zeta') = \dfrac{a_e R_{eff}(\zeta') \operatorname{tg} \vartheta_2}{2} = \dfrac{a_e \operatorname{tg} \vartheta_2}{2} \left(R'^2 + \zeta'^2 div'^2\right)$. (26)

Формула (25) справедлива при условии (22), означающем, что точка наблюдения $\{\zeta', \xi'_{//}, \xi'_{\perp}\}$ находится в рассеивающей среде; это условие можно переписать в виде $\xi'_{//} \leq D(\zeta')$, причем

$$D(\zeta') = (\zeta' - \zeta'_0) \operatorname{ctg} \vartheta_2, \tag{27}$$

– расстояние в плоскости $\zeta' = \text{const}$ от оси пучка до границы рассеивающей среды.

Из выражений (25) и (27) следует, что «энергетический центр» пучка, то есть максимум распределения освещенности в сечении $\zeta' = \text{const}$, сдвинут относительно «геометрического центра» $\xi_{//} = 0$ (оси пучка) на величину $\Delta(\zeta')$,

$$\Delta(\zeta') = \min\{D(\zeta'), S(\zeta')\}. \tag{28}$$

Чтобы существовал интервал значений наклонной глубины $h_0 = \zeta' - \zeta'_0$ проникновения света в рассеивающую среду, на котором энергетический центр распределения освещенности по поперечному сечению пучка находится внутри среды, необходимо и достаточно выполнения условия $S(\zeta') < D(\zeta')$ для соответствующих значений ζ'. Это условие, ввиду равенств (26) и (27), эквивалентно требованию существования вещественных корней квадратного уравнения $S(\zeta') - D(\zeta') = 0$, т.е. положительности его дискриминанта, и сводится к неравенству

$$a_e < \frac{1}{\operatorname{tg}^2 \vartheta_2 div' \left(R' + \zeta'_0 div'\right)}. \tag{29}$$

В противоположном случае сильного эффективного поглощения, т.е. при

$$a_e \geq \frac{1}{\operatorname{tg}^2 \vartheta_2 div' \left(R' + \zeta'_0 div'\right)}, \tag{30}$$

имеет место равенство $\Delta(\zeta') = D(\zeta')$; это означает, что максимум освещенности в сечении пучка при всех ζ' находится на границе рассеивающей среды (пучок «не проникает» в среду).

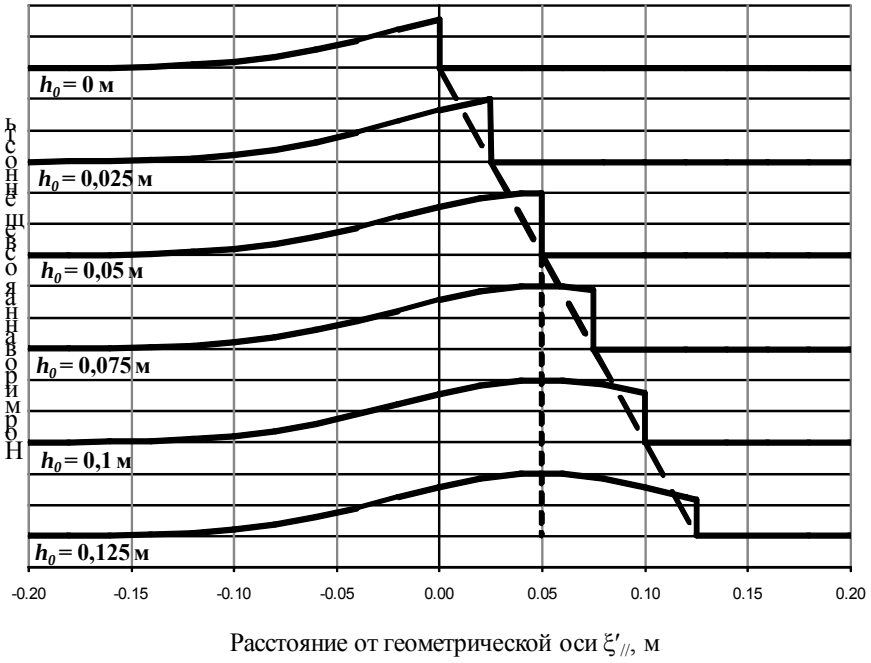


Рис. 3. Распределения освещенности по поперечному сечению пучка на различных глубинах проникновения h_0 в среду

На рис. 3 приведены результаты численных расчетов распределения освещенности по поперечному сечению пучка на различных глубинах проникновения h_0 в рассеивающую среду со слабым эффективным поглощением, то есть при выполнении условия (29). Расчеты проводились при следующих значениях параметров эквивалентной задачи [см. равенства (7)]: $R' = 0{,}1$ м; $\vartheta_2 = 45^{\circ}$; $\zeta_0' = 1$ м; $div' = 0{,}01$рад; $a_e = 10$ м$^{-1}$. Наклонная пунктирная линия на рис. 3 соответствует границе рассеивающей среды; вертикальная пунктирная линия, соединяющая положения максимумов распределений освещенности, совпадает при $h_0 > 0{,}05$ м с кривой $S(\zeta')$.

Заключение

В представленной работе теоретически исследована задача наклонного падения пучка света на границу мутной среды с выраженным поглощением и/или рассеянием; для простоты рассматривается двумерная задача, когда распределение яркости исходного пучка не зависит от координаты, перпендикулярной плоскости падения. Основой проведенного анализа служит уравнение переноса излучения в рассеивающей среде в приближении малоуглового рассеяния, что ограничивает область применимости результатов случаем малой расходимости падающего пучка и сильной анизотропии рассеяния (индикатриса рассеяния вытянута в направлении «вперед»). Показано, что максимум распределения освещенности по поперечному сечению пучка в рассеивающей среде оказывается смещенным относительно геометрической оси пучка в направлении границы раздела, причем величина смещения изменяется с глубиной проникновения света в рассеивающую среду. Детальный анализ, проведенный для ситуации, когда рассеяние вносит вклад только в эффективное ослабление пучка, позволил выделить два случая: при сильном поглощении максимум поперечного распределения освещенности сдвинут

к границе среды (пучок «не проникает» в среду); при слабом поглощении существует интервал значений глубин, для которых максимум распределения освещенности по поперечному сечению локализован внутри мутной среды. Выведено условие реализации того или иного случая в зависимости от геометрических параметров задачи (радиуса и расходимости пучка, угла падения и расстояния от источника до границы среды) и эффективного показателя поглощения в среде, учитывающего ослабление пучка за счет поглощения и рассеяния на большие углы.

Литература

1. Вейко В.П. Лазерная обработка пленочных элементов. – Л.: Машиностроение, 1986. – 248 с.
2. Копилевич Ю.И., Сурков А.Г. Математическое моделирование входных сигналов океанологических лидаров // Оптический журнал. – 2008. – Т. 75. – № 5. – С. 45–51.
3. Апресян Л.А., Кравцов Ю.А. Теория переноса излучения: статистические и волновые аспекты. – М.: Наука, 1983. – 216 с.
4. Долин Л.С., Левин И.М. Справочник по теории подводного видения. – Л.: Гидрометеоиздат, 1991. – 230 с.
5. Оптика океана /Под ред. А.С. Монина. – Т. 1. Физическая оптика океана. – М.: Наука, 1983. – 371 с.
6. Долин Л.С., Савельев В.А. К теории распространения узкого пучка света в стратифицированной рассеивающей среде // Изв. ВУЗов, сер. Радиофизика. – 1979. – Т. 22. – № 1. – С. 1310–1317.

2 ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

MACROMEDIA FLASH КАК ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО ПО СОЗДАНИЮ ТЕСТОВЫХ ЗАДАНИЙ

Н.О. Гордеева
Научный руководитель – к.т.н., доцент Н.Н. Горлушкина

В статье рассмотрены основные преимущества программного продукта Macromedia Flash, позволяющие создавать тестовые задания разного уровня сложности и оформления. Умение создавать тесты является важной составляющей в изучении дисциплины «Педагогические программные средства».

Рассмотрим Macromedia Flash как одно из возможных средств по созданию тестов. Этот программный продукт выбран в связи с его большими возможностями для представления информации путем интеграции текстовых, графических, аудио- и видеоданных, обеспечивающих положительные результаты при создании электронных учебных курсов и графических пользовательских интерфейсов с использованием большой библиотеки готовых компонентов.

В настоящее время обучение созданию тестов осуществляется в рамках дисциплины «Педагогические программные средства» в СПбГУ ИТМО. Дисциплина «Педагогические программные средства» входит в цикл общепрофессиональных дисциплин образовательной программы специальностей «Профессиональное обучение (информатика, вычислительная техника, компьютерные технологии)» и «Профессиональное обучение (охрана окружающей среды и природопользование)». Дисциплина направлена на приобретение будущими педагогами профессионального обучения знаний, необходимых для самостоятельного создания цифровых образовательных ресурсов [1]. Предполагается, что профессиональная деятельность выпускников будет связана с проектированием и созданием компьютерных обучающих программ или их частей, таких как демонстрационные материалы, презентации, компьютерные тесты или игры. Если же выпускники выберут профессию педагога, то их мастерство также будет в значительной степени подкреплено умением создавать педагогические программные средства, так как в последнее время повышение эффективности и скорости образовательного процесса достигается за счет использования педагогических программных средств, таких как обучающие программы, обучающие среды, электронные учебники и так далее.

Изучение дисциплины включает в себя знакомство с общими принципами создания и использования программных ресурсов, охватывает психолого-педагогические, математические, программно-технические, технологические, организационные и экономические аспекты. В программу дисциплины входит изучение всех разновидностей программных средств, их структуры и принципов разработки, знакомство с управлением учебно-познавательной деятельностью. Важную роль в изучении дисциплины играют практические занятия и выполнение курсовой работы, дающие непосредственный навык создания цифрового образовательного ресурса.

Для студентов специальности «Профессиональное обучение (информатика, вычислительная техника, компьютерные технологии)» изучение дисциплины носит обобщающий характер. Уже имея хороший объем знаний в области Multimedia, зная основы Html-программирования и Macromedia Flash, студенты с легкостью справляются с практическими занятиями и написанием курсовой работы.

Более сложная ситуация складывается со студентами специальности «Профессиональное обучение (охрана окружающей среды и природопользование)». К ранее полученным знаниям по педагогике и психологии им нужно гармонично добавить умения

программировать, создавать графическое оформление, проектировать логическую структуру.

Отсутствие знаний по HTML и Macromedia Flash вынуждают первый семестр изучения дисциплины посвятить овладению основными навыками работы в вышеуказанных программах. На лекционных занятиях первого семестра рассматриваются общие вопросы назначения и содержания педагогических программных средств (ППС), виды ППС, принципы проектирования и разработки ППС, графическое оформление, психофизиологические особенности обучаемых и эргономические требования и многие другие особенности и рекомендации. Параллельно с лекциями проводятся практические занятия, на которых разбираются и выполняются следующие задания.

1. Обзор и анализ существующих педагогических программных средств, выявление положительных и отрицательных свойств.
2. Ознакомление с программным продуктом Macromedia Flash, создание анимированного персонажа.
3. Создание анимированной модели процесса (для специализации «Охрана окружающей среды и природопользование» – создание модели «Разлив нефти при столкновении корабля с рифом и возможность остановки этого процесса при нажатии на кнопку»).
4. Изучение основных возможностей HTML, создание нескольких страниц на определенную тематику с перекрестными ссылками.
5. Создание теоретической страницы. Изучение возможностей HTML по редактированию текста, добавление графических изображений.
6. Создание блока контроля в Macromedia Flash.

Задачей второго семестра является создание обучающей программы (курсовая работа). Именно поэтому рекомендуется все задания первого семестра выполнять в одном ключе. Тематика курсовой работы определяется студентом совместно с преподавателем, ведущим дисциплину, и отдается предпочтение той теме, результаты которой могут быть применены в педагогической практике или получить развитие в выпускной квалификационной работе.

Опыт показывает, что для совершенствования преподавания дисциплины «Педагогические программные средства» рекомендуется:

1. формировать в студенте в процессе преподавания дисциплины их творческое отношение к создаваемым ими учебным педагогическим программным средствам;
2. убеждать студентов в том, что дисциплина «Педагогические программные средства» является в определенном смысле центральной дисциплиной образовательной программы подготовки педагогов профессионального обучения в области информатики, вычислительной техники и компьютерных технологий;
3. студентам, приступая к изучению дисциплины, тщательно обдумывать тематику создаваемого в дальнейшем программного средства, возможно, посоветоваться с будущим руководителем, чтобы уже на четвертом курсе приступить к поэтапному созданию выпускной квалификационной работы.

Помимо планомерного создания курсовой работы, студенты на практических занятиях изучают возможности Macromedia Flash для создания тестовых заданий. Четыре практических занятия отводятся на создание четырех видов тестов:

1. на ввод с клавиатуры верного варианта ответа;
2. на выбор правильных вариантов из предложенного перечня;
3. на сопоставление объектов;
4. на перетаскивание (распределение объектов по логическим группам).

Рисунок. Пример создания теста

На каждом из таких занятий вначале рассматриваются и анализируются примеры, затем разбирается последовательность выполнения теста и логическая структура. Для этого уже выбирается один из самых простых примеров (см. рисунок). После этого студенты, руководствуясь вспомогательными материалами – инструкциями, создают тестовое задание по собственной тематике. В результате к окончанию второго семестра изучения дисциплины у каждого студента создано, по крайней мере, 4 тестовых задания, которые могут дополнить курсовую работу.

Важность изучения дисциплины «Педагогические программные средства» заключается в возможности перехода на новый уровень преподавания – переходу от педагогических проповедей к проектированию оптимальных педагогических процессов, к индивидуализации образования. Дисциплина подходит не только для подготовки будущих педагогов или проектировщиков образовательных ресурсов, но и для повышения квалификации существующих кадров.

В настоящее время планируется создание методического пособия по выполнению практических заданий и составлению анимированных демонстраций и тестовых задания в Macromedia Flash. Примерные образцы из пособия могли бы стать наглядным способом быстрого и удобного создания тестов для каждого преподавателя.

Литература

1. Горлушкина Н.Н. Педагогические программные средства: Учебное пособие / Под ред. проф. М.И. Потеева. – СПб.: СПбГИТМО (ТУ), 2002. – 152 с.

ДИСТАНЦИОННАЯ СИСТЕМА ОБУЧЕНИЯ ДЛЯ ДОШКОЛЬНИКОВ И УЧЕНИКОВ НАЧАЛЬНЫХ КЛАССОВ

А.А. Ахмадеева
Научный руководитель – к.т.н., доцент Н.Ф. Гусарова

Большинство существующих обучающих ресурсов для детей дошкольного возраста и начальных классов не имеют временного ограничения и автоматических переходов между различными видами упражнений. Наша система ограничивает время прохождения занятий, т.е. время пребывания ребенка за компьютером, а также устанавливает перерывы во время обучения, при этом на время перерыва монитор становится темным, что позволяет отвлечь ребенка от компьютера.

Введение

В век информационных технологий почти в каждой семье есть компьютер, и дети, естественно, тоже проявляют к нему интерес, особенно если в семье есть старшие братья и сестры. Большинство компьютерных ресурсов не рассчитано на малышей, а рынок, ориентированный на данную группу, не насыщен. Предложенные ресурсы предполагают постоянное присутствие родителя рядом с ребенком для достижения обучающего эффекта и контроля, что не всегда удобно. Также в них не предусмотрено ограничение по времени, т.е. ребенок может сидеть за компьютером сколь угодное для него время, перерывы во время обучения также не предусмотрены. Если родители сами не контролируют время пребывания ребенка за компьютером, то долгое сиденье за монитором может плохо повлиять на здоровье ребенка: во-первых, большая нагрузка на глаза портит зрение, во-вторых, если занятия очень увлекательны, ребенок может долго сидеть в неудобной позе, что плохо отразится на его позвоночнике. Наша система в зависимости от возраста ребенка устанавливает соответствующие ограничения. Ограничивается не только время пребывания ребенка за компьютером в сутки, но и непрерывное нахождение за монитором. Регулярно делаются перерывы, во время которых монитор становится темным, и ребенок вынужден встать из-за компьютера или, по крайней мере, не смотреть на монитор. Во время перерывов идет звуковое сопровождение, которое озвучивает упражнения для глаз или физические упражнения, которые ребенок уже должен знать. Установка ограничений позволяет проводить занятия на компьютере с наименьшим вредом для здоровья ребенка. Автоматическая установка ограничений облегчает задачу родителей, им больше не нужно стоять рядом с секундомером, чтобы точно проследить время нахождения за компьютером. Дети, в свою очередь, обижаются на родителей, считают их слишком строгими из-за того, что им не дают доиграть. В результате отношения портятся. В нашей системе компьютер сам «выключается», когда это нужно, и родители в этом не виноваты.

Основной целью работы является разработка системы, позволяющей обучить ребенка различным дисциплинам с помощью компьютера и с наименьшим вредом для здоровья. Для повышения уровня знаний и навыков учащихся задания и обучающая информация представлены в интересной для детей игровой форме. Физическое развитие поддерживается с помощью регулярной зарядки и упражнений для глаз, при этом экран затемняется, чтобы отвлечь ребенка от монитора.

Другой задачей является ограничение времени непрерывного пребывания за компьютером, а также продолжительности всего занятия в день.

Обзор аналогов

Несколько примеров сайтов с обучающими онлайн-играми представлено в табл. 1.

Существует множество образовательных ресурсов для детей в Интернете. Большинство из них представляют собой сборники обучающих игр, которые на некоторых

сайтах даже тематически отсортированы, а на одном даже есть поэтапные уроки. Что касается обучающих игр, есть много неплохих, но есть некоторые недостатки: они либо не озвучиваются, либо озвучиваются, но визуально плохо сделаны.

Адрес интернет ресурса	Краткая характеристика
http://novakovskiy.narod.ru/kids/kid.html	Не очень удачный дизайн. Некоторые ссылки не работают. Большая часть разделов являются аналогами бумажных источников информации, т.е. книжек и т.п. Раздел «Девичьи секреты» не соответствует тематике «Детских страничек». В итоге осталось два раздела, которые нас заинтересовали: это «Игры-онлайн», так как нас интересуют онлайн-ресурсы, и «Мультфильмы». Эти два раздела представляют собой сборники игр и мультфильмов. Этот сайт в целом можно назвать сборником развлекательной и обучающей информации для детей.
http://www.wunderkinder.narod.ru	Этот сайт также является сборником ресурсов, причем эти ресурсы нужно скачивать, распечатывать, т.е. нельзя воспользоваться ими тут же на сайте в онлайн-режиме.
http://children.kulichki.net	Также представляет собой сборник ресурсов.
http://www.solnet.ee	Сборник игр и другой информации про и для детей. В основном все флеш-игры сделаны таким образом, что повторяется одно и тоже задание. Это хорошо только для выучивания алфавита и цифр, для других игр, например, «домино», в котором нужно выбрать по звуку соответствующее животное, это плохо, так как ребенок может просто запомнить последовательность правильных ответов.
http://detskiy.nm.ru/	Не совсем удобные переходы внутри разделов. Интересные рисунки. Небольшой набор игр.
http://vip.km.ru/vschool/	Бесплатно доступна только часть тематических уроков. Темы, в свою очередь, делятся поэтапно на уроки, что является плюсом, но минус заключается в переходе из урока в урок. Нужно открывать и закрывать различные окна, не хватает перехода на следующий (предыдущий) урок. Некоторые уроки изложены в неинтересной для ученика форме.

Таблица 1. Обзор аналогов

Большинство сайтов нельзя охарактеризовать как обучающую систему. Это скорее агрегаторы, сборники информации из различных источников (от бумажных до сайтов соседей). Есть некоторые интересные решения и идеи, но в целом уровень сайтов подобного рода слабоват, так как ими занимаются либо дети, либо их родители, без должного опыта и квалификации. Ни на одном из найденных сайтов нет должного мониторинга выполнения уроков, и на большинстве вообще нельзя регистрироваться и реализовывать полноценную программу обучения. Рассмотренные сайты ориентированы в основном на родителей, как это не противоречиво звучит. Т.е. родитель должен обязательно находиться рядом и следить за использованием сайта, или ребенок должен обладать достаточными навыками для навигации по сайту, а для этого как минимум должен уметь сразу хорошо пользоваться мышкой и читать. Также ребенок может перейти в «вольном полете» на нехорошие сайты по рекламным баннерам, порой совсем не детского содержания, что также недопустимо. Сейчас существует достаточно средств для размещения более-менее таргетированной (в идеале не медиа) рекламы,

содержание которой не будет противоречить тематикам сайта, но, увы, так как многие сайты созданы достаточно непрофессионально и давно, эти инструменты не используются.

Ни один из рассмотренных ресурсов не имеет ограничения по времени, т.е. если ребенка посадят за игрушку и оставят наедине с компьютером на неопределенное время, то он может сидеть и играть часами, не вставая с места. Это может плохо сказаться на его физическом здоровье. Во-первых, может испортиться зрение из-за достаточно близкого расположения экрана монитора, во-вторых, если ребенок долгое время будет сидеть в неудобной позе, не замечая дискомфорта из-за увлекательной игры, то это может привести к искривлению позвоночника и неправильной осанке.

Стоит отметить, что информационное наполнение найденных сайтов достаточно обширно, однако вопросы «юзабилити» для детей, контроля, мониторинга результатов со стороны взрослых совершенно не проработаны. И уж тем более эти сайты нельзя назвать обучающими системами для детей дошкольного возраста и начальных классов.

Ребенок и компьютер

Основной проблемой, связанной с отношением ребенок–компьютер, является решение вопроса о том, сколько времени может находиться ребенок за компьютером.

Известно [1], что рекомендуемая непрерывная длительность работы, связанной с фиксацией взора непосредственно на экране монитора, на уроке не должна превышать:

–для обучающихся в I–IV классах – 15 минут;

–для обучающихся в V–VII классах – 20 минут;

–для обучающихся в VIII–IX классах – 25 минут;

–для обучающихся в X–XI классах на первом часу учебных занятий – 30 минут, на втором – 20 минут.

Оптимальное количество занятий с использованием компьютера в течение учебного дня для обучающихся I–IV классов составляет 1 урок, для обучающихся в V–VIII классах – 2 урока, для обучающихся в IX–XI классах – 3 урока.

Возраст	Длительность занятия в день	Непрерывное время за компьютером	Перерыв
4–5 лет	Не более 40 минут	Не более 10 минут	10–15 минут
6–7 лет	Не более 45 минут	Не более 15 минут	15 минут
8–9 лет	Не более 1 часа	Не более 15 минут	15 минут
10–11 лет	Не более 1,5 часов	Не более 20 минут	15–20 минут

Таблица 2. Рекомендуемые значения параметров для различных возрастов

В дошкольных образовательных учреждениях (ДОУ) рекомендуемая непрерывная продолжительность работы с компьютерами на развивающих игровых занятиях для детей 5 лет не должна превышать 10 минут, для детей 6 лет –15 минут.

Игровые занятия с использованием компьютеров в ДОУ рекомендуется проводить не более одного в течение дня и не чаще трех раз в неделю в дни наиболее высокой работоспособности детей: во вторник, в среду и в четверг. После занятия с детьми проводят гимнастику для глаз [1].

Опираясь на [1], можно выделить параметры для разных возрастов, которые указаны в табл. 2. Предлагаемая нами методика опирается на [1], но наша методика позволяет освободить взрослого от постоянного присутствия рядом с ребенком. Взрослому нужно задать необходимые параметры, а дальше по установленным значениям система автоматически будет переключать режимы обучения и перемены.

По желанию родителей, они могут просматривать результаты обучения и менять параметры по своему усмотрению. К параметрам относятся:

- возраст (дата рождения) и пол ребенка;
- продолжительность всего занятия в день;
- время непрерывного нахождения за компьютером;
- перечень дисциплин, которые будет изучать ребенок;
- этап, с которого начнется обучение;
- продолжительность перерыва;
- занятия в перерывах;
- варианты поощрения за успехи и в конце занятия.

В зависимости от возраста выбираются значения параметров из табл. 2.

От пола ребенка зависит, какой сказочный персонаж будет его сопровождать на всех этапах обучения. Возможен выбор персонажа.

При регистрации все параметры заносятся в базу данных. Если пользователь (родитель) зарегистрировался, то при следующем входе в систему будут по умолчанию установлены те параметры, которые система считает наиболее подходящими. Возможность изменять параметры по своему усмотрению у родителей остается. Также при каждом последующем запуске системы или после завершения занятия родителям будет выслано сообщение, каких успехов достиг их ребенок, а на какие дисциплины еще нужно обратить внимание.

После задания родителями необходимых параметров и запуска системы окно программы разворачивается на весь экран, так что ребенок не сможет его скрыть и нажать куда-нибудь не туда. С этого момента во взаимодействие с системой вступает ребенок.

Обучение

В основе системы обучения используется ассоциативно-рефлекторная теория обучения (И.М. Сеченов, И.П. Павлов, С.Л. Рубинштейн, А.А. Смирнов, Ю.А. Самарин, П.А. Шеварев) и концепция программированного обучения [2], а также технология развивающих игр (Б.П. Никитин) [3].

Обучение начинается с освоения работы с компьютерной мышкой, так как это основной элемент управления в играх нашей системы. После этого начинается обучение тем дисциплинам, которые выбрали родители. Если выбрано несколько дисциплин, то они чередуются поэтапно, т.е. сначала идет первый этап одного предмета, затем первый этап второго предмета, или в первый день преподается первая дисциплина, во второй день – вторая дисциплина. После определенного промежутка времени кончается время, отведенное на ознакомление с новой информацией, и делается перерыв, после перерыва ребенок проходит обучающий тест, результаты которого заносятся в базу данных, занятие завершается мультфильмом, сказкой или игрой. Все занятия представлены в игровой форме.

Вместе с ребенком учится и сказочный персонаж, он сопровождает его на всех этапах обучения. Герой предлагает поучить вместе буквы или сделать зарядку, пройти интересные обучающие игры-тесты, посмотреть мультфильм или сказку. Также сказочный персонаж учит ребенка здороваться и прощаться.

Перерывы

Основываясь на [1], в разрабатываемой системе через определенные промежутки обучения проводятся перерывы. Во время перерывов компьютер, выступая в роли ведущего, озвучивает упражнения для глаз. Экран во время перерыва становится темным, что позволяет гарантировать, что ребенок отвернется от экрана.

В перерывах нужно также проводить физические упражнения, которые ребенок должен повторять за своим героем. Физические упражнения очень важны, так как ребенок еще находится на стадии развития, постоянно растет. Долгое сидение на одном месте в неудобном положении может плохо отразиться на позвоночнике, поэтому нужно обязательно делать зарядку.

Вместо физических упражнений сказочный персонаж может показывать различные простые танцевальные движения под музыку так, что ребенок сможет их повторять.

Обратная связь

Исследованию проблемы обратной связи посвящена работа [4]. Опираясь на [4], в нашей системе обратная связь осуществляется с помощью тестов в игровой форме, а также с помощью веб-камеры.

Для тех, у кого есть веб-камера, существует возможность «контролировать» поведение ребенка во время перерыва. Пока ребенок не встанет из-за компьютера, занятие в перерыве не начнется. Также не начнется занятие после перерыва, если ребенок сел за компьютер раньше положенного срока или еще не успел подойти к компьютеру после перерыва.

Во время обучения некоторые тестовые занятия могут проводиться с помощью веб-камеры, которая позволяет осуществлять функции обратной связи. Например, ребенку сначала показали цвета и сказали, как они называются, затем предлагают походить по комнатам и принести предмет указанного цвета. Ребенок показывает этот предмет камере, она устанавливает, правильного цвета предмет или нет. Еще один пример: урок был посвящен геометрическим фигурам, ребенку предлагается пойти, поискать предметы, которые похожи на определенную фигуру, или нарисовать на листке бумаги и показать камере.

Примерный сценарий первого занятия

Примерный сценарий обучения русскому алфавиту ребенка пятилетнего возраста. Общая продолжительность одного занятия 40 минут.

Рисунок. Буква «А» из урока «Азбука»

Первые 10 минут идет ознакомление с буквами. На экране появляются большие буквы с рисунками предметов (рисунок), название которых начинается на соответствующую букву, при этом голос озвучивает букву и название предмета. Новая буква повторяется три раза, после чего появляется следующая. После каждой новой буквы, по

одному разу высвечиваются и озвучиваются буквы, начиная с «А» и заканчивая последней новой.

Вторые 10 минут экран становится темным. Компьютер сначала озвучивает упражнения для глаз, а потом и физические упражнения. При этом обратная связь осуществляется с помощью web-камеры, которая позволяет отслеживать, правильно ли ребенок делает упражнения и где он находится.

Еще 10 минут – тест в игровой форме, проверяющий, какие буквы ребенок уже запомнил и знает, а какие буквы ему нужно будет показать еще раз. На экране появляется картинка с хаотично расставленными буквами. Голос говорит: «Найди букву А». Ребенок с помощью мышки должен нажать на букву, если он нажал не на ту букву, то голос говорит: «Неправильно, это буква «Б», нужно найти букву «А». При этом в базу данных заносятся пометки об ошибке напротив букв «А» и «Б». Если ребенок показал на нужную букву, то голос говорит: «Молодец, правильно, это буква «А». А теперь найди букву «В». Система запоминает, с какой попытки ребенок находит правильный ответ, если попыток больше двух, то через два вопроса этот вопрос повторяется. С каждым новым вопросом комбинация расположения букв меняется.

Можно сделать, чтобы было три буквы искомого типа и две других типов. При нахождении правильной буквы она исчезает, а голос говорит: «Молодец, правильно, это буква «Б», найди еще!». Когда все буквы этого вопроса найдены, озвучивается следующий вопрос.

После прохождения теста малышу говорят: «Молодец, теперь можешь послушать сказку». Монитор снова затемняется, и 10 минут рассказывается сказка.

Дополнительное обучение

Кроме занятий из учебной программы, по желанию родителей проводятся занятия по лепке из пластилина [5], рисованию [6], занятия на моторику [7], а также с различными творческими наборами разных производителей. Родителям предоставляется список творческих занятий и описание того, какие материалы или наборы требуются для каждого занятия. Таким образом, можно сочетать данное описание с рекламой производителя или магазина, в котором можно приобрести все, что нужно для выбранного творческого занятия. Творческие занятия могут быть представлены с помощью видеоуроков.

Также создается отдельный раздел (программа или целый курс обучения, как правильно отдыхать без компьютера) с оффлайн-играми, в котором можно выбрать игру на определенное количество детей. Компьютер при этом будет выполнять роль ведущего, или, озвучивая правила игры и последовательность действий в понятной для детей форме, или приводя примеры, как и с чем можно или нельзя играть. Ведь не секрет, что многие взрослые сами не умеют отдыхать правильно, следовательно, не могут этому научить и детей. А детям нужен не столько телевизор, компьютер и все с ними связанное, сколько комплексное развитие – физическое, творческое и т.д.

Заключение

Представленная система интересна детям, а также очень удобна для родителей. Родители, задав нужные параметры, могут спокойно оставить ребенка наедине с компьютером примерно на час и заняться своими делами или немного отдохнуть.

Детей при этом приветствует сказочный герой и предлагает вместе пройти обучение, интересные игры, сделать зарядку и посмотреть мультфильм. Ребенок учится, играя. С каждым годом продолжительность занятий может немного увеличиваться, что будет постепенно приучать ребенка к занятиям в школе, если это дошкольник. Также

ребенок научится правильно распределять время учебы и отдыха: сначала нужно учиться, а потом уже отдыхать. Если в школе задали много уроков, то ребенок будет знать, что после выполнения упражнений по одному предмету нужно встать, сделать зарядку для глаз или физические упражнения, а потом приступать к другому заданию.

Данная система является дополнительным обучающим ресурсом, подготавливающим ребенка к школе и помогающим во время обучения в начальных классах.

Литература

1. Постановление Главного государственного санитарного врача РФ от 03.06.2003 №118 (ред. от 25.04.2007) «О введении в действие санитарно-эпидемиологических правил и нормативов» 2.2.2/2.4.1340-03 (вместе с «санитарно-эпидемиологическими правилами и нормативами» «гигиенические требования к персональным электронно-вычислительным машинам и организации работы» 2.2.2/2.4.1340-03, утв. Главным государственным санитарным врачом РФ 30.05.2003) (Зарегистрировано в Минюсте РФ 10.06.2003 N 4673). – Режим доступа: http://www.consultant.ru
2. Богданов И.В. и др. Психология и педагогика. – Режим доступа: http://www.kspu.ru/ffec/psych/ps12.html#12
3. Лобанова Е.А. Дошкольная педагогика: учебно-методическое пособие / Е. А. Лобанова. – Балашов: Николаев, 2005. – 76 с.
4. Лукьяненко О.Д. Технологическое обеспечение обратной связи в дидактическом информационном взаимодействии педагога с детьми 6–7 лет. – Редакционно-издательский центр АГПУ.
5. Халезова Н.Б. Декоративная лепка в детском саду. – М.: Сфера, 2007.
6. Сахарова О.М. Я учусь рисовать: Игровая методика обучения рисованию; Изображение предметов; Смешивание красок: Для детей 4–7 лет: Пособие для детей, родителей и воспитателей. – М.: Литера, 2005.
7. Мусиенко А.А. Мастерим из бумаги. Пособие для детей 5–-6 лет. – М.: Просвещение, 2007.

ОСОБЕННОСТИ СТРУКТУРИРОВАНИЯ МАТЕРИАЛА ДЛЯ ОБУЧАЮЩЕЙ ПРОГРАММЫ ПО ДИНАМИЧНО РАЗВИВАЮЩЕМУСЯ КУРСУ «СИЛОВАЯ ОПТИКА»

Ю.С. Дементьева
Научный руководитель – к.ф.-м.н., доцент Г.Д. Шандыбина

В докладе представлена разработка электронного учебного материала для динамично развивающегося раздела физической оптики «Взаимодействие лазерного излучения с веществом» («Силовая оптика»). Часть 1. Механизмы поглощения и диссипации энергии в веществе.

Введение

Развитие глобальной компьютерной сети Интернет открыло новые перспективы совершенствования мировой образовательной системы. Это отражается как на технической оснащенности образовательных учреждений, их доступе к мировым информационным ресурсам, так и на использовании новых технологий, методов и форм обучения, ориентированных на активную познавательную деятельность учащихся [1–2].

Благодаря средствам новых информационных и коммуникационных технологий появилась новая технология обучения, а именно – *дистанционное обучение*. При дистанционном обучении учащийся и преподаватель пространственно отделены друг от друга, но при этом они могут находиться в постоянном взаимодействии, организованном с помощью особых приемов построения учебного процесса, форм контроля, методов коммуникации посредством технологий Интернета [3–5].

В то же время, отечественный и зарубежный опыт показывает, что эффективное использование средств вычислительной техники в образовательном процессе возможно только при наличии программного обеспечения, ориентированного на задачи обучения конкретным дисциплинам. На сегодняшний день проблема создания и использования соответствующих компьютерных образовательных программ и учебно-методических комплексов является весьма актуальной.

Особый интерес вызывает разработка обучающего и тестирующего программного обеспечения для динамично развивающихся разделов научных и технических дисциплин, имеющая свои принципиальные особенности.

Во-первых, постоянно появляются новые экспериментальные данные, которые приводят к существенному уточнению, а часто и к кардинальным изменениям принятых на сегодняшний день модельных представлений и гипотез. При формировании учебного материала необходимо обеспечить возможность его постоянного пополнения и уточнения. Это, в свою очередь, требует принципиально отличной организации обучающего и тестирующего программного обеспечения.

Во-вторых, как правило, динамично развивающиеся разделы дисциплин представлены студентам в виде специальных курсов. Восприятие материала подобных специальных курсов требует наличия у студента определенных базовых знаний в области естественнонаучных и общепрофессиональных дисциплин. Эту особенность также необходимо учитывать при разработке обучающего программного обеспечения.

В статье рассмотрен подход к эффективному структурированию электронного учебного материала на базе специальной дисциплины «Взаимодействие лазерного излучения с веществом» («Силовая оптика»).

Силовая оптика – динамично развивающееся научное направление. Известно, что лазерная техника стремительно развивается. В частности, возрастает мощность лазеров, в первую очередь за счет укорочения длительности импульсов лазерного излучения. За последние два десятилетия на смену коротким импульсам пришли сверхкороткие (пикосекундные), затем появились ультракороткие импульсы (фемтосекундная техника), а

теперь на подходе техника аттосекундного диапазона. Как в России, так и за рубежом растет поток новых экспериментальных данных по нелинейным, неравновесным процессам, локализованным как во времени, так и в пространстве. Одни физические модели подтверждаются и уточняются, другие исчезают, и появляются новые. Развитие информационных и телекоммуникационных технологий тесно связано с развитием лазерной техники и знанием физических основ взаимодействия лазерного излучения с веществом. Отсутствие соответствующих отечественных образовательных программ ограничивает уровень понимания и самообразования в этой области знаний.

Другой особенностью создания программного обеспечения является тот факт, что восприятие раздела «Силовая оптика» предполагает наличие у слушателя базовых знаний из курса общей физики, физики твердого тела, квантовой механики, математической физики.

Подход к разработке обучающей программы

Информационные технологии предоставляют в распоряжение преподавателя мощный набор инструментов, который должен эффективно использоваться для достижения целей учебного процесса при дистанционном обучении. С учетом отечественного опыта разработки курсов дистанционного обучения [6] представляется, что в наиболее полном варианте учебный курс должен включать:

- методические рекомендации по изучению курса;
- теоретический материал;
- практикум для выработки умений и навыков применения теоретических знаний с примерами выполнения заданий и анализом наиболее часто встречающихся ошибок;
- справочный материал, глоссарий;
- систему тестирования и контроля знаний;
- библиотеку современных научных зарубежных и отечественных публикаций.

Таким образом, обучающая программа образует программно-методический комплекс, позволяющий самостоятельно освоить учебный курс (или его большой раздел) и объединяющий в себе свойства обычного учебника, энциклопедического справочника, практикума, поисковой системы и системы контроля знаний. Электронный комплекс является дополнением к традиционным формам обучения и не заменяет работу студента с книгами, конспектами, сборниками задач и упражнений и т.п. Он призван, не только сохранить все достоинства книги или учебного пособия, но и в полной мере использовать современные информационные технологии, мультимедийные возможности, предоставляемые компьютером.

Создание обучающей программы потребовало одновременно знаний как в предметной области, для которой создается учебник, так и в области информационных технологий. Можно выделить следующие основные этапы этой работы:

- детальное изучение теоретического материала учебного пособия и подготовка варианта текста учебника;
- разработка «сценария» взаимодействия отдельных частей электронного учебника (на основе рациональной структуры учебника, тщательно продуманной последовательности изложения материала, организации возможных перекрестных ссылок и т.п.) и дизайна обучающей программы, куда входит также начальная подготовка разнообразных иллюстраций и графиков, располагаемых в тексте электронного учебника;
- создание обучающих элементов программы (тестирование, глоссарий, библиотека)[7–9];
- выбор компьютерных средств и реализация составных частей программы на компьютере (написание кодов) [10–12].

Структура и интерфейс обучающей программы

Была разработана логическая структура программы, представленная на схеме (рис. 1) и состоящая из следующих блоков: «Лекционный материал», «Глоссарий», «Библиотека», «Тестирование», «О программе». Под блоком понимается структурный компонент управления представлением учебного материала, содержащий аппарат ориентировки, который включает в себя оглавление, заголовки разделов, параграфов, именные и предметные указатели и должен обеспечивать быстрый поиск необходимой информации; а также систему управления процедурой представления учебной информации реализуемую посредством гипертекста. Совокупность программных блоков образует иерархическую структуру, объединяющую их в единую систему.

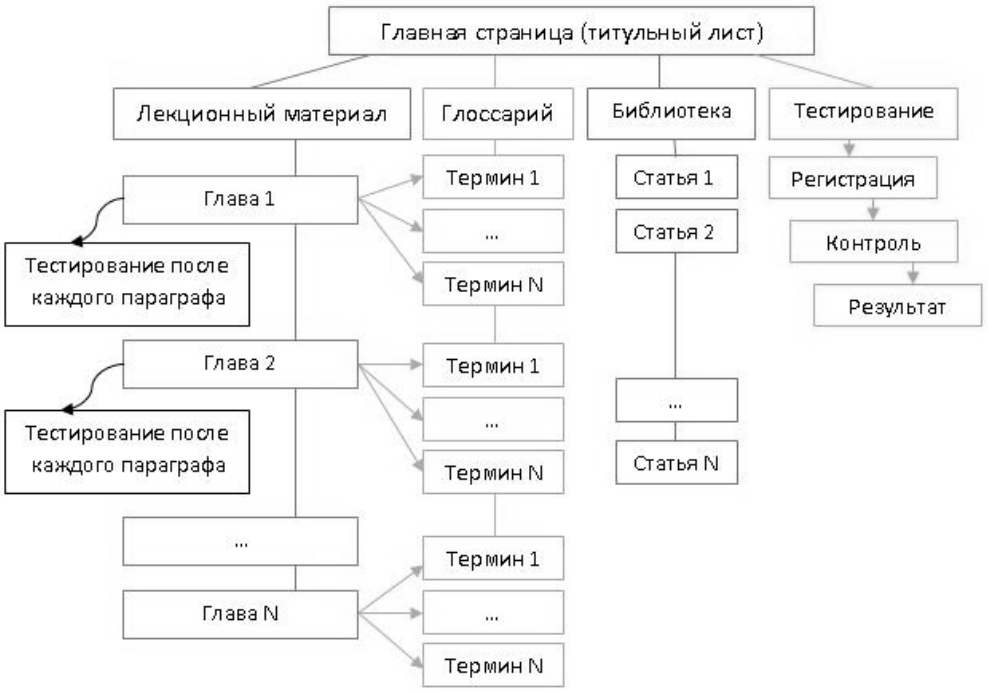


Рис. 1. Логическая структура обучающей и тестирующей программы

Однако наличие выпадающего иерархического меню не определяет дидактические качества электронного учебного средства, оно отражает лишь иерархию содержания учебного материала, т.е. «внешнюю, визуализированную» структуру электронного учебника. Пользовательский интерфейс является аналогом аппарата ориентировки обычного книжного учебника. При запуске программы появляется окно, разделенное на 3 части (рис. 2). В левой части экрана находится меню «Содержание», которое также отображается постоянно и служит для быстрого перехода по главам и разделам учебного курса. По щелчку мыши по названию главы учебника осуществляется переход к этой главе.

В верхней его части находится заголовок электронного учебника и меню навигации, которое отображается постоянно и служит для быстрого перехода по его разделам, названия которых соответствуют названиям структурных блоков.

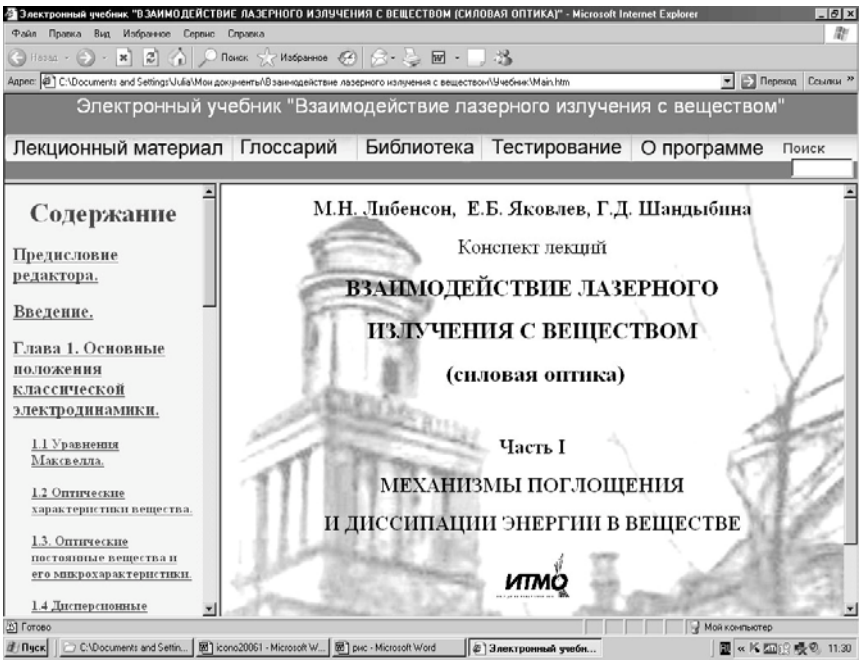


Рис. 2. Окно, отражающее титульный лист обучающей программы

Лекционный материал. Нажав кнопку «Лекционный материал», обучаемый переходит к электронной версии теоретического материала по курсу «Взаимодействие лазерного излучения с веществом». Теория представляет собой методическое учебное пособие Либенсона М.Н., Яковлева Е.Б., Шандыбиной Г.Д. «Взаимодействие лазерного излучения с веществом (силовая оптика). Часть 1». – СПб: СПбГУ ИТМО, 2005. – 84 с.

Основу его содержания составляют пять глав. В первой главе рассмотрены основные положения классической электродинамики: уравнения Максвелла, оптические характеристики вещества, оптические постоянные вещества и его микрохарактеристики, дисперсионные соотношения.

В второй главе представлено исследование распространения электромагнитных волн в проводящих средах с помощью уравнений Максвелла с учетом материальных соотношений.

Третья глава посвящена изучению механизма поглощения излучения в металлах и их оптическим свойствам.

В четвертой главе рассмотрены механизмы поглощения света и передача энергии в полупроводниках, особенности собственного поглощения, внутризонное поглощение, кинетика фотовозбуждения полупроводников лазерным излучением, насыщение межзонного поглощения.

В пятой главе представлены поверхностные электромагнитные волны оптического диапазона: их основные свойства, структура и распределение полей, условия существования, дисперсионные соотношения. Рассмотрены особенности распространения поверхностных плазмон-поляритонов на границе металла с диэлектриком, представлены методы возбуждения ПЭВ, а также дано представление о цилиндрических ПЭВ.

Глоссарий. Пункт навигационного меню «Глоссарий» – это переход к списку специальных терминов и понятий, выявленных в ходе работы над программой и вызывающих затруднение в понимании у студентов. На базе энциклопедических справочников [7] составлена их подробная расшифровка, послужившая основой для глоссария программы. Благодаря использованию гиперссылок в тексте учебника пользователь легко может ознакомиться с малоизвестным ему понятием.

Библиотека. Пункт «Библиотека» используется для перехода к перечню современных научных публикаций по разделам курса. Представлены статьи из отечественных и зарубежных физических журналов. Пользователь может использовать материал статьи для более углубленного анализа современного состояния изучаемого явления.

Тестирование. Тестовый контроль отличается от других методов контроля (устные и письменные экзамены, зачеты, контрольные работы и т.п.) тем, что он представляет собой специально подготовленный контрольный набор заданий, позволяющий надежно и адекватно количественно оценить знания обучающихся посредством статистических методов. Применение компьютерных средств при проведении тестового контроля не только облегчает работу преподавателя по проверке тестов, но и повышает мотивацию учебной деятельности учащихся, одновременно снижая их эмоциональную напряженность в процессе контроля [8].

Блок «Тестирование» используется для перехода к итоговому тесту, целью которого является проверка усвоения материала всего курса лекций, представленного в программе. Этот раздел начинается с регистрации студента, затем производится непосредственно тестирование пользователя по трем разделам курса: взаимодействие лазерного излучения с сильно поглощающими средами (металлы), поглощение света и передача энергии в полупроводник и поверхностные электромагнитные волны оптического диапазона, выводятся результаты. На JavaScript реализовано случайное открытие пяти версий итогового теста. Пользователь заранее не знает, какой из тестов он будет проходить.

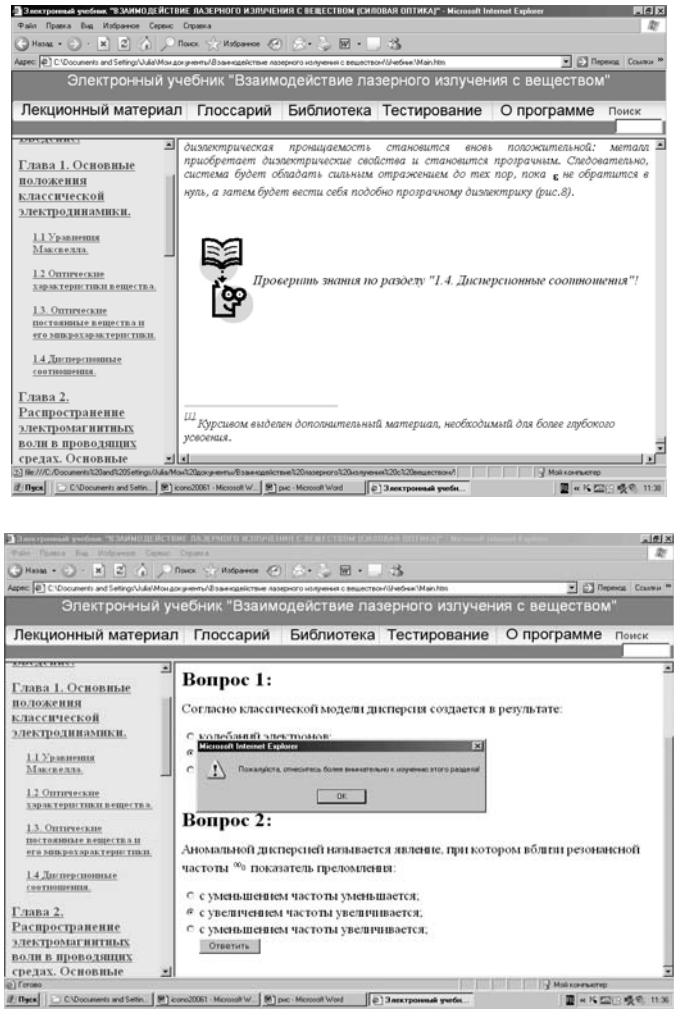


Рис. 3. Окна, соответствующие промежуточному тестированию

После изучения материала каждой части главы обучаемому предлагается пройти промежуточное тестирование (рис. 3). После нажатия на гиперссылку в виде рисунка вместо текста учебника открывается новое окно, в котором написан вопрос и варианты ответа с «флажком». Количество вариантов ответа в каждом таком тесте – 3. Верный ответ может быть только один. В конце окна теста размещена кнопка «Ответить». Студент выбирает галочками верный, на его взгляд, вариант ответа и нажимает кнопку «Ответить». Тест считается засчитанным, если отмечен галочкой верный вариант ответа и не отмечен ни один ложный вариант ответа. Принцип работы описанных тестов можно наглядно представить в виде схемы (рис. 4).

Рис. 4. Логическая схема промежуточного тестирования

После нажатия на кнопку «Ответить» при положительном результате тестирования появляется сообщение «Верный ответ», в противном случае – «Неверный ответ». Если все варианты ответа оказались верными, то программа осуществляет автоматический переход к следующему разделу учебника, в противном случае рекомендует изучить материал прочитанного раздела подробнее и переходит к нему. После всей этой процедуры студент может вновь повторить тестирование. После нескольких таких попыток он находит верный ответ, что стимулирует закрепление знаний.

Тест в конце каждой главы предназначен для закрепления изученного материала. Ответив в первый раз неверно, обучаемый читает главу снова более внимательно и затем снова проходит тест. Если и на этот раз ответ неверный, он читает главу вновь, и т.д. Поскольку вопросы содержат основной смысл главы, такие тесты позволяют основательно закрепить знания, содержащиеся в каждой главе.

Благодаря такому интерфейсу программу удобно использовать, и не требуется открывать множество дополнительных окон для того, чтобы наглядно представить информацию.

Заключение

В результате работы была создана обучающая программа по курсу «Взаимодействие лазерного излучения с веществом» (Механизмы поглощения и диссипации энергии в веществе). В процессе ее создания разработчиком был детально изучен весь теоретический материал данного курса, а также принципы создания обучающих элементов (тестирование, глоссарий). Была разработана структура и дизайна обучающей про-

граммы, написаны программные коды. В программу были включены тестовые вопросы в количестве 50 штук, а также составлен глоссарий из 60 терминов.

Основным средством разработки для рассматриваемой программы явился язык разметки текстовых документов HTML 4.0 и JavaScript. Широко известно, что язык HTML относится к интерпретируемым языкам, и создавался он как язык интерпретируемого типа для работы в сети Интернет, благодаря чему программа может использоваться в дистанционном обучении.

Представленная обучающая программа позволяет обновлять учебный материал в соответствии с современными физическими представлениями в области силовой оптики, дополнять глоссарий, вводить новые тесты и делать свежую подборку научных статей.

Литература

1. Педагогические технологии дистанционного обучения: Учебное пособие для студентов высших учебных заведений / Под ред. Е.С. Полат. – М.: Академия, 2006. – 400 с.
2. Агофонов С.В., Джалиашвили З.О., Кречман Д.Л., Никифоров И.С., Ченосова Е.С., Юрков А.В. Методика, технология, инструментарий/ Под ред. З.О. Джалиашвили. – СПб: БХВ-Петербург, 2003. – 336 с.
3. Монахов В.М. Можно ли использовать традиционную дидактику проектирования модели e-Learning? // Открытое образование. – 2004. – №2. – С.4.
4. Мицель А.А., Молнина Е.В. Дистанционное образование как составляющая процесса формирования единого образовательного пространства // Открытое образование. – 2006. – №2 – С 59.
5. Концепция создания и развития единой системы дистанционного образования в России (утверждена решением Совета ИДО МЭСИ от 29.04.1998 г.) // Открытое образование. – 1997. – №2. – С.4.
6. Подготовка и проведение учебных курсов в дистанционной форме обучения. Методические рекомендации преподавателям / Под ред. И.А. Цикина. – СПб: Изд-во СПбГТУ, 2000. – 69 с.
7. Моисеева М.В., Полат Е.С., Бухаркина М.Ю., Нежурина М.И. Интернет обучение: технологии педагогического дизайна / Под ред. М.В. Моисеевой. – М.: Издат. дом «Камерон», 2004. – 216 с.
8. Аванесов В.С. Композиция тестовых заданий. Учебная книга для преподавателей вузов, учителей школ, аспирантов и студентов педвузов. – М.: Ассоциация инженеров-педагогов Москвы, 1996. – 191 с.
9. Физическая энциклопедия / Под ред. А.М. Прохорова. В 6-ти т. – М.: Сов.энц., 1988. – 1998 с.
10. Матросов А.В., Сергеев А.О., Чаунин М.П. HTML 4.0 – СПб: БХВ-Петербург, 2005 – 672 с.
11. Дронов В.А. Macromedia Dreamweaver 8.0 – СПб.: БХВ-Петербург, 2005 – 706 с.
12. Томас Пауэлл, Фриц Шнайдер. Полный справочник по JavaScript = JavaScript The Complete Reference. 2-е изд. – М.: Вильямс, 2007. – 960 с.

ГРАФИЧЕСКИЙ ЯЗЫК ОПИСАНИЯ ИГРОВЫХ ЭПИЗОДОВ В ФУТБОЛЕ

М.Н. Царев, Ф.Н. Царев
Научный руководитель – д.т.н., профессор А.А. Шалыто

В настоящей статье предлагается графический язык описания игровых эпизодов в футболе. Он позволяет в простой и доступной форме описывать поведение игроков во время футбольного матча. Применение графического языка описания игровых эпизодов позволяет конкретизировать множество вариантов результатов игровых эпизодов и более рационально организовывать тренировки по формированию базовой схемы действий, как отдельного игрока, так и нескольких игроков.

Введение

При подготовке юных футболистов перед тренерами неизменно встает вопрос: как передать своим воспитанникам необходимые знания? Особенно трудно обучить игроков тактике футбола. Объяснить понятно и доходчиво, что и в какой ситуации надо делать, довольно сложно. В традиционных футбольных учебниках [1–5] для описания поведения игроков в различных ситуациях применяются рисунки (рис. 1). Часто они бывают непонятными и могут по-разному трактоваться. Для решения этой проблемы авторами статьи предлагается подход, позволяющий понятно и однозначно описывать поведение игроков в различных ситуациях.

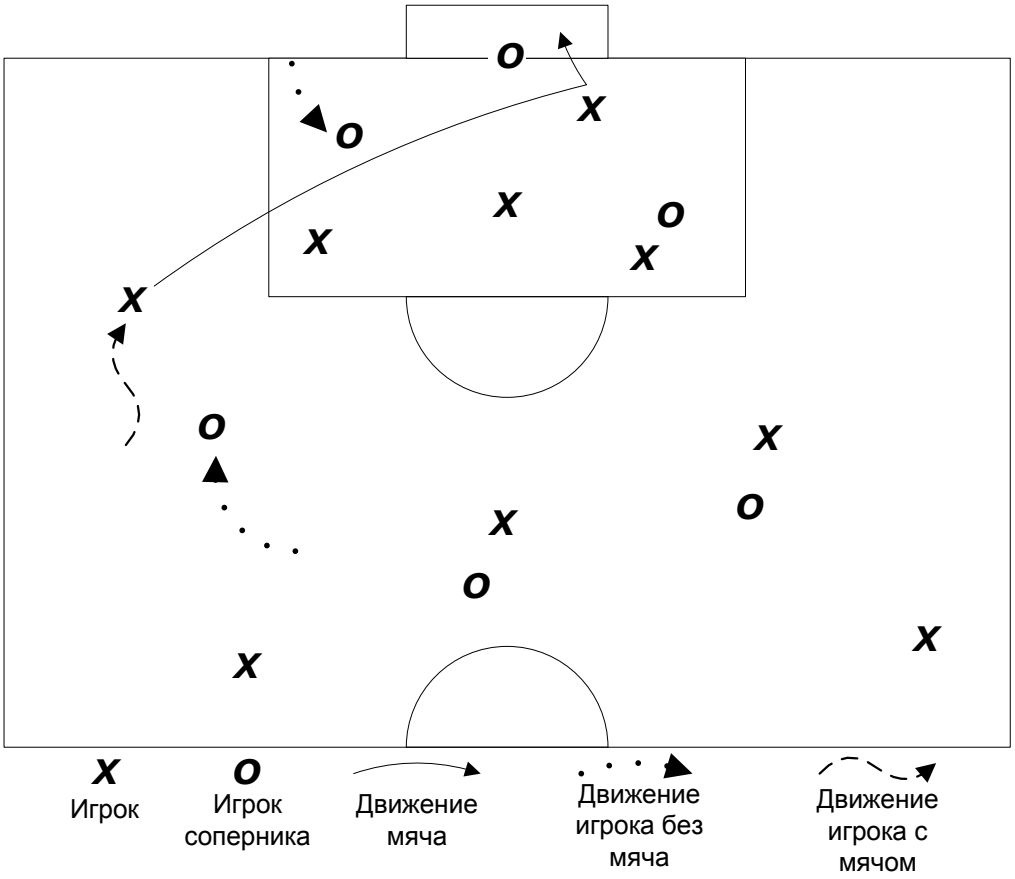


Рис. 1. Пример описания поведения игроков из [4]

Цель настоящей работы – предложить новый подход к описанию действий игроков во время футбольного матча и их обучению – графический язык описания игровых эпизодов.

Концепция подхода

Концепция подхода основана на теории систем [6] – футбольный матч можно разделить на множество взаимосвязанных между собой игровых эпизодов. В каждом игровом эпизоде могут быть определены роли игроков и их взаимные связи.

Таким образом, игру команды можно рассматривать как «большой» алгоритм, состоящий из множества частных алгоритмов, увиденных и реализованных игроками команды. В идеальном случае все игроки команды должны видеть игровой эпизод одинаково и действовать в его рамках по одинаковому алгоритму, свойственному данному игровому эпизоду. С формальной точки зрения футбольный матч можно рассматривать как множество *игровых действий* (ИД) и связей между ними. ИД всегда имеют результат, который может быть положительным, или отрицательным.

Игровым эпизодом (ИЭ) назовем конечное множество связанных между собой ИД. С таких позиций гол можно рассматривать как конечную последовательность ИЭ с положительными результатами (в принципе, голу могут предшествовать и ИЭ с отрицательными исходами, но самый «короткий» путь к взятию ворот – последовательно добиваться положительных исходов ИЭ).

Следовательно, для того, чтобы успешно играть, футболист должен уметь увидеть игровые эпизоды и действовать в них по определенному алгоритму, свойственному данной игровой ситуации.

Метод реализации подхода

Начало игрового эпизода	Этот блок обозначает начало игрового эпизода. Имеет 1 выход и ни одного входа.
Игровое действие	Этот блок обозначает любое игровое действие, например удар по мячу, прием мяча, оценка ситуации. Имеет 1 вход и 1 выход.
Результат игрового действия	Этот блок обозначает оценку результата игрового действия. Имеет 1 вход и 2 выхода.
→	Направленные линии обозначают связи между блоками. На направленных линиях, выходящих из блока «результат игрового действия» ставится пометка «Да» или «Нет».
Отрицательный исход игрового эпизода	Этот блок обозначает окончание ИЭ с отрицательным исходом. Имеет 1 вход и ни одного выхода.
Положительный исход игрового эпизода	Этот блок обозначает окончание ИЭ с положительным исходом. Имеет 1 вход и ни одного выхода.

Таблица. Элементы графического языка описания игровых эпизодов

Для описания ИЭ используются *логические модели игровых эпизодов* (ЛМИЭ). Для графического отображения ЛМИЭ *применяется графический язык описания игровых эпизодов* (ГЯОИЭ), подобный языку блок-схем [7]. В ГЯОИЭ применяются пять типов графических блоков и направленные линии, изображающие связи между блоками. Элементы ГЯОИЭ представлены в таблице.

Отметим, что любой игровой эпизод подразумевает выполнение, по крайней мере, одного игрового действия. Это действие может иметь положительный или отрицательный результат, таким образом, при создании алгоритма действий в игровом эпизоде на графическом языке описания игровых эпизодов обязательно должны использоваться все шесть элементов.

Пример применения метода

На рис. 2 приведен алгоритм действий игрока, выполняющего 11-метровый удар [8, 9]. Заметим, что выполнению 11-метрового удара всегда предшествуют другие игровые эпизоды, но мы их рассматривать не будем.

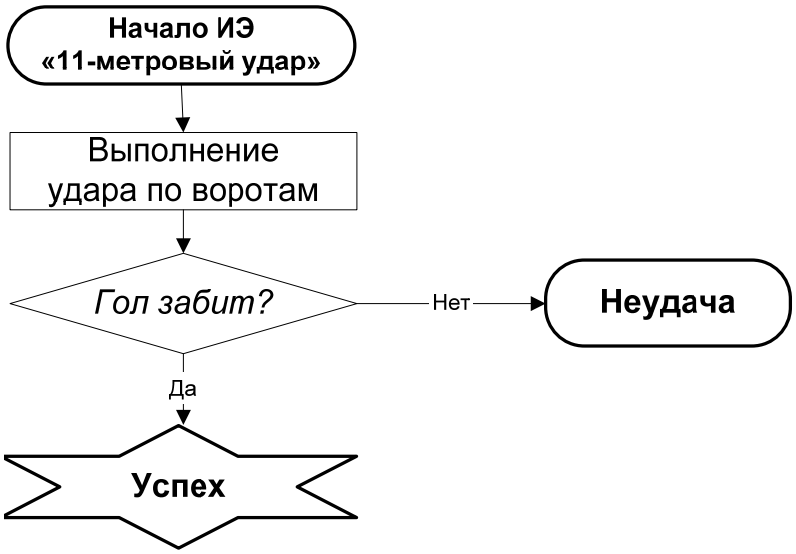


Рис. 2. Алгоритм действий игрока, выполняющего 11-метровый удар

Этот алгоритм состоит из пяти блоков. Первый блок – начало игрового эпизода. С футбольной точки зрения этот блок тривиален: 11-метровый удар выполняется после свистка судьи. Следующий блок – выполнение удара по воротам. Удар по воротам – «сложное» действие. Перед ударом необходимо оценить ситуацию, выбрать способ и направление удара. Удар по воротам достаточно «сложен» и разбивается на более «простые» игровые действия. Проверку условия «забит ли гол?» осуществляет судья. В случае взятия ворот игровой эпизод оканчивается положительно. Если взятие ворот не зафиксировано, то игровой эпизод имеет отрицательный исход. Таким образом, наибольшую трудность представляет действие «выполнение удара по воротам». На рис. 3 представлен расширенный алгоритм действий игрока, выполняющего 11-метровый удар. Заметим, что в данном случае под ударом (третий блок действий в алгоритме) понимается кратковременное целенаправленное силовое воздействие на мяч, т.е. момент непосредственного контакта ноги футболиста с мячом.

Детальное описание игровых эпизодов позволяет лучше организовывать тренировочный процесс: после анализа построенных алгоритмов становится ясно, что для того, чтобы игрок стабильно забивал голы с 11-метрового удара, его необходимо обучить правильно оценивать позицию вратаря, правильно выбирать направление и способ уда-

ра и правильно бить по мячу. Таким образом, абстрактная цель «научить забивать с 11-метрового удара» превращается в несколько более мелких, но конкретных целей.

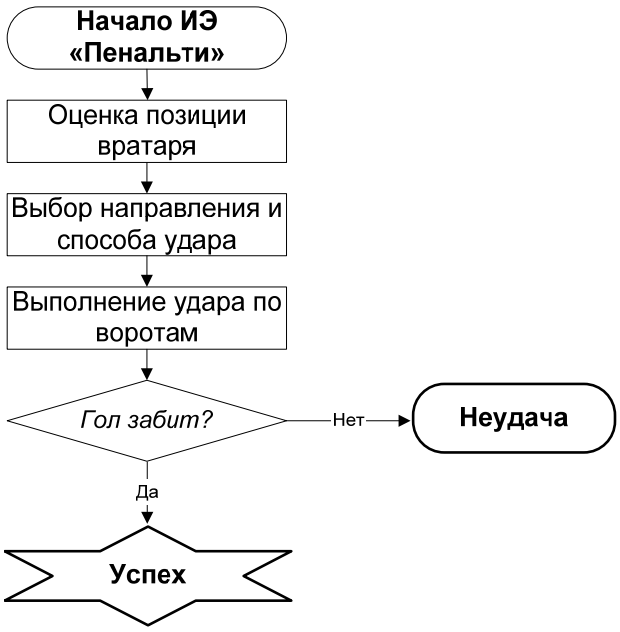


Рис. 3. Расширенный алгоритм действий игрока, выполняющего 11-метровый удар

Рис. 4. Вбрасывание мяча из-за боковой линии в ситуации «два против двух»

Рассмотрим теперь более сложный пример применения изложенного метода. Средствами ГЯОИЭ описана часто встречающаяся в футбольном матче ситуация вбрасывания мяча из-за боковой линии в ситуации «два против двух» – действия двух защитников против двух нападающих (рис. 4). На рис. 5 представлен алгоритм действий игрока Защ1 в данном игровом эпизоде, описанный средствами ГЯОИЭ.

Чтобы игровой эпизод успешно завершился, футболист должен уметь выполнять определенный набор игровых действий (изображены на рис. 5 прямоугольниками: контроль передвижений игрока Нап2, игра на опережение, оттеснение на фланг и т.д.) и выполнять их в правильной последовательности.

Анализ базовых игровых эпизодов позволяет выделить базовый набор игровых действий, которые должен выполнять игрок. Для выполнения этих действий необходимы определенные навыки.

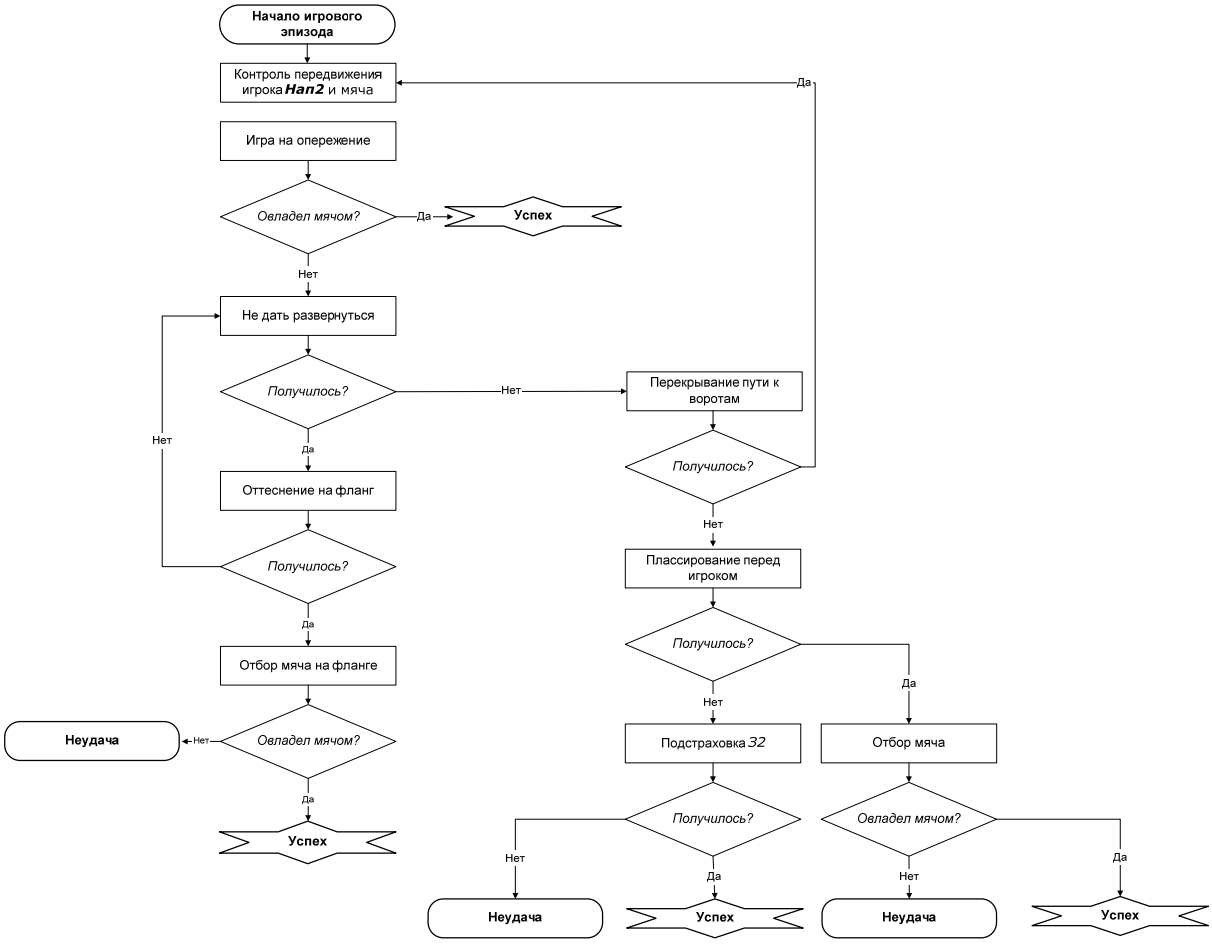


Рис. 5. Алгоритм действий игрока Защ1 в игровом эпизоде «вбрасывание мяча из-за боковой линии»

Если следовать предлагаемому подходу, то техническая подготовка игрока должна заключаться в освоении базовых игровых навыков. Физическая подготовка должна быть организована таким образом, чтобы игрок мог на протяжении всего матча результативно выполнять игровые действия, тем самым достигая удачных исходов в игровых эпизодах. Тактическая подготовка строится на обучении игроков алгоритмам действий в игровых эпизодах.

Хотелось бы отметить, что авторы статьи не считают, что футболист в игре должен действовать исключительно по определенному набору алгоритмов (в таких случаях футбольные комментаторы говорят, что «футболист играет шаблонно»). На наш взгляд, футболист должен обладать базовыми техническими навыками и знаниями в области тактики и на их основании осознанно строить свою игру.

Система изучения игровых эпизодов

В развитие излагаемого подхода авторами была разработана система изучения игровых эпизодов (рис. 6).

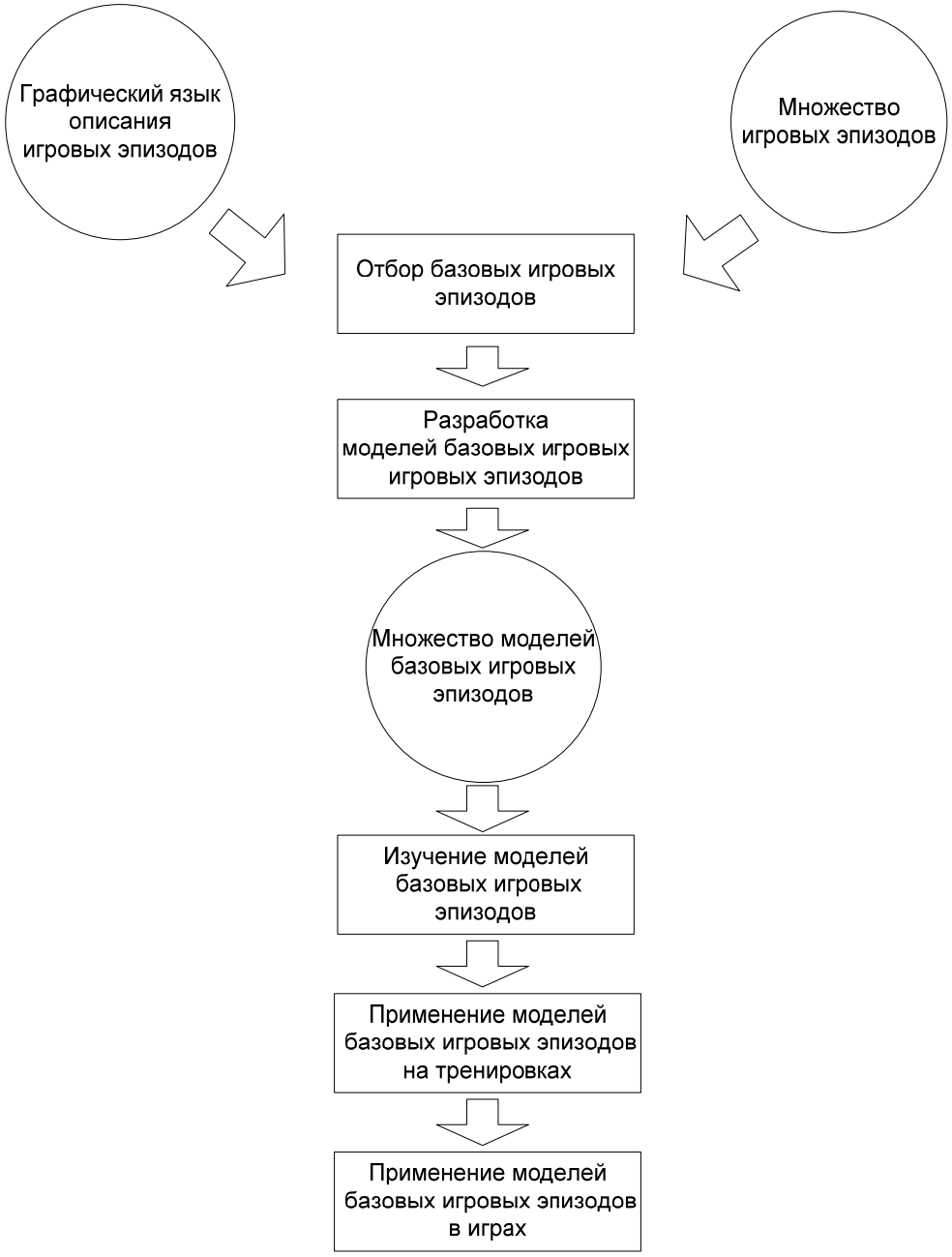


Рис. 6. Система изучения игровых эпизодов

Предлагаемая система моделирования игровых эпизодов позволяет сформулировать критерии и параметры оценки качества подготовки футболистов. При ее использовании перед тем, как приступать к практическим тренировкам, необходимо описать множество игровых эпизодов и множество элементарных действий игроков. При формировании этих множеств тренер и игрок должны учитывать специфику футбола. Следующий этап – создание алгоритмов действий в игровых эпизодах. Они описываются при помощи предлагаемого в настоящей работе графического языка описания игровых эпизодов. Таким образом, создаются модели игровых эпизодов, которые необходимо сначала изучить на тренировках, а потом – применять в играх.

Также данная система позволяет выявить *положительные действия* – действия, приводящие к положительным результатам. Именно положительные действия необходимо отрабатывать на тренировках.

Заключение

Из изложенного следует, что игра в футбол может быть представлена как набор некоторых ситуаций, в которых игроки должны действовать по определенным алгоритмам. Применение изложенного подхода позволяет:

- более отчетливо и точно увидеть многообразие футбола;
- улучшить понимание того, что такое игровой эпизод;
- улучшить понимание сложности игрового эпизода;
- конкретизировать множество вариантов результатов игрового эпизода;
- более рационально организовать тренировки по формирования базовой схемы действий в игровом эпизоде, как отдельным игроком, так и несколькими игроками.

Предлагаемый подход в настоящее время с успехом применяется при обучении футболу в ФК «Дружба». Во многом именно благодаря применению предлагаемого подхода помогло ФК «Дружба» в 2006 г. выйти в высшую группу первенства Санкт-Петербурга по футболу. В 2006 г. юношеская команда ФК «Дружба» (1992 год рождения) стала полуфиналистом кубка Санкт-Петербурга. На момент написания статьи эта команда занимала первое место в чемпионате города по футзалу.

В 2006 и 2008 гг. были проведены занятия с командами футбольных клубов «Зенит» и «Локомотив», на которые были получены положительные отзывы тренеров и игроков.

Литература

1. Козловский В.И. (ред.) Подготовка футболистов. – М.: Физкультура и спорт, 1977.
2. Андреев С.Н. Играй в мини-футбол. – М.: Советский спорт, 1989. – 47 с.
3. Кук М. 101 упражнение для юных футболистов 7–11 лет/ Пер. с англ. Л. Захаровича. – М.: ООО издательство АСТ, ООО издательство Астрель, 2001. – 128 с.
4. Кук М. 101 упражнение для юных футболистов 12–16 лет./ Пер. с англ. Л. Захаровича. – М.: ООО издательство АСТ, ООО издательство Астрель, 2001. – 128 с.
5. Гил Харви и др. Футбол для начинающих: Практический курс./ Пер. с англ. В. Гапарова – М.: ООО издательство АСТ, ООО издательство Астрель, 2001. – 128 с.
6. Ван Гиг Дж. Прикладная общая теория систем. – М.: Мир, 1981. – 730 с.
7. Кнут Д.Э. Искусство программирования. Том 1. Основные алгоритмы/ Дональд Э. Кнут. – М.: Вильямс, 2007. – 712 с.
8. Гойдановский В. 800 вопросов и ответов о правилах футбола. – Тбилиси: Издательство ЦК КП Грузии, 1987.
9. Футбол (Правила соревнований). – М.: Терра-Спорт, 2000. – 72 с.

МЕТОДИКА ПОВЫШЕНИЯ УРОВНЯ ЗАПОМИНАЕМОСТИ УЧЕБНОГО МАТЕРИАЛА НА ОСНОВЕ ПСИХОЛОГИИ ЦВЕТОВОСПРИЯТИЯ

В.А. Кувшинов, И.В. Журкин
Научный руководитель – В.В. Королев

В работе предложена методика цветового оформления учебного материала, основанная на психологических приемах цветооформления. Целью данной методики является повышение процента запоминаемой информации путем подбора индивидуальных цветовых схем пользователю и повышения комфорта просмотра, исходя из личностных характеристик пользователя.

Введение

В современном обществе существует множество методов усвоения информации. Основным источником информации является визуальная, воспринимаемая посредством чтения. Учеными было доказано, что при прочитывании текста запоминается лишь его 25%, и при каждом последующем прочитывании объем усвоенной информации увеличивается на 5% [1].

Рассматриваемая тема весьма актуальна, так как достаточно большое количество людей занимается либо усовершенствованием своей квалификации, либо просто получением высшего или среднего образования и, следовательно, тратит огромное количество времени на запоминание различной информации, которое можно было потратить на другие более важные вещи, если бы запоминаемость при первом прочитывании была увеличена.

Цель работы – разработать методику подбора оптимальных для человека цветов и использовать в учебниках для повышения запоминаемости и сокращения затрат времени на изучение материала.

Задачи исследования:

1. выявление и интерпретация основных параметров психического состояния;
2. создание методики оценки основных параметров психического состояния;
3. разработка методики интерпретации различных вариантов, получаемых при использовании методики.

Предмет исследования – параметры психического состояния, их взаимосвязь между собой.

Основной результат – методика диагностики основных параметров психического состояния с целью подбора цветовых схем для каждого индивида, влияющих на его восприятие информации.

За основу работы было взято два теста: цветовой тест Люшера и тест на темперамент Белова. В основе используется 8 цветов: желтый, зеленый, коричневый, красный, синий, фиолетовый, серый и черный. Так как черный цвет несет в себе значение абсолютного безразличия, его необходимо использовать минимально и желательно в большинстве случаев заменять серым, при формировании таблицы оптимальных цветов для каждого человека нужно использовать все цвета, основными из которых будут являться цвета его темперамента.

Тест А. Белова («формула темперамента»)

Назначение теста

Этот тест является одним из важнейших, так как именно он формирует основные цветовые значения на основе процентного соотношения темпераментов. Известно, что каждому типу темперамента соответствует определенный цвет, а точнее: холерик –

красный, сангвиник – желтый, флегматик – зеленый, меланхолик – синий, также к этим цвет был добавлен серый цвет, который является абсолютно нейтральным и не оказывает никакого влияния на психику человека [2]. Эти значения также подкреплены ключами к тесту Люшера, также эти соответствия были известны еще в древней Индии. Именно по процентному соотношению этих темпераментов, полученному после прохождения представленного ниже теста, формируется основная цветовая схема, которая впоследствии немного изменяется.

Лица с четко выраженными свойствами, относящимися только к одному типу темперамента, встречаются пренебрежительно редко. Гораздо чаще людям свойственны смешанные типы темперамента, характеризующиеся наличием свойств разных типов темперамента с преобладанием одного из них.

Методика А. Белова служит для определения преобладающего типа темперамента и выявления представленности в нем свойств других типов. Испытуемому последовательно предъявляются четыре карточки, на каждой из которых написано по 20 свойств, характерных для представителей каждого типа темперамента.

Инструкция к тесту: внимательно прочитав перечень свойств, испытуемый должен поставить знак (+), если считает, что это свойство ему присуще, и знак (–), если оно у него отсутствует. В сомнительных случаях ничего не ставить.

Тестовый материал

Блок 1.

1. Неусидчивость, суетливость.
2. Невыдержанность, вспыльчивость.
3. Нетерпеливость.
4. Резкость и прямолинейность в отношениях с людьми.
5. Решительность и инициативность.
6. Упрямство.
7. Находчивость в споре.
8. Неритмичность в работе.
9. Склонность к риску.
10. Незлопамятность, необидчивость.
11. Быстрота и страстность речи.
12. Неуравновешенность и склонность к горячности.
13. Нетерпимость к недостаткам.
14. Агрессивность забияки.
15. Выразительность мимики.
16. Способность быстро действовать и решать.
17. Неустанное стремление к новому.
18. Обладание резкими, порывистыми движениями.
19. Настойчивость в достижении поставленной цели.
20. Склонность к резкой смене настроения.

Блок 2.

1. Жизнерадостность.
2. Энергичность и деловитость.
3. Недоведение начатого дела до конца.
4. Склонность переоценивать себя.
5. Способность быстро схватывать новое.
6. Неустойчивость в интересах и склонностях.
7. Легкое переживание неудачи и неприятностей.
8. Легкое приспособление к разным обстоятельствам.
9. Увлеченность любым делом.

10. Быстрое остывание, когда дело перестает интересовать.
11. Быстрое включение в новую работу и переключение с одного вида работы на другой.
12. Тяготение однообразной, будничной, кропотливой работой.
13. Общительность и отзывчивость, не скованность в общении с другими людьми.
14. Выносливость и работоспособность.
15. Громкая, быстрая, отчетливая речь.
16. Сохранение самообладания в неожиданной, сложной ситуации.
17. Обладание всегда добрым настроением.
18. Быстрое засыпание и пробуждение.
19. Частая несобранность, поспешность в решениях.
20. Склонность иногда скользить по поверхности, отвлекаясь.

Блок 3.

1. Спокойствие и хладнокровие.
2. Последовательность и обстоятельность в делах.
3. Осторожность и рассудительность.
4. Умение ждать.
5. Молчаливость, нежелание болтать по пустякам.
6. Обладание спокойной, равномерной речью, без резко выраженных эмоций, жестикуляций и мимики.
7. Сдержанность и терпеливость.
8. Доведение начатого дела до конца.
9. Умение применять свои силы в дело (не растрачивать их по пустякам).
10. Строгое придерживание выработанного распорядка жизни, системы в работе.
11. Легкое сдерживание порывов.
12. Маловосприимчивость к одобрению и порицанию.
13. Незлобивость, проявление снисходительного отношения к колкостям в свой адрес.
14. Постоянство в своих отношениях и интересах.
15. Медленное вовлечение в работу и переключение с одного вида работы на другой.
16. Ровность в отношении со всеми.
17. Аккуратность и порядок во всем.
18. Трудное приспособление к новой обстановке.
19. Обладание выдержкой.
20. Постепенное схождение с новыми людьми.

Блок 4.

1. Стеснительность и застенчивость.
2. Растерянность в новой обстановке.
3. Затруднительность в установлении контактов с незнакомыми людьми.
4. Неверие в свои силы.
5. Легкое перенесение одиночества.
6. Чувство подавленности и растерянности при неудачах.
7. Склонность уходить в себя.
8. Быстрая утомляемость.
9. Обладание тихой речью, иногда снижающейся до шепота.
10. Невольное приспособление к характеру собеседника.

При обработке результатов теста необходимо подсчитать количество плюсов по каждой карточке отдельно, вычислить процент положительных ответов по каждому типу темперамента. Процент положительных ответов по каждому типу темперамента высчитывается по формулам:

Х = (А1 / А) * 100%; С = (А2 / А) * 100%,

Ф = (А3 / А) * 100%; М = (А4 / А) * 100%,

где Х, С, Ф, М – типы темперамента; А1, А2, А3, А4 – число положительных ответов по карточкам соответствующего блока; А – общее число положительных ответов по четырем карточкам.

В конечном виде «формула темперамента» приобретает, например, такой вид:

Т = 35%Х + 30%С + 14%Ф + 21%М.

Это значит, что данный темперамент на 35% – холерический, 30% – сангвинический, 14% – флегматический и 21% – меланхолический. Если относительный результат числа положительных ответов по какому-либо типу составляет 40% и выше, значит, данный тип темперамента у испытуемого доминирующий. Если этот результат составляет 30–39%, то качества данного типа выражены достаточно ярко. Если результат 20–29%, то средне выражены. При результате 10–19% можно утверждать, что черты этого типа темперамента выражены в малой степени.

Тест на настроение САН

Данный тест является второстепенным, так как он накладывается на уже сформированные цветовые схемы.

Тест предназначен для оперативной оценки самочувствия, активности и настроения (по первым буквам этих функциональных состояний и назван опросник).

Испытуемых просят соотнести свое состояние с рядом признаков по многоступенчатой шкале. Шкала состоит из индексов (3 2 1 0 1 2 3) и расположена между тридцатью парами слов противоположного значения, отражающих подвижность, скорость и темп протекания функций (активность), силу, здоровье, утомление (самочувствие), а также характеристики эмоционального состояния (настроение). Испытуемый должен выбрать и отметить цифру, наиболее точно отражающую его состояние в момент обследования.

Тестовый материал

	3	2	1	0	1	2	3	
1. Веселый								Грустный
2. Хорошее настроение								Плохое настроение
3. Счастливый								Несчастный
4. Жизнерадостный								Мрачный
5. Восторженный								Унылый
6. Радостный								Печальный
7. Спокойный								Озабоченный
8. Оптимистичный								Пессимистичный
9. Полный надежд								Разочарованный
10. Довольный								Недовольный

Таблица. Матрица заполнения теста

При подсчете крайняя степень выраженности негативного полюса пары оценивается в один балл, а крайняя степень выраженности позитивного полюса пары в семь баллов. При этом нужно учитывать, что полюса шкал постоянно меняются, но положительные состояния всегда получают высокие баллы, а отрицательные – низкие. Полученные результаты по каждой категории делятся на 10. Средний балл шкалы равен 4.

Оценки, превышающие 4 балла, говорят о благоприятном состоянии испытуемого, оценки ниже четырех свидетельствуют об обратном. Нормальные оценки состояния лежат в диапазоне 5,0–5,5 баллов. Следует учесть, что при анализе функционального состояния важны не только значения отдельных его показателей, но и их соотношение.

На основе результатов данного теста формируются значения яркости для цветов. Контрастность со светлотой не учитываются, так как все равно все цвета, которые формируются при изменении шкалы контрастности, точно также формируются при изменении шкалы яркости. Светлота является величиной, обратной яркости, следовательно, цветовые значения просто обратные. Используя шкалы значений графического редактора, были подобраны значения яркости, а точнее: от 70 до 210, исключая значения от 110 до 145, так как они негативно воспринимаются глазом.

Результаты этого теста формируются по схеме (рисунок).

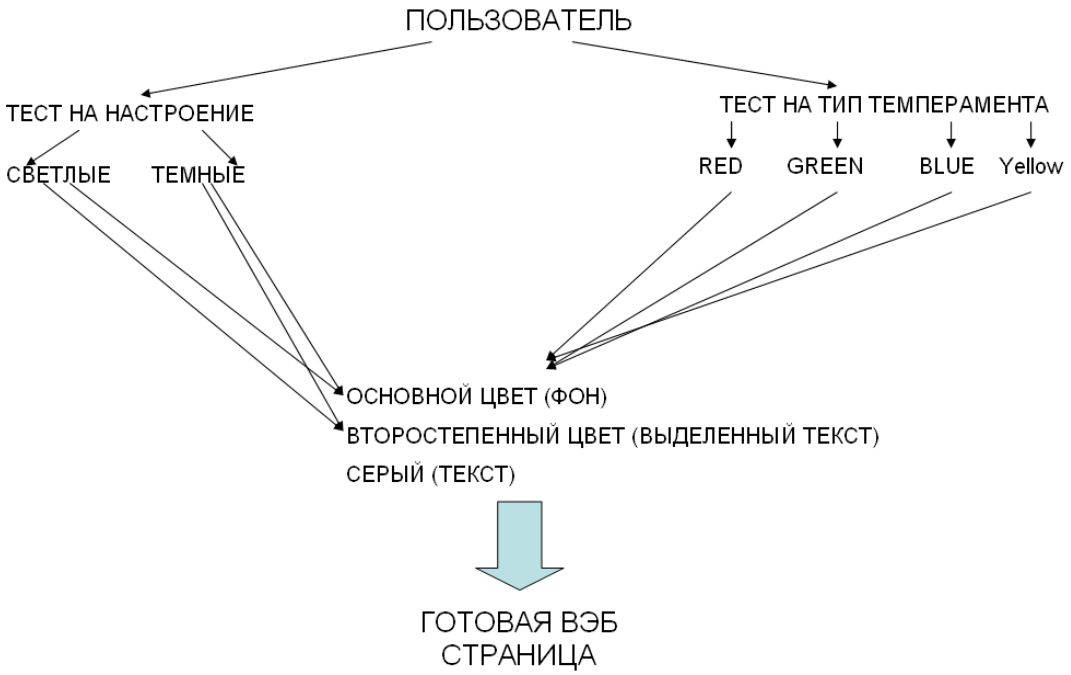


Рисунок. Формирование цветовой схемы

Заключение

Разработанная методика видится адекватной, но ее необходимо проверить посредством статистического исследования. Предполагается исследовать контрольную группу в 1000 человек в нескольких учебных заведениях с целью установления продуктивности представленной методики.

Литература

1. Ильин Е.П. Дифференциальная психофизиология. – СПб: Питер, 2001. – 230 с.
2. Петровская М. Р. Психология. – М.: Альга, 2002. – 160 с.
3. Нелюбова М.В. Психология цвета. Авторский курс лекций. – 2003 [Электронный ресурс]. – Режим доступа: http://www.videoton.ru/Articles/pshiho_color.html
4. Базыма А. Цвет и психика. – 2005. – 180 с.
5. Люшер М. Цветовой тест Люшера. – СПб: Сова, 2005. – 220 с.

МЕТОДИКА СТРУКТУРИРОВАНИЯ УЧЕБНОГО МАТЕРИАЛА НА ОСНОВЕ ПРОПОРЦИЙ ЗОЛОТОГО СЕЧЕНИЯ

В.В. Котов, И.В. Журкин
Научный руководитель – В.В. Королев

Статья посвящена проблеме в области образования, а именно зрительному восприятию и зрительной памяти. В статье представлены некоторые приемы по оформлению страницы, которые, по мнению автора, повысят процент усвоенной информации при ознакомлении с материалом.

Введение

На сегодняшний день инновационные методики применяются в различных сферах человеческой деятельности. Особая роль уделяется новейшим разработкам именно в сфере образования, поскольку состояние этой области далеко от идеала и нуждается в большой доработке. Тематика данной статьи акцентирует внимание на разработке такого метода подачи информации, чтобы его восприятие и усвоение стало максимально быстрым и простым. Чтобы человек быстро воспринимал и запоминал информацию, необходимо подать эту информацию в такой форме, чтобы все внимание было сфокусировано исключительно на изучаемом материале. Для этого следует оформить материал таким образом, чтобы работа с ним была удобна и проста, а наиболее значимые моменты не приходилось искать и выделять из общего текста. Этого эффекта можно достичь при помощи внедрения в оформление страницы известного психологического приема – золотой пропорции или так называемого «кода» красоты.

Считается, что объекты, построенные на основе «золотого сечения», вызывают ощущение зрительной гармонии. Интерес к форме какого-либо предмета может быть продиктован красотой формы. Форма, в основе построения которой лежат сочетание симметрии золотого сечения, способствует наилучшему зрительному восприятию [1]. Это знали и использовали известные философы и творческие люди еще с античных времен. Есть мнение, что египетские мастера пользовались соотношениями золотого сечения при строительстве пирамид и гробниц, возможно, именно поэтому они так притягивают к себе всеобщее внимание. Впервые золотое сечение встречается в «Началах» Евклида. Термин же «золотое сечение» был введен гораздо позднее Леонардо да Винчи, который использовал его как пропорции «идеального человеческого тела». Древнейшая формула красоты, использовавшаяся в те времена только в искусстве, лишь сегодня набирает обороты [2].

Рассмотрим понятие «золотого сечения» с точки зрения геометрии. Золотое сечение – это такое деление целого на две неравные части, при котором большая часть так относится к целому, как меньшая к большей [3].

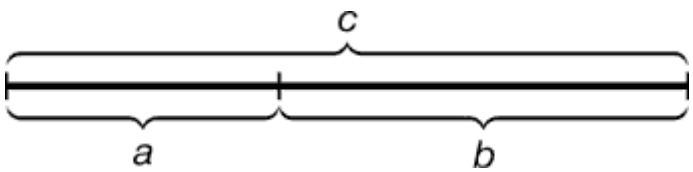


Рис. 1. Графическое представление золотой пропорции

Эту пропорцию принято обозначать греческой буквой φ (встречается также обозначение τ). Примером использования правила «золотого сечения» является расположение основных компонентов кадра в особых точках – зрительных центрах. Таких точек всего четыре, и расположены они на расстоянии 3/8 и 5/8 от соответствующих краев плоско-

сти. Считается, что человек при первом просмотре какого-либо изображения акцентирует свое внимание на этих точках, независимо от формата кадра или картины [3].

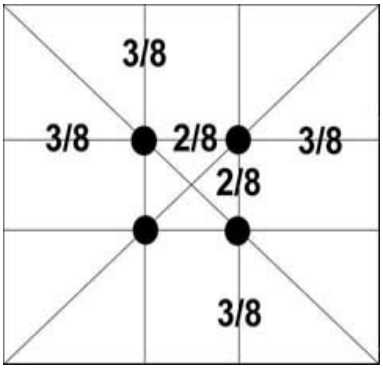


Рис. 2. Схема разбиения рабочей области по методике ЗС

Целое всегда состоит из частей, части разной величины находятся в определенном отношении друг к другу и к целому. Принцип золотого сечения – высшее проявление структурного и функционального совершенства целого и его частей в искусстве, науке, технике и природе [4].

Теперь на основе свойств золотого сечения и зрительных центров автор вносит следующие предложения по оформлению страницы. Гипотетически можно утверждать, что при удачном применении золотых параметров в оформлении учебного материала процесс обучения будет комфортен; применение зрительных центров, а именно манипулирование вниманием, повысит усвоение материала.

Методика структурирования учебного материала на странице. Первоначальная подготовка страницы

Для начала следует расположить рабочее поле страницы таким образом, чтобы границы информационной области (большая к меньшей) находились в золотом отношении друг к другу. При этом размер окна будет задаваться согласно текущему разрешению экрана (золотое соотношение измеряется в таком случае в пикселях).

Далее следует определить на странице четыре зрительных центра. Это делается путем деления сторон экрана на восемь равных частей (см. рис. 2).

В силу того, что на странице существует четыре зрительных центра, следует условно разбить все рабочее поле на равные четверти таким образом, чтобы в каждой находился один зрительный центр. В дальнейшем объекты будут группироваться в каждой из полученных частей. Согласно исследованиям немецкого ученого, профессора Адольфа Цейзинга, опубликовавшего свои труды в «Эстетических исследованиях», из всех приемов именно использование золотого сечения и зрительных центров дают наибольший художественный эффект и доставляет наибольшее удовольствие при восприятии. Исходя из этого, предполагается, что такого типа деление сформирует у пользователя положительное впечатление от внешнего вида страницы, так как каждая область будет иметь золотую структуру.

Рекомендации по структурированию материалов информационного кадра

- Изучение материала будет протекать последовательно по секторам, причем, согласно исследованиям Eyetools Inc. (корпорация, созданная на базе Стенфордского университета передовых исследований визуального восприятия), наиболее привлекающая внимание зона расположена слева сверху, поэтому ознакомление со страницей

будет проходить, начиная с нее. Этот факт считается общепринятым, и многие, даже не задумываясь, чисто интуитивно начинают свое ознакомление со страницей именно в этой области. Значит, именно в этой области должна находиться наиболее значимая информация. Положительное восприятие объекта зависит также и от привычности его отображения, а, следовательно, соблюдение ряда стандартов структурирования полагается немаловажным.

- Во время изучения одного сектора три остальные незадействованные будут находиться в ждущем (неактивном) режиме. Это означает, что вся анимация за пределами рассматриваемого сегмента должна пребывать в неактивном состоянии. В противном случае самовоспроизводящаяся анимация привлечет внимание пользователя на себя, что приведет к потере концентрации пользователя на прежде изучаемом объекте. В таком случае анимационные ролики, размещенные на странице, должны быть снабжены средствами запуска по желанию пользователя, а в тексте на них необходимо делать ссылки, чтобы не терялась структурность излагаемого материала.
- Исходя из факта, что последовательность просмотра страницы, как правило, происходит столбичным или строчным способом, следует учесть это и при размещении объектов, т.е. расположение объектов должно удовлетворять одному из двух выше упомянутых способов.
- Рекомендуется создать мастер подсказок, который будет выдавать нужные указания к работе, рекомендации по ознакомлению с учебником, важные правила и определения. Окно подсказки, также заданное золотой пропорцией, будет «выплывать» в точку зрительного центра соответствующей рабочей области для максимального восприятия важной информации. Учитывая тот факт, что в учебных пособиях нередко встречается объемный графический материал, автор предлагает снабдить текст гиперссылками, выводящими графический объект в область зрительного центра при нажатии на них пользователя. Наиболее важные схемы или рисунки, определения или формулы могут находиться непосредственно в самом тексте (правда, стоит учесть их размещение в областях зрительных центров), а что касается менее значимых, но в то же время необходимых графических объектов, то для них будут установленные анимированные выноски.
- Согласно исследованиям в области конструкторской документации, текст, разделенный на столбцы, удобнее читается и легче запоминается. Этот факт нельзя оставить без внимания. Поэтому текст следует разбивать на столбцы, дабы придать ему максимально читаемый вид. При построении текста следует подвести форму столбца таким образом, чтобы его ширина удовлетворяла золотой пропорции. Автор предполагает, что в таком случае эффективность чтения повысится.

Заключение

Использование полученной методики, по мнению автора, повысит процент запоминания информации и придаст странице удобный для работы вид. Автору предстоит внести еще множество доработок и коррективов в данную структуру, указания к данным коррективам автор планирует получить посредством статистического исследования методики. Рассматриваемая методика, ни по каким критериям не противоречит ни одному ГОСТу по оформлению документации, и, значит, ее использование допустимо в рассматриваемой сфере.

На сегодняшний день свойства золотой пропорции используется уже в некоторых сферах, таких как реклама, фотография и т.д. Например, такие фирмы, как LG и Samsung, внедряют золотые параметры в производство экранов телевизоров и мониторов, а производители фототехники, такие как Canon, Casio, Nikon, используют уникальное свойство зрительных центров для придания гармоничности снимкам.

Все это говорит, что внедрение золотой пропорции в человеческий обиход актуально и приносит положительные результаты. Значит, ее применение в образовательной сфере тоже допустимо, и есть основания рассчитывать на положительные результаты. В ближайших перспективах автора – разработать тестирующую программу для выявления процентного показателя пользы методики.

Литература

1. Ковалев Ф.В. Золотое сечение в живописи. – К.: Высшая школа, 1989. – 250 с.
2. Бердукидзе А.Д. Золотое сечение // Квант. – 1973. – №8. – 300 с.
3. Калюжный О.Н. О Золотой Пропорции и ее квадрате. – 2004. – 190 с.
4. Стахов А. Коды золотой пропорции. – 2000. – 200 с.

ЦВЕТООФОРМЛЕНИЕ И СТРУКТУРИРОВАНИЕ УЧЕБНОГО МАТЕРИАЛА В ЭЛЕКТРОННОЙ ОБРАЗОВАТЕЛЬНОЙ ПЛАТФОРМЕ

И.В. Журкин
Научный руководитель – к.т.н., доцент Н.Н. Горлушкина

Рассматривается возможность использования в обучающих программах разработок в области психологии цветовосприятия для увеличения усвоения предъявляемого обучающимся учебного материала. Показано соотнесение психологических параметров индивида с предпочитаемой цветовой моделью, а также структурирование учебного контента по методике золотой пропорции.

Введение

В настоящее время в науке и технике наблюдается тенденция к внедрению различных инновационных методик. Это справедливо и для сферы образования, которая становится делом не только стратегически важным, но и доходным. Коммерциализация сферы образования диктует новые, рыночные условия работы, что требует доработки и совершенствования старых методик и технологий. Новые технологии образования, как правило, основываются на применении компьютерной техники в образовательном процессе. Информационные технологии, основанные на применении компьютерной техники, позволяют не только значительно упростить и усовершенствовать процесс обучения, но и привносят в эту область возможности ранее труднодоступные или не доступные вовсе.

В этом контексте немаловажную роль занимают электронные обучающие средства. Рассмотрение возможности создания электронного обучающего средства с интегрированным комплексом, использующим инновационные разработки в области психологии цветовосприятия и «золотой» пропорции, а также выгод от такого средства является целью представленной работы. Другими словами, задача состоит в том, чтобы разработать такой электронный учебник, информация в котором будет воспринята обучающимся в большем объеме по сравнению со стандартными средствами обучения.

За основной критерий успешности представленного проекта принимается рост процента усвоенной информации. Также будет рассматриваться такой параметр, как приятность восприятия, термин этот будет раскрыт позже.

Важность учета цветовой модели доказывается следующими положениями. По данным Интернет-школы мнемотехники, человеком при прочтении стандартного текста (черный шрифт, белый фон) усваивается, даже в случае хорошей структурированности учебного материала, не более 25–30%, к аналогичным результатам пришли еще в 1996 г. в центре исследований и статистики науки Министерства образования и науки РФ и РАН [4]. Несомненно, это малый процент усвоения.

Исходя из этого, рассмотрим возможность повышения процента усвоения учебного материала с помощью комплекса инновационных методик. К ним относится, во-первых, соотнесение психологических параметров индивида с предпочитаемой цветовой моделью, а, во-вторых, структурирование учебного контента по методике золотой пропорции.

Принципы цветооформления учебного материала посредством электронной образовательной платформы

На сегодняшний день считается доказанным влияние цвета на человеческую психику. Вопрос этот, конечно, многосложный и малоизученный, но определенные результаты исследований психологии цветовосприятия уже применяются в различных науч-

ных сферах – цветотерапия в медицине, цветодиагностика в психиатрии, дизайн и т.д. [1]. Видится возможным применение результатов подобных исследований в рамках образовательных методик, лежащих в основе рассматриваемой разработки.

За основу методики цветооформления учебного материала взяты цветовой тест Макса Люшера, тест Белова на определение темперамента, а также тесты на оценку текущего эмоционального состояния (тест на настроение) [2]. Перечисленные тесты являются серьезными разработками и широко применяются в психологии и психиатрии.

Основная идея состоит в том, чтобы соотнести входные цветовые таблицы теста Люшера с выходными показателями тестов на темперамент, характер и эмоциональное состояние так, чтобы в результате с помощью специализированной программы была подобрана такая цветовая схема представления учебного материала, которая бы позволила на основе наибольшей приятности восприятия увеличить показатель усвоения.

Под приятностью восприятия в рамках рассматриваемого вопроса будем понимать показатель индивидуального психологического состояния человека по отношению к какому-либо объекту, отражающий комфортность и удобство взаимодействия с этим объектом. В качестве шкалы измерения градуса приятности восприятия, предлагается пользоваться шкалой 100 единиц. Поскольку так называемый градус приятности – величина достаточно субъективная, ее нельзя принимать как абсолютный показатель и измерить тоже не представляется возможным, но, тем не менее, она является необходимым в статистическом исследовании адекватности предложенного проекта.

Под цветовой схемой представления учебного материала будем понимать характер окрашивания элементов электронной страницы (цвет текста, фона, заголовков, определений, формул, схем и т.д.).

Усвоение материала можно определить как процент усвоенного учебного материала от общего количества учебного материала, представленного к изучению, при этом под усвоенным материалом понимается информация, которую индивид в состоянии свободно воспроизводить по памяти, понимать ее структурную и логическую составляющую и идейно-смысловую нагрузку.

Также необходимо упомянуть, что приведенная методика, в частности, учитывает и такие показатели, как гендерный, возрастной и сочетаемости цветов.

В практическом применении вышесказанное можно свести к следующему.

1. При аутентификации в электронной обучающей системе пользователю предлагается пройти ряд тестов на определение характера и темперамента, результаты этого тестирования будут программно привязаны к учетной записи пользователя, и на их основе в дальнейшем без повторного тестирования программа будет самостоятельно формировать и представлять в соответствующем виде учебный материал, уникальный в своем цветовом оформлении для каждого пользователя, тем самым на подсознательном уровне создавая ощущение приятности восприятия у пользователя, за счет чего, по мнению автора, уровень восприятия информации должен повыситься. Подобранные таким образом схемы далее будут называться базовыми.

2. Темперамент и характер являются достаточно статичными показателями психики человека, однако не только они, согласно Люшеру, влияют на цветовосприятие, есть более динамичные показатели, исходя из которых, пользователь может отклоняться от подобранных ранее базовых цветовых схем. Из этого следует необходимость корректировки базовых схем с помощью дополнительных тестов. Наиболее существенным динамическим показателем цветовосприятия будем считать настроение. Исходя из этого, предполагается при каждой аутентификации пользователя предлагать ему короткий тест на определение его текущего психологического состояния. Опираясь на результаты этого теста, программа будет вносить корректировки в базовую цветовую схему, такая схема в дальнейшем будет называться расширенной.

3. После подбора расширенной цветовой схемы программно к ней будут применяться еще несколько корректировок, связанных с проверкой сочетаемости цветов подобранной схемы и с половозрастными предпочтениями. Также предусмотрены общепринятые принципы удобочитаемости материала (фон светлее текста, крупный шрифт, структурированность и пр.). Столь свободная замена цветов полагается автором возможной в силу того, что при работе над тестом Макс Люшер рассмотрел до 4500 оттенков цветов и пришел к выводу, что обеспечивает достаточно широкий выбор [5]. Подбор цветов расширенной цветовой схемы будет происходить путем изменения яркостных показателей цветов базовой схемы при сохранении заданной контрастности и светлоты.

4. В том случае, если программно не удается подобрать адекватную расширенную цветовую схему для конкретного пользователя, к его странице будет применена так называемая универсальная цветовая схема, оставленная на основе общих рекомендаций различных психологов по вопросу комфортности цветовосприятия, широко встречающихся в научной литературе [2]. Эта схема, по мнению автора, будет обладать несколько менее широкими возможностями, но, тем не менее, общей идее проекта она удовлетворяет.

Структурирование учебного материала по методу золотого сечения

После того как программа электронного обучающего средства подберет цветовое оформление конкретному пользователю, уже без вмешательства со стороны пользователя она дополнительно структурирует учебный материал, опираясь на алгоритмы, построенные с учетом применения к структурированию золотой пропорции.

Остановимся подробнее на этом методе.

Известно, что золотая пропорция применялась с дервних времен в живописи, скульптуре, архиктуре. Интерес к форме какого-либо предмета может быть продиктован жизненной необходимостью, а может быть вызван красотой формы. Форма, в основе построения которой лежат сочетание симметрии и золотого сечения, способствует наилучшему зрительному восприятию и появлению ощущения красоты и гармонии. Целое всегда состоит из частей, части разной величины находятся в определенном отношении друг к другу и к целому. Принцип золотого сечения – высшее проявление структурного и функционального совершенства целого и его частей в искусстве, науке, технике и природе. Еще в эпоху Возрождения художники открыли, что любая картина имеет определенные точки, невольно приковывающие наше внимание, так называемые зрительные центры. При этом абсолютно неважно, какой формат имеет картина – горизонтальный или вертикальный. Таких точек всего четыре, и расположены они на расстоянии 3/8 и 5/8 от соответствующих краев плоскости [7].

Леонардо да Винчи и Рафаль использовали в своих картинах смысловые центры картины, размещая их в зрительных центрах. Фрактальные фигуры имеют в своей основе золотую пропорцию, а ведь известно, что фрактальную природу имеет большинство живых организмов. Иоган Кеплер говорил, что геометрия владеет двумя сокровищами – теоремой Пифагора и золотым сечением, причем, если первое из них сравнимо с мерой золота, то второе – с драгоценным камнем. Уже во втором томе евклидовых «Начал» построено золотое сечение [8].

На современном этапе золотое сечение не потеряло своей актуальности, золотая пропорция применяется в таргетинге, в производстве электроники, архитектуре. Кроме того, доказано, что фигуры, построенные по золотому сечению, производят впечатление спокойствия, уравновешенности, округленности, завершенности [6].

Исходя из приведенных фактов, рационально применить методику золотой пропорции в структурировании учебного материала на страницах электронных обучающих

систем. С точки зрения программной реализации осуществление этого не должно вызвать затруднений, так как существуют стандартные функции, определяющие размер рабочей области окна программы, исходя из которого, можно выполнять пропорциональное деление окна на области, в которых будет размещена информация учебного материала.

Основываясь на опыте применения гармонии золотого сечения в искусстве и психологии восприятия этой гармонии, предположим, что внедрение в программный комплекс модуля, отвечающего за разметку и структурирование рабочей области по принципу золотого сечения, позволит пользователю лучше воспринимать информацию. Это должно достигаться за счет целостного восприятия информации и повышения внутреннего и визуального комфорта от просмотра подобным образом оформленных страниц.

Дополнительно необходимо предусмотреть использование зрительных центров, поскольку доказано, что человек воспринимает и подсознательно запоминает графический материал как единое целое при первом взгляде на него [6]. Тогда программа будет автоматически размещать в указанных центрах наиболее важную графическую информацию.

Программная реализация

Программная реализация предлагаемого продукта сводится к созданию специализированного клиентского приложения, настроенного на работу с конкретным сервисом. Это, по сути, специализированный браузер, который занимается парсингом подгружаемых страниц, тем самым за методики золотого сечения отвечает локальное клиентское приложение.

Алгоритмы цветообработки, в свою очередь, хранятся на сервере, цветовые схемы записываются в профайл пользователя и передаются клиенту в зависимости от результатов тестирования настроения. Работа с контентом системы осуществляется посредством визуального редактора, созданного для удобства пользователя.

Функциональное наполнение системы, помимо вышеуказанного, содержит также администраторский модуль. С этим модулем работает администратор учебного заведения, если речь идет о так называемой School Version. Здесь он добавляет списки студентов и преподавателей, а также права участников системы. Посредством преподавательского модуля разработчик курса может в графическом редакторе создавать учебные материалы и размещать их в системе, после чего назначать права для доступа к материалам. Если ученику доступен материал, он автоматически появится в виде гиперссылки в его персональном виртуальном рабочем кабинете.

Если же речь идет о так называемой Single Version, то система представляется в несколько более упрощенном виде. По сути, это конструктор персонального курса, где пользователь может разработать учебный материал персонально для себя, и этот материал будет представлен в соответствующем виде.

В конечном варианте реализации разрабатываемая система будет представлять собой некую систему дистанционного обучения (ДО), автоматически оформляющую материал в соответствии с описанными мнемотехниками. Перспективы развития подобной системы заключаются как в доработке функционала самой системы ДО, так и в выносе мнемотехнических методик за рамки конкретной системы ДО, оформлении их в виде отдельных программных модулей для подключения к уже существующим системам ДО, системам электронных библиотек и другим системам, которые потребуются для совершенствования процесса обучения.

Помимо этого, в систему могут быть интегрированы другие мнемотехники.

Заключение

Рассмотрена возможность использования в обучающих программах разработок в области психологии цветовосприятия для увеличения усвоения предъявляемого обучающимся учебного материала. Предложена методика использования в обучающих программах соотнесения индивидуальных психологических параметров обучающегося с предпочитаемой им цветовой моделью, а также структурирование учебного контента по методике золотой пропорции.

Для проверки адекватности разработанной методики предполагается провести комплексное тестирование в учебном заведении численным составом участников 500 человек. Исходя из результатов, методики подвергнутся доработке, а программный продукт – отладке.

Литература

1. Ильин Е.П. Дифференциальная психофизиология. – СПб: Питер, 2001. – 230 с.
2. Петровская М. Р. Психология. – М.: Изд-во «Альга», 2002. – 180 с.
3. Нелюбова М.В. Психология цвета. Авторский курс лекций. – СПб: Питер, 2004. – 200 с.
4. Базыма А. Цвет и психика. – М.: Амфора, 2005. – 195 с.
5. Люшер М. Цветовой тест Люшера. – СПб: Сова, 2005. – 220 с.
6. Покровский Г.И. Архитектура и законы зрения. – 1998. – 150 с.
7. Кисин Б.М. Графическое оформление книги. – 2001. – 250 с.
8. Энциклопедия замечательных идей и людей [Электронный ресурс]. – Режим доступа: http://www.alleng.ru/edu/inform.htm

«ВИРТУАЛЬНЫЙ» ЛАБОРАТОРНЫЙ КОМПЛЕКС ПО ОСНОВАМ ПОЛУПРОВОДИКОВОЙ ЦИФРОВОЙ ЭЛЕКТРОНИКИ

В.В. Новиков (Санкт-Петербургский государственный университет информационных технологий, механики и оптики, факультет среднего профессионального образования)
Научный руководитель – Д.М. Гриншпун

Представленный в работе «виртуальный» комплекс (Комплекс) предназначен для лабораторного сопровождения дисциплин «Информатика» и «Электрика и электроника», изучаемых при подготовке специалистов СПО по специальности «Программное обеспечение вычислительной техники и автоматизированных систем». На основе аппроксимированных характеристик нелинейных полупроводниковых приборов Комплекс моделирует функционирование электронных устройств от генераторов цифровых сигналов до логических элементов.

Введение

Назначением комплекса является создание педагогических условий для углубления понимания студентами основополагающих принципов работы электронных устройств за счет практического исследования их функционирования. Одновременно студенты могут получить представление об имитационном моделировании.

Очевидно, что теоретические знания, получаемые студентами при изучении дисциплин «Информатика», «Электротехника и электроника», может быть существенно углублены при выполнении лабораторных работ, позволяющих на практике освоить фундаментальные принципы цифровой электроники. Однако применение лабораторных установок, во-первых, не предусмотрено учебными планами дисциплин, во-вторых, трудоемко и дорогостояще, и, в-третьих, не соответствует указанной специальности, предусматривающей преимущественную работу с программными, а не аппаратными средствами ВТ. Следовательно, *актуальной* представляется разработка программного «виртуального» лабораторного комплекса, позволяющего выполнить необходимые работы за счет имитации функционирования реальных установок.

Таким образом, *целью разработки* является повышение мотивации студентов, обучающихся по указанной и родственным специальностям СПО или ВПО, к изучению основ построения компьютеров как устройств электронной цифровой обработки информации.

Для достижения цели техническим заданием предусмотрено решение следующих *задач*:

- Комплекс должен состоять из последовательности лабораторных работ, содержание которых должно соответствовать логике изучения теоретического материала дисциплин «Информатика» и «Электрика и электроника»;
- Комплекс должен быть создан в программной имитационной среде и опираться на самостоятельное изучение студентами соответствующего программного обеспечения;
- в качестве метода имитации следует применить имитационное моделирование;
- каждая лабораторная работа должна предусматривать теоретическую, в том числе математическую, подготовку к ее выполнению;
- каждая последующая лабораторная работа должна опираться на знания и умения, полученные в результате выполнения предыдущей;
- должен быть разработан комплект методических указаний по выполнению работ, в котором указаны цели и задачи, описан порядок выполнения, приведены требования по содержанию и оформлению отчета.

Разработка и структура лабораторного комплекса

В соответствии с техническим заданием Комплекс обеспечивает имитацию работы электрических схем исследуемых узлов, рекомендованных для изучения программами дисциплин и соответствующей учебной литературой. Имитация выполнена программными средствами специализированного пакета LabView на основе математических моделей, вывод которых включен в теоретический материал указанных дисциплин. Выбор пакета LabView обусловлен требованием применения унифицированной программной среды с другими «виртуальными» лабораторными комплексами, разрабатываемыми для единого учебно-методического комплекса (УМК): универсальность LabView обеспечивается развитой библиотекой типовых элементов, встроенностью языка программирования, наличием разнообразных средств индикации, визуализации и управления и т.п.

Комплекс состоит из последовательности связанных между собой лабораторных работ, выполняемых на соответствующих установках, причем каждая последующая лабораторная работа предусматривает использование знаний, полученных в результате выполнения предыдущей.

Лабораторные установки содержат лицевую и монтажную панель. Лицевая панель предназначена для непосредственной работы студентов. На ней размещено изображение изучаемого электронного узла с обозначенными параметрами, элементы управления и индикации. На монтажной панели, скрытой во время выполнения работ, размещены программные имитационные модули, «собранные» в подлежащие исследованию узлы. Исследования осуществляются в соответствии с разработанными методическими материалами, содержащими ссылки на теоретический материал и необходимые указания по их выполнению, формам представления и анализу результатов, составлению отчетов.

Комплекс обеспечивает изучение двух тем: «Формирование цифровых сигналов» (лабораторные работы №1 и №2), «Реализация логических функций» (лабораторные работы №3, №4, №5).

Формирование цифровых сигналов

Лабораторная работа №1 выполняется в два этапа.

1. Формирование цифровых сигналов.
2. Исследование зависимости характеристик цифрового сигнала от параметров электронной цепи.

Оба этапа выполняются на установке №1, содержащей простейший транзисторный каскад (рис. 1). В лабораторной работе №2 изучается транзисторный каскад с элементом отрицательной обратной связи (установка №2), изображенный на рис. 2.

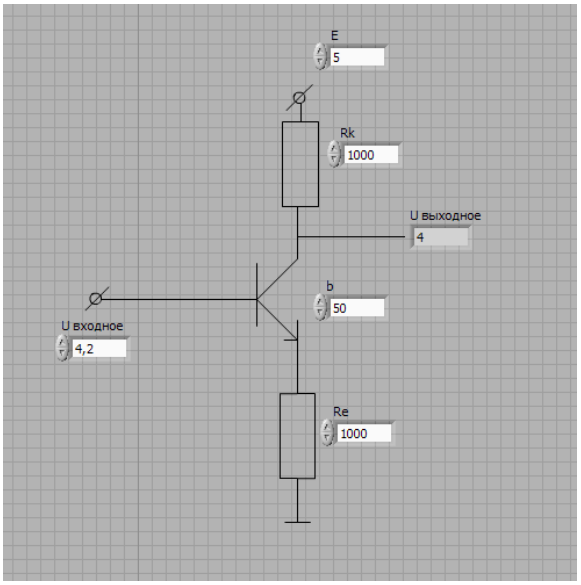


Рис. 1. Схема транзисторного каскада на лицевой панели установки №1

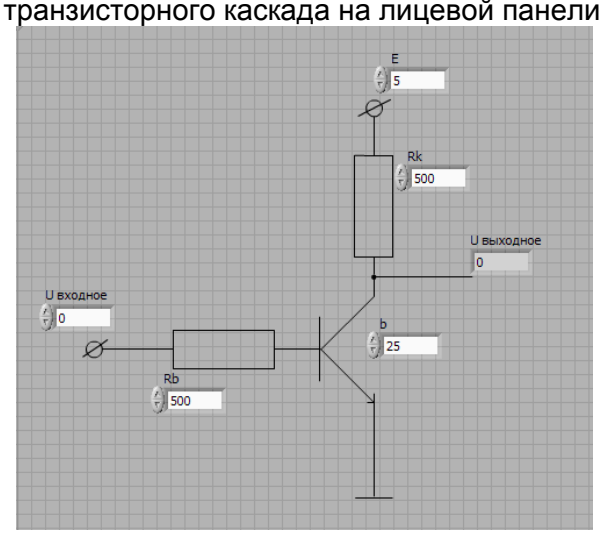


Рис. 2. Схема транзисторного каскада с элементом отрицательной обратной связи на лицевой панели установки №2

Теоретическая база темы – физическое представление логических значений «0» и «1» в ТТЛ; законы Ома и Кирхгофа; характеристики и режимы работы линейных радиоэлементов и нелинейных полупроводниковых приборов; понятие временной диаграммы электрических сигналов; математическая модель транзисторного каскада, разработанная на основе ступенчатой аппроксимации вольтамперной характеристики диодов.

Реализация логических функций

В лабораторных работах №3, №4 и №5 представлены к изучению транзисторные каскады, реализующие логические функции «НЕ» (установка №1, рис. 1), «ИЛИ-НЕ» (установка №3, рис. 3), «И-НЕ» (установка №4). Теоретическая база исследования – логические функции инверсии, дизъюнкции и конъюнкции.

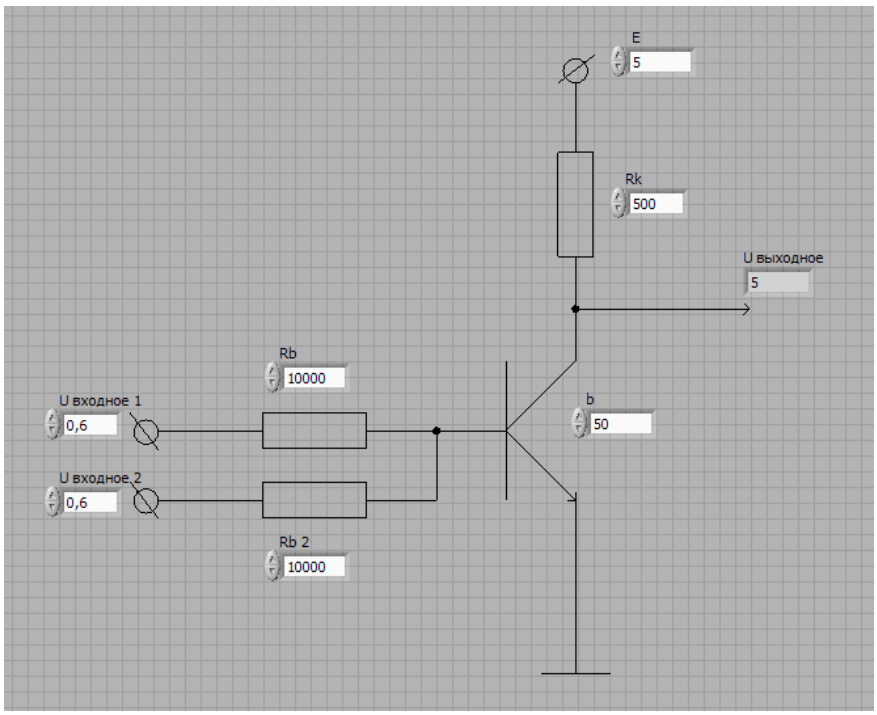


Рис. 3. Схема транзисторного каскада на лицевой панели установки №3

Математический аппарат исследования

Для каждой лабораторной работы создана математическая модель, основанная на аппроксимации параметрических характеристик полупроводниковых приборов, и разработаны в программной среде LabVIEW соответствующие имитационные программы.

Имитационная программа лабораторных работ №1 и №3:

1. float k;
2. float C;
3. k=(b*Rk)/Rb;
4. C=E+k*0.6;
5. uOut=C-k*uInput;
6. if(uInput<0.6) uOut=E;
7. if(uOut<0.4) uOut=0.4;

Имитационная программа лабораторной работы №2:

1. float k;
2. float C;
3. float uE;
4. uE=uInput-0.6;
5. k=(b/(b+1))*(Rk/Re);
6. C=E+k*0.6;
7. uOut=C-k*uInput;
8. if(uInput<0.6) uOut=E;
9. if(uOut-uE<=0.4) uOut=uE+0.4;

Где K и C – коэффициенты

Имитационная программа лабораторной работы №4:

1. if (mode==1)
2. U2=5
3. U1=Uc
4. end
5. if (mode==2)
6. U1=5

```
7.  U2=Uc
8.  end
9.  if (mode==3)
10. U1=Uc
11. U2=Uc
12. end
13. Ib=(Uinput-(Uc+6/10))/Rb;
14. if ((Uc+6/10)>Uinput)
15. Ib=0
16. end
17. Ik=Ib*b;
18. Uout=((Uc-Uinput-6/10)/(Rb2*(E-
    1)-Rk*(1-6/10)))*Rk*Rb2/Rb;
19. if (Uout-Uc<4/10)
20. Uout=Uc+4/10
21. end
22. k=(b2*Rk2)/Rb2;
23. C=E2+k*6/10;
24. Uout2=C-k*Uout;
25. if (Uout<6/10)
26. Uout2=E2
27. end
28. if (Uout2<4/10)
29. Uout2=4/10
30. End
```

Имитационная программа лабораторной работы №5:

```
1. Ib=((U1-6/10)/Rb1)+((U2-6/10)/Rb2);
2. if(Ib<0)
3. Ib=0
4. end
5. Uout=E-Ib*b*Rk
6. if(Uout<4/10)
7. Uout=4/10
8. end
```

Заключение

В качестве эксперимента Комплекс был предложен для опробования двум учебным группам студентов факультета СПО. Результаты проведенных лабораторных работ позволяют сделать вывод о достижении поставленной цели. Эффективность его внедрения подтверждается многочисленными отзывами студентов. В то же время выявлена целесообразность развития Комплекса в двух направлениях расширения – «Интегральные схемы» и «Шинные формирователи и приемопередатчики цифровых сигналов».

Литература

1. Петров К.С. Технология. Радиоматериалы, радиокомпоненты и электроника: учебное пособие. – 2004. –522 с.
2. Безуглов Д.А., Каленко И.В. Цифровые устройства и микропроцессы. – Феникс, 2006. – 480 с.
3. Лагин В.И., Савелов Н.С. Электроника. – Феникс, 2004. – 576 с.
4. Суранов А.Я. LabView 7: справочник по функциям. – ДМК Пресс, 2005. – 512 с.
5. Тревис Дж. LabView для всех. – ДМК Пресс; ПриборКомплект, 2005. – 533 с.
6. Бутырина П.А. Автоматизация физических исследований и эксперимента: компьютерные измерения и виртуальные приборы на основе LabView 7. – ДМК Пресс, 2005. – 264 с.

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ РЕЙТИНГОВОЙ СИСТЕМЫ ОЦЕНИВАНИЯ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ

Д.Г. Киреев, К.А. Кузьмин, П.В. Левин
Научный руководитель – к.т.н., доцент Н.Н. Горлушкина

В статье рассматриваются основные преимущества и недостатки рейтинговой системы оценивания: как влияет использование рейтинговой системы на успеваемость студентов и объективность оценивания, уровень образовательного процесса в вузе. Для объективного представления информации и составления общественного мнения использовался такой простой инструмент, как социологический опрос. По его результатам составлено общее отношение студентов к такой форме измерения знаний. В заключение была консолидирована проработанная информация и дана общая оценка изученной проблеме.

Введение

Россия в 1999 г. подписала Болонскую декларацию, основным принципом которой является формирование единого образовательного процесса в Европе. В вузах страны в связи с участием в Болонском процессе пересматривается сущность всех компонентов педагогического процесса – целей, содержания, форм, методов, системы контроля и оценивания учебных достижений студентов. Заметным новшеством для российских студентов является рейтинговая система контроля и оценивания знаний, умений и навыков.

Английское слово rating имеет несколько значений. В контексте оценки качества обучения одно из них – оценивание при присвоении каждому объекту числового показателя. При сравнении рейтинга с традиционной системой оценивания вытекает ряд психологических и организационных нововведений, связанных с кардинально новым подходом к текущему и итоговому контролю успеваемости обучающихся.

- Что именно оценивать и по каким алгоритмам?
- Кто должен определять критерии оценки?
- Достаточен ли рейтинг для итогового контроля усвоения знаний?
- Действительно ли рейтинговая оценка проводится независимо от личности преподавателя и субъективного его отношения к студенту?
- Как учитывать творческие успехи студента?
- Мотивирует ли рейтинговая система студента для лучшего усвоения знаний?

Таким образом, следует выявить многие «подводные камни» подобной методики. Известно много рейтинговых систем оценки результатов обучения, используемых в учебных заведениях разных стран. У них есть и общие черты, и различия. Иногда эти системы не оправдывают вложенных в свое создание усилий, иногда позитивно влияют на качество образования. История рейтинговых систем измеряется десятилетиями. Общепризнанной рейтинговой модели нет. Тем не менее, такая система должна быть внедрена в вузах нашей страны в ближайшее время с целью формирования единой системы оценивания знаний студентов на территории стран, подписавших Болонскую декларацию.

Преимущества и недостатки рейтинговой системы

Возросшие требования к выпускникам профессиональных учебных заведений в связи с появившейся конкуренцией на рынке труда требуют от преподавателей разработки и внедрения таких инновационных направлений, которые обеспечивали бы высокое качество подготовки специалиста. Рейтинг используется везде, где есть необходимость сравнивать результаты деятельности людей. Рейтинг всегда подразумевает конкурсность, соревнование. Главные задачи рейтинговой системы заключаются в повышении мотивации студентов к освоению образовательных программ путем более вы-

сокой дифференциации оценки их учебной деятельности, а также повышении уровня организации образовательного процесса в вузе.

Какие же положительные стороны можно отметить в использовании рейтинговой системы оценивания?

Прежде всего, стоит сказать о стимулировании и активизации учебного труда обучающихся. Рейтинговая система способна не только детализировать основные показатели качества знаний учащихся, но и поддерживать своевременность выполнения заданий, ритмичность прохождения программ, качество усвоения предмета [1]. По этой системе весь курс разбивается на отдельные блоки, которые оцениваются предварительно заданными баллами. Рейтинговая система контроля включает в себя оценку различных видов учебной деятельности, имеющих разную «стоимость». Учащийся знакомится с условиями рейтинговой системы оценки знаний в начале учебного года. Задача каждого учащегося – набрать больше баллов. При этом стимулируется максимально возможный интерес учащихся к конкретному предмету, а, следовательно, и к дисциплине в целом, а также стремление сдать работу в конкретно заданные сроки, чтобы не быть в «отстающих» и получить максимально возможное количество баллов. Каким образом учащийся может считать свою деятельность успешной? Когда его ожидания, усилия, направленные на выполнение задачи, находятся в оптимальном соотношении с положительными результатами и оценкой его труда. Ведь из практики известно, что успех приносит удовлетворение только ценой особых усилий, напряжения умственной и физической деятельности. Таким образом, стирается явное противоречие между объемами трудозатрат на учебную деятельность и результатами, оценкой этого труда. Чем больше затраченных усилий, тем больше вероятность получить высокий результат, тем выше уровень удовлетворения от успешного выполнения поставленной задачи. Меняется уровень самооценки, появляется стремление к достижению новых побед. А это и есть стимул к активному, продуктивному и творческому процессу обучения. Можно сказать, что повышается мотивация систематического обучения, активность к самостоятельным занятиям**.**

Следующим плюсом рейтинговой системы является активизация научно-исследовательской деятельности. Развиваются элементы творчества и самоанализа, учащиеся стремятся переосмыслить те или иные понятия с учетом собственного опыта. Здесь важно рассмотреть совершенно новый уровень поведения учащегося в направлении более продуктивной и активно-поисковой деятельности. Главное назначение рейтингового контроля знаний – это ранжирование по успешности усвоения изученного материала [2]**.** Студенты, которые не смогли справиться со всеми текущими заданиями, могут в конце семестра набрать баллы, протестировав себя по различным модулям теоретического материала. Рейтинговая система – это регулярный контроль качества усвоения знаний и умений в учебном процессе, выполнения планового объема самостоятельной работы. Ведение многобалльной системы оценки позволяет, с одной стороны, отразить в определенном балльном диапазоне индивидуальные особенности студентов, а с другой – объективно оценить в баллах усилия студентов, затраченные на выполнение отдельных видов работ. В систему рейтинговой оценки включаются дополнительные поощрительные баллы за оригинальность, новизну подходов к выполнению заданий для самостоятельной работы или разрешению научных проблем. У студента имеется возможность повысить учебный рейтинг путем участия во внеучебной работе (участие в олимпиадах, конференциях; выполнение индивидуальных творческих заданий, рефератов; участие в работе научного кружка и т.д.). Так каждый вид учебной деятельности приобретает свою «цену», а рейтинговая система, по сути, является количественной оценкой качества обученности студента [5].

Использование рейтинговой системы позволяет добиться систематического посещения занятий. Ведь процесс обучения охватывает всех учащихся, при этом их поведе-

ние оценивается преподавателем и «коллегами по парте». Возникает возможность для честной конкуренции среди студентов и как результат – стремление улучшить свой результат. Если экзамен не является единственным инструментом оценки, а также учитываются и результаты работы в течение семестра, то вероятность «проскользнуть» на следующий этап обучения станет проблематичной – преподаватель будет вынужден оценивать работу студента на семинаре, практических и контрольных занятиях более объективно.

Наличие возможности просто и регулярно в любой момент времени получить информацию о набранном рейтинге и своих успехах позволяет студенту управлять учебным процессом по изучению отдельных дисциплин**.** Каждый студент вправе сам выбирать, какие работы ему выполнять, а какие – нет. При этом существует возможность выполнять дополнительные работы, за которые начисляются баллы. Таким образом, происходит дифференцирование значимости оценок, полученных студентом за выполнение различных видов работ (самостоятельных, контрольных, лабораторных), отражение текущей или итоговой оценкой количества вложенного учеником труда, направленного на освоение изучаемой дисциплины [4].

Для преподавателя рейтинговая система оценки знаний важна, так как систематическое оценивание позволяет преподавателю более объективно выставлять зачетные и экзаменационные оценки. Кроме того, если существует некий график успеваемости, можно делать важные выводы о необходимости изменений в учебном процессе, составить для каждого студента индивидуальную образовательную линию, что позволит сделать учебный процесс более гибким и мобильным. Таким образом, такая работа позволяет преподавателю раскрыть свои педагогические возможности и воплотить свои идеи совершенствования учебного процесса в жизнь. Введение строгих временных рамок, отведенных для выполнения задания, позволяет снизить количество работ, оставленных студентами «на потом». При этом осуществляется оценивание проделанной работы определенным количеством баллов в соответствии со своевременностью сдачи этой работы. Естественно, пропадает желание сдавать работу позже и получить за нее более низкий балл. Но при этом возникает стремление сделать работу, несмотря на то, что срок вышел, так как за нее можно получить определенное количество баллов. То есть использование рейтинговой системы позволяет добиться более ритмичной работы студента в течение семестра.

Однако, несмотря на все свои плюсы, рейтинговая система оценки знаний имеет и ряд недостатков. Одним из главных недостатков является нехватка дидактического материала по использованию такой системы для конкретной дисциплины, т.е. отсутствие конкретных критериев оценивания, и как результат – субъективное оценивание. Проблема разработки системы весовых коэффициентов для каждого из видов учебной деятельности в рамках каждого модуля и всей учебной дисциплины – четко не определены условия применения и значения для определенной дисциплины. Определение основных видов деятельности для учебной дисциплины вызывает проблему неопределенности в выставлении верхнего предела баллов, необходимых для получения наивысшего результата по изучаемому предмету. Таким образом, основной недостаток рейтинговой системы – реализация ее на практике.

Другой отрицательной стороной рейтинговой системы является отсутствие алгоритмов определения псевдоцелей студентов – не углубление знаний, а гонка за количеством баллов, которая может способствовать не активизации научно-исследовательской деятельности и самостоятельной работы, а стремлению «подготовить» материал в короткие сроки перед коллоквиумом или семинаром, а потом забыть его. При этом, конечно, уже не идет речи о глубоком анализе и детальной проработке материала. Однако многоэтапность рейтинговой системы позволяет отследить таких участников учебного процесса и принять соответствующие меры по пресечению такого

образовательного процесса. Если и существует такая проблема, то только на начальных этапах обучения, ибо без глубокого анализа фундамента образовательные блоки могут дать трещину и, в конце концов, развалиться. При этом не будет достигнута и одна из основных целей получения высшего образования – представление четкой картины мира и процессов, происходящих в нем.

Процесс перехода к другой системе оценивания является трудным не только для студентов, но и для преподавателей. Одна из причин этого явления, с нашей точки зрения, – отсутствие адаптации программы курсов к новым условиям работы. К примеру, увеличение числа контрольных точек до двух в семестр вместо одной, когда нет времени (уже конец семестра) на исправление результата. Другая причина – нежелание преподавателя оценить работу студента. Кроме этих причин, у преподавателя могут возникнуть трудности при оценке в баллах контрольных мероприятий, существует увеличение нагрузки на преподавателя при проведении занятий (необходимо разрабатывать новые тестовые задания), а также дополнительная работа по ликвидации большого количества неудовлетворительных оценок (разработка дополнительных баллов в виде бонусов или дополнительных мероприятий) [3].

Общественное мнение

Чтобы узнать отношение студентов СПбГУ ИТМО к системе рейтингового оценивания, был проведен опрос среди студентов кафедры ТПО (среди первого и четвертого курсов). Первые два вопроса затрагивали общее отношение студентов к данной системе, а также показывали уровень ее реализации непосредственно в нашем университете. Третий вопрос был сделан открытым для того, чтобы каждый мог указать наиболее важные, на его взгляд, преимущества и недостатки. Результаты проведенного опроса приведены на рис. 1–4.

В ходе опроса студентами были также выделены основные, на их взгляд, преимущества и недостатки системы рейтингового оценивания.

Преимущества:

- плотный контроль учебного процесса;
- система позволяет выявить наиболее подготовленных студентов и откровенных разгильдяев;
- автоматизация системы оценивания;
- стимуляция выполнения учебных задач в заданные сроки.

Вопрос №1: **Как вы относитесь к идее системы рейтингового оценивания?**

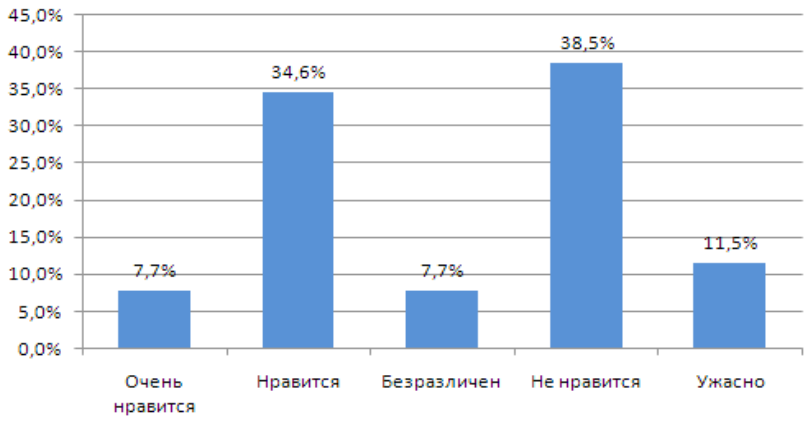


Рис. 1. Результат среди студентов 1-го курса

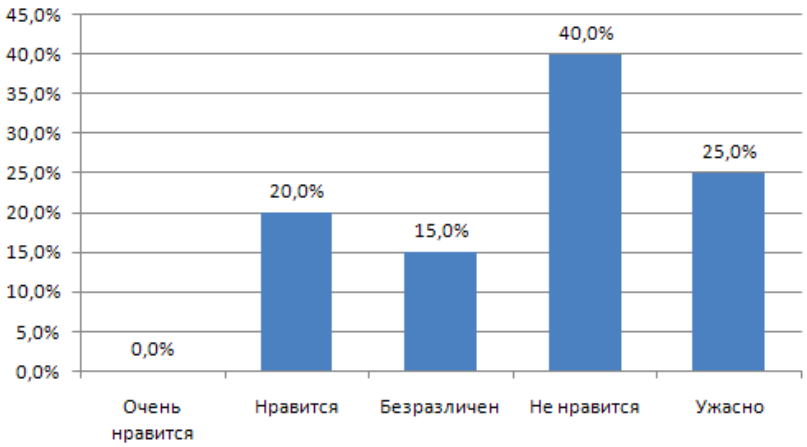


Рис. 2. Результат среди студентов 4-го курса

Вопрос №2: **Оцените по пятибалльной шкале уровень реализации этой системы в нашем университете.**

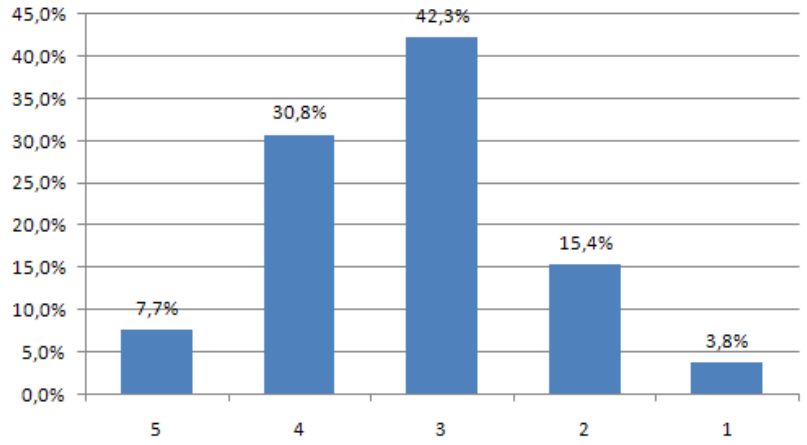


Рис. 3. Результат среди студентов 1-го курса

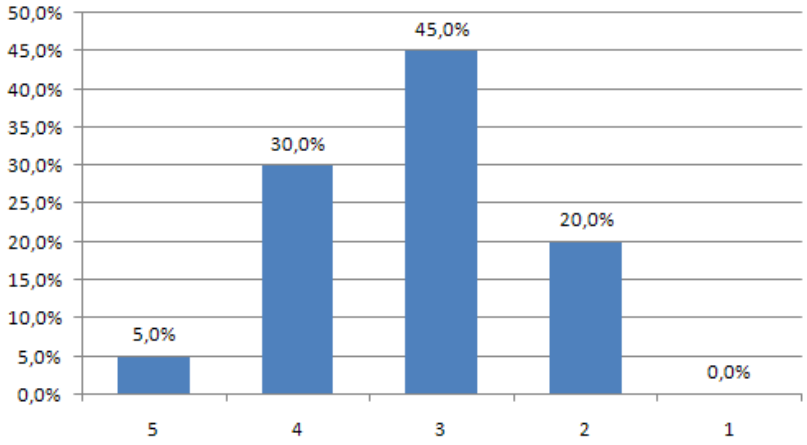


Рис. 4. Результат среди студентов 4-го курса

Недостатки:

- не учитываются индивидуальные особенности студента;
- оценивание посещаемости;
- техническая база;
- субъективность оценивания;
- не всегда адекватно показываются реальные знания студентов и их потенциальные возможности;

- недостаток свободного времени;
- невозможность скомпенсировать потерянные баллы;
- практически нет возможности совмещения учебы и работы;
- неподготовленность преподавателей к данной системе;
- цель – не научиться чему-либо, а набрать баллы.

В целом результаты опроса наглядно показали общее отношение опрошенных студентов к рейтинговой системе. Несмотря на то, что отношение студентов 1-го курса к системе более лояльное, необходимо учитывать тот факт, что у студентов 4-го курса больший опыт взаимодействия с подобным методом оценивания учебной деятельности (не модульной, а именно рейтинговой системой). Таким образом, большинство опрошенных негативно относятся к предмету обсуждения и оценивают уровень ее реализации применительно к нашему университете в среднем на 3 балла.

Заключение

Использование рейтинговой системы оценивания студентов направлено на повышение качества учебного процесса. Однако на данный момент с помощью этой системы происходит не столько повышение качества, сколько автоматизация учебного процесса и оценка знаний студента на каждом этапе обучения по той или иной дисциплине.

Безусловно, рейтинговая система нуждается в дальнейшей доработке и совершенствовании. Несмотря на то, что оценивание каждого этапа обучения, а также таких моментов, как посещаемость и выполнение заданий строго в определенный срок, позволяет более точно оценить знания и отношение обучающихся к тому или иному предмету, данная система все равно не до конца учитывает индивидуальные особенности каждого студента, а также не исключает субъективной оценки его деятельности со стороны преподавателя. Кроме того, необходима единая система оценивания по всем дисциплинам, которая на данный момент отсутствует. Преподаватели должны выставлять баллы по заранее определенным правилам, а не по собственным. В противном случае система рейтингового оценивания практически ничем будет отличаться от старой пятибалльной системы.

Но наиболее важным моментом является то, что с введением такого способа оценивания образовательный процесс для большинства теперь ориентирован на получение баллов, а не знаний.

Литература

1. Маруда Т.Ю. Педагогическая наука и образование в России и за рубежом: региональные, глобальные и информационные аспекты [Электронный ресурс]. Выпуск №2 2006. Раздел 3. Педагогика, дидактика, лингвокультурология. – Режим доступа: http://rspu.edu.ru/university/publish/pednauka/2006_2/Maruda.htm, свободный.
2. Internet школа Института повышения квалификации работников образования. Урок «Подходы к оценке образовательных достижений учащихся в универсальном образовании» [Электронный ресурс]. – Режим доступа: http://www.prosv-ipk.ru/demo/245614?page=2, свободный.
3. Сорокина Т.П., Сорокин Б.П., Баранова В.К. Анализ балльно-рейтинговой системы контроля знаний // Международная заочная научная конференция Красноярского государственного аграрного университета – 15.10.2007 г.
4. Сероусов И.Ю. О рейтинговом методе преподавания. – Брянск, 2001.
5. Тешев Р.Ш. Положение о рейтинговой системе оценки знаний учащихся. – Нальчик, 2000.

ПРЕДСТАВЛЕНИЯ СТУДЕНТОВ О РЫНКЕ ТРУДА И ИХ АДАПТАЦИЯ К РЕАЛЬНОСТИ

О.В. Зеленская
Научный руководитель – к.т.н., ст.н.с., Н.Н. Горлушкина

Каким представляют себе рынок труда студенты? Насколько их представления соответствуют действительности? Нужно ли более детальное знакомство с рынком труда для студентов вузов во время обучения? В сложившейся ситуации система профессионального образования призвана найти способы преодоления кризиса, осуществить профессиональную адаптацию молодежи к новым жизненным условиям, повысить их профессиональную мобильность и уверенность на рынке труда.

Образованность и интеллект все больше относятся к разряду национальных богатств, а духовное здоровье человека, разносторонность его развития, широта и гибкость профессиональной подготовки, стремление к творчеству и умение решать нестандартные задачи превращаются в важнейший фактор прогресса страны. Исходя из этого, главной целью образования является формирование разносторонне развитой личности, способной реализовать творческий потенциал в динамичных социально-экономических условиях как в собственно жизненных интересах, так и в интересах общества. Профессиональное образование рассматривается как процесс, направленный на рост социальной и профессиональной мобильности личности, расширение возможностей компетентного выбора личностью жизненного пути и на развитие личности.

Высшее профессиональное образование имеет целью подготовку и переподготовку специалистов соответствующего уровня, удовлетворение потребностей личности в углублении и расширении образования на базе среднего (полного) общего, среднего профессионального образования.

Исследование положения выпускников вузов дает возможность представить обзор трудностей, с которыми приходится сталкиваться молодым специалистам на рынке труда. Недостатки в системе воспроизводства трудового потенциала, противоречивый характер социально-экономических реформ отрицательно сказывается на положении выпускников высшей школы. Перед ними встают проблемы, связанные с трудоустройством и безработицей, с необходимостью переподготовки и психологической неготовностью к ней, с невостребованностью знаний, недостаточным качеством подготовки. Моральное и материальное стимулирование профессионального роста и труда также оставляет желать лучшего. Печальный вывод из вышеизложенного: прямая связь между образованием и устойчивостью положения работника отсутствует. Покидая вуз, выпускник оказывается социально незащищенным.

Сфера труда – важная и многоплановая область экономической и социальной жизни общества. Она охватывает как рынок рабочей силы, так и ее непосредственное исследование в общественном производстве. На рынке труда получают оценку стоимость рабочей силы, определяются условия ее найма, в том числе величина заработной платы, условия труда, возможность получения образования, профессионального роста, гарантии занятости и т.д. Рынок труда отражает основные тенденции в динамике занятости, ее основных структурах, также мобильность рабочей силы, безработицу.

Рынок труда является одним из наиболее сложных рынков, которые существуют и функционируют. Отличие от других рынков состоит в том, что здесь объектом контрактов выступает сам человек, его способность к труду. Рынок труда, как и любой другой рынок, описывается кривыми спроса и предложения, т.е. в целом подчиняется законам спроса и предложения. Он представляет собой рынок особого рода, имеющий ряд существенных отличий от других товарных рынков. Здесь регуляторами являются не только макро- и микроэкономические факторы, но и многие факторы социального и социально-психологического характера. Поэтому рынок труда – элемент экономических и социальных отношений, характер и содержание процессов, происходящих на

нем, в конкретный промежуток времени обусловлены характером и содержанием процессов, происходящих в политике, экономике, социальной сфере общества. Задачу устранения или смягчения действия факторов, порождающих безработицу, а также смягчения негативных последствий безработицы можно решить только, если политика занятости станет частью социально-экономической политики.

Руководителей вузов интересуют представления студентов о возможностях собственной социализации в первые годы после окончания вуза и связанной с этим мотивацией учебной и профессиональной деятельности; этой проблеме было посвящено исследование, проведенное в МГТУ им. Н.Э. Баумана в 2003 году [3].

Целью его было выявление и соотнесение трех компонентов: мотивов обучения в вузе, представлений о возможностях профессионального самоопределения через три года после окончания вуза, некоторых основных характеристик личности. Выявилась тенденция: чем более выражена у студентов установка на высокий уровень социальной мобильности, тем более значимыми в их структуре мотивации обучения предстают мотивы – стать дипломированным специалистом в узкой области, приобрести полезные связи и знакомства, хорошо зарабатывать, материально обеспечивать себя и свою семью, занять высокую руководящую должность. Низкие места занимают такие мотивы, как приобретение научных знаний, получение ученой степени, открытие или создание чего-то нового.

Наиболее типичным для всей обследованной выборки студентов является предположение о том, что будущая работа будет близка к полученной в вузе специальности. Таких студентов 62,1%. Именно они характеризуются установкой на средний уровень профессиональной мобильности, ориентированы главным образом на карьеру грамотного, добросовестного специалиста. Самой же малочисленной является группа с установкой на высокий уровень профессиональной мобильности. Входящие в нее в наибольшей степени ориентированы на успех, психологически готовы к жесткой конкурентной борьбе. Этих студентов в обследованной выборке 15,5%. Промежуточную по величине группу составляют студенты, имеющие установку на низкий уровень профессиональной мобильности, – 22,4%. Свою будущую профессиональную деятельность они рассматривают как способ самореализации, возможность заниматься любимым делом. Результаты этой деятельности и ее общественная оценка их мало волнуют [3].

Можно констатировать, что наиболее типичным для обследованной выборки студентов является ожидание того, что через 3 года после вуза их ежемесячный заработок будет находиться в интервале от 300 до 1000 долл. Таких студентов 81,1%. Небольшая группа студентов – 8,6% – ориентирована на ежемесячный заработок через 3 года после вуза в размере, не превышающем 300 долл. Относительно также небольшая группа студентов – 10,3% – ожидает, что через 3 года после вуза ежемесячный заработок будет превышать 1000 долл. Эти наиболее социально и психологически адаптированные студенты ориентированы на научную карьеру, которая рассматривается ими, скорее всего, как продолжение семейной традиции.

Студенты предполагают следующие четыре варианта развития событий: а) работа на том же месте, что и сразу после вуза, и характер ее непосредственно связан с полученной в вузе специальностью; б) смена одного места работы, и характер ее близок к полученной в вузе специальности; в) смена одного места работы при условии полного несовпадения ее характера с полученной в вузе специальностью; г) смена двух и более мест работы при условии непосредственной связи ее с полученной в вузе специальностью.

Из полученных ответов следует, что студенты более готовы к смене места работы, чем к получению новой специальности. Приобретение новой специальности для них как бы идет на шаг позади установки смены места работы. Данная логика достаточно

ясна: приобретение новой специальности все же является более трудоемким занятием, чем поиск нового места работы [3].

Активная социальная адаптация и трудоустройство молодежи всегда решались через взаимодействие системы профессионального образования, обеспечивающей готовность молодежи осуществлять профессиональную деятельность и потребностями народного хозяйства в молодых специалистах. В период реформ отраслевые связи были разрушены, а механизм, отвечающий современным требованиям ситуации и обеспечивающий оптимальное взаимодействие системы профессионального образования с народным хозяйством, на сегодняшний день отсутствует. Резко увеличилось количество безработных, почти полностью разрушились существовавшие между образовательными учреждениями и предприятиями учебно-производственные связи, а также система трудоустройства молодых специалистов.

Профессиональное самоопределение – это определение человеком себя относительно выработанных в обществе (и принятых данным человеком) критериев профессионализма. Один человек считает критерием профессионализма просто принадлежность к профессии или получение специального образования, соответственно, и себя оценивает с этих позиций. Другой человек полагает, что критерием профессионализма является индивидуальный творческий вклад в свою профессию, обогащение своей личности средствами профессии, соответственно, он иначе, с более высокой планки себя самоопределяет и далее самореализует [3].

Профессиональное самоопределение – это процесс формирования личностью своего отношения к профессионально-трудовой среде и способ ее самореализации. Это длительный процесс согласования внутриличностных и социально-профессиональных потребностей, который происходит на протяжении всего жизненного и трудового пути. Профессиональное самоопределение предполагает выбор карьеры, сферы приложения сил и личностных возможностей [3].

По результатам исследования [5] было определено, что существуют различия в образе мышления студентов естественнонаучного, гуманитарного, технического профиля, что обосновано сферой предстоящей деятельности и системой подготовки специалистов. Так, студенты гуманитарных факультетов наиболее мобильны, уверены в своих силах и считают возможным трудоустроиться по смежной специальности. Однако нет необходимости аргументировать тезис о том, что, несмотря на бум экономических и юридических специальностей, облик грядущего общества все же в значительной мере определяют именно те, кто прямо связан с высокими технологиями и сетевыми информационными структурами, т.е. нынешние студенты университетов технического типа.

В современных условиях рынка труда способность обучаться становится важнее способности трудиться. Знания об окружающем мире и себе самом дают большую уверенность в собственных силах, способности самообразования. Таким образом, более глубокое изучение психологии, философии с хорошей технической базовой подготовкой дают шанс на мобильность, что подтверждают данные некоторых исследований [6].

Вопрос перспективы трудоустройства не решен в силу того, что в практике обеспечения занятости молодежи технологии трудоустройства устарели, и большинство учащихся полагаются на помощь родителей, друзей, знакомых в решении этого вопроса.

Обучение профессиональной деятельности и степень готовности молодого специалиста к работе следует рассматривать в связи с жизненными планами, социальными ориентациями, диспозициями личности, что, в свою очередь, позволит решить вопрос о качестве обучения студентов, качестве производственной деятельности молодых специалистов. В целях снижения адаптационного периода следует определить факторы успеха профессиональной деятельности студента, слагаемые его профессионализма в условиях рынка труда еще во время обучения.

Существенные изменения во всех сферах социальной и духовной жизни общества отражаются на формировании личности молодого человека. С одной стороны, у молодежи отсутствуют стимулы социальной активности, наблюдается резкий спад интереса к учебе, труду, проявляется эгоизм, агрессивность, жестокость, с другой – рост деловитости молодежи, ее предприимчивости, рачительное отношение к делу и т.д. Осознанным становится для них стремление соответствовать современным требованиям: энергичность, оптимизм, ответственность. Большинство молодых людей связывают успехи в жизни с хорошим образованием. Запланированная молодым человеком жизненная и профессиональная перспектива является мощным стимулом самопознания, самовоспитания, самореализации, самоконтроля. Особенностью формирования профессионального самоопределения студентов является непрерывность процесса формирования профессионального самоопределения в системе «школа–вуз», неуверенность молодежи в возможности работать по приобретенной профессии, существование у студентов нескольких профессиональных планов, необходимость рассмотрения жизненных перспектив студентов в соотношении с получаемым образованием.

Сформировался новый тип студенческой молодежи, которая предъявляет к высшему образованию высокие требования, рассматривая его в качестве гаранта своей профессиональной деятельности, и при этом сама проявляет в выборе жизненного пути социальную активность.

Рынок труда требует, чтобы при подготовке специалистов у них формировались не только профессиональные качества, но также личностные качества, как коммуникативность, способность к самообразованию, широта интересов.

Из повседневного опыта известно, что основным средством достижения и поддержания желательного (или приемлемого) для каждого конкретного человека уровня жизни, его потенциальных возможностей, достижения самостоятельности поведения и адаптируемости к реальным социально-экономическим условиям является профессиональная деятельность человека. Необходимым условием ее успешности является наличие у человека соответствующего образования, точнее, профессионального образования. Таким образом, готовность к профессиональной деятельности - психическое состояние, предстартовая активизация человека, включающая осознание человеком своих целей, оценку имеющихся условий, определение наиболее вероятных способов действия; прогнозирование мотивационных, волевых, интеллектуальных усилий, вероятности достижения результата, мобилизацию сил, самовнушение в достижении целей [2].

Определение научного смысла адаптации личности возможно только на основе понятия онтогенетической социализации, если оно, в свою очередь, правильно отражает тот реальный и сложный процесс, благодаря которому индивид превращается в личность, обладающую некоторыми основными чертами личностной зрелости. Социализация понимается, с одной стороны, как усвоение индивидом социального опыта путем вхождения в социальную среду, систему социальных связей, а с другой стороны, процесс воспроизводства системы социальных связей индивидом за счет его активной деятельности, активного включения в социальную среду [4].

Адаптация является одной из сторон процесса социализации, который непременно переживает каждый индивид в ходе своего взросления. Собственно социализация определяется как процесс влияния социальных условий на жизнедеятельность индивида с целью включения его в качестве дееспособного субъекта в систему общественных отношений [4].

По результатам исследования [7] можно сказать, что молодые люди изначально настраиваются отнюдь не на трудовую деятельность, а на те возможности, которые может предоставить социальный статус обладающего специальностью.

При определении представлений об успехе в жизни подавляющим количеством респондентов был отмечен фактор наличия связей, возможности все достать – 80 %,

затем идут признание, слава – 60%, самостоятельность, свобода – 58%. Отношение выпускников к выбранной специальности и перспективы их трудоустройства выражаются, как ни странно, в отношении студентов к вузу, к организации и качеству учебного процесса в вузе.

Становление личности специалиста в вузе имеет два аспекта: 1) профессионально-ролевую социализацию личности и 2) профессионализацию как определенную степень овладения личностью профессиональной деятельностью, специальностью. В этом смысле становление личности профессионала осуществляется через его профессиональную социализацию и профессионализацию, а механизмом такого становления личности выступает ее профессиональная адаптация.

В самом общем плане профессиональная адаптация определяется как «процесс приобщения подрастающего поколения к трудовой деятельности» (В.С. Немченко и др.). Эта мысль о профессиональной адаптации как «вхождении», «активном приспособлении» личности к определенной профессиональной деятельности присуща большинству авторов. Однако «вхождение» в профессию раскрывается по-разному. В одних случаях оно предполагает целенаправленное, «планомерно организованное вхождение в профессиональную деятельность» (В.В. Сергеев), как «вхождение человека в профессию и гармонизацию взаимодействий его с профессиональной средой» (В.А. Сластенин), в других – «врастание», приспособление к характеру, требованиям профессиональной деятельности (О.Н. Бендерская, А.И. Кагальняк). По определению Н.Н. Захарова и В.Д. Симоненко, профессиональная адаптация представляет собой «процесс приспособления молодого человека к производству, новому социальному окружению, условиям труда и особенностям конкретной специальности, является одним из критериев правильного выбора профессии». В.М. Рогинский понимает профессиональную адаптацию как «приспособление к структуре высшей школы, содержанию и компонентам учебного процесса в вузе, особенностям избранной профессии».

Авторы Мелекесов Г.А., Сыромицкая И.А. в своей статье «Адаптационный процесс студентов педагогического вуза и его трудности» дают следующее определение: профессиональная адаптация в условиях обучения в вузе – это процесс приспособления студента – будущего специалиста к особенностям избранной профессии [4].

Смысл профессиональной деятельности – это основания для оценки человеком значимости профессиональной деятельности лично для себя, т.е. пристрастное, личностно опосредованное индивидуальным опытом отношение человека к труду. Зрелой личности свойственно постоянно искать все новые, более глубокие или более индивидуальные смыслы труда [3].

Профессиональное самоопределение – это процесс формирования личностью своего отношения к профессионально-трудовой среде и способ ее самореализации. Это длительный процесс согласования внутриличностных и социально-профессиональных потребностей, который происходит на протяжении всего жизненного и трудового пути. Профессиональное самоопределение предполагает выбор карьеры, сферы приложения сил и личностных возможностей [3].

На основе теоретического осмысления проблемы важнейшим для нас является признание профессиональной адаптации не как простого приспособления личности к профессиональной среде и требованиям профессии, а активной сознательной деятельности, направленной на приобретение необходимых профессиональных знаний и умений, выработку профессионально значимых качеств и закрепление навыков адаптивного поведения. Именно активная преобразующая деятельность субъекта профессиональной адаптации служит решающим условием достижения высокого уровня адаптированности. Из всех аспектов профессиональной адаптации личности наименее научно разработанной является проблема профессиональной адаптации молодежи на этапе профессионального обучения и воспитания. Адаптация студента вуза к профессиональ-

ной деятельности предполагает его активность, направленную на овладение комплексом теоретических знаний и практических навыков, приобретенных в результате специальной подготовки и опыта работы [4].

Очень пристальное внимание со стороны правительства уделяется социальной адаптации студентов и выпускников к современному рынку труда. По окончании вуза подавляющее большинство выпускников не подготовлено к конкуренции на рынке труда. Возникает необходимость проводить мероприятия, направленные на знакомство студентов университета с условиями их будущей профессиональной деятельности, уровнем зарплаты. Профессиональное обучение должно обеспечивать общество не просто работниками, а конкурентоспособными и профессионально мобильными работниками. Исследование положения выпускников вузов дает возможность представить обзор трудностей, с которыми приходится сталкиваться молодым специалистам на рынке труда. Недостатки в системе воспроизводства трудового потенциала, противоречивый характер социально-экономических реформ отрицательно сказывается на положении выпускников высшей школы.

Прямая связь между образованием и устойчивостью положения работника отсутствует. Покидая вуз, выпускник оказывается социально незащищенным. Вопрос перспективы трудоустройства не решен в силу того, что в практике обеспечения занятости молодежи технологии трудоустройства устарели, и большинство учащихся полагаются на помощь родителей, друзей, знакомых в решении этого вопроса.

Обучение профессиональной деятельности и степень готовности молодого специалиста к работе следует рассматривать в связи с жизненными планами, социальными ориентациями, диспозициями личности, что, в свою очередь, позволит решить вопрос о качестве обучения студентов, качестве производственной деятельности молодых специалистов. В целях снижения адаптационного периода следует определить факторы успеха профессиональной деятельности студента, слагаемые его профессионализма в условиях рынка труда еще во время обучения.

Наряду с ведущими традиционными функциями – образовательной, воспитывающей и развивающей – образованию и его институтам приходится все более полно брать на себя функции культуропреемственности и культуротворчества, социальной защиты педагогов и воспитанников, выполнять роль социального стабилизатора и катализатора социально-экономического развития [2].

Суть решения проблемы выбора профессии опирается на долговременную программу совместных действий в профессиональной сфере, направленных на проведение в соответствие интересов личности интересам общества. Эта программа должна охватывать максимально возможный срок, давая при этом свободу выбора, согласованную с общественными обязательствами. Задача современной высшей школы состоит не в том, чтобы дать профессию одну и на всю жизнь, а в том, чтобы обеспечить условия для профессионального самоопределения личности на всех этапах её жизненного и профессионального пути.

Литература

1. Энциклопедия профессионального образования: В 3 т. / Под ред. Батышева С.Я. МАПО. Т.1: 1998. – 568 с.; Т.2.: 1999. – 440 с.; Т.3: 1999. – 449 с.
2. Загвязинский В.И., Атаханов Р. Методология и методы психолого-педагогического исследования: Учеб. пособие для студ. высш. пед. учеб. заведений. – М.: Издательский центр «Академия», 2001. – 208 с.
3. Багдасарьян Н.Г., Немцов А.А., Кансузян Л.В. Послевузовские ожидания студенческой молодежи // Социологические исследования. – 2003. – №6. – С.113–116.

4. Мелекесов Г.А., Сыромицкая И.А. Адаптационный процесс студентов педагогического вуза и его трудности // Вестник ОГУ. – №2. – 2004. – С. 57–62.
5. Областной информационно- ресурсный центр по проблемам развития СПО [Электронный ресурс] / Организация практического обучения в колледже как один из путей формирования социально-профессиональной мобильности специалиста; Рыбникова Л.И. – Режим доступа: http://www.rc.igpk.ru/default.asp?P=000005&id=62 , свободный. – Загл. с экрана. – Яз. рус.
6. Шевченко Д.А. Две стороны рынка труда и образования // Комсомольская правда. – 2003. – №120-п (23065-п). – С.7
7. Сабирьянова К. Перераспределение человеческого капитала: исследование профессиональной мобильности в России в период трансформации // Трансформация. – 2001. – №6. – С. 26–28.

«ВИРТУАЛЬНЫЙ» ЛАБОРАТОРНЫЙ КОМПЛЕКС ПО ОСНОВАМ КОМБИНАЦИОННОЙ ЛОГИКИ

И.А. Костин (Санкт-Петербургский государственный университет информационных технологий, механики и оптики, факультет среднего профессионального образования)
Научный руководитель – Д.М. Гриншпун

Введение

В работе представлен «виртуальный» лабораторный комплекс (Комплекс), предназначенный для изучения основ комбинационной логики в рамках дисциплин «Информатика» и «Электротехника и электроника», изучаемых при подготовке специалистов СПО по специальности 230105 «Программное обеспечение вычислительной техники и автоматизированных систем». Приведено обоснование актуальности разработки, описание лабораторных установок, их математические модели, описание последовательности выполнения лабораторных работ. Приводятся результаты экспериментального опробования их выполнения.

Назначением Комплекса является приобретение студентами навыков проектирования, сборки и исследования основных характеристик комбинационных логических схем. Одновременно осваиваются принципы разработки «виртуальных» лабораторных установок.

Лабораторный комплекс создавался для решения образовательных задач, связанных с изучением информационной электроники – основ комбинационной логики. Целесообразность его разработки вызвана тем, что преимущественно теоретический характер изучения материала, предусмотренный примерным учебным планом, приводит к затруднениям его изучения, повышенной трудоемкости освоения, вследствие чего студенты теряют интерес к соответствующим дисциплинам. К тому же содержание учебных программ этих дисциплин, включающее изучение принципов работы цифровых электронных устройств, не совсем соответствует приобретаемой специальности, ориентированной на разработку и применение программных средств. Таким образом, целью разработки является повышение мотивации к изучению дисциплин, достигаемое за счет стимулирования интереса к получению практических результатов методом «виртуального» моделирования и изучения соответствующего прикладного программного обеспечения.

Поставленная цель достигается решением следующих задач, предусмотренных техническим заданием на проектирование Комплекса:

- Комплекс должен состоять из последовательности лабораторных работ, содержание которых должно соответствовать логике изучения теоретического материала дисциплин «Информатика» и «Электротехника и электроника»;
- Комплекс должен быть создан в программной имитационной среде и опираться на самостоятельное изучение студентами соответствующего программного обеспечения;
- в качестве метода имитации следует применить функциональное моделирование;
- каждая лабораторная работа должна предусматривать теоретическую, в том числе математическую, подготовку к ее выполнению;
- каждая последующая лабораторная работа должна опираться на знания и умения, полученные в результате выполнения предыдущей;
- должен быть разработан комплект методических указаний по выполнению работ, в котором указаны цели и задачи, описан порядок выполнения, приведены требования по содержанию и оформлению отчета.

Разработка и структура лабораторного комплекса

Поскольку Комплекс является составной частью создаваемого УМК, содержащего также лабораторные комплексы по изучению некомбинационной логики, физических процессов в полупроводниковых материалах и т.д., то при его разработке учтено требование применения единой программной среды, включающей средства как функционального, так и имитационного моделирования. В качестве такой среды выбран программный пакет LabView. Этот пакет содержит: библиотеки логических элементов, органов управления, индикации и визуализации; инструменты формирования лицевых панелей исследуемых приборов и сборки приборов на монтажных панелях; технические средства имитационного программирования электронных узлов, также располагаемых на монтажных панелях. В представленном Комплексе применены средства функционального моделирования.

Анализ рабочих учебных программ дисциплин «Информатика» и «Электротехника и электроника», выполненный в соответствии с техническим заданием, показал, что практическому изучению и освоению подлежат:

1. изучение функционирования логических элементов;
2. изучение комбинационных схем малой и средней степени интеграции;
3. разработка таблиц истинности для заданных целевых логических функций;
4. разработка математических моделей в совершенных формах на основе таблиц истинности;
5. разработка карт Карно;
6. разработка математических моделей в минимальных формах на основе карт Карно;
7. синтез комбинационных схем по математическим моделям.

В соответствии с этим для практической реализации определены темы практических работ, формирующие соответствующие умения студентов (табл. 1).

Как видно из таблицы, освоение материала осуществляется по принципу «от простого к сложному».

Назначение первой работы – не столько дать студентам представление о логических элементах, что, во-первых, несложно, и, во-вторых, в достаточной степени подробно проходится в рамках лекционных занятий, сколько ознакомить с программной средой «виртуального» моделирования, ее инструментами, библиотеками, техническими средствами экспериментирования. Методическими рекомендациями предусматривается поиск функциональных элементов библиотек, выбор элементов управления и индикации, настройка их параметров, выполнение монтажных работ на рабочих панелях и формирование лицевой панели исследуемых устройств.

Вторая–четвертая работы опираются на навыки, полученные в ходе выполнения первой, и посвящены более серьезной задаче: проектированию, сборке и исследованию комбинационных схем, разрабатываемых на основе математических моделей различных форматов. Студенты получают практические результаты теоретических работ, выполненных на лекционных занятиях, осуществляют их сравнительный анализ.

Завершающими являются пятая–седьмая работы, при выполнении которых студенты учатся создавать целевые приборы, т.е. устройства, выполняющие логические задачи. Проектируются приборы по мере усложнения их функций и, соответственно, электрических схем. Одновременно с помощью терминальных средств изучается создание микросхем многокаскадной логики и их монтажа в сборном приборе.

Большинство лабораторных работ предусматривает самостоятельную разработку студентами таблиц истинности и математических моделей в различных форматах: СДНФ, СКНФ, МДНФ, МКНФ. В табл. 2 и формулах (1)–(4) представлен пример разработки таблицы истинности и математических моделей второго сегмента дешифратора, проектируемого в лабораторной работе №5.

№	Наименование (тема)	Цель
1	Изучение электронных логических элементов малой степени интеграции	Практическое изучение логических элементов, освоение методики сборки виртуальных электронных установок и выполнения лабораторных работ по предмету
2	Синтез и сборка комбинационных схем, соответствующих математическим моделям СДНФ и СКНФ, на основе заданных таблиц истинности	Получение практических навыков разработки совершенных (не минимизированных) комбинационных схем
3	Синтез и сборка комбинационных схем, соответствующих математическим моделям МДНФ и МКНФ, на основе заданных карт Карно	Получение практических навыков разработки оптимальных (минимальных) комбинационных схем
4	Исследование сравнительных характеристик комбинационных схем, соответствующих форматам СДНФ, СКНФ, МДНФ, МКНФ математических моделей	Сравнение трудоемкости синтеза и сборки схем, разработанных на основе разных форматов математических моделей
5	Разработка целевого прибора: дешифратора для семисегментного индикатора, отображающего в десятичном формате числа, набранные в двоичном коде	Получение практических навыков разработки и сборки целевого прибора
6	Разработка целевого прибора: шифратора десятичных чисел в двоичный код	Получение практических навыков разработки и сборки целевого прибора
7	Разработка целевого прибора: сумматора (с функцией вычитания) чисел в двоичном коде	Получение практических навыков разработки и сборки целевого прибора

Таблица 1. Темы лабораторных работ

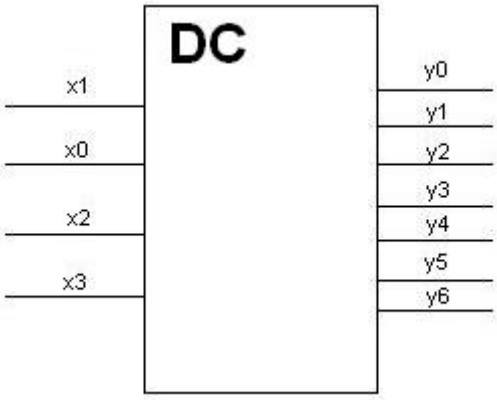


Рис. 1. Дешифратор

Формат МДНФ: $y2 = x3 \vee \bar{x}2 \vee x0x1 \vee \bar{x}0\bar{x}1$ (1)

Формат МКНФ: $y2 = (x3 \vee x1) \cdot (x2 \vee x3) \cdot (x2 \vee x1 \vee \bar{x}0) \cdot (x0 \vee x2 \vee \bar{x}1)$ (2)

Формат СДНФ: $y2 = (x0 \wedge \bar{x}1 \wedge x2 \wedge \bar{x}3) \vee (\bar{x}0 \wedge x1 \wedge x2 \wedge \bar{x}3)$ (3)

Формат СКНФ:

$$y2 = (\bar{x}0 \vee \bar{x}1 \vee \bar{x}2 \vee \bar{x}3) \wedge (x0 \vee \bar{x}1 \vee \bar{x}2 \vee \bar{x}3) \wedge$$
$$\wedge (\bar{x}0 \vee x1 \vee \bar{x}2 \vee \bar{x}3) \wedge (x0 \vee x1 \vee \bar{x}2 \vee \bar{x}3) \wedge$$
$$\wedge (\bar{x}0 \vee \bar{x}1 \vee x2 \vee \bar{x}3) \wedge (x0 \vee x1 \vee x2 \vee x3) \wedge \quad (4)$$
$$\wedge (\bar{x}0 \vee \bar{x}1 \vee \bar{x}2 \vee x3) \vee (x0 \vee \bar{x}1 \vee \bar{x}2 \vee x3)$$

входные сигналы				выходные сигналы						
x0	x1	x2	x3	y1	y2	y3	y4	y5	y6	y7
0	0	0	0	1	1	1	1	1	0	1
1	0	0	0	0	1	1	0	0	0	0
0	1	0	0	1	1	0	1	1	0	0
1	1	0	0	1	1	1	1	0	0	0
0	0	1	0	0	0	1	0	0	1	1
1	0	1	0	1	0	1	1	0	1	1
0	1	1	0	1	1	1	1	1	1	1
1	1	1	0	1	1	1	0	0	0	0
0	0	0	1	1	1	1	1	1	1	1
1	0	0	1	1	1	1	1	0	1	1

Таблица 2. Таблица истинности

Педагогический эксперимент

Разрабатываемый Комплекс экспериментально опробован в двух вариантах применения:

- как демонстрационный материал при проведении теоретических занятий;
- в качестве лабораторных установок в соответствии с табл. 1.

С первой целью он был предложен двум учебным группам, со второй – одной группе. В обоих случаях основным результатом была явно выраженная заинтересованность студентов, причем более высокая во втором, так как кроме выполнения самих лабораторных работ обеспечивалось изучение новой для них программной среды, что соответствует интересам студентов, обучающихся по специальности 230105. В то же время выявилась потребность в доработке методических материалов в части включения в них типовых примеров получаемых результатов экспериментов.

Литература

1. Петров К.С. Технология. Радиоматериалы, радиокомпоненты и электроника: учебное пособие. – М.: Феникс, 2004. – 522 с.
2. Безуглов Д.А., Каленко И.В. Цифровые устройства и микропроцессы. – М.: Феникс, 2006. – 480 с.
3. Лагин В.И., Савелов Н.С. Электроника. – М.: Феникс, 2004. – 576 с.
4. Суранов А.Я. LabView 7: справочник по функциям. – М.: ДМК Пресс, 2005. – 512 с.
5. Тревис Дж. LabView для всех. – М.: ДМК Пресс; ПриборКомплект, 2005. – 533 с.
6. Бутырина П.А. Автоматизация физических исследований и эксперимента: компьютерные измерения и виртуальные приборы на основе LabView 7. – М.: ДМК Пресс, 2005. – 264 с.

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СЕРИИ «ЭКОЛОГ» В ОБРАЗОВАТЕЛЬНОЙ И ВОСПИТАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

А.А. Павлова, А.Ю. Пишко
Научный руководитель – к.т.н., доцент М.А. Кустикова

Рассмотрено применение программного обеспечения серии «Эколог» при изучении студентами дисциплины «Экология» для формирования практических умений работы с экологическими программами расчета воздействия на окружающую среду, повышения мотивации к изучению дисциплины путем моделирования ситуации, приближенной к реальности.

Дисциплина «Экология» как федеральный компонент образовательного стандарта преподается как студентам технических и гуманитарных специальностей, для которых экологическое направление не является профильным, так и студентам, чья будущая деятельность связана с экологией. При подготовке специалистов экологического направления проблема заключается в том, что недостаточно отведено часов на практические занятия. Причем зачастую используются программные продукты, которые используют простые, ограниченные модели. Они учитывают не все параметры, соответственно, они не дают адекватного представления о процессе, явлении, которое они моделируют [1, 2].

Программное обеспечение серии «Эколог» – это пакет программ, с которыми на сегодняшний день работают многие экологи на предприятиях, проектировщики. Умение работать с экологическими программами пригодится в будущей профессиональной деятельности, и будет являться преимуществом при устройстве на работу по специальности. Использование экологического программного обеспечения в процессе обучения студентов, для которых экология не является профильным направлением, повышает мотивацию к изучению предмета за счет наглядности, моделирования реальной ситуации. Использование программного обеспечения формирует связь между теоретическими знаниями и практическими умениями.

Программы серии «Эколог» целесообразно использовать при обучении будущих инженеров, проектировщиков, специалистов, деятельность которых связана с принятием решений.

Экологическое образование в России

В настоящее время экологическое образование стало одним из основополагающих фундаментов для развития образования в области устойчивого развития. Во-первых, идеи устойчивого развития внедряются во многие читаемые курсы, а, во-вторых, идет процесс формирования цикла курсов по устойчивому развитию, используя методику «проникающего образования», когда материал уже читаемых курсов широко используется в преподавании устойчивого развития и компонуется в самостоятельные учебные блоки или курсы по устойчивому развитию.

Взаимосвязь между образованием вообще, экологическим образованием и образованием для устойчивого развития несомненна. Очевидно также, что всякое подлинное образование, по определению, работает на устойчивое развитие. Менее очевидно, что внедрение образования для устойчивого развития как системного инновационного проекта это – уникальная возможность укрепления образования как социального института в целом, особенно в России [3].

В начале 90-х годов одним из ответов на востребованное тогда обществом внимание к проблемам окружающей среды стало создание экологического образования, которое довольно быстро нашло свое место в классических университетах России. Обра-

зование, подготовка кадров и информирование населения об экологических проблемах, возникающих при взаимодействии человека с окружающей средой, стали считаться одним из главных условий перехода стран к устойчивому развитию и решения проблем будущего выживания человечества. Было признано, что лица, принимающие управленческие решения, а также значительная часть населения должны иметь соответствующие экологические знания.

В Советском Союзе и затем в России экологическое образование в начале имело природоохранную направленность. В начале 90-х гг. в связи с начавшимся процессом перехода на многоступенчатую систему образования создалась благоприятная возможность организационно оформить экологическое образование в классических и технических университетах. Стало ясно, что целесообразно иметь две основные системы экологического образования. Первая из них реализуется в классических университетах и имеет более фундаментальный естественнонаучный характер. Вторая система экологического, точнее инженерно-экологического, образования со специальностями «Безопасность жизнедеятельности» и «Защита окружающей среды» реализуется в технических университетах.

Для становления и реализации определенных знаний, умений и навыков у будущих специалистов необходима особая система ценностей и отношений, которые смогут влиять на поведение в окружающей среде. Для воплощения в жизнь концепции устойчивого развития обучающимся необходимы:

- умение анализировать изменения в окружающей среде и прогнозировать последствия этих изменений;
- осознание того, что сегодняшний образ жизни влияет на будущие поколения;
- принятие общечеловеческих ценностей;
- способность применять знания к жизненным ситуациям;
- способность к аналитическому, критическому, творческому мышлению;
- понимание взаимосвязей в окружающей среде;
- навыки сотрудничества в решении разнообразных проблем;
- понимание того, что действия на местном уровне оказывают влияние на глобальные процессы;
- уважительное отношение к разнообразию в природе и обществу [4].

Экологическое образование в СПбГУ ИТМО

При подготовке студентов технических специальностей (например, по направлениям «Приборостроение», «Оптотехника», «Информационные технологии») в учебном плане отводится мало времени изучению такого предмета естественнонаучного цикла, как экология. При этом практически все время отводится под лекционные занятия, и очень мало на лабораторные занятия. Курс лекций, как правило, рассматривает общие вопросы экологии, глобальные проблемы человечества. За счет недостаточных связей между теоретическим курсом и практическими (лабораторными) занятиями у будущих специалистов не формируются целостная картина окружающего мира, студенту трудно представить, как применить на практике знания, полученные на лекции.

Время, отведенное на изучение этого предмета, составляет всего 34 часа. Студент, нацеленный на создание новых приборов, применение и разработку современных технологий, разработку новейших программных продуктов, не всегда готов понять и воспринять, что именно пытаются донести до него преподаватели.

Занятия по экологии могут быть успешными, если творческая активность и интерес учащихся постоянно поддерживаются. Помочь может оформление игры как лабораторной работы, где формулируются цели, условия и выводы. Лабораторные занятия

можно организовывать с целью развития способности анализировать последствия происходящих вокруг событий.

В СПбГУ ИТМО на практических занятиях используют такие формы и методы обучения, как выступление и обсуждение докладов, дискуссии, выполнение кейс-заданий. Также в процессе обучения используются компьютерные экологические игры, как например, «Озеро», «Спасти леопарда».

Экологическая игра «Озеро» представляет собой графическое отображение математической закономерности. В ней нужно найти оптимальное соотношение между доходом от выловленной рыбы и ущербом, наносимым окружающей среде, при этом учитывается только изменение численности популяции вида. Эта игра, по сути, не несет новую информацию для обучающегося, являясь дополнительным иллюстративным методом обучения.

Возможно, процесс обучения будет более эффективным, если в него включить элементы работы с современными программами, которые используют экологи на предприятиях, проектировщики. Эти программы изначально созданы для работы с реальными объектами, для оценки и прогнозирования их воздействия на окружающую среду. Результаты этих расчетов используются для создания проектов, выполнения отчетов. Умение работать с подобными программами будет преимуществом при поступлении на работу, связанную с природоохранной деятельностью.

Например, программное обеспечение серии «Эколог» разработано для решения задач, касающихся вопросов охраны атмосферного воздуха, расчета акустического воздействия, расчета класса опасности отходов и др. На сегодняшний день эти программы используются многими специалистами в России и за ее пределами.

Использование программ серии «Эколог» в процессе обучения студентов, для которых экология не является профильным направлением, повысит мотивацию к изучению предмета за счет наглядности, моделирования реальной ситуации. Использование этого программного обеспечения поможет сформировать связь между теоретическими знаниями и практическими умениями.

Описание реализации

С февраля 2008 г. ведется пробный курс занятий со студентами СПбГУ ИТМО специальностей «Охрана окружающей среды и природопользование», «Экологический менеджмент», на которых используются программы серии «Эколог».

Программное обеспечение содержит нормативно-методическую литературу. Эти программы прошли необходимые согласования в НИИ «Атмосфера», ГГО им. А.И. Воейкова, сертифицированы Госстандартом России и имеют сертификаты экологического соответствия. Все программы, реализующие методики по расчету выбросов загрязняющих веществ от различных производств, согласованы НИИ «Атмосфера» в установленном порядке и входят в список согласованных программ.

На рис. 1 приведена примерная структура объектов, с которыми работает программа.

Город является самой крупной структурной единицей, он может состоять из одного или нескольких районов. На территории района могут располагаться одно или несколько предприятий, состоящие из цехов. Для цехов задаются источники загрязнений с набором технических параметров. Также программа учитывает метеопараметры на уровне города и фоновые концентрации загрязняющих веществ. Чтобы произвести расчет, обучающийся задает параметры, создает топографическую основу, определяет границы расчетной площадки и отдельные точки, в которых необходимо произвести расчет. Результаты расчетов представлены в двух вариантах: табличные данные (концен-

трации загрязняющих веществ в расчетных точках) и графическое отображение результатов на топографической основе (изолинии изображены на рис. 2).

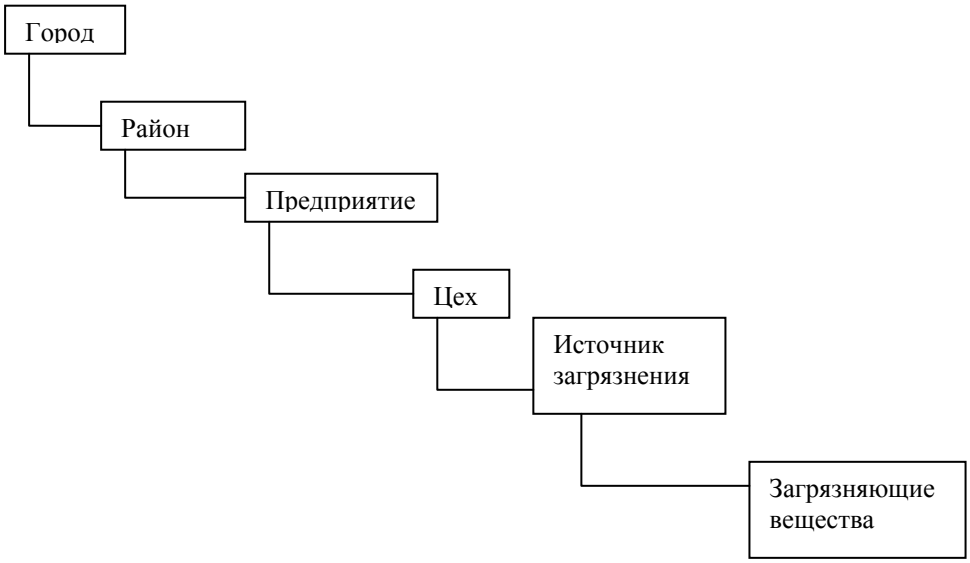


Рис. 1. Структура объектов

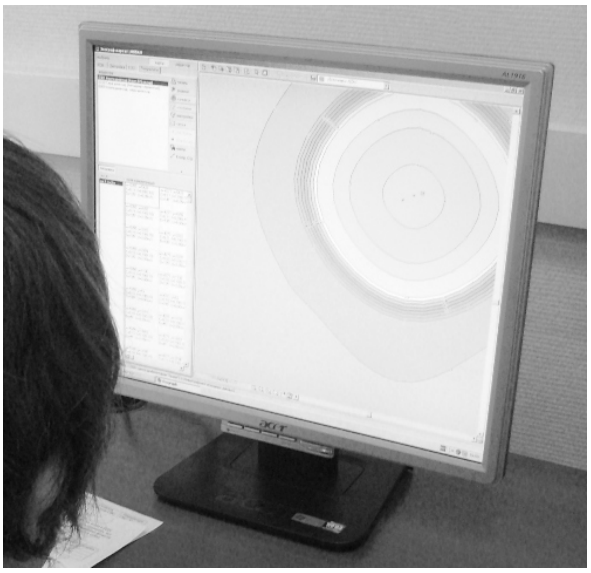


Рис. 2. Работа с программой УПРЗА «Эколог»

В качестве топографической основы в программу можно подгрузить карты местности (в формате jpeg) и планы из программы AutoCad. Таким образом, студенты могут смоделировать ситуации, максимально приближенные к реальным. Это делает работу с программой более привлекательной для обучающихся.

Неожиданное погружение в практическую деятельность эколога, оперирование множеством влияющих факторов помогают студентам технических специальностей понять роль тех знаний, которые они приобретают, изучая общую экологию и другие естественнонаучные дисциплины, понять взаимосвязь между состоянием окружающей среды и любой деятельностью человека.

С целью формирования у студентов экологического мышления, развития творческого подхода к изучаемым предметам необходимо использовать различные формы и методы организации учебного процесса. При изучении дисциплин экологического профиля, помимо традиционных лекционных, лабораторных, семинарских работ, применяют системы обучения, основанные на компьютерных обучающих программах.

Литература

1. Государственный образовательный стандарт высшего профессионального образования. Направление подготовки дипломированного специалиста 653700 – Приборостроение.
2. Государственный образовательный стандарт высшего профессионального образования. Направление подготовки дипломированного специалиста 654000 – Оптотехника.
3. Косов Ю.В. // Экология и образование. – 2002. – № 1–2.
4. Вебстер К., Жевлакова М.А., Кириллов П.Н., Корякина Н.И. От экологического образования к образованию для устойчивого развития. – СПб.: Наука, САГА, 2005. – 137с.

ЭЛЕКТРОННОЕ УЧЕБНОЕ ПОСОБИЕ ПО АНГЛИЙСКОЙ ТЕРМИНОЛОГИИ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Д.В. Дроздова, М.В. Захаревич
Научный руководитель – к.т.н., профессор М.И. Потеев

Рассмотрена структура пособия, отмечены основные методические особенности, дано обоснование программного обеспечения, проанализированы результаты педагогического эксперимента с первой версией учебного пособия.

Введение

Как известно, в области информационных технологий превалирует использование английской терминологии. Достаточно значимое число научных достижений в этой сфере опубликовано на английском языке. В связи с этим современный специалист по разработке и использованию информационных технологий должен владеть английской терминологией, иметь опыт коммуникаций на английском языке в профессиональной сфере.

Для получения таких навыков студенты пятого курса специальности «Информационные технологии в образовании», обучающиеся на кафедре технологий профессионального обучения Санкт-Петербургского государственного университета информационных технологий, механики и оптики (СПбГУ ИТМО) в качестве одной из дисциплин специализации изучают дисциплину «Английский язык в сфере профессиональной коммуникации».

Для методического обеспечения преподавания этой дисциплины потребовалось разработать соответствующие учебно-методические материалы. Одним из них является электронное учебное пособие по английской терминологии в области информационных технологий. В статье рассматривается структура пособия, основные методические особенности, а также анализируются результаты педагогического эксперимента и выбор программного обеспечения.

Описание структуры пособия

При создании электронного учебного пособия по английской терминологии в области информационных технологий решались следующие задачи:

– сформировать у студентов представление о специальности «Информационные технологии в образовании» как о системе;
– сформировать умение описывать все элементы этой системы и соотношения между ними на английском языке.

Для решения этих задач студентам необходимо проработать темы, связанные со специальностью «Информационные технологии в образовании». Это нужно осуществлять последовательно на всех уровнях системы «английский язык». К числу этих уровней относятся: фонетический, графический, морфологический, лексический, грамматический, синтаксический [1]. Учитывая это, структура пособия сформирована следующим образом:

1. вводный раздел;
2. тематические разделы;
3. тестовые задания;
4. глоссарий.

Каждый тематический раздел имеет общие подразделы. Он состоит из текста, аудиозаписи текста, лексической карты, показывающей соотношение терминов на основе латинских терминоэлементов и заданий для самоконтроля.

Для того чтобы студент проработал дисциплину на всех уровнях английского языка, в каждом разделе темы «Информационные технологии в образовании» создан текст, описывающий соотношения между элементами данной подсистемы в системе дисциплины. Студент последовательно прослушивает текст, повторяет в паузах за диктором, пытается понять на слух, читает, переводит и заучивает наизусть. Для усвоения различных грамматических конструкций текст по каждой теме насыщен примерами использования одной из распространенных грамматических конструкций английского языка.

Для каждого раздела темы создана «лексическая карта». В «лексических картах» в схематическом виде представлены соотношения и связи между всеми терминами данной темы. С их помощью студент учится строить высказывания, описывающие связи между элементами системы. Чтобы в дальнейшем понимать незнакомые термины по знакомым элементам, за счет «лексических карт» проводят морфологический разбор терминов, часто требующий знания латинских морфем.

Важной частью пособия является глоссарий. В нем приводится толкование всех использованных терминов и проводится их морфологический разбор, в том числе на латинские морфемы.

При изучении любой области английской терминологии студент сталкивается с большим количеством латинских терминоэлементов. Одна из основных задач электронного пособия – способствовать изучению и переводу из пассивного в активный словарный запас наиболее употребительных элементов. Для этого создана еще одна лексическая карта. На ней слова классифицированы в соответствии с общими или сходными латинскими терминоэлементами, встречающимися в их составе.

Упражнения по каждой теме включают узнавание терминов по контексту или знакомым элементам, правильное их использование в контексте, а также высказывания, описывающие соотношения между разными терминами. В качестве заключительного задания предлагается создать мини-презентацию и провести на английском языке лекцию по одному из разделов дисциплины.

Отбор терминов для создания пособия производился по ключевым текстам для специальности «Информационные технологии в образовании». В качестве ключевых выбраны следующие тексты:

1) английские и англо-русские глоссарии терминов, связанных с компьютерами или образованием [2–5];
2) журналы и книги на английском и русском языках, посвященные информационным технологиям в образовании [6–8];
3) тексты на соответствующие темы из справочных Интернет-изданий [11, 12].

Программное обеспечение

При создание электронного учебного пособия было решено отталкиваться от классификации компьютерных обучающих программ по целевому назначению [9]. В соответствии с ней различают следующие виды компьютерных обучающих программ:

1) демонстрационные;
2) формирующие;
3) управляющие;
4) контролирующие.

К *демонстрационным программам* относятся программы, которые или предъявляют визуальную информацию, или демонстрируют явления и процессы. *Формирую-*

щие программы разделяются на программы, формирующие знания, умения или навыки. *Управляющие программы* ориентированы на управление процессом обучения в условиях индивидуальной или групповой работы. Они позволяют последовательно задавать учащимся те или иные вопросы, анализировать полученные ответы, определять уровень усвоения материала. *Контролирующие программы* рассчитаны на проведение текущего или итогового опроса учащихся.

Разработанное учебное пособие относится к программам, формирующим знания. Его программная оболочка хранит организованный набор теоретических сведений, терминов, развернутых пояснений, обеспечивает возможность поиска, выборки необходимой тематической информации и реализации запросов.

Для эффективного использования электронного пособия программное обеспечение должно соответствовать требованиям обучающегося и преподавателя.

Инструментальные средства для создания электронных учебных пособий многочисленны и разнообразны. К ним относится, например, оболочка WebCT, разработанная одноименной американской компанией. Программа имеет инструментальные средства разработки электронных учебных пособий на нескольких языках с использованием удобных шаблонов и библиотек мультимедийных файлов, средства одновременного обслуживания до 30000 студентов, в том числе средства самотестирования. В WebCT также реализованы технологии «электронной доски объявлений», текстового диалога, электронной почты, работы над общим проектом и многие другие.

Помимо WebCT, к специально ориентированным инструментальным средствам можно отнести Learning Space фирмы Lotus, ToolBook Instructor компании SumTotal Systems, AuthorWare компании Adobe, отечественную система HyperMethod и другие. Зачастую подобные средства реализуют не только функции разработки учебных материалов, но также и другие функции, присущие автоматизированным обучающим системам, и включают средства обучения и управления обучением.

Так как перечисленные инструментальные средства довольно дороги, программы, ориентированные на Web-технологии, не включающие дорогостоящих специальных средств, выглядят предпочтительней. К ним относятся недорогие или свободно распространяемые программные продукты, такие как, например, HTML- и XML-редакторы, редакторы иллюстративной и презентационной графики (векторные и растровые), 3D графические редакторы, перекодировщики текстовых и графических форматов, редакторы звуковых файлов, редакторы видеофайлов, инструментальные средства создания анимации, почтовые клиенты, средства организации чатов, теле-, аудио- и видеоконференций, средства информационного поиска [10].

Первая версия электронного учебного пособия создана с помощью Adobe Dreamweaver CS3. Используя гиперссылки, разработана удобная навигация. Сценарии JavaScript позволяют проводить тестирования по заданным вопросам, следить за обучением пользователей, хранить их характеристики, подчитывать количество заходов на определенные разделы сайта, а также определять время, потраченное обучаемым на прохождение определенной части курса. С помощью Flash-технологий и графических редакторов (Adobe Photoshop, CorelDraw) создан красочный, современный интерфейс.

Эксперимент

Эксперимент по внедрению электронного учебного пособия по английской терминологии в области информационных технологий проведен со студентами пятого курса специальности «Информационные технологии в образовании» по дисциплине «Английский язык в сфере профессиональной коммуникации». Эксперимент показал, что использование такого пособия позволяет сформировать у студентов работающую подсистему английского языка «терминология в области информационных техноло-

гий». Контроль результатов обучения подтвердил, что студенты не только знают терминологию, но и могут использовать ее в неподготовленной речи и на письме. Обучающиеся научились воспринимать на слух, конспектировать и анализировать лекции по специальности на английском языке, делать доклады по различным разделам дисциплины.

Заключение

Первая версия электронного учебного пособия по английской терминологии в области информационных технологий разработана и успешно внедряется на кафедре технологий профессионального обучения СПбГУ ИТМО. Использование пособия в учебном процессе позволяет студентам освоить английский язык в сфере профессиональной коммуникации и успешно овладеть своей специальностью.

Литература

1. Аверина Е.Д. Иностранный за 200 часов. – СПб: Руди-Барс,1994. –129 с.
2. Глоссарий современного образования / Под общ. ред. В.И. Астаховой, А.Л. Сидоренко. – Харьков: ОКО, 1998. – 269 с.
3. A Glossary of computing terms / Ed. by the Brit. computer soc. Schools comm. Glossary working party. 10th ed. – Harlow etc., 2002. – p. 379.
4. Полонский В.М. Словарь по образованию и педагогике. – М.: Высшая школа, 2004. – 512 с.
5. Глоссарий / Сост. Голуб В.В. – Ростов-на-Дону, 2002. – 82 с.
6. Современное состояние и тенденции развития информационных ресурсов в образовании: Лекция–доклад / В.В. Попов; Школа-семинар «Создание единого информационного пространства системы образования». – М., 1998. – 23 с.
7. Материалы международной научной конференции «Информационные технологии и телекоммуникации в образовании и науке» – М., 2006. – 228 с.
8. Korhonen M. Project as a Learning Method in Expert Development/Informatics in Education. 2002. Vol. 1.
9. Горлушкина Н.Н. Педагогические программные средства: Учебное пособие / Под ред. проф. М.И. Потеева – СПб, 2002. – 152 с.
10. Норенков И.П., Зимин А.М. Информационные технологии в образовании. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 352 с.
11. Information Technology Association of America.– Режим доступа: http://www.itaa.org
12. The UNESCO Institute for Information Technologies in Education.– Режим доступа: http://www.iite.ru

СТАНДАРТЫ И ФОРМАТЫ ДАННЫХ ДЛЯ РАБОТЫ С ПРОФАЙЛАМИ КОМПЕТЕНЦИЙ, ВОЗМОЖНЫЕ ПУТИ ИХ РАЗВИТИЯ

Д.Ф. Сулейманов, Я.И. Поршнев
Научный руководитель – к.ф.-м.н., доцент М.В. Сухорукова

В статье рассмотрены некоторые современные стандарты хранения и работы с компетенциями в системах электронного обучения. Выдвинуты предположения о будущем развитии этих стандартов для более гибкой работы с данными о компетенциях с использованием Web-онтологий и средств Datamining.

Введение

По мере того, как Internet-технологии становятся неотъемлемой частью повседневной жизни, люди все ближе подходят к осознанию новых возможностей общения, и одна из таких возможностей – электронное обучение (e-learning). Возникновение этого термина прочно связано с распространением сети Internet, точно так же, как и появление «электронных версий» процессов в различных областях социальной жизни, прежде всего в экономике, например, e-commerce (электронная коммерция).

В целях превращения электронного обучения в повседневную обыденность необходимо уделить должное внимание вопросам унификации и стандартизации в этой сфере. Вопросы стандартизации, выбора платформы унификации сегодня активно обсуждаются заинтересованными организациями, в частности, IMS (Instructional Management Systems Global Learning Consortium – Всемирный Консорциум по системам управления обучением). Созданные им спецификации RDCEO и ePortfolio связаны с описанием компетенций и истории обучения студента. Но развитие этих спецификаций – лишь шаг на пути к созданию новых платформ электронного обучения. Для их развития требуются средства улучшения интероперабельности, при которой системы смогут бесконфликтно и динамически обмениваться не только контентом и сценариями обучения, но и инструментами, функциональностью, семантикой и средствами управления. Для возможности обмена семантикой при работе с компетенциями мы предлагаем использовать средства онтологий и техники Datamining.

Развитие платформ электронного обучения

В области e-learning создаются все более динамичные платформы, которые приходят на смену традиционным «пассивным». При активном электронном обучении используется широкий спектр Internet-технологий, подобных персонификации, моделированию и мобильности, что позволяет внедрять недоступные для традиционных видов обучения методики. Растет спрос на модульные и персонифицированные платформы электронного обучения: традиционные платформы не обладают достаточной гибкостью из-за своей монолитной внутренней структуры.

На протяжении последних двух десятилетий в области e-learning доминируют LMS (Learning Management Systems) – системы управления обучением. Следующее поколение систем дистанционного обучения будет опираться на сервисные архитектуры [1].

Эволюция открывает путь к платформам электронного обучения следующего поколения. Разделение функциональности LMS и системы управления учебным контентом (Learning Content Management System, LCMS) обеспечит поддержку еще большей интероперабельности, при которой системы смогут бесконфликтно и динамически обмениваться не только контентом и сценариями обучения, но и инструментами, функциональностью, семантикой и средствами управления.

Одна из трудностей при развитии подобных платформ связана с обеспечением более высоких уровней интероперабельности. Композиция сервисов позволит таким платформам электронного обучения динамически обнаруживать и компоновать соответствующие сервисы для того, чтобы добиться особых целей, которые ставит каждый конкретный пользователь.

Организации по стандартизации уже в течение ряда лет изучают различные оболочки, спецификации и принципы построения сервисных платформ электронного обучения. IMS Abstract Framework (www.imsglobal.org/specifications.html) выявляет и представляет основные компоненты и интерфейсы для систем электронного обучения. E-Learning Framework (ELF; www.elframework.org) иллюстрирует общую функциональность систем электронного обучения. Open Knowledge Initiative (OKI; www.okiproject.org) определяет уровни сервисов для разработки платформ электронного обучения. Общий подход, лежащий в основе этих создаваемых стандартов, заключается в модуляризации функциональности.

Оболочки, спецификации и принципы организации, в свою очередь, определяют поуровневые подходы к созданию систем электронного обучения из наборов ранее определенных сервисов. Такие спецификации определяют представления личной и групповой информации (IMS Enterprise), профиля студента и истории его обучения (IMS Learner Information Package and ePortfolio), оценки (IMS Question and Test Interface), группировки изучаемого контента (IMS Content Package и SCORM), динамического программирования контента (IMS Simple Sequencing), компетенций учащегося (IMS Reusable Definition for Competence and Educational Objectives), операций обучения (IMS Learning Design), поиска в федеративных базах данных (IMS Digital Repositories Interoperability) и связывания различных инструментов электронного обучения. На низком уровне эти стандарты и спецификации описывают синтаксис, который различные сервисы должны реализовать для внешнего представления информации.

Так как обзор всех этих спецификаций занял бы много места, в данной статье мы ограничимся обзором двух связанных с компетенциями и историей обучения студента IMS RDCEO и IMS ePortfolio.

Все спецификации IMS основаны на формате XML, предлагающем мощный синтаксис и позволяющем создавать структуры для эффективного обмена информацией.

RDCEO

Эта спецификация содержит информационную модель для определений компетенции или образовательной цели (RDCEO (Reusable Definition Competency or Educational Objective)), прежде всего в контексте онлайнового и распределенного обучения. Понятие компетенции здесь интерпретируется в самом широком смысле, включая образовательные цели (то, к чему стремятся) и результаты, достигаемые в ходе обучения. Слово «компетенция» также используется для обозначения всего того, в чем можно быть осведомленным, хотя некоторые профессиональные сообщества используют слово с ограничениями – только навыки, исключая знание или понимание. Информационная модель может использоваться для обмена определениями компетенций между системами управления учебным процессом, кадровыми системами, системами учебного контента и другими подобными системами. RDCEO обеспечивает уникальные ссылки на описания компетенций или целей для включения в другие информационные модели, в чем и заключается возможность многократного использования определения компетенции или образовательной цели.

Основная информация в RDCEO – неструктурированное текстовое определение, на которое можно сослаться через глобально уникальный идентификатор, что обеспе-

чивает уникальные ссылки на описания компетенций или учебных целей для включения в другие информационные модели.

Спецификация RDCEO обеспечивает средство создания общих соглашений о компетенциях, которые могут выступать как часть плана обучения или карьеры, могут описывать начальные и конечные знания и навыки обучающегося. Файлы, которые соответствуют этой спецификации, предназначены для обмена машинами, но информация, которую они содержат, в настоящее время предназначается для интерпретации человеком.

Кратко опишем основные элементы XML документа, соответствующего спецификации RDCEO.

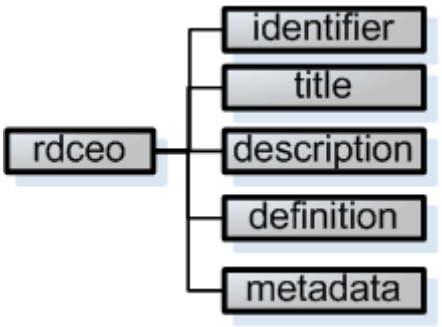


Рис. 1. Основные элементы спецификации RDCEO

Определение компетенции или образовательная цель (<rdceo>). Это корневой элемент, содержащий одно многократно используемое определение.

Идентификатором (<identifier>) служит URI (Uniform Resource Identifier) с синтаксисом, определенным в RFC 2396. Он состоит из двух элементов данных: идентификатор каталога и запись в самом каталоге. Примером идентификатора может служить строка «http://www.imsglobal.org/fictional/rdceo_cat1.xml#definition1», где «http://www.imsglobal.org/fictional/rdceo_cat1.xml» определяет каталог, а «definition1» – запись в этом каталоге. Данные элементы являются обязательными.

Заголовок (<title>), представляющий собой краткий текст определения компетенции или образовательной цели. Для многократно используемого определения может быть только один заголовок. Заголовок может быть записан на разных языках.

Описание (<description>) является текстовым описанием в сфободной форме компетенции или образовательной цели. Может быть записано на разных языках.

Определение (<definition>) содержит структурированное определение компетенции или образовательной цели. Является необязательным элементом, содержащим ссылку на структуру определения и более подробное определение компетенции или образовательной цели в соответствии с этой структурой.

Метаданные (<metadata>) представляет собой контейнер для произвольных метаданных к элементу <rdceo>. Может включать в себя данные об используемой схеме RDCEO (по умолчанию принимается «IMS RDCEO») и о её версии (по умолчанию принимается «1.0»).

ePortfolio

Автором термина ePortfolio, под которым понимается личное электронное образовательное досье каждого учащегося – необходимый инструмент эффективного взаимодействия учебного заведения и учащегося в процессе индивидуализации личных образовательных траекторий в процессе электронного обучения – является Серж Равэ, ис-

полнительный директор Европейского Института e-learning (European Institute for e-Learning) в Париже. В соответствии со спецификацией IMS ePortfolio может содержать следующую информацию:

- деятельность, в которой принимал, принимает или планирует принимать участие владелец портфолио;
- компетентности (навыки и т.д.) владельца;
- достижения владельца, подтвержденные и не подтвержденные сертификатами;
- предпочтение владельца;
- цели и планы владельца;
- результаты разнообразных тестирований, пройденных владельцем.

В качестве примера приведем два варианта использования ePortfolio.

Презентационные ePortfolio могут использоваться как свидетельства знаний или достижений владельца. Они часто содержат инструкции о том, как их содержание должно быть интерпретировано. Например, инженер-программист может создать ePortfolio для демонстрации отношения между полученными профессиональными сертификатами, написанным кодом и историей занятости, чтобы убедить потенциального работодателя нанять его.

Учебные ePortfolio используются для планирования, документирования, контроля учебного процесса в течение долгого времени и интеграции разных учебных курсов. Например, студенты могут создать и использовать ePortfolio для контроля и отображения улучшения их знаний и навыков в течение учебного года.

В соответствии со спецификацией IMS, ePortfolio определяется как пакет контента IMS Content Package, содержащий в себе манифест – XML документ, manifest.xml, с описанием структуры и ресурсов пакета, и собственно контент – файлы ресурсов. Ресурсы включают в себя разнообразные материалы, описываемые как часть портфолио, такие как примеры работы, копии сертификатов, результаты тестирований.

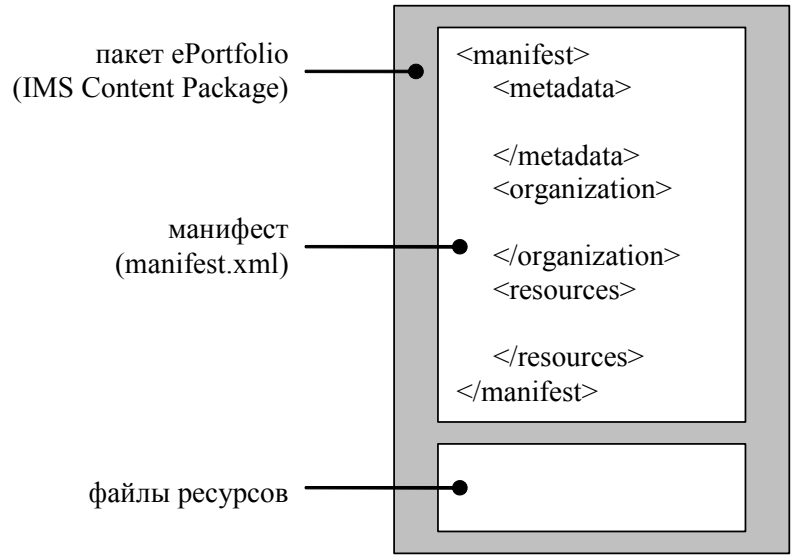


Рис. 2. Структура ePortfolio

Манифест состоит из следующих основных частей:

- <metadata> содержит данные о пакете в целом;
- <organization> содержит описание структуры материалов пакета;
- <resources> содержит описание ресурсов, входящих в пакет.

При описании компетенций в ePortfolio ссылаются на данные, соответствующие спецификации IMS RDCEO.

Возможные пути развития

Рассмотренные спецификации, как и другие разрабатываемые в настоящее время стандарты, направлены на обеспечение более высоких уровней интероперабельности платформ электронного обучения. Одной из важных проблем при разработке подобных платформ может служить необходимость не только импортировать и экспортировать информацию, но и обмениваться ею в гетерогенных средах. Современные платформы электронного обучения, например, могут пересылать пользовательскую информацию или информацию о контенте между средами. Однако пока нет возможности «понять» семантику такой информации, выяснить, как ее анализировать или как ее могут использовать различные среды. Для такого уровня интероперабельности среды должны обмениваться синтаксисом информации и ее семантикой. Так как на самом деле люди (главная составляющая информационных систем) совершенно по-разному описывают объекты, гибкие решения должны выявлять и поддерживать динамические семантические соответствия, чтобы обеспечивать подлинную семантическую интероперабельность. Именно в этом направлении серьезную работу проводит сообщество Semantic Web.

Ключевое допущение для считываемой машиной информации и сервисов состоит в том, что сервисы могут взаимодействовать и договариваться «на лету». Разработки в области Semantic Web начинались с RDF и DAML+OIL и с тех пор продвинулись до языка онтологий OWL (Web Ontology Language, www.w3.org/TR/owl-features/), который недавно стал стандартом консорциума W3C. Язык OWL может использоваться для описания «онтологий» – баз знаний о концепциях, к которым могут обращаться сервисы с запросами на получение информации. В частности, онтологии помогают создавать новые знания, в которых вывод может формироваться в базе знаний с учетом поставленной цели, вне зависимости от информации, непосредственно занесенной создателем онтологии. Эта способность распространяется на мир Web-сервисов с помощью подмножества языка онтологий – OWL for Services (OWL-S).

Использование онтологий сможет облегчить поиск и обмен информацией о компетенциях между Web-сервисами, однако создание самих онтологий представляет собой достаточно длительный процесс. Мы полагаем, что для сокращения времени на разработку средств управления и контроля компетенций можно также использовать средства Datamining. Сейчас они могут быть использованы для быстрого анализа компетенций, а в дальнейшем помогут в автоматизации работы по созданию и наполнению онтологий. Средства для решения таких задач интеллектуального анализа данных, как классификация (определение класса объекта по его характеристикам), кластеризация (разделение множества объектов на группы), ассоциация (нахождение зависимостей между объектами), сейчас активно применяются в сети Internet вообще и социальных сетях, в частности. Со временем даже появились отдельные определения для анализа неоднородной, распределенной и значительной по объему информации в Internet: Web Mining, Web Usage Mining и Web Content Mining. В последнем случае речь идет об автоматическом поиске и извлечении качественной информации из источников сети. Мы полагаем, что подобные средства могут быть эффективно использованы для работы с информацией о компетенциях в разрабатываемых платформах электронного обучения. Так с помощью кластеризации можно будет группировать компетенции по разным тематикам и направлениям, классификация поможет в добавлении новых компетенций к уже существующим онтологиям, а поиск ассоциативных правил поможет в выделении взаимосвязей между компетенциями.

С использованием описанных выше технологий становится возможным построение систем дистанционного обучения с расширенными функциями анализа учебных курсов, учебных планов, эффективности тех или иных курсов в обучении выбранным компетенциям. Так, например, становится возможным создание систем, которые по за-

просу пользователей могут предложить варианты учебных программ для освоения новых компетенций. Программы могут быть составлены из курсов разных образовательных учреждений, сами курсы могут быть как дистанционными, так и требующими очного посещения занятий. Всю информацию для анализа и предоставления результатов система получает из некоторых централизованных хранилищ данных или от систем самих образовательных учреждений. И там, и там данные для анализа хранятся в соответствии с общими стандартами и спецификациями [1]. При наличии средств централизованного тестирования появляется возможность собирать и анализировать статистику успешности обучения пользователей выбранным компетенциям в ходе предложенных курсов. Эти данные в дальнейшем могут быть использованы для ранжирования курсов и учебных программ.

Заключение

Таким образом, для дальнейшего развития платформ электронного обучения и более продуктивного использования их совместно с социальными сетями необходимо развитие средств обмена не только контента учебных курсов, но и семантики. Для реализации этой задачи можно использовать активно развивающиеся средства Datamining или Web-онтологии.

Литература

1. Сулейманов Д.Ф., Сухорукова М.В. Образование на базе идеологии ВЕБ 2.0 // Научно-технический вестиник СПБ ГУ ИТМО. – 2007. – Вып. 44. Современные технологии. – С. 16–20.
2. Declan Dagger, Alexander O'Connor, Séamus Lawless, Eddie Walsh and Vincent Wade. Service Oriented eLearning Platforms: From Monolithic Systems to Flexible Services // IEEE Internet Computing. – Режим доступа: https://www.cs.tcd.ie/~slawless/papers/ieee2007.pdf (May/June 2007)
3. IMS Reusable Definition of Competency or Educational Objective Specification // IMS Global Learning Consortium. – Режим доступа: http://www.imsglobal.org/competencies/rdceov1p0/imsrdceo_infov1p0.html (25 October 2002)
4. IMS Reusable Definition of Competency or Educational Objective - Best Practice and Implementation Guide // IMS Global Learning Consortium. – Режим доступа: http://www.imsglobal.org/competencies/rdceov1p0/imsrdceo_bestv1p0.html (25 October 2002)
5. IMS ePortfolio Best Practice and Implementation Guide // IMS Global Learning Consortium. – Режим доступа: http://www.imsglobal.org/ep/epv1p0/imsep_bestv1p0.html (02 June 2005)
6. IMS ePortfolio Information Model // IMS Global Learning Consortium. – Режим доступа: http://www.imsglobal.org/ep/epv1p0/imsep_infov1p0.html (02 June 2005)
7. Семантическая паутина // Wikipedia. http://ru.wikipedia.org/wiki/Semantic_Web
8. Интеллектуальный анализ данных // Wikipedia. – Режим доступа: http://ru.wikipedia.org/wiki/Интеллектуальный_анализ_данных
9. Берсегян А.А Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP / А.А. Берсегян, М.С. Куприянов, В.В. Степаненко, И.И. Холод. – 2-е изд., перераб. и доп. – СПб: БХВ-Петербург, 2007. – 384 с.

ПРИНЦИПЫ ОРГАНИЗАЦИИ ОБРАТНОЙ СВЯЗИ С УЧАСТНИКАМИ КОМПЬЮТЕРНЫХ ОБУЧАЮЩИХ ИГР В РАМКАХ РЕШЕНИЯ ЗАДАЧИ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ НАВЫКОВ

Г.О. Котелкова
Научный руководитель – к.п.н., доцент А.В. Маятин

Рассмотрены принципы организации обратной связи с участниками компьютерных обучающих игр в рамках решения задачи формирования профессиональных навыков позволяют реализовать в игре геймплей, обеспечивающий саморегуляцию системы обучающийся – игровая среда.

Современные условия жизни требуют от человека высокого уровня профессиональных знаний и навыков, мотивации к работе. Для соответствия этим стандартам и, следовательно, достижения успеха в карьере, необходимо со школы начинать выбирать профессию и осваивать профессиональные навыки. Однако нельзя рассчитывать на то, что обучение, каким бы глубоким и разносторонним оно ни было, в состоянии дать исчерпывающие рекомендации на каждый конкретный случай, с которым может встретиться человек в его практической деятельности. Неотъемлемым критерием успешности специалиста сегодня является профессиональный опыт, позволяющий решать новые, нестандартные задачи и работать в условиях недостатка информации.

В рамках социально-когнитивного подхода в психологии, объясняющего поведение и психику посредством анализа сознания субъекта и взаимного влияния личности и среды [1, 2, 3, 6, 9], проведено большое количество исследований, посвященных факторам успешности личности в различных областях. В частности, в работе [2] было показано, как формируется профессиональная компетентность человека. Круг обучения (рис. 1) показывает, что этот процесс является непрерывным переходом от получения новой информации и первых попыток применения уже имеющихся знаний к практической деятельности до максимально отточенных умений и навыков. В круге обучения можно выделить четыре стадии между первоначальным знакомством с новым материалом и компетентностью.

1. Неосознанная некомпетентность – у обучающегося еще нет навыка, и он не знаете о его отсутствии или вообще о возможном существовании такового. Когда осознается недостаток навыка, происходит переход на вторую стадию.
2. Осознанная некомпетентность – обучающийся узнает, что у него нет какого-то навыка. Понимание собственной некомпетентности может мотивировать на приобретение недостающего навыка.
3. Осознанная компетентность следует за процессом сознательного обучения навыку. Вначале действия на этой стадии регулируются самосознанием: воспроизведение того или иного действия требует постоянного мысленного контроля.
4. Неосознанная компетентность – это заключительный этап обучения, когда навык полностью усвоен и отработан. Обучающийся бессознательно справляется с ними самостоятельно, а его сознание свободно для обучения новому навыку. Эта стадия характеризует мастерство.

Переход на этап неосознанной компетентности является наиболее труднодостижимым в процессе обучения, однако именно на этом этапе, когда обучающийся не задумывается о каждом своем шаге, а большинство технологических навыков отработано до автоматизма, складываются наиболее благоприятные условия для формирования личностно значимого (в том числе профессионального) опыта — собственных ценностных ориентаций, стратегий поиска решения новых задач и т.п.

Переход на этот этап сопряжен с рядом трудностей, в первую очередь в связи с тем, что обучающийся для его достижения должен абстрагироваться от особенностей

технологических навыков и сконцентрироваться на комплексной постановке решаемой задачи. При традиционных подходах к обучению, основанных на поэтапном освоении и закреплении определенных навыков, разрешить эти трудности и достичь целостного личностно-ориентированного профессионального отношения к изучаемой предметной области практически невозможно. С другой стороны, любой ребенок уже решал подобную задачу формирования личностно-значимого опыта общественных отношений, который тоже требует для формирования огромного количества отдельных навыков, но ценен только при комплексном восприятии. И делал он это через игру.

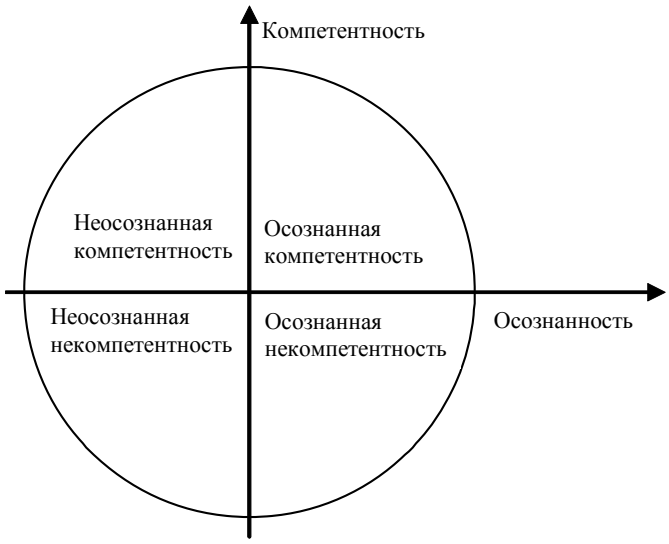


Рис. 1. Круг обучения [2]

Игра, которая в дошкольном и младшем школьном возрасте позволяла безопасно учиться и пробовать новые социальные роли, старшим школьникам может позволить легче переходить к неосознанной компетентности в профессионально-ориентированных областях, снимая психологическое напряжение перед обучением и страх неудачи. Игра является эффективным методом обучения, поскольку снимает противоречия между абстрактным характером учебного предмета и реальным характером профессиональной деятельности [7], позволяя формировать профессиональную компетентность.

Опыт использования различных методов и подходов в обучении показывает, что одним из важнейших мотивационных факторов в обучении является уверенность обучающихся в своих силах, их самостоятельная оценка собственных способностей и компетентности: они с большим энтузиазмом выполняют задания, когда считают, что владеют необходимыми знаниями и навыками. С другой стороны, неуверенность в своих силах относительно того или иного вида деятельности может стать сильным тормозящим развитие фактором: из-за опасения не справиться с поставленной задачей обучающиеся не будут даже пробовать браться за них.

Успешный опыт игровой деятельности, приобретенный в прошлых (детских и подростковых) играх, и восприятие игровой деятельности как привычной и безопасной позволяют нивелировать страх недостаточной компетентности и возможной неудачи при отработке профессиональных навыков.

В процессе получения новых знаний и навыков за первоначальным интересом часто следует снижение мотивации из-за того, что не получается использовать новые умения. В некоторый момент обучающийся доходит до так называемого барьера преодоления: на этом этапе без поддержки извне обучающиеся могут вернуться к старым навыкам, дающей хоть какой-то результат. В случае благополучного преодоления этого барьера вырабатывается стратегия, неизменно приводящая к результату, и соответст-

венно оттачивается профессиональная компетентность, а со временем осуществляется переход на новый уровень бессознательной компетентности.

На оценку обучающимся своей компетентности, помимо опыта успеха и неудач, влияет наблюдение за достижениями других людей. Когда школьник видит, что его «коллега» успешно справился с проблемой, это прибавляет ему уверенности в собственных силах. Участие в играх позволяет обучающимся получать необходимую поддержку от других играющих (через реальную помощь или путем наблюдения за их достижениями, что оказывает непосредственное влияние на оценку собственных способностей и возможностей), а также от самой игровой среды, формируя благоприятные условия для развития профессионально значимых качеств и навыков.

Специфику игровой технологии в значительной степени определяет игровая среда: различают игры с предметами и без предметов, настольные, комнатные, уличные, на местности, с различными средствами передвижения, а также компьютерные и с ТСО.

Однако при несомненной эффективности игр в практическом их использовании в учебном процессе часто возникает ряд трудностей. Эффективность использования игровых технологий в значительной степени зависит от устойчивой и длительной активности обучающихся, от уровня их мотивации. Стоит отметить еще одну существенную особенность игр как метода обучения: на передачу учебного материала тратится больше времени, чем при использовании традиционных методов.

Достоинства компьютерных средств обучения давно известны в педагогике: они позволяют длительное время удерживать устойчивое внимание обучающихся и высокий уровень мотивации, а также уменьшить время, необходимое для передачи информации от обучающихся к педагогу (эффективный способ реализации обратной связи) [5]. При условии адекватного выбора методик применения и сценариев игр интеллектуальные компьютерные игры могут помочь даже в таких сложных задачах, как формирование профессиональных навыков и осуществление профессиональной пробы.

В рамках работы над исследовательским проектом авторы разработали набор сетевых интеллектуальных игр, позволяющих школьникам осуществить профессиональную пробу в IT-сфере, в частности, «Путешествие в Рисовлянидию» (для учащихся 7–9 классов) в жанре квест и «Морской бой» (для учащихся 10 – 11 классов) в жанре «Бои роботов».

Проведенные исследования показали, что особое внимание при использовании в обучении компьютерных игр необходимо уделять мотивационной компоненте (чтобы максимально реализовать преимущества компьютерных игр в этом аспекте образовательного процесса) и организации обратной связи с обучающимися как средству поддержки мотивации и координации образовательного процесса.

Известно, что ожидания обучающихся в процессе обучения отличаются от того, что происходит на самом деле (рис. 2) [3].

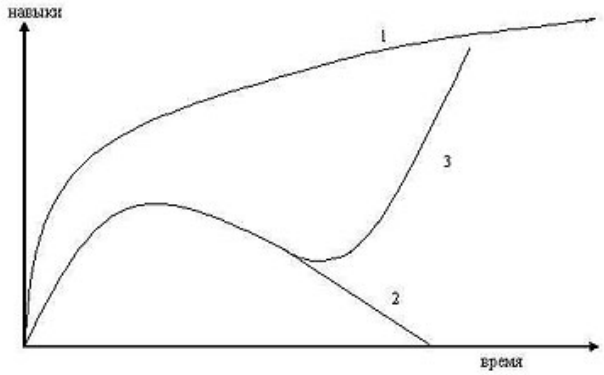


Рис. 2. Динамика достижений и мотивации обучающихся

Первая кривая – это ожидания обучающегося. Со временем полученные результаты начинают отставать от ожидаемых, причем расхождение становится все больше и больше. Через некоторое время рост достижений совсем останавливается, и обучающийся либо отказываемся от своего нового навыка (кривая 2), либо ищет другие пути развития (кривая 3). Для того чтобы процесс пошел по третьему варианту, в точке, где наступил барьер, нужно привлечь дополнительные ресурсы. Они могут быть самыми разными. Например, это может быть совет учителя, прочитанная книга или увеличение интенсивности занятий. В любом случае это должна быть адекватная обратная связь с источником необходимых знаний и опыта.

Образовательную систему можно рассматривать [4] как сложную динамическую систему, а ее развитие – как целенаправленный информационно-управленческий процесс. Соответственно, в ее структуре можно выделить множество контуров управления или самоуправления, образующих контуры прямой и обратной связи. При этом единичное управленческое воздействие не может привести к фиксированию полезных признаков, к этому ведет серия таких актов. Механизм управления, позволяющий прийти к желаемой организации системы, объединяет в себе две взаимосвязанные функции: саморегулирование и саморазвитие.

Саморегулирование – это самостоятельное реагирование системы на внешние воздействия, нарушающие ее нормальное функционирование. Саморегулирование достигается с помощью оперативной информации, обратной связи и осуществляется в форме самонастройки и самоорганизации. Показано [10], что чем более развита система (техническая, экономическая, социальная или педагогическая), тем больше механизмов обратной связи требуется создать для приобретения ею желаемых качеств.

Для преодоления барьера (рис. 2) компьютерные средства обучения, особенно компьютерные обучающие игры, предоставляют широкие возможности организации обратной связи, позволяющей реализовать постоянный отклик на действия обучающегося и, тем самым, обеспечить саморегуляцию педагогической системы ученик – КОИ. В общем случае в понятие обратной связи входят вообще все действия игры. Но нас интересует ее применение для достижения конкретной задачи: как сделать так, чтобы у школьника возник наиболее интенсивный и положительный профессиональный опыт в игровой форме, поэтому сконцентрируем внимание на принципах организации обратной связи, направленной на формирование профессиональных навыков, доведенных до уровня неосознанной компетенции.

Наш опыт показал, что для создания эффективной компьютерной обучающей игры, как и для развлекательных компьютерных игр, в первую очередь необходимо спроектировать эффективный игровой процесс (геймплей). Именно он обеспечивает и поддерживает целостность восприятия игрового пространства, что является обязательным условиям поддержки вовлеченности обучающегося в игру, его мотивации.

Опыт разработчиков компьютерных развлекательных игр [8] показал, что для поддержания мотивации к игре необходимо, чтобы обратная связь в геймплее была непрерывной, моментальной, интенсивной и целенаправленной. Как показывает наш опыт, этим же критериям должна соответствовать обратная связь в профессионально-направленной компьютерной игре. Так как в педагогических играх успешное выполнение дидактического задания связывается с игровым результатом, а учебная деятельность подчиняется правилам игры, то для того, чтобы сформировался нужный набор профессиональных навыков, обучающемуся необходимо выполнить все обязательные игровые задания – скорее всего, пройти игру до конца. Только в этом случае можно будет говорить о формировании первоначальной профессиональной компетентности и, как следствие, отрицательной или положительной профессиональной пробе.

Для создания качественного и интересного для обучающихся геймплея вначале необходимо определить навык (или навыки), который будет осваивать игрок. После этого для создания обратной связи необходимо выбрать, какая именно реакция системы позволит реализовать использование этого навыка в профориентационной игре.

В игре «Путешествие в Рисовляндию» обучающийся закрепляет навыки, полученные при изучении темы «Компьютерная графика». Для достижения поставленной цели игровой процесс проходит в «сказочном» королевстве, а все действия игрока представлены в виде «магических» манипуляций, что не позволяет сформироваться аналогии действий и инструментов конкретного программного пакета.

Для школьников ситуация, когда учебные знания необходимо применять в компьютерной игре, является нетипичной, что может привести к барьерам и регрессу навыков, поэтому для достижения педагогических задач необходимо интегрировать (в первую очередь семантически) различные каналы обратной связи в геймплей. Ненавязчивые механизмы поддержки в игровом процессе позволяют, не потеряв целостности восприятия ребенком сюжета и мотивационной ценности игры, исключить возможность попадания его на вторую кривую (рис. 2), подсказав возможность и путь движения к третьей. Так, обучающийся может в любой момент получить помощь виртуального спутника – Пикселя (аналог Скрепки из Microsoft Word), это может показаться излишним, однако не следует забывать о возрасте целевой аудитории (12–15 лет). Кроме того, на каждое действие игрока, как правильное, так и неправильное, реагируют другие персонажи и появляются подсказки. Чтобы даже самый увлекающийся школьник обратил внимание на реакцию программы и его навыки не совпали со второй кривой, в игре реализована очень интенсивная обратная связь: графическая, аудио, текстовая.

И, что самое главное, любая реакция системы направлена на то, чтобы показать обучающемуся, в каком направлении нужно развиваться. Именно поэтому последовательность прохождения заданий, квестов, жестко задана, а если игрок не знает, куда ему двигаться дальше, то он в любой момент может посмотреть «Журнал заданий».

Таким образом, игра «Путешествие в Рисовляндию» позволяет обучающимся осуществить профессиональную пробу в сфере компьютерной графики и сформировать первичную мотивацию к овладению необходимыми знаниями и навыками и получению профессии.

Игра «Морской бой», представляет собой сражение кораблей. Обучающиеся создают программу на языке Java, управляющую кораблями, т.е. тренируются и развиваются навыки программирования. Для того чтобы они могли прочувствовать трудности создания программ, необходимо было создать такую обратную связь, которая моделировала бы окружение профессиональных программистов – самостоятельный поиск информации, общение с коллегами и соревнование с конкурентами.

Необходимо отметить, что у игры «Морской бой» существуют обучающие миссии, что позволяет обучающимся быстрее преодолеть этапы бессознательной некомпетентности и сознательной некомпетентности (рис. 1). Для взаимодействия обучающихся различной квалификации и тьюторов было организовано предметно направленное компьюнити. С его помощью обеспечивается достижение педагогических задач и, следовательно, саморегуляция системы в целом, что позволяет преодолеть барьер и подсказать возможность и путь движения по третьей кривой (рис. 2).

Непрерывность обратной связи обеспечивается в основном за счет взаимодействия с другими игроками и тьютором в рамках комьюнити, возможности использовать программный код других игроков, выложенный в открытом доступе, а также использовании справочных материалов.

Для игры такого типа целесообразно было создать систему рейтингов, отражающую учебные достижения школьников, таким образом, мотивация обучающихся на по-

беду в игре (получение рейтинговых баллов) обеспечивает целенаправленное достижение педагогических результатов.

Моментальность обратной связи реализована в самих боях: результаты сражения двух кораблей пользователь получает по первому запросу, кроме того, он может посмотреть систему рейтингов, сравнив тем самым свои достижения с достижениями других игроков. Интенсивность связи обеспечивается эмоциональной значимостью результатов сражения для игрока (гибель собственного корабля). Использование в разработанных играх моделей, имитирующих реальный инструментарий, применяемый в профессиональной сфере (библиотека кодов, подсветка синтаксиса и другие), позволяет задействовать инструментальное научение.

Таким образом, в рамках игры «Морской бой» была создана саморегулирующаяся система, позволяет обучающимся осуществить профессиональную пробу в сфере программирования на языке Java и сформировать первичную мотивацию к овладению необходимыми знаниями и навыками и получению профессии.

Итак, развитие информационных и компьютерных технологий сегодня позволяют реализовать педагогическую игру с помощью новых средств. Однако для того, чтобы решить образовательные и профориентационные задачи, необходимо, чтобы были четко сформулированы дидактические требования к компьютерным обучающим играм.

Можно сделать вывод, что выработанные принципы организации обратной связи с участниками компьютерных обучающих игр в рамках решения задачи формирования профессиональных навыков позволяют реализовать в игре геймплей, обеспечивающий саморегуляцию системы обучающийся – игровая среда. Применение этих принципов при проектировании компьютерных обучающих игр позволяет обучающимся наблюдать улучшение специфических профессиональных навыков, т.е. предоставляет им наглядную информацию относительно успешного выполнения заданий, поэтому они начинают ощущать себя более компетентными в моделируемой деятельности. Геймплей компьютерной обучающей игры позволяет школьникам видеть их игровые и образовательные результаты в динамике, что увеличивает процессуально-содержательную мотивацию обучающихся.

Литература

1. Аронсон Э., Уилсон Т., Эйкерт Р. Социальная психология. Психологические законы поведения человека в социуме. – СПб: Прайм-ЕВРОЗНАК, 2002. – 560 с.
2. Бандура А. Теория социального научения. – СПб: Евразия, 2000. – 320 с.
3. Боричев А., Гришина Н. Гештальт-психология и социально-когнитивная теория личности. К. Левин и А. Бандура. – СПб: Прайм-ЕВРОЗНАК, 2007. – 125 с.
4. Волкова В.Н., Денисов А.А. Теория систем. – М.: Высшая школа, 2006 г. – 512 стр.
5. Коджаспирова Г.М., Петров К.В. Технические средства обучения и методика их использования. – М.: Академия, 2007. – 352 с.
6. Салливан Г., Роттер Дж. и Мишел У. Теория межличностных отношений и когнитивные теории личности. – СПб: Прайм-ЕВРОЗНАК, 2007. – 128 с.
7. Селевко Г.К. Современные образовательные технологии. - М.: Народное образование, 1998. – 256 с.
8. Стремовский И. Психологическая модель геймплея как обучающей деятельности. – Режим доступа: http://www.dtf.ru/articles/read.php?id=1251
9. Первин Л., Джон О. Психология личности: Теория и исследования / Пер. с англ. под ред. В.С. Магуна — М.: Аспект Пресс, 2001.— 601 с.
10. Перегудов Ф.И., Тарасенко Ф.П. Основы системного анализа. – Томск: НТЛ, 2001. – 396 с.

ОРГАНИЗАЦИЯ СЕТЕВЫХ СООБЩЕСТВ НА БАЗЕ ПРОФОРИЕНТАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО ПОРТАЛА

Е.А. Козьмина
Научный руководитель – к.т.н., доцент Н.Ф. Гусарова

Социальные сети предоставляют пользователю возможность быстрого и оперативного нахождения нужной информации. Особенно это касается специализированных сетей. Рассмотрены принципы и методики организации соцпальных сетей в рамках портала по профессиональной ориентации молодежи

Введение

Сегодня все чаще и чаще слышатся признания молодых людей, что ту или иную профессию они выбрали, так как она престижна, может принести неплохой доход, ее посоветовали родители, друзья или преподаватели. В последнее время нередки случаи, когда на втором-третьем курсах студенты понимают, что это не их стезя, и переводятся, поступают снова или заканчивают учебное заведение и идут на второе высшее. Пользуясь понятием внутренней позиции личности, введенным Л.И. Божович, можно утверждать, что развитие личности внутренней позиции взрослого человека определяется, прежде всего, развитием личности как профессионала [1]. Таким образом, нельзя недооценивать важность выбора будущей специальности, а впоследствии и профессии, молодым человеком.

Однако методы, которыми продолжают пользоваться консультанты, помогающие определиться с выбором профессии, остаются практически такими же, какие были ранее. Анкетирование, психологические тесты, личная беседа – выбор по-прежнему не очень широк. Многие не учитывают, что огромное давление на подростка в плане выбора профессии оказывают уже не только родители и преподаватели, а, прежде всего, его сверстники и, благодаря популярности Интернета, виртуальные друзья. Например, начитавшись «романтических историй» о взломах сайтов, познакомившись с хакерами, подросток «идет на программиста» или «защитника информации»; насмотревшись рисованных мультфильмов, попробовав азы Photoshop, молодой человек выбирает специальность «Компьютерная графика». И при этом остается по-прежнему мало ресурсов, в том числе и электронных, которые могут дать действительно адекватную картину того или иного занятия. Таким образом, просто необходимо не только давать подробную информацию о направлении и специальности, но и вести подростка по выбранному им пути, отвечать на его вопросы, давать общаться ему со своими единомышленниками. Вопрос – только в средстве организации подобного типа деятельности.

В последнее время наиболее популярными сайтами, в первую очередь среди молодых людей, становятся социальные сети (vkontakte, odnoklassniki), блоги (livejournal, blogs.mail) и форумы. Пользователи перестали воспринимать Интернет только как средство получения материала. Все больше и больше людей приходят в Сеть за общением, поиском новых или восстановлением старых связей. Интерес сдвигается от всемирной аудитории, состоящей из слушателей и зрителей, к местным сообществам, где люди общаются между собой и помогают друг другу [2]. Численность, состав, цель общения подобных сообществ (от «любителей кошек» и до «сообщества менеджеров проектов») порой очень различны. Однако глобальная идея всех сообществ едина – обмен знаниями. И тем интереснее использовать принципы сетевых сообществ в образовательном процессе.

Особенно актуально эта идея звучит, если взглянуть на результаты исследования аудитории социальных сетей от компании Forrester Research [3]. На рис. 1 изображено распределение по 6 уровням общения, возрастным группам и регионам. Как видно из рисунка, множество пользователей, в особенности представителей младшего поколе-

ния, не только просматривают или комментируют чужие записи (66%), но и готовы сами делиться своими знаниями, ведя собственный блог или даже сайт (39%).

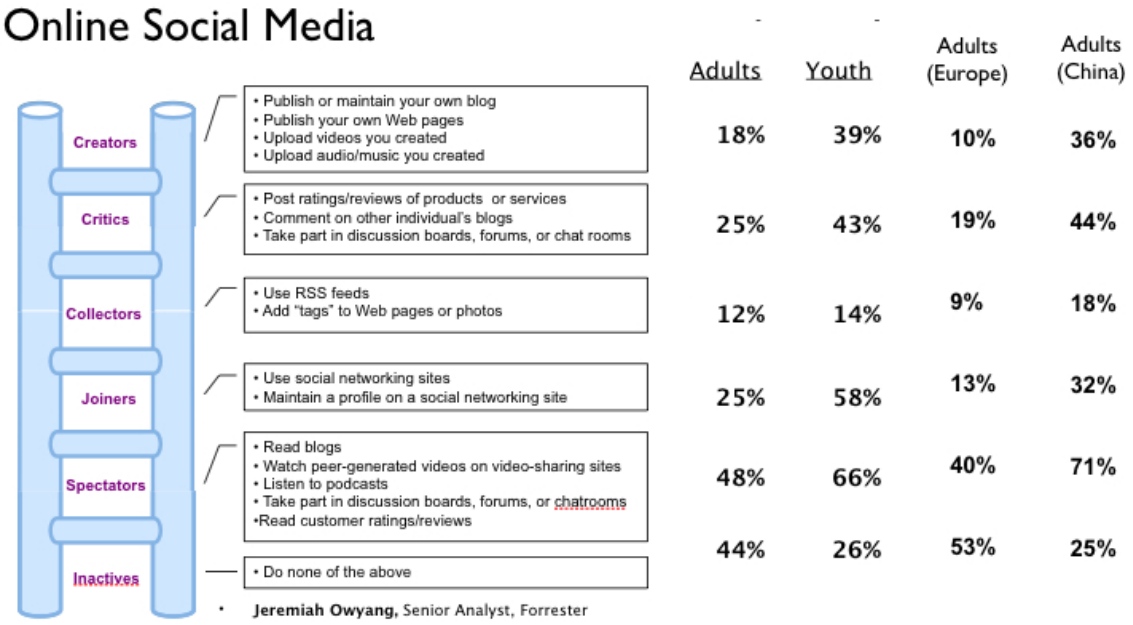


Рис. 1. Результаты исследования социальных сетей

Кроме того, необходимо говорить не только об активности уже привлеченных пользователях социальных сетей, но и тех, кто еще или не нашел «необходимый ресурс», или не знает о существовании подобного типа ресурсов. Так, например, исследование, проведенное компанией Synovate в 2008 г. среди 13 тысяч респондентов в возрасте от 18 до 65 лет в 17 странах мира [4], показало, что 58% людей вообще не знают, что такое социальные сети. И только около 26% опрошенных признали, что являются участниками социальных сетей. Таким образом, существующие сайты для общения (прежде всего, социальные сети) не охватывают даже половины потенциальных участников. Причин в этом случае несколько:

- отсутствует первичное информационное наполнение;
- пользовательские инструменты не позволяют организовать полноценное общение участников;
- не учитываются особенности психологии целевой аудитории;
- при организации ресурса не принимаются в расчет особенности информационного наполнения;
- низкий уровень usability;
- а также ряд других, свойственных отдельным ресурсам.

При построении профориентационного портала «iTech4U» [5] нами учтены эти и другие ошибки создателей социальных сетей.

Форма ведения сетевого сообщества

Общение в Сети ведется не между конкретными личностями, но образами, сформированными пользователями. Американский психолог Дж. Сулер предлагает говорить о четырех сценариях поведения личности в виртуальной реальности: «остаться самим собой, говорить от имени дискретной части своей целостности, принять выдуманные

индивидуальности или остаться полным анонимом, а в некоторых случаях еще при этом сделаться человеком-невидимкой» [6].

Таким образом, у организаторов сетевых сообществ остается несколько вариантов развития ресурсов.

1. Искусственно ограничить пользователя, заставляя его действовать только от своего имени. Технически это возможно реализовать с помощью тотальной проверки всех членов сетевого сообщества (в том числе по IP-адресу) или посредством организации закрытого сообщества, например, работников компании, где «вычисление реальной личности» не составит труда. Целесообразно организовать сообщества такого типа в случае циркуляции в подобных ресурсах конфиденциальной информации или наличия необходимости ведения «реального» диалога посредством средств сетевой коммуникации.
2. Предложить пользователю заполнить форму с обязательными и необязательными полями, позволяющими идентифицировать пользователя в случае необходимости. Пользователю нужно, в том числе, предоставить право редактирования «личных данных». Таким образом, не нарушается право пользователя на личную зону, но остается возможность проверки. По этому принципу действует большинство ресурсов в настоящее время. Однако стоит отметить, во-первых, проблему контроля большого количества пользователя, во-вторых, уровень безопасности заносимой информации пользователя. С этими проблемами столкнулись уже создатели vkontakte, odnoklassniki и большинства других российских и зарубежных аналогов. В средствах массовой информации периодически появляются сообщения о наличии уязвимостей в этих ресурсах, позволяющих осуществить взлом персональных страниц пользователей, вирусных атаках и спам-рассылках, организуемых злоумышленниками, вычисление которых обычно затруднено.
3. Убрать обязательность регистрации на ресурсе, предоставляя пользователям возможность общаться анонимно. Однако в этом случае появляется проблема однозначного идентифицирования собеседника, т.е. отсутствуют гарантии ведения диалога с одной и той же личностью. Кроме того, в случае оскорбления, разжигания конфликтов и других проблем практически невозможно отследить виновных.

Таким образом, наиболее популярным способом организации сообществ остается ресурс с обязательной регистрацией пользователей (обычно с подтверждением регистрации по электронной почте), с указанием личных данных (в том числе заполнением обязательных и необязательных полей). Соответственно, при проектировании ресурса iTech4U был учтен этот аспект. Практически весь материал доступен для незарегистрированных пользователей для чтения. Это позволит новичку, еще не до конца заинтересовавшемуся тем или иным направлением, получить первичную информацию и сформировать некое мнение о ней. Таким образом, за пользователем остается возможность выбора: оставаться пассивным членом сообщества или участвовать в обсуждении выкладываемого материала в качестве полноценного участника.

Базовые потребности участника сетевого сообщества

У любого пользователя Сети (соответственно, у любого участника сетевого сообщества), согласно исследованию Л.И. Баланина [7], есть следующие потребности:

- потребность в аффилиации проявляется в стремлении пользователей найти в Интернете свою группу, принять ее ценности, найти свое место в группе;
- потребность в самоутверждении может носить характер научного или художественного творчества, коммуникативной активности, социальной карьеры, стремления к лидерству, саморазвития личности;
- потребность в сотрудничестве состоит в поиске единомышленников в сети;

- потребность в коммуникации состоит в том, что Интернет позволяет преодолевать коммуникативный дефицит, возникающий в обыденной жизни.

На профориентационном портале «iTech4U», соответственно, вышеуказанные потребности удовлетворяются следующим образом.

1. На портале сформировано несколько видов групп: группы по созданным направлениям портала (все направления отрасли информационных технологий), по играм, опубликованным на портале, а также группы, созданные по просьбе пользователей. Таким образом, решается вопрос общения молодого человека среди своих единомышленников, в том числе и тех, у кого уже есть опыт работы в том или ином направлении.
2. Пользователи могут выкладывать свои работы: аудио-, видео-, работы в Photoshop, 3DMax и многие другие. Любые работы, выкладываемые пользователями, могут быть оценены другими участниками сообщества, на них можно получить комментарии и рекомендации специалистов в соответствующей области. На портале ведется единый рейтинг пользователей и их работ. Таким образом, пользователь, благодаря оценкам своих сверстников и старших наставников, получает не только моральное удовлетворение, но и рекомендации по развитию или смене направления своих интересов.
3. На портале поощряется совместная работа пользователей. В случае необходимости каждый из пользователей может обратиться к соответствующему специалисту для получения помощи.
4. Реализовано несколько способов коммуникации:
    a. диалоговая коммуникация – внутренняя почта ресурса;
    b. полилоговая коммуникация – общение на форумах;
    c. однонаправленная коммуникация – отзывы, комментарии, оценки.

Моделирование отношений в сетевом сообществе

Любое сетевое сообщество является моделью реальной группы людей. Соответственно, необходимо спроецировать некоторые правила построения отношений внутри объединений людей на сетевые сообщества.

1. В любом обществе есть ведущие, ведомые и «аутсайдеры». Для сетевого сообщества эта градация характеризуется следующим образом [7]:
    a. «гуру» – обычно это те пользователи, которые в совершенстве владеют тематикой сообщества, они же чаще всего образуют ядро группы;
    b. «пользователи» – участники сообщества, которые на равных могут общаться друг с другом;
    c. «гало» – пользователи, не разделяющие кодекса сообщества.

    В качестве гуру на начальном этапе лучше всего использовать представителей группы разработчиков ресурса или приглашенных специалистов, в том числе и консультантов по профессиональной ориентации. Во-первых, создатели ресурса страхуют себя от «боязни чистого листа» пользователей, т.е. пользователей не принуждают организовывать и вести дискуссии самостоятельно. Во-вторых, задается общее направление дискуссий, поднимаются актуальные для отрасли проблемы, снижается возможность отхождения пользователей от темы. Со временем в зависимости от активности пользователей можно выделить «внутренних гуру».
2. В любом сообществе развита система норм и правил. Для всего ресурса действуют правила, запрещающие оскорбления, разжигание конфликтов, а также ряд других действий. Кроме того, в рамках отдельной группы могут быть созданы свои правила. Соответственно, как и в каждом сообществе, есть те, кто следит за соблюдением правил. На портале реализована следующая иерархия управления:

a. администратор ответственен за ресурс в целом, его техническую составляющую, а также выбор направления работ по развитию портала;
b. модераторы разделов ответственны за своевременное обновление материалов портала, удаление нецензурных комментариев, записей, выкладываемых материалов;
c. модераторы групп ответственны за ведение дискуссий в своих группах, созданию новых тем, оперативной адресации входящих вопросов соответствующим специалистам.

3. В любом обществе развита система наказаний и поощрений. На описываемом портале ведется единый рейтинг пользователей, который формируется на базе следующих аспектов:
   - наличие комментариев на выкладываемые материалы ресурса (в том числе пользовательские);
   - наличие оценок на материалы других участников сообщества;
   - наличие благодарностей от других пользователей;
   - наличие и качество собственных выкладываемых работ;
   - наличие оценок от других пользователей;
   - наличие и качество сообщений в организуемых в сообществе дискуссиях;
   - участие в опросах ресурса;
   - участие в викторинах ресурса;
   - игровой рейтинг.

   Таким образом, в результате своей деятельности пользователь зарабатывает или теряет баллы, которые могут быть использованы для:
   - открытия новых возможностей по настройке существующих модулей;
   - доступа к новым приложениям и играм;
   - увеличения ранга в группе, в которую входит пользователь.

Заключение

Существует мнение, что социальные сети изживают себя: людям перестает быть интересна сама идея социальных сетей – объединение по интересам, обмен знаниями, общение. Существует также и иное мнение, что социальных сетей уже слишком много. Вопреки этому открываются все новые и новые сетевые сообщества: педагогов, менеджеров, врачей, юристов и многих других. Можно отметить тенденцию перемещения пользователей от многоцелевых сообществ к нишевым ресурсам. Причина проста: общение ради общения среднестатистического пользователя уже не устраивает.

Всемирно известный эксперт в области дизайна и юзабилити Якоб Нильсен опубликовал свой ежегодный отчет о привычках пользователей Сети, а также об их манере работы [8]. Нильсен отмечает, что сейчас уже практически не осталось пользователей, которые хотят просто «побродить» по сайтам. Подавляющее большинство пользователей четко представляют себе, что именно они хотят сделать и как это сделать. После того, как требуемая задача выполнена, пользователи просто выходят из Сети.

Социальные сети предоставляют пользователю возможность быстрого и оперативного нахождения нужной информации. Особенно это касается специализированных сетей. Объединенные общей целью, обычные пользователи нередко достигают лучших результатов по сравнению с экспертами-одиночками.

Таким образом, в рамках портала решаются следующие проблемы профессиональной ориентации:

- пользователи получают достоверную информацию о той или иной специальности;
- организована возможность получения личной консультации как у специалиста выбранного направления, так и у консультанта по профессиональной ориентации;

- реализована возможность проведения в ненавязчивой форме анкетирования пользователей;
- благодаря возможности сбора статистики активности пользователя, можно провести анализ его интересов и увлечений.

Литература

1. Лукина В.С. Исследование мотивации профессионального развития // Вопросы психологии. – 2004. – №5. – С. 25–32
2. Патаракин Е.Д.: Устройство сетевых сообществ. – Режим доступа: http://window.edu.ru/window_catalog/redir?id=23859&file=comm-building-pat.pdf
3. The ladder of participation in social media. – Режим доступа: http://internettime.com/2008/10/03/the-ladder-of-participation-in-social-media/
4. Global survey shows 58% of people don't know what social networking is, plus over one third of social networkers are losing interest. – Режим доступа: http://www.synovate.com/news/article/2008/09/global-survey-shows-58-of-people-don-t-know-what-social-networking-is-plus-over-one-third-of-social-networkers-are-losing-interest.html
5. Асташкина В.А., Козьмина Е.А., Попов А.А. Создание и поддержка электронного ресурса для привлечения внимания школьников старших классов к информационным технологиям // Научно-технический вестник СПбГУ ИТМО. – 2007. – Вып. 41. – С. 76–84.
6. The Basic Psychological Features of Cyberspace. – Режим доступа: http://www.rider.edu/~suler/psycyber/basicfeat.html
7. Феномен сетевого сообщества. – Режим доступа: http://vio.fio.ru/vio_35/cd_site/Articles/art_2_1.htm
8. Якоб Нильсен: Интернет-пользователи стали более торопливыми. – Режим доступа: http://www.cybersecurity.ru/net/48747.html

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ИГР ДЛЯ РЕАЛИЗАЦИИ НА МОБИЛЬНЫХ ПЛАТФОРМАХ

А.Ю. Агеев

Научный руководитель – к.т.н., доцент Н.Ф. Гусарова

Разработан и программно реализован сборник обучающих игр с динамически изменяемым контентом и поддержкой беспроводных стандартов связи на мобильных платформах.

Введение

Мобильные устройства все прочнее входят в нашу жизнь, а собственный мобильный телефон имеет почти каждый молодой человек, вне зависимости от уровня культуры и образования. Мотивационный потенциал и обучающие возможности проигрываемого на мобильных устройствах контента исключительно важны для молодежной аудитории.

Рынок мобильных игр – важная развивающаяся область игровой индустрии. Его развитие связывается с тем, насколько мобильные приложения будут ограничены возможностями мобильных устройств. Последнее поколение мобильных устройств имеет цветные экраны высокого разрешения, улучшенную память и другие функциональные возможности, позволяющие сделать мобильные игры более привлекательными, снизить стоимость разработки и приблизить их к играм на «традиционных» платформах.

Быстрая модернизация и ценовая доступность мобильных технологий и приложений делает их использование как средств обучения очень привлекательным и сильно повышает интерес к области обучения с использованием мобильных устройств (m-learning) [1]. В то же время для удовлетворения нужд молодежной аудитории, которая в основном и является пользователями мобильных устройств, недостаточно просто адаптировать существующие методики e-learning [2] к мобильным технологиям. Молодежи нужно, чтобы средства были не только когнитивно-доступны, но и вовлекали их в процесс обучения. Целесообразно, в частности, использовать здесь игровые методики. Такие игры должны:

- напрямую поддерживать обучение путем предоставления возможностей для развития знаний и когнитивных навыков – вовлекая и побуждая к этому на эмоциональном уровне;
- не напрямую мотивировать пользователей обращаться к другим источникам («классическим» библиотекам, документам и т.д.) для обучения.

Анализ обучающего игрового мобильного контента

Проведенный нами анализ показывает, что представленный на рынке обучающий игровой мобильный контент [3] покрывает все существующие на персональных компьютерах игровые жанры (квесты, аркады, стратегии, спортивные игры, симуляторы и т.д.). Они обладают интересной графикой и чаще всего нетривиальной концепцией реализации. Однако, как показывает анализ, с точки зрения возможной технологической базы для организации m-learning в игровой форме они обладают и рядом недостатков.

- Отсутствие расширяемости. Конечный продукт чаще всего состоит только из одной игры, чем существенно уменьшает продолжительность жизни данного приложения, так как любая игра в скором времени надоедает. Приложения, имеющие в своем составе несколько игр, обладают явными преимуществами.
- Узконаправленная специализация. К сожалению, большинство игр ориентировано на школьников начальных классов и является тематически специализированным, при этом огромная часть аудитории остается неохваченной.
- Платный доступ. Наличие бесплатного игрового контента существенно увеличило бы количество конечных пользователей.

Концепция построения игры

Поясним предлагаемую концепцию организации обучающих игр на мобильных платформах на примере конкретной игры. В ходе игры в центре экрана мобильного устройства пользователя появляется различного рода обучающая информация. Интервал обновления информации выбран 9 секунд, что допускает неоднократное прочтение. В ходе игры при наступлении определенных событий, таких как прохождение круга, покупка участка, попадание на особые поля и др., пользователю предоставляется возможность ответить на один из вопросов, показанных ранее. В случае правильного ответа игрок получает вознаграждение.

Обобщенная схема геймплея представлена на рис. 1.

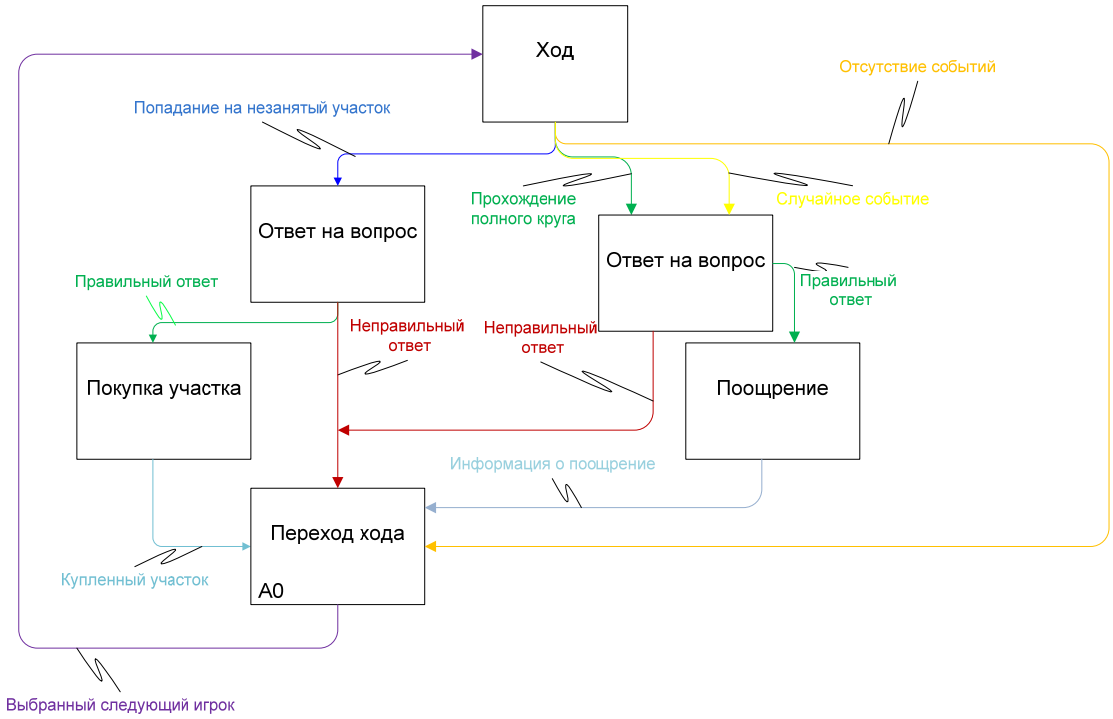


Рис. 1. Обобщенная схема геймплея

В ходе реализации разработанного геймплея были выявлены технологические ограничения, специфичные для интеллектуальных игр на мобильных платформах, а также предложены пути их преодоления:

- сложность организации обратной связи может быть скомпенсирована за счет выбора жанра игры; в реализованном варианте используется такой жанр, как аркада;
- ограниченный базовый функционал, предоставляемый мобильными платформами, расширяется за счет написания собственных программных компонентов;
- ограниченные графические возможности мобильных устройств могут быть скомпенсированы за счет использования графических изображений в качестве управляющих контролов;
- необходимость реализации нескольких игр в одном приложения без существенного усложнения программной реализации, что достигается за счет модульной структуры приложения.

Кроме того, для повышения интереса к игре в концепции предусмотрены следующие возможности:

- организация многопользовательской (сетевой) игры. С этой целью используется технология Bluetooth, встроенная в большинство мобильных устройств;

- легкость внесения и изменения информации разнообразного типа в качестве изучаемого материала. Задаваемые в ходе игры вопросы не зашиты в программу, а могут создаваться программой и храниться в формате XML;
- организация соревновательной среды. Предусмотрен механизм сравнения рейтингов игроков и рекордов игры, который реализуется либо на созданном сайте игры, либо при соединении игроков по Bluetooth.

Перечисленные особенности концепции позволяют динамически создавать специализированные игры образовательной направленности в короткие сроки.

Особенности программной реализации

В качестве платформы для игры выбрана ОС Windows Mobile [4] компании Microsoft, так как доля рынка мобильных устройств, поддерживающих эту ОС, составляет около 60% , что обеспечивает большее количество конечных пользователей. Для реализации была использована SDK Windows Mobile версии 3.5, вышедшая в сентябре 2008 года, что дало наиболее полный функционал доступный на данное время.

Рис. 4. Модульная структура приложения

В качестве среды разработки был взят продукт Microsoft Visual Studio 2008 Team Suite [5] компании Microsoft, так как он дает возможность наиболее полного контроля и управления выбранной платформой. В качестве языка программирования был выбран C#, так этот язык дает возможность быстрого создания приложений и максимально упрощает его.

Разрабатываемое приложение имеет модульную структуру (рис. 4), что делает его достаточно гибким и легким в использовании, дает возможность добавлять свой контент и расширять уже имеющийся. Написанные модули позволяют, основываясь на использовании готовых компонентов, в короткие сроки создавать игры различных типов, в том числе типа карточных, а так же игр, использующих в качестве движущего механизма кубики.

В приложении использованы следующие классы (рис. 4).

- Классы управления:
  - PlayerClass – содержит информацию о всех пользователях и функции изменения их свойств;
  - EducationClass – содержит обучающую информацию, имеет возможности загрузки и последующей ее обработки;
  - BlackJeckClass – содержит информацию о правилах карточных игр и все функции необходимые для расширения игрового спектра;
  - DieClass – содержит информацию о кубике и позволяет встраивать его в любой контент;
  - NetConnections – служит для беспроводной передачи данных;
  - Decode – класс декодирования зашифрованных сообщений;
  - Resourses – содержит все ресурсы, используемые в программе, что также позволяет использовать их при расширении контента.
- Классы графических форм: каждый из них служит для отрисовки отдельной формы и показывает возможности взаимодействия с классами управления; каждый из них может быть взаимозаменен, и на их основе может быть собрана другая игра.

Как отмечалось выше, одной из основных трудностей создания мобильного контента является ограниченность базового функционала, в частности:

- ограничение количества перегружаемых прототипов функций,
- недоступность множества классов и их функций.

Например, стандартный класс `picturebox` имеет порядка 100 методов и около 100 свойств и 100 событий, из них на мобильных устройствах поддерживается меньше половины. В этой ситуации для того, чтобы наложить рисунок на уже имеющийся, вместо того, чтобы изменить значение одного свойства `TransparencyKey`, отвечающего за прозрачность цвета, приходится использовать пространство имен:

```
System.Drawing.Drawing2D;
System.Drawing.Imaging;
```

Используя события отрисовки обьекта, рисуем на нем вручную:

```
Bitmap img = Properties.Resources.house;
ImageAttributes atr = new ImageAttributes();
atr.SetColorKey(Color.Black, Color.Black);
  e.Graphics.DrawImage(img, 0, 0);
```

В процессе работы над приложением был выявлен ряд неисправленных системных ошибок со стороны разработчиков среды разработки. Так, например, класс `Marshal`, служащий для взаимодействия `managed` и `unmanaged` кода и содержащий около 100 функций, из которых на мобильных платформах доступна только половина, имеет ряд системных багов. Эти баги связаны с невозможностью преобразования напрямую ряда типов данных, что приводит к потере данных или к `ArgumentException`. Данную проблему удалось решить путем перегрузки функций преобразования структуры в `IntPtr`, заменив ее на побайтное конвертирование каждого типа данных в отдельности методами того же класса, что заметно утяжелило код.

Так как обучающая информация хранится в XML файле, то вся информация шифруется. Для шифровки используется алгоритм шифрования MD5, достаточный для приложений этого типа. Кроме того, для повышения целостности данных используется проверка на CRC, что полностью исключает подмену информации. Также при попытке исключить обучающую информацию из игры путем удаления файла XML программа будет использовать вопросы, хранящиеся в коде программы.

Ниже представлены схема (рис. 5) и основные фрагменты программной реализации перечисленных характеристик приложения.

Рис. 5. Программная реализация приложения

1. В конструкторе класса основной формы `MainForm` вызывается функция загрузки информации из XML файла, находящаяся в классе `EducationClass`, в случае неуспешного выполнения загрузки выполняется функция загрузки вопросов из памяти программы, находящаяся в том же классе:

```
public EducationClass Education;
public MainForm()
{
//…
      Education = new EducationClass();
      if (!Education.DownloadQuastion())
           {
                Education.SetQuestion();
           }
      //…
}
```

2. Функция загрузки информации `DownloadQuastion` открывает файл с вопросами и считывает информацию, находящуюся в нем, далее проверяет на совпадение CRC, подсчитанное и загруженное из файла, и в случае совпадения вызывает функцию декодирования информации `Decode()` `класса Decoder`.

```
public bool DownloadQuastion()
       {
           try
           {
               XmlDocument Quastion = new XmlDocument();
               Quastion.Load("Question.xml");
               XmlNode QuastionNode = Quastion;
```

```
    //Заголовок
    int QuestionCount = 0;
      XmlNodeList NodeList =
QuastionNode.SelectNodes("Question/Check/");
    CrcRecv = Convert.ToInt32(NodeList[0].InnerText);
    if (CrcCheck(CrcRecv))
    {
            NodeList =
            QuastionNode.SelectNodes("Question/QuestionCount/")
            ;
        QuestionCount = Convert.ToInt32(NodeList[0].InnerText);
        for (int i = 0; i < QuestionCount; ++i)
        {
            NodeList =
            QuastionNode.SelectNodes("Question/Question" + i +
            "/");
             Question[i] = Decode(NodeList[0].InnerText);
            NodeList =
            QuastionNode.SelectNodes("Question/Answer" + i +
            "/");
             Answer[i] = Decode(NodeList[0].InnerText);
        }
        return true;
    }
    return false;
}
catch (Exception c)
{
    String s = c.ToString();
}
return false;}
```

Выводы

Разработан и программно реализован сборник обучающих игр с динамически изменяемым контентом и поддержкой беспроводных стандартов связи на мобильных платформах. Эффективность такого сборника получила первоначальное подтверждение на фокус-группе. В настоящее время ведутся исследования в направлении методической и технологической проработки таких игр.

Литература

1. Rich-media mobile learning (m-learning) [Электронный ресурс]. – Режим доступа: http://www.m-learning.org/
2. Электронное обучение (e-learning) [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/E-learning
3. RESOURCES DOWNLOADS. Educational Software [Электронный ресурс]. – Режим доступа: http://downloads.zdnet.co.uk/0,1000000374,39000759r,00.htm?o=a%2B&p=4
4. SDK Windows Mobile 3.5 [Электронный ресурс]. – Режим доступа: http://www.microsoft.com/downloads/details.aspx?FamilyID=333325FD-AE52-4E35-B531-508D977D32A6&displaylang=ru#Overview
5. Microsoft Visual Studio 2008 Team Suite [Электронный ресурс]. – Режим доступа: http://www.microsoft.com/downloads/details.aspx?FamilyId=D95598D7-AA6E-4F24-82E3-81570C5384CB&displaylang=en

3 БЕЗОПАСНОСТЬ И ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ. ЗАЩИТА ИНФОРМАЦИИ

ИСТОЧНИКИ «МЕРТВОГО КОДА» ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ IBM RATIONAL

Ю.А. Торшенко
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Цель работы – определить, каким образом, и на каком этапе проектирования появляются уязвимости типа неиспользуемого «мертвого кода», к каким последствиям может привести их реализация и какими методами можно не допустить их появление. В статье рассмотрены методы, позволяющие диагностировать появление «мертвого кода» и «вычистить» исходный код приложения от уязвимостей подобного характера.

Введение

На сегодняшний день для разработки приложений масштаба предприятия в короткие сроки все чаще применяются многофункциональные программные среды, построенные на базе CASE-технологий. Использование данного инструментария позволяет ускорить и облегчить процесс разработки, однако привносит с собой в исходный код новые уязвимости, связанные с появлением неиспользуемого «мертвого кода».

К причинам, приведшим к подобному положению, можно отнести частое изменение и недостаточно четкую формулировку требований по безопасности к программному обеспечению (ПО) как со стороны заказчика, так и со стороны руководителей проекта, нехватку ресурсов (в первую очередь временных) и т.п. Таким образом, ощущается острая необходимость в детальном анализе и регулировании всего процесса разработки ПО с точки зрения обеспечения его безопасности в процессе создания и разработки.

Потребность контролировать процесс разработки ПО, прогнозировать и гарантировать стоимость разработки, сроки и качество результатов привела еще в конце 70-х гг. к необходимости перехода от кустарных к индустриальным способам создания ПО и появлению совокупности инженерных методов и средств создания ПО, объединенных общим названием «программная инженерия»(software engineering) [1].

Понятие «программная инженерия» подразумевает, что сам процесс проектирования и создания ПО может являться объектом для исследования. Совершенствование методов проектирования, средств создания и систем контроля функциональности ПО поможет повысить качество вновь разрабатываемых информационных систем (ИС), увеличить их надежность и долговечность.

Уязвимости программного проектирования

Перечисленные выше проблемы породили потребность в программно-технологических средствах специального класса – CASE (Computer-Aided Software Engineering)-средствах, реализующих CASE-технологию создания и сопровождения ПО ИС. В рамках программной инженерии CASE-средства представляют собой основную технологию, используемую для создания и эксплуатации систем ПО [2].

Под CASE-средством (согласно стандарту ISO/IEC 14102:1995) понимается программное средство, поддерживающее процессы жизненного цикла ПО, включая анализ требований к системе, проектирование прикладного ПО и баз данных, генерацию кода, тестирование, документирование, обеспечение качества, управление конфигурацией

ПО и управление проектом, а также другие процессы. CASE-средства вместе с системным ПО и техническими средствами образуют среду разработки ПО. В результате при использовании данных технологий количество ролей персоналий, задействованных в разработке ИС, в целом возросло и приняло следующий вид: автор исходной задачи, системный аналитик, системный аналитик-программист, прикладной программист и системный программист [3].

Таким образом, весь процесс проектирования с использованием CASE-технологии можно схематично представить в виде последовательности действий, выполняемых различными персоналиями (см. рис. 1)

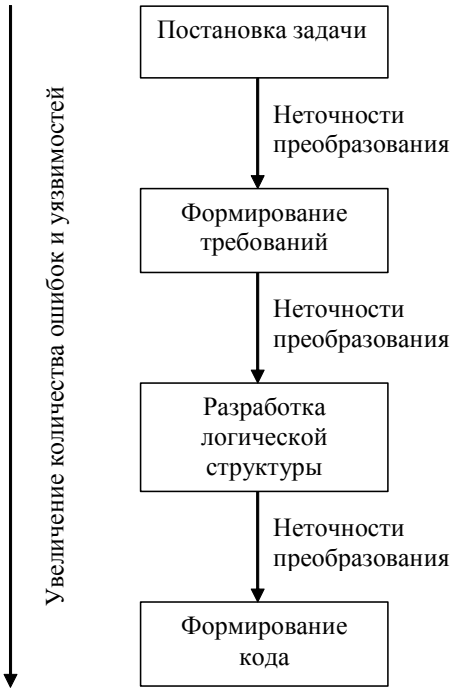


Рис. 1. Этапы проектирования приложения

Каждый из этапов данного процесса выполняется собственным исполнителем (или исполнителями) на подходящем для данной конкретной цели описательном языке, отсюда возникают проблемы, связанные с переходом от одного этапа проектирования к следующему. Интуитивно понятные для одного человека инструкции могут быть неверно истолкованы следующим участником разработки. Как следствие, возникают ошибки, связанные с неточностями преобразования моделей одного уровня в модели другого. А поскольку конечный продукт проходит как минимум три таких преобразования, вероятность появления подобных ошибок чрезвычайно велика. Их наличие в процессе производства ПО может повлиять не только на функциональность продукта, но и на его надежность, так как при возникновении подобных ошибок появляются уязвимости, связанные с тупиковыми технологическими процессами и, как следствие, с избыточностью конечного кода программы.

Методология Rational Unified Process

Одним из наиболее успешных примеров комплексной реализации CASE-технологии можно назвать серию программных продуктов компании IBM, объединенную в методологию Rational Unified Process (RUP). Методология RUP позволяет объединить проектную команду, предоставляя в ее распоряжение проверенные мировой практикой лучшие подходы к разработке ИС. К ним относятся такие процессы жизненного цикла создания ПО, как управление проектами, бизнес-моделирование, управле-

ние требованиями, анализ и проектирование, тестирование и контроль изменений. Внедрение RUP в организации способствует выработке качественных внутрикорпоративных стандартов и повышению общей культуры разработки [4].

Основа RUP – итеративный процесс разработки. В условиях активно развивающегося мирового бизнеса практически невозможно создавать современные сложные программные системы последовательно, т.е. сначала выявлять все проблемы, затем принимать проектные решения, потом формировать программное обеспечение и, наконец, проверять полученное изделие. Итеративный подход позволяет улучшать понимание проблем на основе последовательных усовершенствований и конкретизировать их в эффективных решениях. Этот подход обеспечивает большую гибкость при изменяющихся требованиях и тактических коррективах в бизнес-целях, что позволяет более эффективно и заблаговременно идентифицировать и снижать проектные риски. RUP – управляемый процесс. Итеративный подход предполагает управление требованиями и изменениями, чтобы между всеми участниками проекта обеспечивать единое понимание ожидаемых функциональных возможностей, требуемый уровень качества, наилучшее управление затратами и графиками выполнения работ [4].

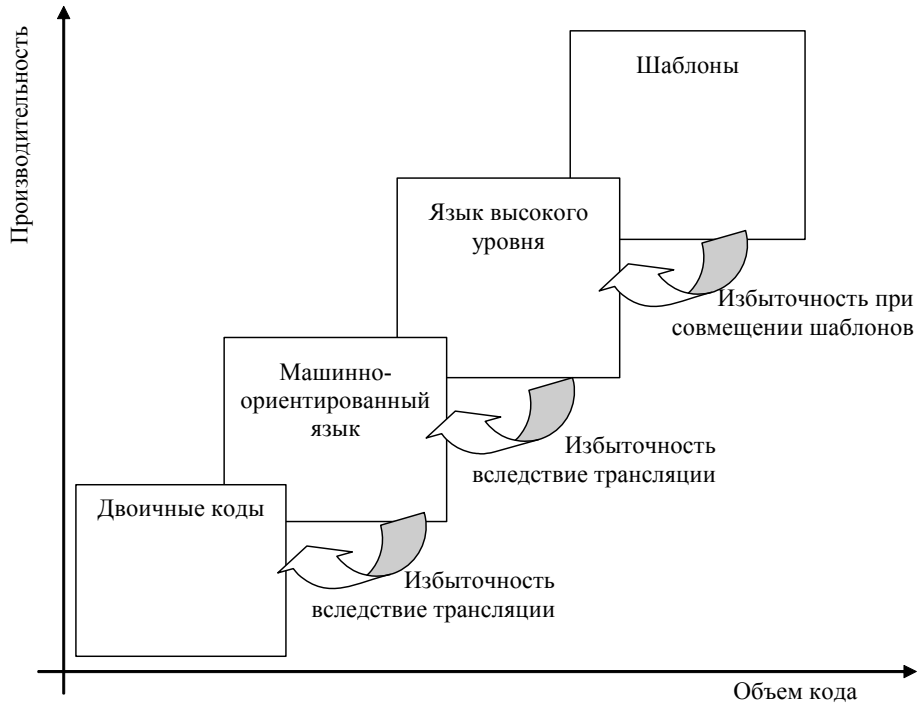


Рис. 2. Усложнение исходного кода при переходе на более высокий уровень программирования

Применение комплексной методологии, такой как RUP, позволяет уменьшить риск возникновения описанных выше ошибок, связанных с неточностями преобразования моделей различного уровня. Однако на данном этапе могут появиться и новые уязвимости: различные элементы модели более высокого уровня преобразуются в элементы моделей более низких уровней программно при помощи заранее предопределенных функций, следовательно, при подобном преобразовании не могут быть учтены все случаи взаимодействия этих элементов друг с другом, что может вызвать за собой усложнение модели и увеличение кода проектируемого программного продукта вследствие повторения некоторых функций или появления ненужных, тупиковых путей развития бизнес-процессов.

Но не только проблемы перехода между моделями влияют на качество конечного программного продукта. Сам процесс непосредственного формирования кода программы нуждается в пристальном рассмотрении (см. рис. 2).

Пути поиска уязвимостей в процессе разработки ПО

На сегодняшний день текст программы формируется при помощи уже имеющихся у программиста шаблонов, библиотек функций, которые при сборке их в единое целое могут неожиданным образом могут повлиять на работу программы. Также использование подобных программных вставок может увеличить и усложнить код относительно того, если бы программа была написана без их использования (что в наше время практически неприемлемо, так как сильно увеличивает время разработки).

Еще одна проблема возникает при компиляции программы, когда компилятор транслирует стандартные функции языка высокого уровня (ЯВУ) в машинные коды. Конечно, каждая функция или оператор ЯВУ в большинстве случаев транслируются оптимальным образом, однако, как показывает практика, программа, написанная на ЯВУ, занимает больший объем памяти, так как совместное использование различных функций языка может отразиться на оптимальности уже откомпилированной программы. Вследствие компиляции могут появиться фрагменты «мертвого» (неисполняемого) кода. Наличие таких фрагментов приводит не только к увеличению кода, но и является значительной уязвимостью, так как увеличивает вероятность появления в данном ПО дефектов и облегчает проникновение в программу вирусов.

Чтобы обнаружить данные уязвимости, необходимо отслеживать процесс производства программного продукта, начиная с самого первого этапа проектирования – постановки требований. Действительно, грамотно сформулированные требования уже представляют собой некоторую логическую структуру будущей программы, а значит – могут быть представлены в виде графа логических взаимодействий. В подобной форме описываются и все промежуточные модели, и исходный код программы. Получив представления продуктов каждого этапа проектирования в идентичной форме, мы будем иметь возможность сравнивать их логику и проверять правильность преобразования моделей и трансляции кода на низкоуровневые языки.

Заключение

В настоящее время для качественной организации бизнес-процессов и обеспечения конкурентоспособности фирм и предприятий требуется все больше функционального ПО, создание которого происходит с использованием инструментально-технологических средств промышленного производства, примером которых является технология IBM Rational. Поэтому сейчас крайне важно уделять внимание решению проблем, связанных с появлением избыточного кода, неточностями преобразования моделей разного уровня, появляющихся в программных продуктах в процессе разработки.

Литература

1. Вендров А.М. Проектирование программного обеспечения экономических информационных систем. – М.: Финансы и статистика, 2005. – 544 с.
2. Вендров А.М. Case-технологии Современные методы и средства проектирования информационных систем. – М.: Финансы и статистика, 1998. – 176 с.
3. Громов Г.Р. От гиперкниги к гипермозгу: информационные технологии эпохи Интернета. Эссе, диалоги, очерки – М.: Радио и связь, 2004. – 208 с.
4. IBM Rational Software. Обзор продуктов и решений 2007. – М., 2007. – 92 с.

ПРЕДОТВРАЩЕНИЕ WORMHOLE АТАК В БЕСПРОВОДНЫХ СЕТЯХ С ПОМОЩЬЮ ПАКЕТНЫХ МЕТОК

И.Ю. Иващук
Научный руководитель – к.т.н., доцент А.В. Птицын

Рассмотрены атаки на беспроводные сети, действующие по принципу червя. Приведена классификация подобных атак на основе методики их реализации. Для предотвращения подобных атак вводятся понятия географических и временных меток, которые ограничивают дальность передачи пакетов в сети.

Введение

В беспроводных сетях свободной конфигурации (так называемых ad-hoc сетях) требования, предъявляемые к безопасности, являются одними из основополагающих. Перспективы развития подобных сетей все больше привлекают к себе внимание широкого круга пользователей. Большинство предыдущих исследований в этой области было сфокусировано на проблемах маршрутизации и коммуникации между узлами сети в доверенной среде. В то же время большинство приложений работает во враждебной окружающей среде и, соответственно, предъявляет серьезные требования к безопасности.

В рамках данной статьи будут рассмотрены wormhole (действующие по принципу червя) атаки, которые представляют серьезную угрозу для беспроводных сетей. Суть данного вида атак заключается в том, что атакующая сторона прослушивает весь трафик сети, записывает его и передает по виртуальному каналу узлу-соучастнику, расположенному на достаточном отдалении, который уже непосредственно передает информацию в сеть. Причем передаваться может не полностью весь трафик, а отдельные пакеты или даже отдельные биты этого пакета. Это чрезвычайно негативно сказывается на протоколах маршрутизации, которые используются в сети, потому что становится практически невозможно построить правильные маршруты между узлами, находящимися на расстоянии более одного либо двух «прыжков».

Для защиты беспроводных сетей от подобных атак введем понятие пакетных меток. Под этим мы будем понимать некоторый служебный маркер, который добавляется в пакет и накладывает ограничения на максимально возможную дальность его передачи. Различают два вида подобных меток: географические и временные. Прежде, чем приступать к рассмотрению средств защиты от атак, действующих по принципу червя, рассмотрим сами атаки, вернее их классификацию.

Классификация атак, действующих по принципу червя

Wormhole атаки на беспроводные сети стали настолько распространены, что уже появилось несколько видов их классификации. Одна из них рассматривает подобные атаки с точки зрения их развертывания в сети.

По средствам инкапсуляции пакетов. Используются в сетях, которые строят свои таблицы маршрутизации на протоколах, основывающихся на поиске наикратчайшего пути между конечными точками. При развертывании подобной сети первым этапом является построение самой таблицы маршрутизации. Для этого все узлы широковещательно рассылают специальные служебные сообщения. Когда любой узел в сети получает такое сообщение, то он его обрабатывает и высылает узлу-отправителю свой ответ на него. На основе этих ответов и строится таблица маршрутизации. Наилучшим маршрутом считается тот, который составляет наименьшее число «прыжков» до требуемого узла. Один из способов двум узлам-злоумышленникам принять участие в маршрутизации пакетов – это создать иллюзию того, что маршрут через них является наикратчайшим, хотя на самом деле они могут находиться в разных концах сети.

Рассмотрим, как это происходит. Пусть узлы A и B хотят найти наикратчайший маршрут между собой. Для этого узел A широковещательно рассылает служебные запросы в сеть. Предположим, что в этой же сети находятся два злонамеренных узла X и Y. Когда узел X получает подобный запрос от узла A, он инкапсулирует его и по туннелю, существующему между узлами X и Y через другие узлы, передает своему «напарнику». Узел Y, в свою очередь, распаковывает пакет и возвращает его в сеть так, чтобы его смог получить узел B. Особо следует отметить, что при инкапсуляции пакета счетчик «прыжков», имеющийся в каждом пакете, не возрастает, хотя при туннелировании он и обрабатывается узлами, располагающимися между X и Y. Поэтому зачастую для узла B этот маршрут будет казаться самым выгодным, хотя на самом деле это не так.

Все беспроводные сети, в которых используются протоколы маршрутизации на основе метрик расстояния между узлами, уязвимы к данному классу атак, действующих по принципу червя. Это, пожалуй, самые тривиальные wormhole атаки для реализации в сети, так как узлам, участвующим в ней, совсем не обязательно знать какие-либо криптографические ключи либо иметь в своем распоряжении дополнительные ресурсы, такие как высокомощный передатчик сигнала.

Один из самых простых способов для предотвращения подобных атак – это использование в сети протоколов маршрутизации, основывающихся на других метриках при построении маршрутов, например, на быстроте ответа на запрос о маршрутизации, таких как ARAN (*Authenticated Routing for Adhoc Networks*) [1].

С использование внеполосного канала передачи сигнала. Этот класс атак основывается на том, что между двумя злоумышленными узлами существует внеполосный высокоскоростной канал. Соответственно, маршрут, который пройдет через подобный туннель, будет короче и быстрее по сравнению с маршрутами через легитимные узлы. Он более сложен в реализации, так как для организации подобной атаки необходимо дополнительное оборудование.

С использование высокомощных передатчиков. Для реализации этого класса атак злоумышленный узел при получении широковещательного сообщения передает его на другом энергетическом уровне, который значительно выше по сравнению с уровнем, принятым в сети, поэтому другие узлы не могут его использовать. Любой узел, который слышит высокомощную широковещательную передачу, ретранслирует сигнал сразу же напрямую получателю. При использовании подобного метода значительно возрастают шансы атакующей стороны, что необходимый маршрут между источником и приемником будет проложен через скомпрометированный узел даже без участия так называемого узла-соучастника.

Самый простой способ противостоять данной атаке – это измерение мощности принимаемого сигнала каждым узлом в сети, в этом случае беспроводные узлы независимо друг от друга смогут определить, была ли передача легитимной или нет.

С использованием ретрансляции пакетов. В данном классе wormhole атак узел-злоумышленник ретранслирует пакеты между двумя удаленными узлами, чтобы убедить их, что они являются соседями. Данная атака может быть реализована даже одним скомпрометированным узлом. Взаимодействие большего количества узлов на атакующей стороне может привести к тому, что беспроводные интерфейсы, находящиеся на расстоянии нескольких «прыжков» друг от друга, будут считать себя соседствующими. Противостоять подобным атакам можно лишь программными средствами, например, с помощью внедрения специальных протоколов аутентификации пакетов между узлами.

С использованием девиации протоколов. Некоторые протоколы маршрутизации, например ARAN (Authenticated Routing for AdHoc Networks), строят таблицу маршрутизации, основываясь на минимальной задержке при передаче пакета, а не на кратчайшем расстоянии между узлами. Причем при получении пакета-запроса узел

ретранслирует его в сеть через случайный промежуток времени. Это связано с широковещательной природой передачи в сеть подобных запросов, отсюда возникает требование к уменьшению коллизий на MAC уровне. Узел, участвующий в проведении атаки, может ретранслировать пакеты-запросы в сеть вообще без задержек. Это делается для того, чтобы пакет от узла-злоумышленника пришел первым, и маршрут между узлами проходил именно через него.

Суммируя все сказанное, составим таблицу, в которой приведены основные требования для реализации разных классов беспроводных атак, действующих по принципу червя [2].

Название класса атаки	Минимальное количество скомпрометированных узлов для проведения атаки	Специальные требования
Пакетная инкапсуляция	Два	Отсутствуют
Внеполосной канал	Два	Внеполосный канал
Высокомощная передача	Один	Высомощный передатчик
Ретрансляция пакетов	Один	Отсутствуют
Девиация протоколов	Один	Отсутствуют

Таблица. Требования для реализации wormhole атак по классам

Пакетные маркеры

Для нахождения и предотвращения подобных атак в сети существует достаточно много различных методик – как аппаратных (использование направленных антенн), так и программных (использование протоколов аутентификации, например TrueLink). Рассмотрим одну из методик, основывающуюся на добавлении в информационный пакет специального маркера, который накладывает некоторые ограничения на дальность распространения пакета. Как уже упоминалось выше, существует два вида подобных маркеров: географические и временные. Географические метки подтверждают тот факт, что получатель пакета находится в пределах зоны действия его отправителя. Временные же метки вводят в пакет его время жизни, в соответствии с которыми и ограничивается расстояние для его передачи, так как пакет не может передвигаться в сети быстрее скорости света. Оба вида этих меток помогают предотвратить wormhole атаки, так как они позволяют получателю пакета определить, прошел ли пакет большее расстояние, чем то, которое позволяет ему маркер.

Географические метки

Для введения такого понятия, как географические метки, каждый узел должен знать свое местоположение, а все узлы рассматриваемой сети должны обладать примерно синхронизированными между собой часами.

Когда узел формирует пакет для передачи другому узлу, он включает в него координаты своего расположения p_s и время, когда этот пакет был отослан t_s. При получении пакета взаимодействующим узлом он сравнивает эти значения со своим расположением p_r и временем, когда он получил данный пакет t_r. Если часы между отправителем и получателем синхронизированы с точностью $\pm\Delta$, а v является верхним пределом возможной скорости передачи любого из узлов в сети, то узел-получатель может вычислить предельное расстояние между отправителем и самим собой d_{sr}.

Основываясь на временных метках t_s и t_r, максимальной допустимой ошибке при определении местоположения узла δ и непосредственно на местоположениях узла-отправителя и узла-получателя p_r и p_s соответственно, максимально возможное рас-

стояние между двумя узлами при передаче сообщения можно представить в следующем виде:

$$d_{sr} \le \|p_s - p_r\| + 2v \cdot (t_r - t_s + \Delta) + \delta .$$

Стандартная схема цифровой подписи или другие подобные методы для аутентификации могут быть использованы для того, чтобы узел-получатель мог корректно аутентифицировать в полученном пакете географическую либо временную метку. Этот подход близок к тому, который описывается в [3].

Но при определенном стечении обстоятельств накладываемые ограничения на дальность передачи информационных пакетов не всегда могут предотвратить wormhole атаку. Это может произойти в том случае, если между двумя узлами, которые находятся в радиусе передачи друг друга, расположена какая-либо непреодолимая преграда. В сетях, которые используют местоположения узлов для генерации географических меток, можно исключить подобные случаи. Для этого каждый узел должен знать модель прохождения собственного сигнала. Тогда узел-получатель сможет определить любое возможное местоположение узла-отправителя (сигнал будет распространяться на следующую величину $\delta + v(t_r - t_s + 2\Delta)$).

Временные метки

Для генерации временных меток все узлы в сети должны обладать точно синхронизированным временем, причем максимальное отклонение не должно превышать величины Δ. Значение параметра Δ должно быть известно также всем узлам и не должно превышать нескольких микросекунд или даже сотен наносекунд. Такой высокий уровень синхронизации может быть достигнут с помощью GPS [4] или атомных часов. Но стоит отметить, что подобное оборудование не является неотъемлемой частью беспроводной сети. Это связано с тем, что оно довольно-таки недешево, а также энерго- и ресурсоемко. Это требование значительно ограничивает сферу применения временных меток, но в то же время атаки, действующие по принципу червя, являются далеко не тривиальными и могут нанести непоправимый вред работоспособности сети, что оправдывает подобные затраты.

Для использования временных меток узел-отправитель при отправке пакета включает в него время отправки t_s; при получении пакета узел-получатель сравнивает это время со временем получения пакета t_r. При этом можно определить, как долго шел пакет, основываясь на значениях времени передачи и скорости света.

Еще один способ использовать временные метки – это включать в пакет его время жизни, после истечения которого узел-получатель не будет принимать подобные пакеты. Также, основываясь на максимальном радиусе передачи пакета и скорости света, узел-отправитель вычисляет время жизни пакета, и эта величина включается в пакет как смещение относительно времени отправки пакета. Как и в случае с географическими метками, можно использовать цифровую подпись либо любой другой протокол аутентификации, чтобы узел-получатель смог корректно аутентифицировать временную метку в полученном пакете. Очевидно преимущество географических меток над временными, так как их применение не нуждается в точной синхронизации времени между узлами сети.

Введем величину $\delta'(t)$, которая будет определять максимально допустимую ошибку при определении местоположения узла за некоторое время t. По определению $\delta'(t) \le 2\delta$. При достаточно малом значении t значение $\delta'(t)$ будет тоже достаточно мало, так как алгоритм для определения местоположения узла должен учитывать физические ограничения по скорости беспроводных узлов. Если мы предположим, что один из узлов находится в точке p_1 и p_2 соответственно в момент времени t_1 и t_2, то он является злонамеренным при выполнении следующего условия

$$\frac{\|p_2 - p_1\| - \delta'(|t_2 - t_1|)}{|t_2 - t_1|} > \nu .$$

Любой узел в сети по полученным двум пакетам сможет определить легитимность узла-отправителя и с помощью широковещательных сообщений сообщить другим узлам о злонамеренных действиях одного их них. Любой узел, получивший такое сообщение, идентифицирует его отправителя, а затем анализирует само сообщение. Если не было найдено никаких отклонений, то впоследствии он широковещательно отправляет его в сеть, но уже от своего имени. Чтобы избежать при такой рассылке широковещательного шторма, каждый узел обладает так называемым «черным списком», каждая запись в котором содержит адрес узла и время существования этой записи. Когда узел получает сообщение о странном поведении одного из узлов сети, он проверяет, существует ли уже запись об этом в его черном списке. Если она уже есть, то увеличивается предельное время существования данной записи и широковещательные сообщения не рассылаются. Если же при проверке совпадение не находится, то в черный список добавляется новая запись и осуществляется широковещательная рассылка.

Неявная проблема при использовании временных меток заключается в том, что при использовании ассоциативных MAC протоколов узел-отправитель может и не знать точного времени отправки пакета. Например, при использовании MAC протоколов стандарта IEEE 802.11 узел-отправитель сможет узнать время отправки пакета только в пределах одного такта времени (т.е. не ранее, чем за 20 мкс до непосредственной отправки).

На генерацию цифровой подписи с использование малоэффективного шифра, как, например, на основе алгоритма RSA с 1024-битным ключом, может потребоваться чуть ли не в три раза больше времени, чем один такт (т.е. порядка уже 10 мс). В то же время существует два подхода, которые могут уменьшить влияние времени задержки при генерации цифровой подписи: увеличение значения минимально возможного такта времени либо использование более эффективных схем для создания цифровой подписи, например схемы Шнайера [5].

Анализ безопасности при применении маркеров

Пакетные метки позволяют узлам убедиться в том, что взломщик, реализующий wormhole атаку, не распространяет сигнал дальше, чем это возможно. При использовании географических меток узлы также могут определить, туннелируется ли сигнал через имеющиеся препятствия, например горы, которые являются преградой на пути распространения радиосигнала.

Со временем любые атаки становятся все более сложными и изощренными, и уже недостаточно включать в пакет географическую или временную метку, чтобы выявить атаку, действующую по принципу червя. Если узел-отправитель является злоумышленником, то он может запросто подменить необходимый маркер в пакете. Это может привести к тому, что узел-получатель не сможет определить, был ли туннелирован пакет перед этим или нет. Для защиты маркеров в пакете вводятся различные криптографические примитивы, которые и позволяют получатель аутентифицировать не только легитимность пришедшего пакета, но и легитимность содержащейся в нем географической либо временной метки.

Сравнение географических и временных меток

Временные метки намного более эффективны для защиты беспроводной сети от wormhole атак, особенно при введении специального протокола TIK (*Tesla with Instant Key disclosure*) [6]. Если же с этих позиций посмотреть на географические метки, то

они предъявляют не такие жесткие требования к механизму аутентификации, что в результате приводит к увеличению как циркулирующей в сети служебной информации, так и нагрузки на сеть в целом.

Преимущество географических меток заключается в том, что они используют модель распространения радиосигнала, что позволяет с их помощью обнаруживать туннели даже при наличии помех в сети. Также, как уже неоднократно упоминалось выше, географические метки не требуют точной синхронизации времени по сравнению с временными. В частности, временные метки не могут быть использованы, если максимальная дальность передачи сигнала менее $c\Delta$, где c – скорость света, а Δ – максимальная ошибка при синхронизации времени. В то же время географические метки могут быть использованы, даже если максимальная дальность передачи – менее $2v\Delta$, где v – максимальная скорость перемещения любого узла.

Чтобы оценить практичность использования географических меток, введем рассмотрим пример. Пусть дальность передачи сигнала у любого узла равна 300 м, максимальная скорость движения узла 50 м/с, относительная ошибка при определении местоположения узла 3 м и ошибка при синхронизации времени 1 мс. Соответственно $t_r - t_s \le 2мс$, так как время распространения сигнала не превышает 1 мс, как и ошибка при синхронизации времени. Отсюда получаем:

$$d_{sr} \le \|p_s - p_r\| + 100м/с \cdot 2мс + 3м = \|p_s - p_r\| + 3{,}2м .$$

Так как $\|p_s - p_r\|$ не может превышать 3 м, как следует из первоначальных условий, то эффективный диапазон передачи сигнала любого интерфейса в сети уменьшается до 6,2 м.

При сравнении эффективности использования географических и временных меток мы сопоставляем расстояние между двумя узлами при передаче для одного и второго подходов: $d_{sr} \le \|p_s - p_r\| + 2v \cdot (t_r - t_s + \Delta) + \delta$ – для географических меток; $d_{sr} \le c \cdot (t_r - t_s + \Delta)$ – для временных меток. Мы вводим величину $\frac{d_{\max}}{c}$ для обозначения максимального времени распространения сигнала. Из этого следует, что максимальная ошибка при его определении составляет $\delta + 2v\left(\frac{d_{\max}}{c} + 2\Delta\right) + \delta = 2\delta + 4v\Delta + 2v\frac{d_{\max}}{c}$ – для географических меток; $2c\Delta$ – для временных меток.

Поэтому географические метки наиболее эффективны при $\delta < c\Delta - 2v\Delta - \frac{v}{c}d_{\max}$. Учитывая, что v много меньше *c,* и исходя из имеющийся вычислительной мощности и пропускной способности сети, географические метки следует использовать в том случае когда $\delta < c\Delta$, а временные – при $\delta \ge c\Delta$ [7].

Заключение

В данной статье представлены сравнительно мощные wormhole атаки, которые могут привести к серьезным последствиям для протокола маршрутизации в ad-hoc сетях. Также эти атаки могут быть реализованы в других классах беспроводных сетей, например, в беспроводных системах контроля доступа. Чтобы выявить и впоследствии предотвратить атаки, действующие по принципу червя, были разработаны пакетные метки. Они бывают двух видов – географические и временные – и ограничивают максимальную дальность передачи информационного пакета. Также для улучшения качеств временных меток был разработан протокол TIK, который позволяет осуществить мгновенную аутентификацию полученного пакета.

Географические метки немного менее эффективны по сравнению с временными, так как для них необходима широковещательная аутентификация, но зато подобные метки можно применять в сетях, в которых невозможно реализовать точную синхронизацию времени. Доминирующим фактором при использовании географических меток является возможность точного нахождения местоположения узла, потому что движение любого узла в сети очень незначительно относительно скорости света.

Литература

1. Johnson D.B., Maltz D.A., Broch J. The dynamic source routing protocol for multihop wireless ad-hoc networks. – Addison-Wesley, 2001. – 569 p.
2 . Khalil I., Bagchi S., Shroff N.B. LiteWorp: a lightweight countermeasure for the wormhole attack in multihop wireless networks // Dependable System and Networks. – 2006. – Vol. 1. – P. 612–621.
3. Desmedt Y. Major security problems with the «Unforgeable» (feige) fiat-shamir proofs of identity and how to overcome them // Proceedings of the 6th worldwide computer congress on computer and communications security and protection. – 1998. – Vol.3. – p. 147–149.
4. Clark T. Totally accurate clock synchronization. – Maryland: Greenbelt, 2002. – P. 247.
5. Schnorr C.P. Efficient signature generation by smart-cards // Journal of cryptology. – 2001. – Vol. 4. – P. 161–174.
6. Perrg A., Canatti R., Tygar D., Song D. Efficient authentication and signature of multicast streams over lossy channels // Proceedinds of the IEEE symposium on research in security and privacy. – 2000. – Vol. 5. – P. 56–73.
7. Hu Y-C., Perrig A., Johnson D.B. Wormhole attacks in wireless networks // IEEE design & test of computers. – 2004. – Vol. 24. – P. 370–396.

МОДЕЛИРОВАНИЕ ПРОЦЕССА ПЕРЕДАЧИ ЗАКРЫТОЙ ИНФОРМАЦИИ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

А.И. Спивак
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Создание системы безопасного взаимодействия все чаще является неотъемлемой частью построения всей информационной структуры организации. Это позволяет наравне с мобильностью и простотой использования внутренних ресурсов организации сотрудниками сохранять защищенность и безопасность внутренней сети организации.

Введение

Безопасная передача закрытой информации по открытым каналам связи представляет собой достаточно важную составляющую защищенной работы практически любой информационной системы. Необходимо совершенствовать не только средства, позволяющие должным образом закрывать информацию, но и пытаться на основе знаний о среде передачи строить наиболее безопасные маршруты следования защищаемой информации, рассчитывать степень угрозы раскрытия информации при передаче по разным участкам пути следования защищаемой информации. Знание всех этих параметров передачи информации позволяет производить моделирование процесса передачи информации по открытым каналам связи. Хотя шифрование данных и является достаточно мощным средством закрытия информации, на него нельзя всецело надеяться, поскольку, как правило, неизвестны вычислительные мощности стороны, к которой могут попасть передаваемые зашифрованные данные [1]. Конечно, пренебрегать этим средством защиты тоже нельзя, необходимо комплексное использование всех доступных методов защиты передаваемой информации.

Описание метода моделирования

Для расчетов модели предлагается перенести законы теории электротехники на процессы передачи информации с целью их формализации.

Для использования ТОЭ при расчете каналов передачи данных необходимо переопределить понятия, используемые в стандартной электротехнике. Напряжению тока больше всего соответствует защищенность процесса передачи, силе тока – пропускная способность, сопротивлению – деструктивное воздействие со стороны злоумышленников. Таким образом, переопределив понятия, определим простейшие формулы.

$$I = \frac{q}{t}. \qquad (1)$$

– при делении количества передаваемой информации на время, за которое она была передана, получим пропускную способность системы передачи.

$$I = \frac{U}{R}. \qquad (2)$$

– пропускная способность прямо пропорциональна защищенности и обратно пропорциональна деструктивному воздействию со стороны злоумышленников:

$$W = IUt. \qquad (3)$$

– работа по обеспечению защищенной передачи информации за время t равняется произведению времени, защищенности и пропускной способности.

$$P = IU. \qquad (4)$$

– эффективность работы по защите равняется произведению защищенности и пропускной способности.

Необходимо отметить, что понятие пропускной способности в данной теории имеет несколько характерных особенностей. Прежде всего, она напрямую зависит от защищенности: чем выше защищенность, тем выше пропускная способность за счет более совершенных средств защиты (работают с большей производительностью) и оптимизированных алгоритмов. Деструктивное воздействие снижает пропускную способность, так как количество угроз безопасности в таком случае увеличивается и системе безопасности необходимо тратить большее количество ресурсов (вычислительных, дисковых и разделяемых) на их нейтрализацию.

Рассмотрим варианты изменений величин, входящих в формулу $I = \frac{U}{R}$. При увеличении деструктивного воздействия происходит снижение пропускной способности из-за увеличения затрат ресурсов системы защиты, а при уменьшении имеет место обратный процесс. При увеличении защищенности пропускная способность растет благодаря увеличению эффективности работы систем защиты. При уменьшении защищенности падает пропускная способность – требуется больше вычислительных мощностей и ресурсов.

Заключение

Основным применением рассмотренной теории можно назвать выбор наиболее приемлемого пути следования защищаемой информации на основе расчета показателей защищенности, деструктивного воздействия со стороны канала связи и узлов, а также пропускной способности. В частности, действующие в настоящий момент протоколы маршрутизации в открытых сетях используют для выбора того или иного маршрута следования пакета информации метрики. В качестве метрик могут использоваться пропускная способность канала, количество узлов до пункта назначения либо более совершенные алгоритмы расчета кратчайшего пути. Но ни один и протоколов не учитывает важность передаваемой по каналу связи информации. В дальнейшем возможно подключение такого рода возможностей к открытым протоколам маршрутизации, например OSPF [2], включение в алгоритм принятия решения еще одной метрики либо изменение существующего алгоритма расчета таблицы маршрутизации.

Литература

1. Данилов И.А., Иванов П.М. Общая электротехника с основами электроники. – М.: Высшая школа, 1999.
2. Антонова О.А., Глудкин О.П. и др. Электротехника и основы электроники. / Под ред. проф. О.П. Глудкина. – М.: Высшая школа, 1993.

МЕТОДЫ КОЛИЧЕСТВЕННОГО ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Д.А. Котенко
Научный руководитель – д.т.н., профессор А.А. Молдовян

В статье проанализированы существующие методы количественного оценивания безопасности автоматизированных систем. Приведены примеры реализации и выявлены недостатки методов. Сделан вывод о предпочтительности использования методов логико-вероятностного моделирования для оценки защищенности автоматизированных систем.

Введение

Согласно действующим стандартам (ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 13335-1), обеспечение информационной безопасности (ИБ) автоматизированных систем (АС) организуется в виде совокупности управляемых процессов, реализуемых на базе циклической модели корпоративного менеджмента с использованием установленных подходов к анализу риска (ГОСТ Р ИСО/МЭК ТО 13335-3, ТО 13335-5), выбора механизмов обработки риска (ГОСТ Р ИСО/МЭК ТО 13335-4), а также процедур менеджмента инцидентов (ISO/IEC TR 18044) и менеджмента качества (ГОСТ Р ИСО 9001). Устойчивость и равновесие системы обеспечения ИБ АС достигается путем регулярного оценивания соответствия ИБ требованиям, формируемым в рамках подхода к профилированию защиты (ГОСТ Р ИСО/МЭК 15408, ГОСТ Р ИСО/МЭК 18045).

Во многих случаях качественных оценок (бинарного типа: соответствует/не соответствует требованиям; балльного типа: низкое, среднее, высокое соответствие требованиям и т.п.) недостаточно, чтобы ответить на вопрос, насколько обеспечена безопасность АС, и, таким образом, наметить ясные пути совершенствования системы обеспечения ИБ. В этой связи детерминистский подход к оцениванию ИБ, связанный с общей проверкой требований, содержащихся в системе нормативных документов, регламентирующих ИБ, представляется хотя и важным, но не единственно возможным подходом к оцениванию безопасности.

Для получения вполне обоснованных оценок соответствия ИБ требованиям ГОСТ более приемлемыми оказываются количественные методы. Поскольку эти методы используют положения теории вероятности, они получили название вероятностных методов. Следует отметить, что вероятностные и детерминистские методы не могут рассматриваться без взаимосвязи друг с другом. При необходимости детального анализа рисков АС эти методы являются взаимодополняющими. В ходе комбинированного анализа рисков любой из методов может оказаться приоритетным, в зависимости от требований к уровню безопасности выделенного компонента АС. В ряде случаев используется рекурсия, когда детерминистские показатели ссылаются на вероятностные и наоборот, что приводит к наиболее верному и обоснованному результату. Часто вероятностные методы можно вообще рассматривать как методы, оперирующие набором детерминистских показателей, характеризующихся определенной вероятностью проявления.

Вероятностные методы оценивания защищенности АС

К вероятностным методам относятся методы многокритериальной оптимизации, логико-вероятностные методы, имитационное моделирование и др.

Основой методов многокритериальной оптимизации является агрегирование информации о частных показателях качества. Среди них выделяют методы лексикографи-

ческого упорядочивания, итерационные методы предпочтительного выбора, аксиоматический подход с использованием теории полезности и пр.

Рассмотрим, например, один из итерационных методов – метод «смещенного идеала». Пусть задано n объектов, оцененных по *m* критериям: $k_1 ... k_m$. Процедура оптимизации такова.

1. Моделируются два многокритериальных объекта (МКО): $МКО^+ = \{k_1^+, ..., k_m^+\}$, $МКО^- = \{k_1^-, ..., k_m^-\}$ – «условно предпочтительный», формируемый из максимальных по полезности значений критериев, и наихудший – из минимальных по полезности значений критериев.

2. Задается вектор предпочтений, например, $w_1 = (4,3,3,2)$. Он отражает предпочтения лица, принимающего решение в отношении оптимизируемых показателей эффективности.

3. Чтобы выявить объекты, которые не претендуют на предпочтительные, их сравнивают с идеальным, вычисляя «расстояние» (метрику) до идеального. Так, объекты ранжируются по расстоянию от идеального объекта, например: $B_1 > B_4 > B_2 > B_3$. Наименее предпочтительный объект исключается из рассмотрения, после чего процедура повторяется. Таким образом, исключая неподходящие объекты, в конце получаем один, наиболее предпочтительный.

Логико-вероятностные методы позволяют получить количественную оценку риска как меры опасности. Они давно применяются в отечественной практике для анализа надежности и безопасности систем. В основе лежат два понятия – степень риска $K_{риск}(y)$ и уровень защищенности $K_{защ}(y) = 1 - K_{риск}(y)$ Степень риска – вероятность невыполнения системы обеспечения информационной безопасности (СОИБ) своей целевой функции. Обратная величина характеризует уровень защищенности. Оценка защищенности представляет собой процедуру оценки показателей $K_{риск}$ и $K_{защ}$ для активов информационной системы (ИС). Процедура анализа следующая.

1. Составляется сценарий развития опасности (граф вида «дерево»), представляющий собой логико-вероятностную модель функционирования ИС. Сценарий содержит события трех видов: инициирующие, промежуточные и конечные. Инициирующие события описывают входные воздействия на систему (несанкционированный доступ (НСД) к ресурсам информационной системы, имитация процедуры идентификации/аутентификации и пр.). Промежуточные события – логическая комбинация (конъюнкция или дизъюнкция) исходных. Конечное событие описывает опасное состояние системы (успешная реализация атаки нарушителя пр.).

2.Аналитически граф описывается с помощью функции опасности системы, где $z_1 ... z_n$ инициирующие события, а значение $y(z_1 ... z_n)$ – конечное (опасное) событие. По этой функции можно выделить так называемые кратчайшие пути опасного функционирования. Каждый из них представляет собой минимальный набор инициирующих событий, конъюнкция (совмещение) которых приводит к опасному состоянию.

3. С помощью логико-вероятностных преобразований функция опасности системы приводится к одной из канонических форм и заменяется вероятностной функцией $P\{y(z_1 ... z_n)\}$. При этом необходимо иметь вероятности инициирующих событий (например, вероятность НСД, вероятность взлома системы идентификации и аутентификации и пр.). Значение вероятностной функции P, при которой значение функции опасности y равно 1 (это означает наступление опасного события), и определяет степень риска, присутствующего в системе:

$$K_{риск}(y) = P\{y(z_1 ... z_n) = 1\}$$

Трудность здесь заключается в обеспечении достоверности исходных данных (характеристик ИС, моделей угроз, моделей уязвимостей и т.д.). Объективными являются характеристики ИС по результатам натурных испытаний. Качественно иную (субъективную) природу имеют результаты анализа уязвимости, отражающие интуитивные представления о возможности и характере реализации угрозы.

Еще один метод – имитационное моделирование. Это вычислительный эксперимент, основанный на том известном факте, что при увеличении числа испытаний n относительная частота появления случайного события A в серии испытаний стремится к его вероятности в единичном испытании, $w \Rightarrow P(A)$ при $n \Rightarrow \infty$. С помощью генератора случайных чисел получают выборки случайных величин, распределенных по известному закону с известными математическим ожиданием и дисперсией. Приведем пример. В информационной системе используется система обнаружения вторжений с вероятностью обнаружения $P_{обн} = 0{,}95$. Для имитационного моделирования работы такой системы «разыгрывается» равномерно распределенное случайное число K от 0 до 1. Если $K \le 0{,}95$, система сработала, в противном случае – нет. Таким же образом моделируется действия нарушителя и другие случайные процессы в ИС, приводящие к нарушениям информационной безопасности.

Каждая конфликтная ситуация в ИС просчитывается много раз, по результатам набирается статистика нарушений ИБ. Эффективность СОИБ оценивается статистически как отношение числа нарушений к общему числу испытаний $W=m/n$. Количество опытов определяется исходя из того, что при заданной доверительной вероятности необходимо обеспечить требуемую точность оценки.

Заключение

Достоинством детерминистического подхода является то, что в руки проектировщика даются четкие и ясные критерии того, как должна быть построена система обеспечения информационной безопасности. Основная проблема – способ получения интегрального показателя. Наиболее распространена операция осреднения частных показателей. Но, необходимо помнить, что операция осреднения имеет смысл, если частные показатели однотипны, то есть имеют одинаковую физическую природу. Если это не так, такой интегральный показатель не имеет физического смысла.

Достоинством имитационного моделирования является физически обоснованный критерий эффективности (вероятность). Недостаток – трудность его интерпретации и нормирования. Пусть в результате анализа получено значение $P_{рез}$. Не ясно, много это или мало, достаточен уровень защиты объекта или нет?

В результате использования логико-вероятностных методов для анализа эффективности СОИБ тоже получается число $K_{риск}(y)$. Но смысл здесь не в цифре, а в том, что логико-вероятностное моделирование позволяет построить модель безопасного функционирования ИС, определить «уязвимые места» системы и оценить «вклад» каждого из них, ранжируя их по степени опасности. В качестве недостатков здесь можно отметить трудоемкость логических преобразований при анализе сложных сценариев (переход от функции опасного состояния к вероятностной функции), а также разнородность исходных данных (объективных, которые можно достоверно оценить, и субъективных, отражающих «ожидания угрозы»).

Литература

1. Цуканова О.А., Смирнов С.Б. Экономика защиты информации / Учебное пособие. – СПб: СПбГУ ИТМО, 2007. – 59 с.

2. Шахраманьян М.А., Акимов В.А., Козлов К.А. Оценка природной и техногенной безопасности России: теория и практика. – М., 1998. – 218 с.
3. Владимиров В.А., Воробьев Ю.Л., Малинецкий Г.Г. и др. Управление риском. Риск, устойчивое развитие, синергетика. – М., 2000. – 431 с.
4. Малашихина Н.Н., Блокрылова О.С. Риск-менеджмент / Учебное пособие. – СПб.: ООО «ЛЕКС СТАР», 2001. – 128 с.
5. Петренко С.А., Симонов С.В. Экономически оправданная безопасность. – М.: ДМК, 2003. – 381 с.

МЕРТВЫЙ КОД

А.В. Разумовский
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

С каждым годом активность вирусов увеличивается. Если раньше они чаще играли роль шутки или уничтожали данные, то теперь они являются частью общего механизма кражи информации. Давно встал вопрос о борьбе с вирусами. Однозначного решения пока нет. В качестве решения предлагается исследовать код, получающийся в результате компилирования программы на предмет «мертвого» кода.

Введение

Защита от новых вирусов всегда была не очень эффективна. Исследование происхождения вирусов показывает, что даже если программный код написан безупречно, потенциальная опасность все равно остается. Дело в том, что после появления первого языка программирования человек старался упростить процесс написания программ и ускорить его. Для этого были придуманы языки так называемого высокого уровня, которые позволяют за более короткие сроки относительно просто решать сложные задачи. Но от преобразования в машинный код еще никто не ушел, и компиляторы, которые тоже писались людьми, далеко не всегда оптимально транслируют код языка высокого уровня в машинный.

Постановка задачи

При компиляции практически всегда появляется мертвый код. Данный код не писался программистом, он не несет в себе функциональности, но он существует. А если он существует, то можно попытаться каким-то образом заставить его работать. Злоумышленники как раз и занимаются тем, что ищут такой код и пытаются его использовать для собственных целей.

То же самое относится к троянским коням. Как, возможно, самое яркое проявление троянских коней вспоминают эпизод арабо-израильской войны, когда во время воздушного сражения в долине Бекаа была парализована система управления сирийской авиацией. Тогда соотношение сбитых самолетов было колоссальным в пользу израильских летчиков, потому что сирийские «ослепли» [1].

На практике троянские кони встречаются очень широко. Помимо нанесения какого-то вреда, троянские кони могут использоваться и как средство защиты от несанкционированного распространения компьютерных программ. Производители, ищущие средства защиты от бесплатного использования их продуктов, вносят троянских коней, которые в случае незаконного копирования приводят к постепенной деградации системы. Это существенная проблема, особенно для систем с ограниченной памятью. Мертвый код может занимать до 30% программы, особенно его много получается при развитии приложений, ведь в них вносятся все новые и новые куски. Проблема мертвого кода алгоритмически неразрешима. Это значит, что невозможно создать такой инструмент, который для любой программы находил бы мертвый код. Но бороться с этой проблемой надо, нужно создавать инструменты, которые помогают человеку находить мертвый код. И в некоторых сомнительных случаях решение должен принимать человек.

Методы исследований

Нет общепринятого формального определения вируса. В академической среде термин был употреблен Фредом Коэном в его работе «Эксперименты с компьютерными вирусами»[2], где он сам приписывает авторство термина Лену Эдлмэну [3]. Формально вирус определен в [4], со ссылкой на машину Тьюринга [5]

$M : (S_M, I_M, OM : S_M \times I_M \rightarrow I_M)$, (1)

$N_M : (S_M \times I_M \rightarrow S_M, D_M : S_M \times I_M \rightarrow d)$. (2)

с заданным множеством состояний S_M, множеством входных символов I_M и отображений (O_M, N_M, D_M), которая на основе своего текущего состояния $s \in S_M$ и входного символа $i \in I_M$, считанного с полубесконечной ленты, определяет выходной символ $o \in I_M$ для записи на ленту, следующее состояние машины $s' \in S_M$ и движение по ленте $d \in \{-1,0,1\}$.

Для данной машины M, последовательность символов $v : v_i \in I_M$ может быть сочтена вирусом тогда и только тогда, когда обработка последовательности v в момент времени t влечет за собой то, что в один из следующих моментов времени t последовательность v (не пересекающаяся с v) существует на ленте, и эта последовательность v была записана M в точке t", лежащей между t и t.

Данное определение было дано в контексте вирусного множества

$VS = (M, V)$, (3)

– пары, состоящей из машины Тьюринга M и множества последовательностей символов

$V: v, v' \in V$. (4)

Из данного определения следует, что понятие вируса неразрывно связано с его интерпретацией в заданном контексте – окружении. В [6] показано:

- любая самовоспроизводящаяся последовательность символов – одноэлементный VS;
- существует бесконечное количество VS и не-VS, для которых существуют машины, для которых все последовательности символов является вирусом, и для которых ни одна из последовательностей символов не является вирусом;
- любая конечная последовательность символов является вирусом для какой-либо машины.

Там же средствами, которыми доказывается неразрешимость проблемы Останова, приведено доказательство того, что в общем виде вопрос о том, является ли данная пара $(M, X) : X_i \in I_M$ вирусом, неразрешим (т.е. не существует алгоритма, который мог бы достоверно определить все вирусы), Другие исследователи доказали, что существуют такие типы вирусов (вирусы, содержащие копию программы, детектирующей вирусы), которые не могут быть безошибочно определены ни одним алгоритмом.

Большая часть компиляторов переводит программу с некоторого высокоуровневого языка программирования в машинный код, который может быть непосредственно выполнен центральным процессором [7]. Как правило, этот код также должен выполняться в среде конкретной операционной системы, поскольку использует предоставляемые ей возможности (системные вызовы, библиотеки функций). Архитектура (набор программно-аппаратных средств), для которой производится компиляция, называется целевой машиной.

Некоторые компиляторы (например, Java) переводят программу не в машинный код, а в программу на некотором специально созданном низкоуровневом языке. Такой язык – байт-код – также можно считать языком машинных команд, поскольку он подлежит интерпретации виртуальной машиной. Например, для языка Java – это JVM (язык виртуальной машины Java) или так называемый байт-код Java (вслед за ним все промежуточные низкоуровневые языки стали называть байт-кодами). Для языков программирования на платформе .NET Framework (C#, Managed C++, Visual Basic .NET и другие) – это MSIL (Microsoft Intermediate Language, «Промежуточный язык фирмы Майкрософт»).

Программа на байт-коде подлежит интерпретации виртуальной машиной либо еще одной компиляции уже в машинный код непосредственно перед исполнением. Последнее называется «Just-In-Time компиляция» (JIT) по названию подобного компилятора для Java. MSIL-код компилируется в код целевой машины также JIT-компилятором, а библиотеки .NET Framework компилируются заранее.

Для каждой целевой машины (IBM, Apple и т. д.) и каждой операционной системы (семейства операционных систем), работающих на целевой машине, требуется написание своего компилятора. Существуют также так называемые кросс-компиляторы, позволяющие на одной машине и в среде одной ОС получать код, предназначенный для выполнения на другой целевой машине и/или в среде другой ОС. Кроме того, компиляторы могут быть оптимизированы под разные типы процессоров из одного семейства (путем использования специфичных для этих процессоров инструкций). Например, код, скомпилированный под процессоры семейства i686, может использовать специфичные для этих процессоров наборы инструкций – MMX, SSE, SSE2.

Существуют программы, которые решают обратную задачу – перевод программы с низкоуровневого языка на высокоуровневый. Этот процесс называют декомпиляцией, а программы – декомпиляторами. Но, поскольку компиляция – это процесс с потерями, точно восстановить исходный код, скажем, на C++ в общем случае невозможно. Более эффективно декомпилируются программы в байт-кодах — например, существует довольно надежный декомпилятор для Flash.

Структура компилятора

Процесс компиляции состоит из следующих этапов.

1. Лексический анализ. На этом этапе последовательность символов исходного файла преобразуется в последовательность лексем.
2. Грамматический анализ. Последовательность лексем преобразуется в дерево разбора.
3. Семантический анализ. Дерево разбора обрабатывается с целью установления его семантики (смысла) – напр. привязка идентификаторов к их декларациям, типам, проверка совместимости, определение типов выражений и т.д. Результат обычно называется «промежуточным представлением/кодом» и может быть дополнен деревом разбора, новым деревом, абстрактным набором команд или чем-то еще, удобным для дальнейшей обработки.
4. Оптимизация. Выполняется удаление излишних конструкций и упрощение кода с сохранением его смысла. Оптимизация может быть выполнена на разных уровнях и этапах, например, над промежуточным кодом или над конечным машинным кодом.
5. Генерация кода. Из промежуточного представления формируется код на целевом языке.

В конкретных реализациях компиляторов эти этапы могут быть разделены или совмещены в том или ином виде.

Трансляция и компоновка

Важной исторической особенностью компилятора, отраженной в его названии (англ. compile – собирать вместе, составлять), являлось то, что он мог производить и компоновку (т.е. содержал две части – транслятор и компоновщик). Это связано с тем, что раздельная компиляция и компоновка как отдельная стадия сборки выделились значительно позже появления компиляторов, и многие популярные компиляторы (например, GCC) до сих пор физически объединены со своими компоновщиками. В связи с этим вместо термина «компилятор» иногда используют термин «транслятор» как его синоним – либо в старой литературе, либо когда хотят подчеркнуть его способность переводить программу в машинный код (и наоборот, используют термин «компилятор» для подчеркивания способности собирать из многих файлов один).

В любом случае компилятор при генерации кода формирует дополнительное количество кода, которой должен позволить выполняться основному алгоритму. Этот дополнительный код может и не выполнять какую-то полезную функцию. Этой пробле-

мой заинтересовались в начале 50-х гг. [8]. При разработке алгоритмов появилось проблема алгоритмической разрешимости того или иного класса задач.

Переход от интуитивного понятия «алгоритм» к математическому понятию «машина Тьюринга» позволяет уточнить вопрос об алгоритмической разрешимости того или иного класса задач. Теперь этот вопрос следует понимать так: существует ли машина Тьюринга, решающая данный класс задач, или же такой машины не существует? На этот вопрос теория алгоритмов в ряде случаев дает отрицательный ответ.

Задачи о нахождении алгоритмов для вычисления значений функций называют обычно алгоритмическими проблемами; если алгоритма для вычисления той или иной функции не существует, говорят, что соответствующая алгоритмическая проблема неразрешима. Обнаружение алгоритмически неразрешимых проблем создало в науке такую ситуацию, когда математик, стремящийся к построению желаемого алгоритма, должен считаться с тем, что такого алгоритма может и не существовать. Поэтому параллельно с усилиями, направленными на поиски желаемого алгоритма, приходится прилагать усилия к доказательству невозможности такого алгоритма. В зависимости от того, на каком из этих направлений будет достигнут успех, и выяснится окончательно картина – либо будет найден разрешающий алгоритм, либо будет установлена алгоритмическая неразрешимость проблемы. Естественно задаться вопросом, какие свойства вычислимых функций можно алгоритмически распознать по их «программам»; оказалось, что никакие, кроме тривиальных. Доказывает это теорема Райса [9].

Зафиксируем класс s одноместных частично рекурсивных функций, т.е. sIK^1ЧРФ. Рассмотрим множество номеров функций этого класса:

$Z«\{x|j_xIs\}$. (5)

Пусть H_z – характеристическая функция для Z. Каждому свойству функций отвечает некоторое множество функций, возможно, пустое, которое ему удовлетворяет.

Рассмотрим содержательные определения.

1. Свойство функции называется тривиальным свойством, если ему удовлетворяют либо все функции класса K^1ЧРФ, либо ни одна функция из K^1ЧРФ. В противном случае назовем данное свойство нетривиальным.

2. Две машины Тьюринга, имеющие один и тот же внешний алфавит, будем называть эквивалентными, если, каково бы ни было слово в их общем алфавите, не содержащее пустого символа, они либо перерабатывают его в одно и то же слово, либо обе к нему неприменимы. Свойство машин Тьюринга называется инвариантным, если любые две эквивалентные машины либо обе обладают этим свойством, либо обе не обладают. Свойство машин Тьюринга называется нетривиальным, если существуют как машины, обладающие этим свойством, так и не обладающие.

Теорема Райса

Каково бы ни было нетривиальное свойство частично рекурсивной функции, не существует общерекурсивной функции, характеристической для множества номеров функций класса s, удовлетворяющих этому свойству.

Пусть задано подмножество sIK^1ЧРФ. Характеристическая функция множества $Z«\{x|j_xIs\}$ является общерекурсивной тогда и только тогда, когда

$s=Æ$, (6)

или

$s=K^1$ЧРФ. (7)

Ни для какого нетривиального инвариантного свойства машин Тьюринга не существует алгоритма, позволяющего для любой машины Тьюринга узнать, обладает ли она этим свойством.

Теорема Райса доказана в [10]. Она имеет широкое применение. Этот глубокий результат избавляет исследователя от необходимости каждый раз доказывать неразрешимость той или иной проблемы. Тем не менее, это не значит, что эта проблема не имеет решения. На основе современных программных продуктов вполне возможно создать программы, которые будут анализировать код на предмет наличия мертвого кода. Мертвый код может использоваться вирусами для заражения программ, а также для проникновения в программы, вывода их из режима нормального выполнения.

Заключение

В настоящее время вирусы стали все чаще использоваться для кражи денежных средств и проникновения в банковские институты. Этот факт заставляет придумывать новые способы борьбы с вирусами. Одним из таких способов является анализ кода, порождаемого компиляторами при создании программ написанных на языке высокого уровня.

В статье рассмотрена проблема возникновения ненужного, избыточного кода, порождаемого при компиляции программ, написанных на языке высокого уровня. Дан анализ проблемы возникновения такого кода, а также рассмотрена связь между мертвым кодом и вирусами.

Необходимо научиться исследовать куски кода, которые создаются компилятором, на предмет их использования в недобросовестных целях. Данное исследование лучше всего проводить с помощью ПО, проверенного временем, например продуктов компании IBM Rational [11], в частности Rational Application Developer [12] и WebSphere Application Server (WAS) [13]. Данные программные продукты позволяют проанализировать работу компиляторов при создании конечного кода из языка высокого уровня и выявить участки мертвого кода.

Литература

1. Куприянов П. Закон «о мертвом коде», 2006. – Режим доступа: http://www.osp.ru/cw/2006/20/1576600
2. Fred Cohen. Computer viruses – theory and experiment, 1984. – Режим доступа: http://vx.netlux.org/lib/afc01.html
3. Leonard Adleman. Advances in Cryptology // CRYPT0 '88. – 1990. – № 4. – С. 354–374.
4. Fred Cohen. Computational aspects of computer viruses // Computers & Security. – 1989 – №. 8. – С. 325–344.
5. Alan M. Turing. On computable numbers, with an application to the Entscheidungs Problem // Proceedings of the London Mathematical Society. – 1936. – №. 2. – С. 230–265.
6. IEEE Transactions on Information Theory. – 2003. – Vol. 49. – № 1. – P. 280–284.
7. Чернов А.В. Анализ запутывающих преобразований программ. 2003. – Режим доступа: http://www.citforum.ru/security/articles/analysis
8. Бест С. Анализ покрытия кода. 2003. – Режим доступа: http://fuxx.h1.ru/cgi-bin/wiki.cgi?CodeCoverage
9. Теорема Райса. – Режим доступа: http://ru.wikipedia.org/wiki/Теорема_Райса
10. Основы теории вычислимых функций. – Режим доступа: http://www.intuit.ru/department/calculate/basecalfun/2/
11. IBM Rational Application Developer. – Режим доступа: http://www.interface.ru/home.asp?artId=317
12. Введение в Rational Application Developer – Режим доступа: http://www.ibm.com/developerworks/ru/library/719_app/index.html
13. IBM WebSphere Developer Technical Journal. – Режим доступа: http://www.ibm.com/developerworks/ru/library/0512_gawor

КОМПЛЕКСНАЯ СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ПРОДУКТОВ КОМПАНИИ COMPUTER ASSOCIATES

Д.А. Гусарова
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Цель информационной безопасности – обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму. Построение системы информационной безопасности современного предприятия, которая состоит из целого ряда компонентов – это сложный и ответственный процесс, требующий приложения серьезных знаний, опыта, времени и средств. Построение системы безопасности на базе продуктов одного производителя позволяет избежать проблем с несовместимостью продуктов между собой и значительно упростить процесс внедрения и последующей эксплуатации комплексной системы информационной безопасности современного предприятия.

Введение

Управление информационной безопасностью позволяет коллективно использовать информацию, обеспечивая при этом ее защиту и защиту вычислительных ресурсов. Информационная безопасность состоит из трех основных компонентов:

- конфиденциальность – защита конфиденциальной информации от несанкционированного раскрытия или перехвата;
- целостность – обеспечение точности и полноты информации и компьютерных программ;
- доступность – обеспечение доступности информации и жизненно важных сервисов для пользователей, когда это требуется.

Информация существует в различных формах. Ее можно хранить на компьютерах, передавать по вычислительным сетям, распечатывать или записывать на бумаге, а также озвучивать в разговорах. С точки зрения безопасности все виды информации, включая бумажную документацию, базы данных, пленки, микрофильмы, модели, магнитные ленты, дискеты, разговоры и другие способы, используемые для передачи знаний и идей, требуют надлежащей защиты.

Информация и поддерживающие ее информационные системы и сети являются ценными производственными ресурсами организации. Их доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения конкурентоспособности, движения денежной наличности, рентабельности, соответствия правовым нормам и имиджа организации. Современные организации могут столкнуться с возрастающей угрозой нарушения режима безопасности, исходящей от целого ряда источников. Информационным системам и сетям могут угрожать такие опасности, как компьютерное мошенничество, шпионаж, саботаж, вандализм, а также другие источники отказов и аварий. Появляются все новые угрозы, способные нанести ущерб организации, такие, как компьютерные вирусы или хакеры. Последнее время заголовки не только компьютерных, но и обычных изданий пестрят упоминаниями о новых вирусах, нападениях хакеров и других страшных опасностях, которые грозят современным информационным ресурсам. Невольно возникает вопрос: что мешает защитить от них эти ресурсы? Если ответить кратко, то это – большое разнообразие таких опасностей, защита от которых требует такого же (а вернее, большего) разнообразия защитных средств.

Основная часть

Для более детального освещения этой проблемы попытаемся построить комплексную систему информационной безопасности современного предприятия, которая

смогла бы предотвратить любые попытки нанести ущерб информационным ресурсам этого предприятия.

Построение системы начнем с построения «внешнего контура». «Внешним контуром» для информационной системы современного предприятия являются точки соединения внутренней локальной сети с внешней или с Интернет, если брать наиболее распространенный случай. Для защиты «внешнего контура» необходим Firewall, или межсетевой экран, или брандмауэр – все это разные названия одного и того же средства информационной безопасности. Firewall – это программно-аппаратный комплекс, который позволяет пользователю закрыть все порты входа-выхода, кроме тех, которые нужны ему для работы. В классическом случае это компьютер с двумя сетевыми картами, одна из которых соединена с внутренней сетью, а вторая с внешней. В память этого компьютера загружена программа, которая управляет TCP/IP портами и контролирует, кто или что имеет право пользоваться этими портами и в каких целях.

На рынке существует множество готовых устройств и программ, реализующих функцию Firewall, а также есть «конструкторы» типа бесплатных ОС Linux или FreeBSD, из которых опытный пользователь может самостоятельно собрать Firewall. Примером готовой программы является eTrust Firewall компании Computer Associates. Преимуществом готовых продуктов является простота установки и настройки, а также расширенный набор полезных функций. Например, eTrust Firewall, наряду с выполнением стандартных функций Firewall, позволяет:

- управлять несколькими Firewall из единого интерфейса;
- использовать существующую информацию о легальных пользователях NT или RADIUS серверов;
- применять готовые фильтры для популярных сетевых служб, таких как FTP, RealAudio и др.;
- информировать администратора о внештатных ситуациях, посылая сообщения на пейджер или факс;
- выполнять другие функции, облегчающие контроль за безопасностью «внешних границ» любой информационной системы.

Следующим шагом при создании комплекса по защите информации будут системы обнаружения попыток вторжения (Intrusion Detection System) проверки содержимого входящего и исходящего сетевого трафика (Content Inspection System). Упрощенно говоря, такая система хранит в памяти набор шаблонов, описывающих типичные признаки, присущие той или иной попытке незаконного проникновения в информационную систему. Intrusion Detection System отслеживает текущее состояние компьютеров и сетевого трафика и сравнивает его с шаблонами. При обнаружении совпадения с одним из шаблонов Intrusion Detection System предпринимает заранее запрограммированные действия, сложность и эффективность которых зависит от совершенства Intrusion Detection System. Простейшая система может проинформировать администратора(ов) и зарегистрировать попытку вторжения в журнале, более совершенные системы могут предпринять определенные действия для предотвращения вторжения.

На рынке существуют различные варианты Intrusion Detection System: программно-аппаратные и чисто программные. Computer Associates предлагает программную систему eTrust Intrusion Detection. Данная система обладает следующими отличительными особенностями.

- *Контроль доступа.* eTrust Intrusion Detection использует правила для определения того, к каким ресурсам могут иметь доступ какие пользователи.
- *Обширная библиотека шаблонов атак.* eTrust Intrusion Detection автоматически определяет атаки, соответствующие шаблонам. Шаблоны регулярно обновляются.

- *Контроль за WWW-трафиком.* eTrust Intrusion Detection позволяет ограничить доступ к Интернет узлам с помощью правил, содержащих ключевые слова, например, «совращение».
- *Механизм защиты от вирусов* позволяет предотвратить закачивание зараженных данных.
- *Контроль загрузки сети.* eTrust Intrusion Detection ведет количественный учет трафика в сети.
- Другие функции позволяют использовать eTrust Intrusion Detection и как самостоятельную систему безопасности, и как компонент более сложной системы.

Таким образом, хорошая Intrusion Detection System позволяет предотвратить, как неавторизованный доступ извне, так и контролировать ситуацию внутри информационной системы предприятия. Но защита, основанная на анализе содержимого сетевых пакетов, может не выявить опасности, которая станет реальной только после того, как пакеты соберутся в программный код на компьютере клиента. В этом случае нужна система, способная обнаруживать присутствие опасных программ в легальном сетевом трафике (фильтровать все типы скриптов на основе набора правил фильтрации) и блокировать их распространение, т.е. Content Inspection System.

Компонента Content Inspection программнго продукта eTrust Antivirus обладает следующими особенностями.

- *Защита в реальном времени.* Работающая в режиме реального времени система сочетает в себе высокую производительность с надежной защитой от вредоносных исполняемых файлов.
- *Защита на основе цифровых сертификатов* выполняет анализ цифровых сертификатов, проверяя «подписанные» Java-аплеты, компоненты ActiveX и др. Базовый список известных сертификатов (Certificates of Authority) поставляется вместе с продуктом. Новые сертификаты можно добавить в список, импортировав их из реестра, файла сертификатов или из других объектов, имеющих цифровую подпись.
- *Централизованное управление* упрощает создание и внедрение правил защиты.
- *Шаблоны* позволяют легко создавать гибкие правила защиты.
- *Средства аудита* имеет полный набор средств для аудита и создания отчетов.
- *Блокировка «неблагонадежных» URL.* Пользователей можно ограничивать или блокировать доступ к определенным URL на основании списка «неблагонадежных» слов.
- *Поддержка всех основных протоколов.* Поддерживаются три основных протокола Интернет – SMTP, FTP и HTTP – обеспечивая защиту от вредоносного кода, распространяемого через e-mail, при скачивании файлов с Web-сайта и при передаче файлов.
- *Эвристический механизм обнаружения вирусов.* Благодаря этому механизму возможно обнаружение даже неизвестных макро-вирусов.

Таким образом, установив Firewall, Intrusion Detection System и Content Inspection System, мы защитим информационную систему предприятия по «внешнему контуру». Теперь можно переходить к обеспечению внутренней защиты, которая по важности не уступает, а даже превосходит внешнюю.

В информационной системе современного предприятия каждый пользователь имеет идентификационное имя (одно или несколько) и пароль, используя которые, он получает доступ к различным информационным ресурсам – серверам, принтерам, базам данных и т.д. Права доступа к этим ресурсам назначаются администратором информационной системы. Аналогом в традиционной системе безопасности может служить пропускная система, которая одному сотруднику пропуск позволяет попасть только на свое рабочее место, а другому – пройти в любое помещение предприятия. Чем больше ресурсов и пользователей, тем сложнее избежать ошибок в распределении прав доступа

к ресурсам, последствия которых могут быть самыми разнообразными: от несанкционированного использования сетевого цветного принтера (сопутствующие убытки: повышение расходов на цветной тонер и качественную бумагу) до доступа к файлам, содержащим секретную информацию (сопутствующие убытки: прямые коммерческие, вплоть до полного разорения фирмы).

Необходима удобная система контроля за тем, кто, когда, к каким ресурсам и с каким правами имеет доступ. В принципе, в любой сетевой операционной системе или грамотно написанном приложении ведется такой контроль, но если на предприятии используется не одна операционная система и не одно сетевое приложений, то синхронизировать такую систему становится очень трудно.

Помочь в этой ситуации может универсальная система контроля доступа eTrust Access Control компании Computer Associates. Последняя позволяет управлять доступом и защищать следующие компоненты.

- *Файлы.* eTrust Access Control защищает безотносительно к ограничениям ОС. Например, если пользователь не имеет доступа к какому-либо файлу, то он его и не получит, даже если зайдет суперпользователем.
- *Процессы.* Критические системные и прикладные процессы могут быть завершены только авторизованными пользователями.
- *Привилегированные программы.* eTrust Access Control позволяет контролировать запуск программ, запускающихся с правами конкретного пользователя.
- *Сетевые соединения.* eTrust Access Control контролирует доступ к сетевым программам с помощью ограничения доступа к портам.
- *Терминалы.* eTrust Access Control позволяет контролировать, кто и с какого терминала может войти в систему.
- *Ресурсы.* С помощью eTrust Access Control администраторы могут создавать собственные правила для контроля доступа к любым ресурсам.

Теперь вспомним о том, что каждый пользователь может иметь несколько сетевых имен – например, различные имена для доступа к различным информационным ресурсам – и он должен все время помнить, какое имя и пароль нужно ввести в ответ на запросы разных систем. Или, даже если он имеет одно имя и пароль, при обращении к новым ресурсам ему может потребоваться каждый раз заново вводить одно и тоже, раз за разом. А ведь правила безопасности требуют периодически менять пароли. И в случае увольнении сотрудника администратор должен последовательно удалить все его регистрационные данные во всех ресурсах, к которым он имел доступ. Если администратор пропустит хотя бы один ресурс, то это становится потенциально уязвимым местом в системе информационной безопасности предприятия. Все это может стать достаточно трудоемким и утомительным процессом. Решением этой проблемы является модуль единого входа в информационную систему eTrust Single Sign-On компании Computer Associates.

Модуль единого входа в информационную систему eTrust Single Sign-On позволяет пользователю, прошедшему аутентификацию в eTrust Single Sign-On один раз, получить доступ ко всем системам, к которым он имеет право доступа. Перечислим отличительные особенности eTrust Single Sign-On.

- *Персонализированная Web-страница.* После успешной аутентификации пользователь получает доступ к персонализированной Web-странице, на которой находятся ссылки на доступные для него приложения и Web-ресурсы.
- *Интеграция с рабочим столом Windows.* Пользовательский интерфейс eTrust Single SignOn интегрируется с рабочим столом: после успешной аутентификации пиктограммы приложений, доступных для конкретного пользователя, появляются в отдельной группе в Start Menu или на рабочем столе.

- *Автоматизированный процесс входа в информационную систему.* eTrust Single SignOn позволяет автоматически входить в любую систему, требующую ввода пароля, включая e-mail, базы данных, Web-ресурсы, и т.д.
- *Поддержка различных механизмов аутентификации*. eTrust Single Sign-On поддерживает широкий диапазон механизмов аутентификации, включая системы аутентификации Windows NT и NetWare, eTrust -сертификаты, и т.д.
- *Управление паролями.* Механизм управления паролями позволяет автоматически генерировать пароли, создавать одноразовые пароли, вводить ограничения на пароли и т.д.
- *Защита сетевого трафика.* Вся информация, передаваемая между компонентами Single Sign-On, шифруется.
- *Наличие API-инструменария* (API Toolkit). API-инструментарий позволяет интегрировать eTrust Single Sign-On с другими продуктами.

Дальнейшее усиление защиты информационной системы предприятия в современных условиях невозможно без использования новейших технологий. Одной из наиболее широко используемых сегодня технологий аутентификации для обеспечения безопасного использования информационным ресурсам является Public Key Infrastructure (PKI) – инфраструктура публичных ключей. Существуют доверительные организации, которые выдают каждой обратившейся к ним организации два специальных кода: public key (публичный ключ) и private key (частный ключ). При обмене информацией между двумя сторонами используются зашифрованные цифровые сертификаты, подтверждающие легальность сторон. Шифрование и расшифровка сертификатов происходит с использованием этих кодов-ключей.

Архитектура PKI является широко принятым в мире стандартом для обеспечения защиты пользователей, данных и прикладных программ. Однако большинство программ управления PKI требуют проведения обширных настроек для интеграции с существующей инфраструктурой и бизнес-процессами пользователя этих программ. eTrust PKI от Computer Associates, наоборот, обеспечивает быструю интеграцию в информационную систему предприятия и облегчает возможности администрирования в масштабе всего предприятия, что является наиболее критичными для эффективного внедрения. Его новаторская архитектура гарантирует строгую аутентификацию и секретность, обеспечивая возможность создания, утверждения и управления цифровыми сертификатами X.509 по всему предприятию. eTrust PKI, таким образом, снижает риски безопасности, связанные с неполным или неправильным администрированием сертификатов. Кроме того, eTrust PKI интегрируется с eTrust Single Sign-On (SSO), позволяя получить законченное решение управления правами доступа пользователей к информационным ресурсам любого предприятия.

При создании системы защиты информации необходимо помнить, что на современном предприятии и в его информационной системе может эксплуатироваться самое разнообразное оборудование и технологии. В одной информационной системе может использоваться несколько служб каталогов, конкурирующих производителей, в которых, тем не менее, нужно поддерживать актуальные списки пользователей и ресурсов. Сотрудники предприятия могут использовать для работы (а часто – не только для работы) носители информации, которые могут содержать вирусы. Отправляясь в командировки или работая на дому, пользователи информационной системы предприятия могут нуждаться в удаленном доступе к ее ресурсам. Чтобы соответствовать этим и другим требованиям современных информационных технологий и не жертвовать при этом безопасностью, приходиться использовать дополнительные средства.

Предположим, что в информационной системе предприятия в разных подразделениях используется масса различных служб. Каждая из этих служб по отдельности относительно легко контролируется и управляется с помощью встроенных инструментов.

Но, объединенные вместе, они составляют очень сложную для администрирования систему, в которой инструмент управления одной службой не может использоваться для управления другой. Администратор, внеся изменения в одну службу каталогов, вынужден каждый раз дублировать эти изменения во всех других службах. Все это не только ведет к непродуктивным потерям рабочего времени, но и неизбежно ведет к ошибкам, который влияют на эффективность работы и безопасность информационной системы предприятия. Чтобы избежать этого, нужно использовать автоматизированную систему интеграции служб каталогов от различных производителей в единое дерево каталогов – eTrust Directory.

eTrust Directory реализует стандарты X.500 и LDAP V3. Каждый источник данных, поддерживающий LDAP, может быть инкорпорирован в общий каталог eTrust Directory. Перечислим ртличительные особенности eTrust Directory.

- *Производительность* – высокая скорость выполнения запросов к единой реляционную базе данных объектов, содержащей миллионы записей.
- *Надежность* – автоматическое восстановление системы после сбоев питания, а также резервное копирование и восстановление в реальном времени.
- *Неограниченная масштабируемость.* eTrust Directory не имеет ограничений на размер каталога.
- *Контроль доступа.* по стандарту X.500 к поддеревьям, записям и атрибутам.
- *Мониторинг и управление.* Мониторинг в стандарте SNMP и X.700.

Использование служб каталогов удобно для управления ресурсами и пользователями, но недостаточно надежно с точки зрения безопасности. Чтобы повысить уровень безопасности, необходимо использование цифровых сертификатов. Самым надежным подходом при проверке цифровых сертификатов является использование протокола, который бы позволял клиентам проверять статус конкретного сертификата в режиме реального времени. Но это является отходом от обычной схемы, по которой клиент получает CRL (Certificate Revocation List) от Certification Authority, и которая имеет два ограничения:

- CRL обновляется периодически, что порождает задержки, в течение которых недействительный сертификат будет иметь действие;
- с ростом размера списка CRL осложняется управление и распространение списком.

Чтобы разрешить эти проблемы, Internet Engineering Task Force (IETF) разработала Online Certificate Status Protocol (OCSP), который позволяет взаимодействовать с системами, включающими тысячи Certification Authorities и миллионы сертификатов.

eTrust OSCPro от Computer Associates является реализацией протокола OCSP, предоставляя клиентским приложениям текущий статус цифрового сертификата от его владельца в реальном времени. eTrust OCSPro предоставляет гибкое и надежное решение для организаций, желающих использовать OCSP. eTrust OCSPro тесно интегрирован с eTrust Directory.

Компьютерные вирусы являются самой распространенной и самой быстроразвивающейся опасностью, угрожающей современным информационным ресурсам. Даже если мы применим все описанные выше компоненты системы безопасности, все равно останется опасность проникновения вирусов в информационную систему предприятия. Поэтому совсем не лишней в системе информационной безопасности будет антивирусная система. Современная антивирусная система должна сочетать в себе мощное централизованное управление и всестороннюю, многоуровневую защиту. Она должна охватывать сервера, рабочие станции и системы обмена сообщениями. Этим требованиям полностью соответствует eTrust Antivirus от Computer Associates. eTrust Antivirus обеспечивает:

- поиск и «лечение» вирусов в режиме реального времени;
- единый интерфейс для просмотра, отслеживания и управления заданиями по поиску вирусов для всего предприятия;

- защиту от проникновения вирусов на сервера, рабочие станции и системы обмена сообщениями через Internet/Intranet;
- автоматическую загрузку и распространение сигнатур вирусов, а также новых версий антивирусного программного обеспечения;
- централизованный журнал, в котором регистрируются все события, касающиеся работы антивирусной системы: файлы, подвергшиеся проверке, обнаруженные вирусы, предпринятые действия;
- наличие агентов для защиты систем Lotus Notes и Microsoft Exchange Server;
- простую интеграцию с другими продуктами Computer Associates.

Построив систему информационной безопасности предприятия, необходимо проверить ее надежность (а еще лучше делать это постоянно). Для этого можно использовать eTrust Policy Compliance – систему поиска уязвимостей в системе безопасности от Computer Associates. eTrust Policy Compliance определяет «дыры» в системе безопасности и автоматически генерирует скрипты, которые их закрывают. eTrust Policy Compliance позволяет выполнять разнообразные проверки на уязвимость, обследовать отдельные узлы, базы данных или подсети. eTrust Policy Compliance выполняет проверки по рекомендациям CERT и Microsoft Security. Имеется возможность сравнивать отчеты за разные промежутки времени. Он позволяет одновременно осуществлять мониторинг операционных систем Windows NT, UNIX и OpenVMS, баз данных Oracle и Sybase, а также Web-серверов Apache, значительно экономя время и средства. eTrust Policy Compliance позволяет проверять политики eTrust Access Control, если он установлен в вашей информационной системе.

Перечислим отличительные особенности eTrust Policy Compliance.

- *Анализ томов и файловых систем.* eTrust Policy Compliance находит файлы с некорректными правами доступа и позволяет автоматически исправлять этот недостаток.
- *Анализ имени пользователя и паролей.* eTrust Policy Compliance отслеживает имена пользователей, которые уже не существуют или используются сразу несколькими лицами. Он также выявляет пароли, которые были утеряны или могут быть легко «взломаны».
- *Разностный анализ результатов сканирования.* Имеется возможность сравнивать отчеты за разные промежутки времени, позволяя доводить число уязвимостей до минимума.

Для облегчения труда администраторов ИТ существует два удобных инструмента: eTrust Admin и eTrust Audit от Computer Associates.

Одной из наиболее важных задач в современной информационной среде является эффективное администрирование всех сетевых ресурсов, таких как учетные записи, группы пользователей и сетевые диски. Независимые исследования доказали, что стоимость их администрирования может оказаться наиболее крупной составляющей затрат на обслуживание сети. eTrust Admin представляет собой централизованное средство администрирования объектов в разнородной среде. Этот продукт позволяет создавать, модифицировать и удалять объекты, такие как учетные записи пользователей для доменов Windows NT, рабочих групп, UNIX, Novell Netware NDS, Lotus Notes, Microsoft Exchange и т.д. eTrust Admin поддерживает более 20.000.000 записей в базе данных и более 1000 запросов в секунду к своим объектам.

При использовании eTrust Admin предприятие получает следующие преимущества:

- *Уменьшаются затраты на обслуживание*, так как системный администратор имеет возможность внести изменения лишь один раз и затем автоматически распространить и применить эти изменения ко всем соответствующим объектам во всем предприятии.
- *Увеличивается производительность* благодаря централизованному интерфейсу администратора.

- *Усиливается защита.* Ролевая модель гарантирует, что пользователи имеют согласованные права по всему предприятию.

eTrust Audit предназначен для сбора и анализа информации из системных журналов. eTrust Audit позволяет обрабатывать информацию для удобного просмотра и создания отчетов, а также выполнять заранее определенные действия в случае обнаружения следов подозрительных действий. eTrust Audit предоставляет системным администраторам уникальную возможность собирать информацию из журналов UNIX, Windows NT, OS390, Web серверов и СУБД, а также других продуктов семейства eTrust в централизованную базу данных обработки событий. Информация из этой базы данных представляется в едином формате, вне зависимости от ее источника.

Перечислим отличительные особенности eTrust Audit.

- *Кросс платформенная обработка событий.* eTrust Audit собирает информацию из разнообразных источников, например, системных журналов UNIX, Windows NT, OS/390, СУБД Oracle, MS SQL Server, Web-серверов Netscape и Apache. Также eTrust Audit может получать информацию из любого SNMP источника.
- *Обнаружение вторжения.* eTrust Audit поставляется с предопределенными политиками для анализа журналов с точки зрения поиска вторжения в систему.
- *Мониторинг в режиме реального времени.* Критические события могут быть отфильтрованы и направлены на консоль.
- *Централизованное управление политиками.* Правила обнаружения вторжения могут быть растиражированы с центральной машины на клиентские рабочие станции.

Описание комплексной системы информационной безопасности предприятия было бы неполным, если забыть о таком важном и широко используемом сегодня понятии, как «"виртуальные частные сети» – virtual private network (VPN).

К сожалению, межсетевые экраны (Firewall) не могут решить всех проблем безопасности, связанных с использованием Интернет-каналов. При этом некоторые проблемы, такие как защита информации от прослушивания при ее прохождении по каналам Интернет, могут быть решены путем добавления в программное обеспечение межсетевых экранов возможности шифрования данных (целый ряд программных межсетевых экранов включают в себя так называемую клиентскую часть, что позволяет шифровать весь сетевой трафик между клиентом и сервером). Однако, по мере развития информационных систем в сторону все более широкого использования Интернет, значительную роль начинают играть технологии, созданные без привязки их к использованию совместно с межсетевыми экранами. Имеется в виду последняя мода на Интернет-порталы, используемые, в том числе и в CRM-системах.

Одной из непреодолимых сложностей для межсетевых экранов с их статической конфигурацией портов становится использование RMI (remote method invocation) в современных системах, ориентированных на широкое использования Java, когда неизвестно заранее, какие и сколько сетевых портов понадобится открыть для каждого конкретного запроса. Одним из решений проблемы может быть создание виртуальной частной сети с помощью аппаратных или программных средств. В этом случае сетевой обмен по всем сетевым портам между компьютерами, организованными в VPN, осуществляется по открытым каналам в шифрованном виде, образуя таким образом подобие локальной сети «внутри» Интернет/Интранет. Важно, что для работы в VPN не требуется внесения каких-либо изменений в используемое программное обеспечение – все выглядит, как обычная работа в сети. Но надо учитывать, что в большинстве случаев VPN не заменяет собой межсетевой экран. Вы не можете установить VPN клиента на каждый компьютер, с которого обращаются на ваш корпоративный Web сервер. Оптимальным представляется совместное использование межсетевых экранов и VPN там, где это возможно. Например, eTrust Firewall можно настроить таким образом, что он будет дополнять VPN, т.е. с помощью eTrust Firewall в список открытых портов добав-

ляется еще один, через который осуществляется зашифрованный обмен с компьютерами, организованными в VPN, при этом порт можно открыть не для всех, а для конкретной группы компьютеров.

Заключение

Построение системы информационной безопасности современного предприятия, которая состоит, как мы увидели, из целого ряда компонентов – это сложный и ответственный процесс, требующий приложения серьезных знаний, опыта, времени и средств. Сегодня на рынке существуют множество продуктов от разных производителей, призванных облегчить и ускорить этот процесс. Один производитель награжден за самый лучший Firewall, другой – за Intrusion Detection System, третий – за Antivirus. Можно отобрать самые лучшие продукты разных производителей и построить из них систему безопасности. Наверняка она будет работать, но управлять такой системой будет нелегко. Простота управления системой защиты информационной системы является одним из важных условий информационной безопасности. Именно поэтому на протяжении всего обзора использованы в качестве примеров продукты компании Computer Associates из семейства eTrust. Построив систему безопасности на базе продуктов одного производителя, вы избежите проблем с несовместимостью продуктов между собой и значительно упростите процесс внедрения и последующей эксплуатации комплексной системы информационной безопасности современного предприятия.

Литература

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и Техника, 2004.
2. Соколов А., Степанюк О. Защита от компьютерного терроризма. / Справочное пособие. – СПб: Арлит, 2002.
3. Купцевич Ю.Е. Альманах программиста. Том IV: Безопасность в NET. Шифрование. Защита кода и данных. – М.: Издательско-торговый дом «Русская Редакция», 2003.

УСОВЕРШЕНСТВОВАННАЯ ЭЦП: ОБЗОР РЕШЕНИЯ АРХИВНОГО ХРАНЕНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

И.В. Головков
Научный руководитель – к.т.н., доцент А.В. Птицын

Со способами обмена электронными документами и методами обеспечения их долговременного хранения тесно связаны проблемы обеспечения их аутентичности.

Введение

До сих пор главным средством аутентификации электронной документации служат протоколы аудита сетевых ресурсов. С их помощью можно проследить историю документов и выявить случаи несанкционированного доступа к ним. Однако слабым местом такой системы аутентификации являются сами протоколы, находящиеся в практически бесконтрольной власти сетевых администраторов.

Другая проблема – обеспечение аутентичности в межсетевом (межкорпоративном) пространстве. Без четких представлений о происхождении электронных документов и твердых гарантий их целостности суды отказываются признать за ними доказательную силу и принимать в качестве письменных свидетельств. Обмен электронными документами осуществляется на доверительной основе (например, электронная почта), и их достоверность гарантируется лишь авторитетом владельца информационного ресурса или электронного адреса. В свое время именно нерешенность вопросов аутентичности и целостности электронных документов помешала реализации идей «безбумажного офиса».

Электронная цифровая подпись

В правовом отношении ЭЦП долгое время находила применение лишь в частноправовой сфере. Для ее применения необходимо было заключение двусторонних или многосторонних договоров (на бумаге), в которых определялись все нюансы генерации, верификации, хранения ЭЦП и ответственность сторон. Рубеж веков стал периодом массового правового признания электронных средств аутентификации в открытых информационных сетях. Законы об ЭЦП или электронном документе были приняты в большинстве развитых и многих развивающихся странах.

Правовое признание ЭЦП превращает этот реквизит в надежное средство, обеспечивающее аутентичность и целостность электронных документов, однако только тех, которые находятся в оперативном использовании, со сроком хранения пять, максимум 10 лет. Для аутентификации документов на протяжении десятков лет ЭЦП не годится. Чтобы понять, почему это происходит, нужно несколько слов сказать о том, что собой представляют технологии криптографической аутентификации и защиты информации, определяемые законодательством как «аналог собственноручной подписи».

Российский закон об ЭЦП помогает раскрыть сущность этой технологии. В нем ЭЦП определяется как «реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе».

ЭЦП выглядит как последовательность цифр и других символов, что, собственно, и позволяет говорить о ней как о реквизите, обособленном от других реквизитов элек-

тронного документа. Технологически ЭЦП возникает в результате выполнения системой криптозащиты так называемого асимметричного алгоритма шифрования, т.е. шифрования с использованием ключа (опять же последовательность цифр), который отличается от ключа, применяемого потом для расшифрования сообщений. Первый ключ называется закрытым (тайным, личным) ключом. Им может владеть только тот человек, от лица которого документ подписывается. Второй ключ – открытый, его значение может узнать любой, кому необходимо удостовериться в подлинности ЭЦП. Эта пара ключей взаимосвязана, но при этом закрытый ключ не может быть за обозримое время вычислен, исходя из значения открытого ключа. Таким образом, использование открытого ключа при аутентификации надежно связывает подписанный документ с обладателем закрытого ключа.

В то же время особенностью ЭЦП, которая отличает ее от собственноручной подписи человека, является то, что идентифицирует она не столько лицо, подписавшее электронный документ, сколько конкретный документ: два разных документа, подписанные с использованием одного и того же закрытого ключа, будут иметь разные числовые выражения ЭЦП. Связано это с тем, что, кроме закрытого ключа, в алгоритм вычисления ЭЦП включены и другие параметры, в первую очередь, так называемый хэш-код файла с электронным документом.

Основным моментом, который следует отметить, это то, что подтверждение подлинности ЭЦП – процесс технологически кратковременный. Он зависит от жизненного цикла средства ЭЦП – конкретной системы криптографической защиты данных. В частности, аутентификация электронного документа становится невозможной после смены технологической платформы или бесполезной после утраты юридической силы сертификата средства ЭЦП. Это значит, что под вопросом оказывается подлинность документов, подписанных ранее. Но главная проблема при аутентификации электронных документов, подписанных ЭЦП, состоит в том, что этот реквизит (как и значение отдельного хэш-кода или контрольной суммы, гарантирующих целостность документа) неразрывно связан с форматом документа. При переформатировании электронного документа (что неизбежно при долговременном хранении) проверка подлинности ЭЦП становится бессмысленной.

Наиболее приемлемым методом обеспечения аутентичности электронных документов при долговременном хранении (особенно заверенных ЭЦП) можно было бы считать применение эмуляторов или конверторов при их воспроизведении. Но подобная практика пока мало изучена. Проблемы здесь видятся как в ограниченном наборе этих программных средств, так и в возможных ошибках воспроизведения документов, которые могут возникать при эмуляции или конвертировании, что опять-таки негативно сказывается на доказательной силе электронных документов при долговременном хранении. Инкапсуляция – вероятно, самый перспективный способ. Именно способ решения проблемы аутентичности электронных документов видят в нем американские архивисты. Но он требует долговременной апробации и дальнейшего развития.

Усовершенствованная электронная цифровая подпись

Необходимость переформатирования электронных документов при долговременном хранении приводит к тому, что, по существу, появляется другой документ с измененными реквизитами и контрольными характеристиками: датой последнего сохранения, объемом, контрольной суммой, хэш-кодом, ЭЦП и т.п. Получается, что подлинник электронного документа будет невозможно прочитать и использовать, а его миграционная копия не будет иметь юридической силы.

Проблема обеспечения аутентичности электронных документов в долговременной перспективе – на сегодняшний день, пожалуй, самая острая и сложная. При использовании

классической ЭЦП в юридически значимом электронном документообороте в случае возникновения спора достаточно трудно, а подчас и невозможно доказать подлинность ЭЦП и момент подписи (создания) ЭЦП. Эти трудности могут привести к тому, что арбитр не примет электронный документ в качестве письменного доказательства. Данные трудности порождаются рядом проблем, присущих «классической» ЭЦП, а именно:

- нет доказательства момента подписи;
- трудность доказательства статуса сертификата открытого ключа подписи на момент подписи (или действителен, или аннулирован, или приостановлен).

Предлагаемый отечественной компанией КРИПТО-ПРО стандарт применения усовершенствованной подписи позволяет решить все основные трудности, связанные с применением ЭЦП, и обеспечить участников электронного документооборота всей необходимой доказательной базой (причем собранной в самой ЭЦП в качестве реквизитов электронного документа), связанной с установлением момента подписи и статуса сертификата открытого ключа подписи на момент подписи. Усовершенствованная ЭЦП базируется на использовании новых сервисов, таких как:

- онлайновая проверка статуса сертификата по протоколу OCSP (Online Certificate Status Protocol);
- служба штампов времени TSP (Time-Stamp Protocol).

Усовершенствованная электронная цифровая подпись, определяемая в данном стандарте, представляет собой структурированную двоичную запись в формате ASN.1, закодированную в соответствии с правилами DER, описанными в разделе 8.7 X.209). Формат усовершенствованной электронной цифровой подписи, определяемый в настоящем стандарте, представлен на рисунке. Ниже перечислен состав формата.

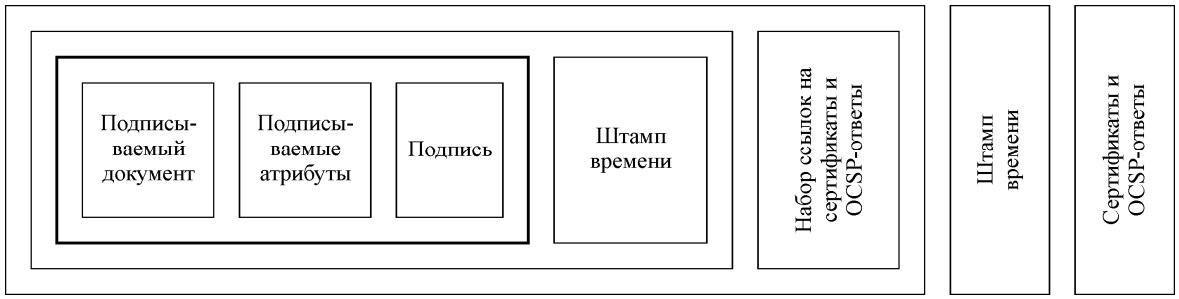


Рисунок. Формат усовершенствованной электронной цифровой подписи

(1) Подписываемый документ (может храниться отдельно от всех остальных полей). Формат подписываемого документа определен в CMS (RFC 3852).

(2) Подписываемые атрибуты, описанные в CMS (см. RFC 3852) и в ESS (RFC 2634). Обязательными атрибутами являются:

   (а) тип содержимого. Представляет собой атрибут Content-type, определенный в RFC 3852. Данный атрибут указывает на то, что содержимое поля ContentInfo является подписываемыми данными;

   (б) хэш-код сообщения. Представляет собой атрибут Message-digest, определенный в RFC 3852 и содержит хэш-код подписываемого документа;

   (в) хэш-код от набора полей сертификата, позволяющих однозначно его идентифицировать, – определенный в ETSI TS 101 733 атрибут other-signing-certificate.

(3) ЭЦП, полученная на данные, указанные в перечислениях (1) и (2) по алгоритму, определенному в ГОСТ Р 34.10-2001.

(4) Штамп времени, полученный на данные, указанные в перечислении в) по алгоритму, определенному в RFC 3161. Штамп времени позволяет удостовериться, что

ЭЦП, указанная в перечислении (3), была создана не позднее указанного в штампе момента времени.

(5) Хэш-коды каждого из перечислений (а)–(е) (см. ниже), составляющих доказательства подлинности. Доказательства подлинности включают в себя:
   (г) сертификат ключа подписи, указанной в перечислении (3);
   (д) OCSP-ответ, позволяющий удостовериться в действительности сертификата ключа подписи;
   (е) сертификат OCSP-сервера, позволяющий удостовериться в действительности OCSP-ответа;
   (ж) сертификат службы штампов времени, позволяющий удостовериться в действительности штампа времени, заверяющего ЭЦП;
   (з) сертификаты промежуточных УЦ, если таковые имеются;
   (и) OCSP-ответы, позволяющие удостовериться в действительности сертификатов ключей подписи промежуточных УЦ, указанных в перечислении 5, либо, если сертификаты таких УЦ не содержат поля AIA (содержащего адрес службы OCSP), соответствующие CRL.

(6) Штамп времени, полученный на данные, указанные в перечислениях (3), (4) и (5), по алгоритму, определенному в RFC 3161. Это обеспечивает целостность и доказательство моментов создания всех элементов и атрибутов усовершенствованной электронной цифровой подписи, что может послужить защитой сертификатов, CRL и/или OCSP-ответов в случае последующей компрометации или плановой смены ключей.

(7) Доказательства подлинности, указанные в перечислении (5) (значения сертификатов и информация об отзыве), требуемые для проверки ЭЦП. Хранение доказательств подлинности вместе с ЭЦП предохраняет их от потери и не требует наличия сети для проверки усовершенствованной ЭЦП. Доказательства подлинности содержатся в следующих атрибутах:
   (к) Certificate-values. Определяется в ETSI TS 101 733 и содержит полный набор сертификатов, требуемый для проверки ЭЦП;
   (л) Revocation-values. Определяется в ETSI TS 101 733 и содержит CRL и/или OCSP-ответы.

Заключение

Применение усовершенствованной электронной цифровой подписи для архивного хранения электронных документов также имеет ряд особенностей и ограничений. При проверке хранящейся в архиве усовершенствованной ЭЦП необходимо наличие действующего сертификата уполномоченного лица удостоверяющего центра, выдавшего сертификат подписи, а также действующий сертификат оператора службы штампов времени. Обеспечить данные условия для успешной проверки усовершенствованной ЭЦП по прошествии десятков лет, когда удостоверяющий центр, выдавший сертификат подписи, может уже кануть в небытие, представляется невозможным.

Литература

1. Тихонов В.И. Архивное хранение электронных документов: проблемы и решения, 2006. – Режим доступа: http://www.delo-press.ru/magazines/documents/issue/2006/2/1554/
2. Стандарт применения усовершенствованной электронной цифровой подписи. – М.: КриптоПро, 2006.
3. Кустов В.Н. Реализация стандарта усовершенствованной ЭЦП в системе электронного документооборота, 2007. – Режим доступа: http://www.ank-pki.ru/conference/2007/tesis/Kustov_GIS.pdf

БАЗОВЫЕ ПАРАМЕТРЫ ПОЛУФОРМАЛЬНЫХ МОДЕЛЕЙ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Н.В. Андреева, С.В. Шустиков
Научный руководитель – к.т.н., доцент А.В. Любимов

В работе представлены результаты анализа и выбора базовых параметров полуформальных моделей системы управления информационной безопасностью (СУИБ). От этих параметров существенным образом зависит объем результирующей модели, область ее применимости и ее конкретное наполнение. В статье результаты выбора параметров модели показаны на примере построения функциональной модели СУИБ по стандарту ISO 27001:2005.

Введение

В настоящее время достаточно широко распространено моделирование бизнес-процессов. Этот вид деятельности эффективен при сборе и объективном анализе информации о проводимых в организации операциях, способствует выявлению ошибок на ранних стадиях проектирования систем, распространению информации о системе между заинтересованными лицами (например, сотрудниками и руководством организации, оценщиками) и др.

Предметом моделирования в данной работе является система управления информационной безопасностью организации. Основными документами в области управления информационной безопасностью принято считать международные стандарты серии ISO 2700x. Для систематизации сведений, содержащихся в данных стандартах, выявления потенциальных неточностей в их положениях или возможности их дополнения, а также для получения наглядного представления о том, что нужно сделать для построения/сертификации СУИБ конкретной организации, предполагается построение совокупности моделей, включающей в себя структурную (объектную и процессную) и функциональную модели.

Все предполагаемые модели являются полуформальными. При этом под полуформальными понимаются модели, для построения которых используются любые формализмы, кроме математических.

Рассматривая в общем формальное моделирование на соответствие требованиям международных стандартов в области безопасных информационных технологий, можно назвать три аналога. Среди зарубежных – это комплексная модель процесса оценки ИТ по «Общим критериям» (стандарт ISO 15408), построенная в Центре безопасности информации стран Британского содружества (CISC) в 2002 году [1]. Упомянутая работа содержит несколько функциональных диаграмм, которые получены по методике, напоминающей SADT. При построении диаграмм реально не использовалась какая-либо определенная методика или метод, фактически они представляют собой иллюстрации, а не формализованную модель. Модель построена не по стандарту, а по описанию сценария оценки некоторого условного продукта, что не позволяет серьезно говорить ни о ее полноте, ни об адекватности. Диаграммы модели не привязаны друг к другу по ресурсам, и она имеет, таким образом, чисто иллюстративный характер.

Среди отечественных аналогов можно назвать модель Системы менеджмента качества по стандарту ISO 9001:2000 [2] и функциональную модель (более полную, чем подобная ей зарубежная) процессов оценки безопасности информационных технологий по методологии Общих критериев, которая была предложена в [3] и получила практическое приложение в [4]. В обеих представленных моделях для построения используется полнофункциональная методика SADT в совокупности с методикой DFD.

В статье [5] также дано наглядное представление СУИБ организации в соответствии со стандартом ISO/IEC 27001:2005, но сделано это в виде отдельных иллюстраций

и пояснительного текста к ним, без использования специальной методики и метода моделирования. Поэтому работа, представленная в данной статье, не является формализованной моделью. Кроме того, в ней представлены только основные этапы работ по созданию СУИБ без строгой привязки к тексту стандарта.

При построении полуформальных моделей предметной области существенное значение имеет набор базовых параметров предполагаемой модели, таких как нотация, контекст, включая цель и точку зрения моделирования, определение модели и границы моделирования. От этих параметров, выбираемых априорно, существенным образом зависит не только объем результирующей модели и область ее применимости, но и ее конкретное наполнение.

В работе представлены результаты выбора этих параметров в задаче построения функциональной модели систем управления информационной безопасностью по стандарту ISO 27001:2005.

Теоретическое описание основных параметров моделирования

Базовыми свойствами модели являются нотация, контекст, включая цель и точку зрения моделирования, определение модели и границы моделирования.

Под нотацией моделирования обычно понимают способ графического отображения модели. AllFusion Process Modeler (ранее BPwin) – инструментальное средство, используемое для построения модели СУИБ, основные свойства которой рассматриваются в данной работе – поддерживает 3 нотации моделирования: IDEF0, DFD и IDEF3.

IDEF0 – стандарт функционального моделирования – используется для отображения функциональной структуры предметной области. Данная методология позволяет описать выполнение работ на верхнем уровне и не учитывает временной аспект при их выполнении, предусматривая описание только логической соподчиненности.

DFD – методика диаграмм потоков данных – позволяет отобразить информационные потоки в моделируемой деятельности. Удобна для описания документооборота и требований к информационной системе. DFD-диаграммы могут включать хранилища данных, к которым осуществляется доступ и внешние по отношению к системе источники и адресаты данных. В отличие от IDEF0 и IDEF3, не является стандартом и не предусматривает выполнение четких правил.

IDEF3 – стандарт описания потоков работ – используется для отображения логической последовательности выполнения процедур, акцентируя внимание на ходе выполнения работ и взаимоотношениях процессов и объектов системы. Используется для описания процессов предметной области на нижнем уровне. Позволяет дать представление о процессе в целом и описать сценарии из реальной деятельности организации [6].

После выбора нотации можно приступать непосредственно к моделированию, которое начинается с определения самого абстрактного уровня описания моделируемой системы в целом – контекста модели.

На контекстной диаграмме показываются взаимоотношения между субъектом моделирования (самой моделируемой системой) и окружающей средой. На DFD-диаграммах, кроме входящих и исходящих ресурсов, также отображаются внешние по отношению к субъекту моделирования источники и приемники данных. Помимо этого, в контекст модели входит описание цели, точки зрения и области моделирования. При формулировке цели моделирования аналитик отвечает на ряд вопросов:

- Почему этот процесс должен быть смоделирован?
- Что должна показывать модель?
- Что может получить заказчик?

При построении модели могут учитываться мнения различных специалистов, но все они должны придерживаться единой точки зрения на модель, которая, в свою оче-

редь, должна соответствовать цели моделирования. Обычно в качестве точки зрения моделирования принимают позицию того специалиста (или объекта), со стороны которого моделируемая система в действии видна наиболее полно.

Помимо цели и точки зрения на моделируемую систему значительное влияние оказывает определение границ моделирования. При этом принято учитывать как широту (какие процессы включены в систему, а какие остаются снаружи), так и глубину (максимальный уровень детализации диаграмм) моделирования [7].

Результаты выбора основных параметров моделирования в задаче построения функциональной модели СУИБ

Нотация модели

В качестве нотации (и метода) функционального моделирования была выбрана методика диаграмм потоков данных (Data Flow Diagrams, DFD). Данная нотация позволяет отразить последовательность работ, выполняемых по ходу процесса, и потоки информации, циркулирующие между этими работами, включая хранение потоков данных, для достижения максимальной доступности и минимального времени ответа. Также с помощью методики DFD можно описывать потоки документов и материальных ресурсов [6].

Этот методика изначально создавалась как средство проектирования информационных систем. Практически любой класс систем успешно моделируется при помощи DFD-ориентированных методик: в этом случае вместо реальных объектов рассматриваются отношения, описывающие свойства этих объектов и правила их поведения. Данная методика успешно применяется для моделирования систем управления, богатых разнообразными отношениями [8].

При внедрении процессного подхода к управлению организацией также в основном используется методика DFD, так как она позволяет максимально снизить субъективность описания бизнес-процессов. С помощью схемы процессов в DFD выявляют основные потоки данных, что важно для последующего создания моделей структуры данных и разработки требований к информационной системе организации [6]. Кроме того, для соответствия модели PDCA необходимо отразить связи СУИБ организации с внешними (по отношению к моделируемой системе) заинтересованными сторонами. Представление внешних сущностей (как и необходимых хранилищ документов и записей) возможно только при использовании методики DFD. Данная методика, по сравнению с более распространенным стандартом IDEF0, позволяет, во-первых, гораздо более полно отразить на диаграммах роли сущностей, инициирующих, выполняющих, заканчивающих или использующих результаты выполнения процессов, а во-вторых, дает возможность гораздо более полно представить обмен ресурсами (в частности – документами) между сущностями процессов.

Контекст модели

Контекстная диаграмма. Субъектом моделирования является система управления информационной безопасностью организации. Контекст модели составляют взаимоотношения между СУИБ и различными заинтересованными сторонами: как внешними, так и внутренними, которые отображаются в виде внешних сущностей.

В результате анализа текста стандарта ISO/IEC 27001:2005 были выделены 7 основных внешних сущностей:

Organization (Организация) – Organization itself, regardless of it's type (e.g. commercial enterprises, government agencies, non-profit organizations), where ISMS is being established and operated (организации любого типа – коммерческие, государственные, некоммерческие – в которых создается и функционирует СУИБ) [9], 1.1.

Management (Руководство) – Top management of the organization (высшее руководство организации) [9], 1.1.

Interested parties (Заинтересованные стороны) – Parties, interested in organization's activity or successful result of organization's activity: it's owners, employees, creditors, customers, suppliers, insurers, partners, society (лицо или группа лиц, заинтересованные в деятельности или успехе организации – потребители, владельцы, работники организации, поставщики, банкиры, ассоциации, партнеры или общество) [10], 3.2.2.

Note. Parties can be an organization, part of the organization, or number of organizations (примечание – группа лиц может состоять из организации, ее части или нескольких организаций) [11].

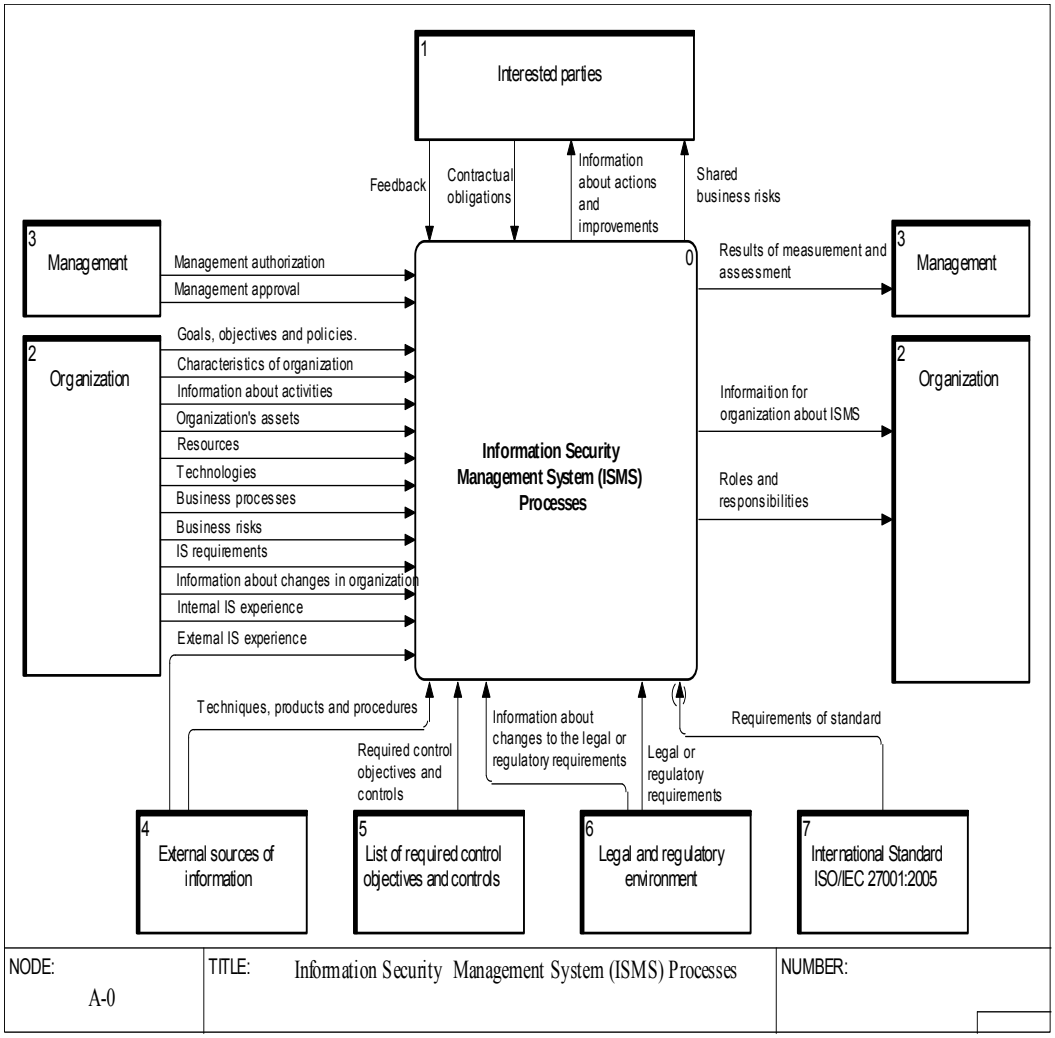


Рис. 1. Контекстная диаграмма модели СУИБ

External sources of information (Внешние источники информации) – Other parties possessing the information and experience that could be used for ISMS establishing, e. g. consulting companies (другие участники, чей опыт в области безопасности можно использовать при организации СУИБ, например, консалтинговые фирмы).

List of required control objectives and controls (Список обязательных целей и средств управления) – List of required control objectives and controls, represented in ISO/IEC 27001 Annex A, or ISO/IEC 17799:2005, clauses 5–15 (список целей и средств управления, предоставляемый ISO/IEC 27001:2005, Annex A или ISO/IEC 17799:2005, clauses 5–15).

Legal and regulatory environment (Законодательное и регламентирующее окружение) – Legislation and regulatory requirements, applied to information security management systems and overall management systems (законодательные и нормативно-методические требования в области управления безопасностью информации и систем управления в целом) [9], A.15.

International Standard ISO/IEC 27001:2005 (Стандарт ISO/IEC 27001:2005) – Text of International Standard ISO/IEC 27001:2005 (текст международного стандарта ISO/IEC 27001:2005).

Контекстная диаграмма представлена на рис. 1.

Назначение модели (Purpose). Основными понятиями методологии SADT являются цель и точка зрения моделирования [12], которые составляют основное свойство модели – ее назначение (Purpose). Данная модель разрабатывалась в качестве вспомогательного материала при подготовке к сертификации на соответствие требованиям международного стандарта ISO/IEC 27001:2005 (в том числе). Соответственно, *целью моделирования* в данном случае является описание процессов создания и функционирования системы управления информационной безопасностью и их взаимодействия в соответствии со стандартом ISO/IEC 27001:2005. Кроме того, модель может использоваться в образовательных целях, а также в качестве шаблона при проектировании СУИБ.

В состав целевой аудитории входят консультанты (те, кто проводит предварительный – репетиционный аудит) и аудиторы (те, кто проводит сертификационный аудит) СУИБ, заявители и спонсоры оценивания СУИБ, а также ее пользователи (заинтересованные стороны, персонал организации).

На начальном этапе моделирования необходимо выбрать *точку зрения* моделирования (Viewpoint), т.е. позицию, с которой будет рассматриваться модель. Результат данного выбора в дальнейшем существенно влияет как на границы моделирования в целом, так и на процедуры детализации, осуществляемые в ходе построения самой модели.

В данной работе модель рассматривается с точки зрения потенциального разработчика СУИБ – руководителя отдела Информационной безопасности (Chief Information Security Officer, CISO), так как, скорее всего, именно он будет ответственен за моделируемую систему в целом. Соответственно, при моделировании с точки зрения этой роли мы получим наиболее универсальную функциональную модель.

Область моделирования. После формулировки цели и точки зрения на модель необходимо дать ей определение (definition) и обозначить границы моделирования (scope).

Модель содержит представление взаимосвязанных процессов создания, внедрения, эксплуатации, мониторинга, анализа, поддержки и улучшения системы управления информационной безопасностью. Данная система дополнена процессами, лежащими вне цикла PDCA, но предусмотренными стандартом ISO/IEC 27001:2005. В качестве примера таких «дополнительных» процессов можно привести документирование СУИБ.

Границы моделирования: в данной модели проводится максимальная детализация процессов в соответствии с пунктами и подпунктами стандарта ISO/IEC 27001:2005. Наиболее подробно рассмотрены процессы оценки рисков (включая их идентификацию, анализ и оценивание), поскольку именно система управления рисками, представляющая собой подсистему анализа рисков является ключевым элементом СУИБ [13].

Контекст модели составляют взаимоотношения между СУИБ и заинтересованными сторонами (такими как организация, государство, органы по стандартизации, другие заинтересованные участники и организации).

В модели рассматривается деятельность владельцев (информационных) активов и иных пользователей данной системы по управлению информационной безопасностью. Также внимание уделяется реализации ответственности руководства – в части предос-

тавления ресурсов для СУИБ и организации ее функционирования в целом, связи с внешними заинтересованными сторонами, а также организации эффективной работы персонала. Кроме того, в модели отображены процессы управления документами и записями, которые могут являться как внешними, так и внутренними ресурсами.

Деятельность внешних аудиторов не рассматривается в модели, но в нее включаются элементы деятельности внутренних аудиторов (проводят периодические плановые аудиты СУИБ в целях организации), а также руководства организации – по мониторингу и анализу СУИБ.

Описание модели

В соответствии с методологией SADT и выбранной нотацией, функциональная модель представляет собой иерархию DFD диаграмм, описывающих потоки данных между процессами. Каждая диаграмма модели получена путем детализации процесса, принадлежащего диаграмме более высокого уровня. Этот исходный процесс представлялся в виде разбиения на несколько подпроцессов в соответствии с ISO 27001:2005. При недостаточности сведений данного стандарта для определения процессов и ресурсов использовались другие нормативно-методические документы в данной области или мнения экспертов.

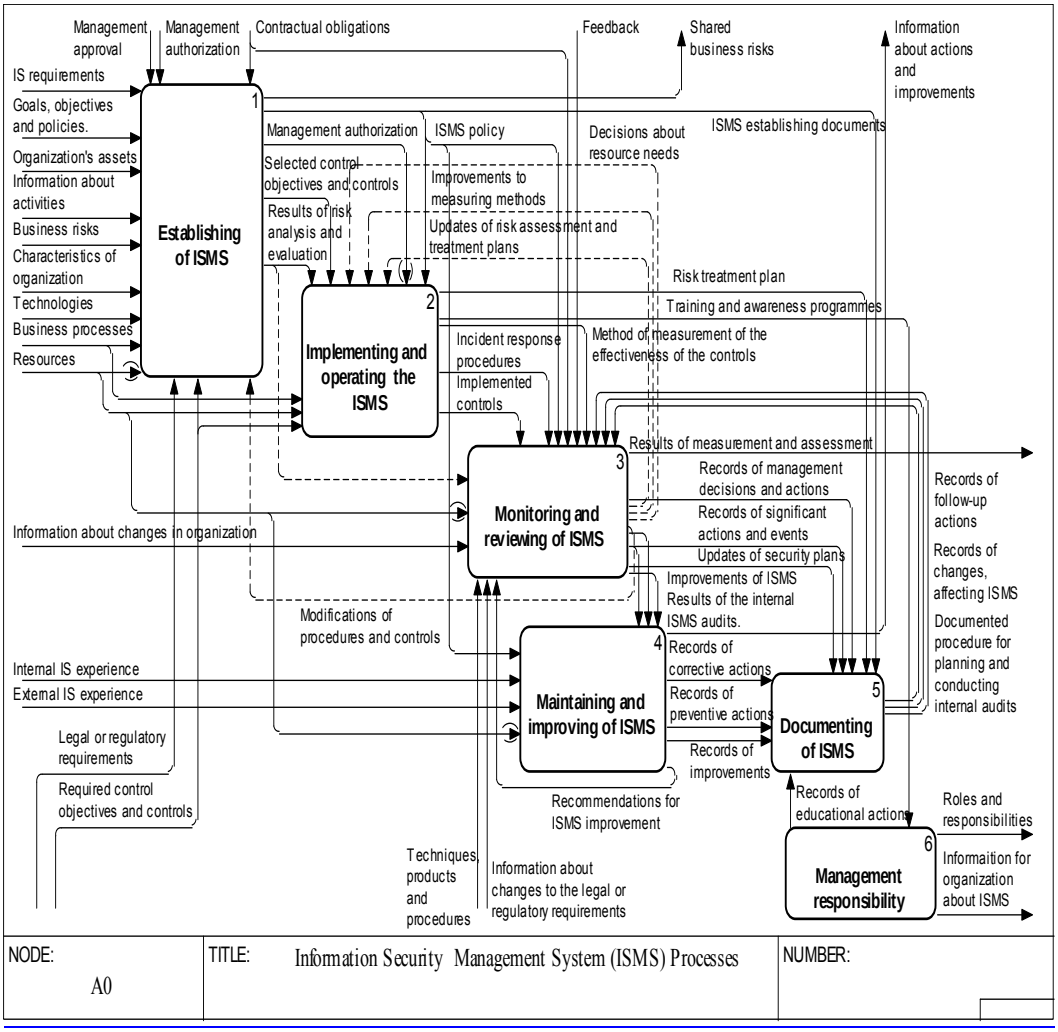


Рис. 2. Диаграмма детализации процесса «Maintaining and improving of ISMS»

Для примера на рис. 2 представлена одна из диаграмм детализации второго уровня действий по процессу «Maintaining and improving of ISMS» («Сопровождение и

улучшение СУИБ»). К настоящему моменту модель содержит 11 функциональных диаграмм, в которых представлена детализация деятельности по управлению информационной безопасностью организации – в основном до процессов второго уровня – детализация деятельности по управлению рисками, представляющей собой ключевой элемент СУИБ, представлена до процессов четвертого уровня. Иерархия функциональности включает в себя 53 процесса. В контекст модели входят 7 внешних сущностей.

В рассматриваемой функциональной модели используется более 75 ресурсов, которые были выделены на основе анализа текста стандарта ISO/IEC 27001:2005 и определений (definition) процессов. Ресурсы в покое описываются с помощью 2 хранилищ данных: ISMS documentation storage (хранилища документов СУИБ) и ISMS records storage (хранилища записей СУИБ).

Для рецензирования и использования модели средствами BPWin может быть сгенерирован отчет в виде html файла.

Заключение

Предметом рассмотрения в данной работе являлась система управления информационной безопасностью организации, моделирование которой производилось на основе текстов международных документов в области обеспечения информационной безопасностью – стандартов серии ISO 2700x.

Основополагающее значение при построении полуформальных моделей предметной области имеет определение базовых параметров будущей модели (нотации, контекста, цели и точки зрения моделирования, определения модели и границ моделирования). В данной работе представлены результаты анализа и выбора этих параметров в задаче построения функциональной модели систем управления информационной безопасностью по стандарту ISO 27001:2005.

Литература

1. Prieto-Diaz R. The Common Criteria Evaluation Process. Process Explanation, Shortcomings, and Research Opportunities. - Commonwealth Information Security Center Technical Report CISC-TR-2002-03, 2002 – CISC, James Madison University, USA.
2. Любимов А.В. Модели процессов СМК по стандарту ISO 9001:2000. Препринт кафедры Распределенных вычислений и компьютерных сетей. – СПб: СПбГТУ, 2004.
3. Любимов А.В. Функциональная структура общих критериев оценки безопасности информационных технологий // Труды 9-й научно-технической конференции «Теория и технология программирования и защиты информации. Применение вычислительной техники». – Санкт-Петербург, 18 мая 2005 г. – С. 20–24.
4. Николаев А.Ю., Любимов А.В., Суханов А.В. Автоматизация оценки объектов информатизации в соответствии с требованиями руководящих документов «Безопасность информационных технологий» Гостехкомиссии России // IV ежегодная всероссийская конференция «Обеспечение информационной безопасности. Региональные аспекты». – Сочи, 13–17 сентября 2005 г. – Тезисы докладов. – С. 27–31.
5. Носаков В. Создание комплексной системы управления информационной безопасностью. – JetInfo online, №7 (158), 2006. – Режим доступа: http://www.jetinfo.ru/2006/7/2/article2.7.2006.html
6. Волков О. Стандарты и методологии моделирования бизнес-процессов. – Связьинвест онлайн, №6, 2005. – Режим доступа: http://www.connect.ru/article.asp?id=5710.
7. Грекул В.И. Проектирование информационных систем (учебный курс): Лекция 7. Моделирование бизнес-процессов средствами BPwin, 2005. – Режим доступа: http://www.intuit.ru/department/se/devis/7/

8. Калянов А.Н., Козлинский А.В., Лебедев В.Н. Сравнительный анализ структурных методологий. // Системы управления базами данных. – 1997. – №05–06.
9. ISO/IEC FDIS 27001:2005(E). Information technology – Security techniques – Information security management systems – Requirements.
10. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения.
11. ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь.
12. Марка Д.А., МакГоуэн К. Методология структурного анализа и проектирования SADT. – Электронная библиотека, 1999. – Режим доступа: http://www.interface.ru/fset.asp?Url=/case/sadt0.htm
13. Горобец Н.И. BSI и BS 7799 – Видение разработчиков. 2005. – Режим доступа: http://www.globaltrust.ru/security/Pubs/Pub10_NIG_BS7799.htm

ИССЛЕДОВАНИЕ КОНКУРИРУЮЩЕГО ВЗАИМОДЕЙСТВИЯ КОРПОРАТИВНЫХ РЕСУРСОВ НА ОСНОВЕ АНАЛИЗА ИСТОРИЧЕСКИХ ПРОЦЕССОВ

М.В. Береговой
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Исторические процессы, рассмотренные в контексте как межгосударственных отношений, так и отдельно взятого государства фактически могут быть применимы для исследования корпоративных структур. Изучение исторических процессов может помочь более широко взглянуть на корпоративную теорию.

Введение

В процессе развития информационных технологий наличие конкурирующего взаимодействия между компонентами системы и борьба за установление контроля отдельных компонентов над однородными общесистемными ресурсами привело к обострению вопросов защиты и безопасности информации.

Конкуренция может возникать как за ресурсы индивидуумов, не входящих в корпорацию, так и входящих в нее. Естественно, ни одна корпорация не стремится к одномоментному захвату ресурсов другой корпорации, так как это требует, как правило, слишком значительных затрат. В данной работе предполагается, что корпорации примерно равны, следовательно, приведенный выше силлогизм верен. Конкурирующая корпорация стремится взять под контроль индивидуумов и их ресурсы, тем самым ослабляя соперника.

Конкуренция в любой момент времени представляет собой взаимодействие двух индивидуумов. Один индивидуум при помощи языка и информации оказывает влияние на другого, например, передавая ложную информацию и/или выдавая себя за члена корпорации. Целью является получение доступа к части корпоративных ресурсов, которыми владеет индивидуум. Также возможна компрометация индивидуума и, как следствие, компрометация корпоративных ресурсов и нарушение нормального информационного взаимодействия в корпорации.

Понятие корпорации, ресурсов и системы

Корпоративную систему можно рассматривать как совокупность субъектов, обладающих частью общих характеристик. Между такими субъектами существуют информационные взаимодействия, т.е. взаимный или односторонний обмен данными. Из этого утверждения следует, что корпоративную систему можно представить как информационную систему, обладающую совокупностью субъектов, осуществляющих информационное взаимодействие. Особенность корпоративной системы как информационной системы заключается в корпоративном характере информационных процессов.

Информационное взаимодействие возникает только при наличии других подобных и конкурирующих субъектов, т.е. системы субъектов, что является основой для возникновения между субъектами с целью организации совместной и конкурентной борьбы за ресурсы развития и существования как системы в целом, так и субъектов этой системы. Естественно, подразумевается, что субъекты системы находятся в постоянном информационном взаимодействии между собой.

Субъекты такой системы разделяются по уровням сложности, и используемые ими ресурсы также можно разделить по уровням комплексности, т.е. чем сложнее субъект, тем большее разнообразие ресурсов он может использовать.

Объединение во временные объединения – корпорации – связано с необходимостью обеспечения «секретности», по Шеннону, от других членов [4]. Поэтому свойства языка корпорации определяются числом возможных объединений в корпорации, при соблюдении определенных правил безопасности. Также имеет смысл учитывать воз-

можность субъектов объединения в корпорацию и отсутствие таковой. Здесь имеется в виду территориальная разрозненность субъектов и параметры каналов связи. Логично, что подобное объединение при сильном удалении субъектов друг от друга потребует значительных затрат на физическое обеспечение взаимодействия.

В определенный момент возникает внутрикорпоративная конкуренция за ресурсы, как материальные, так и информационные. Защита и безопасность информации становятся важнейшей частью существования и правильного функционирования как системы в целом, так и индивидуального, заключающегося в оптимальном изменении и использовании ресурсов [2].

Время жизни и возникновение конкуренции

Образование, развитие и функционирование любой системы аналогично биологическим процессам в природе. Поэтому сравнение возможно, и далее будут использоваться термины «популяция», т.е. совокупность субъектов, и «индивидуум» – собственно сам субъект.

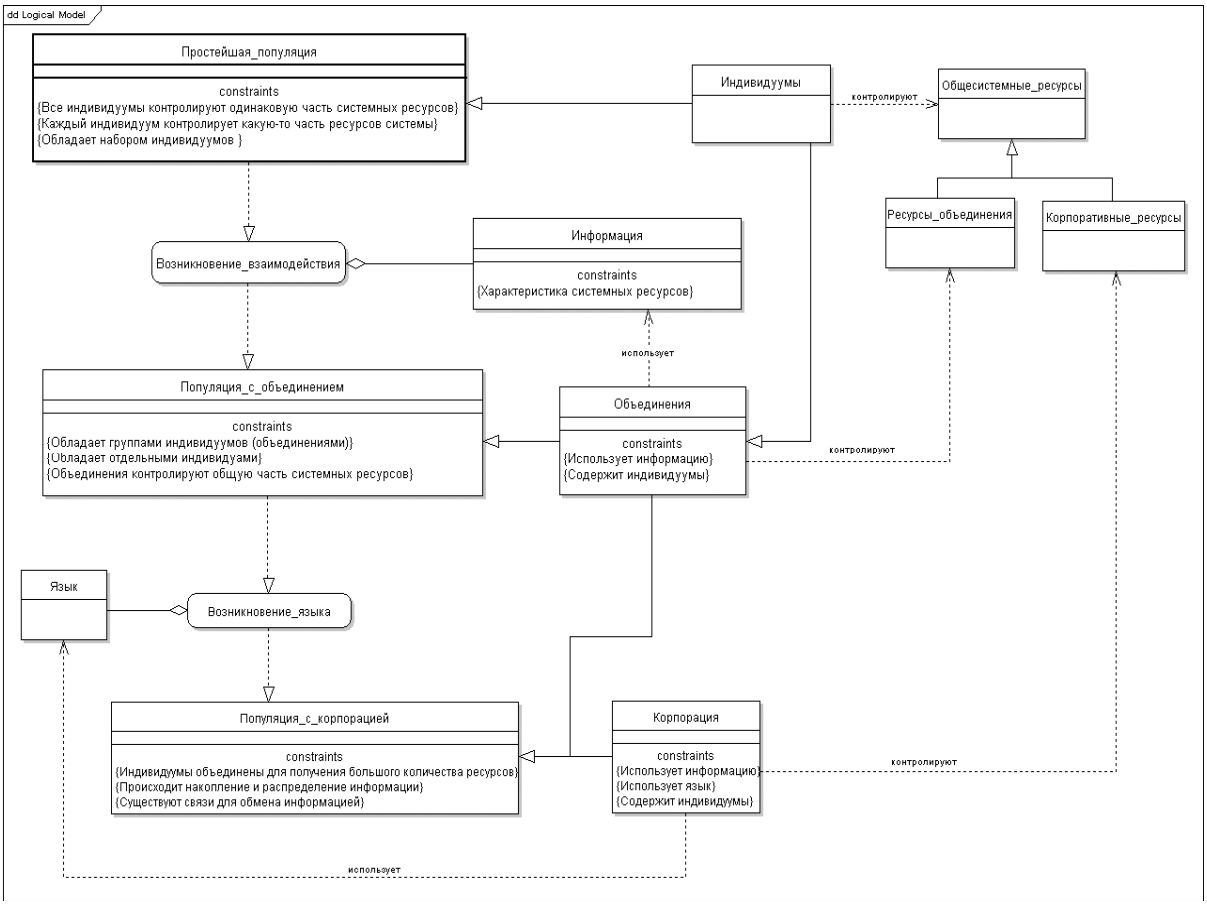


Рисунок. Процесс развития популяции

Каждый индивидуум имеет время жизни, в течение которого создает, перераспределяет и приобретает информацию, участвует в создании новых индивидуумов и защищенных образований. Время жизни корпорации больше, чем у индивида. Время жизни корпорации тратится на приобретение ресурсов и увеличение количества индивидов. Для лучшей конкуренции необходимо большее количество субъектов, соответственно корпорация растет. Как только численность индивидов в корпорации стабилизируется, конкуренция приобретает вид перераспределения и обработки информации.

При наличии информации как инструмента борьбы за системные ресурсы, возникают объединения, т.е. группы индивидуумов, контролирующих общую часть системных ресурсов. Здесь информация выступает в роли характеристики системных ресурсов, т.е. помога-

ет противостоять остальным индивидуумам популяции. При помощи информации индивидуум в объединении контролирует часть системных ресурсов объединения, которая заведомо больше, чем часть ресурсов, которые контролирует отдельный индивидуум.

После того, как образовались несколько объединений, необходим новый элемент для борьбы за ресурсы, которые или еще не распределены по объединениям, или за ресурсы самих объединений, причем между индивидуумами этих объединений. В этот момент и появляется язык, который способствует распределению информации между индивидуумами. Появление языка влечет за собой появление корпораций, в которых индивидуумы объединены для получения большого количества ресурсов и существуют связи для обмена информацией, т.е. происходит как само накопление информации, так и ее распределение.

В модели, изображенной на рисунке, отражен процесс развития популяции, ее составляющие и связи между ними.

В корпорации каждый индивидуум при помощи языка устанавливает различные отношения с другими индивидуумами. В результате таких отношений возникает распределение информации внутри корпорации. Такая деятельность корпорации направлена на накопление корпоративных ресурсов и их сохранение. Так как информация – это инструмент для накопления ресурсов, то возникает необходимость в ее защите. Потеря информации, которой располагают индивидуумы, не может привести к большим потерям корпоративных ресурсов.

Конкуренция в историческом контексте

Исторические процессы, рассмотренные в контексте как межгосударственных отношений, так и отдельно взятого государства, фактически могут быть применимы для исследования корпоративных структур. Это в полной мере относится и к религиям как к неотъемлемой части истории.

Корпорацию можно рассматривать как систему различных индивидуумов, между которыми происходят постоянные взаимодействия по обмену формализованными данными. Для взаимодействия между индивидуумами необходим инструмент, этим инструментом являются информация и язык. Корпорация может изолировать индивидуума, если таковой мешает нормальному функционированию системы в целом или ее компонентов (пример – тюремное заключение).

Между корпорациями может возникать конкурирующее взаимодействие, более того, как показывает история – это нормальное состояние для корпораций.

Конкуренция может возникать как за ресурсы индивидуумов, не входящих в корпорацию, так и входящих в нее. Естественно, ни одна корпорация не стремится к одномоментному захвату ресурсов другой корпорации, так как это требует, как правило, слишком значительных затрат. Конкурирующая корпорация стремиться взять под контроль индивидуумы и их ресурсы, тем самым ослабляя соперника. Также возможна компрометация индивидуума и, как следствие, компрометация корпоративных ресурсов и нарушение нормального информационного взаимодействия в корпорации. Подобное конкурирующее взаимодействие можно рассмотреть на примере любого восстания. Одна из корпораций стремится избавиться от влияния другой, ослабляя индивидуумов, получая контроль над ресурсами. Это может реализовываться за счет языка и информации, свойственных корпорации-противнику. Зачастую это позволяет получать контроль над ресурсами без применения активных действий, например агитации.

Развитие цивилизаций по своим параметрам схоже с биологическими процессами, в частности, с вирусами. Здесь возможно найти достаточно показательный пример в истории нашей цивилизации, а именно противостояние католиков и протестантов. Католическое общество можно рассматривать как корпоративную систему, обладающую определенными характеристиками, набором индивидуумов и процессами информаци-

онного обмена. Появление протестантства можно сравнить с внедрением вируса в систему через одного или несколько индивидуумов. Далее следуют инкубационный период и этап репродуцирования. Во время этих периодов все большее количество индивидуумов заражаются (принимают иную веру).

На этапе саморазмножения активизируется иммунная система, пытаясь сдержать рост зараженных индивидуумов. Корпорация пытается защитить свои объекты и ресурсы от поражения. В истории это выражалось в неприятии и отторжении новой идеи.

Одновременно с внедрением или после некоторого промежутка времени определенного числа внедренных копий и т.д. вирус приступает к выполнению специальных функций, именуемых еще логическими бомбами, которые вводятся в программное обеспечение и срабатывают только при выполнении определенных условий, например, по совокупности даты и времени, и частично или полностью выводят из строя компьютерную систему. В биологических системах это проявляется через симптомы болезни, в исторических процессах – через народные волнения и т.п. На этапе проявления вируса система переходит на режим повышенного воспроизведения антител, за счет чего пытается нейтрализовать инородные тела, фактически применяя естественный антивирус (например, Варфоломеевская ночь). Подобный метод можно применить к различным историческим, биологическим и информационным процессам.

Формирование языковых и информационных связей

Язык всегда являлся важнейшим компонентом развития мировых цивилизаций. На планете насчитывается от 2500 до 7000 языков. Но эти цифры более чем приблизительны, а точное количество неизвестно из-за отсутствия единого подхода к выделению диалектов одного и того же языка и условности различий между разными языками. Точно так же нет единого подхода к классификации языков. Наиболее популярна генеалогическая классификация, основывающаяся на историческом родстве языков, которые возникли из одного источника – праязыка. Согласно этому подходу, языки делятся на языковые семьи, которые, в свою очередь, подразделяются на группы близких друг другу языков.

Сегодня есть семь языков, являющиеся «мировыми языками». Это английский, испанский, арабский, русский, французский, немецкий, португальский. Каждый из этих языков распространен на территориях нескольких государств, что имеет свои исторические причины. В силу этих причин на этих языках говорит достаточно большое количество людей. Такие языки, как китайский, хинди и урду, тоже входят в число важнейших языков мира, но на международной арене менее популярны.

Носители одного языка стремятся образовывать корпорации. Это может быть как территориальное, так и информационное образование. Территориальная формация может находиться в пределах государства, где данный язык является национальным, и в пределах другой страны. Яркий пример – китайские и арабские кварталы.

Информационная формация наибольшее значение приобрела сравнительно недавно, вследствие глобализации и повышения доступности информационных средств. В этих формация язык и информация являются средствами для установления связей между индивидуумами, посредством чего сохраняется уклад жизни и обычаи, т.е. принципы построения корпорации.

В современных обществах государство не фиксирует национальную принадлежность гражданина в документах, удостоверяющих его личность (например, в паспорте, который, впрочем, во многих странах не обязателен), и не спрашивает человека о его национальности (например, при переписях населения). В ряде полиэтничных стран (Финляндия, Бельгия, Швейцария, Австрия, Испания, Турция, Пакистан, Индия, Канада, Мексика, Гватемала) национально-языковая тема переписи ограничена вопросом о родном языке.

Родной язык относится к тем измерениям человека, которые не выбираются. Природа речевой деятельности человека двойственна: в ней есть и врожденное (генетическое), и приобретенное. Генетически в людях заложена способность в первые годы жизни усвоить язык, причем любой язык. Однако отнюдь не от генетики, а от социальных условий зависит то, какой именно этнический язык (белорусский, немецкий, армянский, эскимосский) усвоит ребенок. Во многих случаях первым языком человека оказывался язык не физических, а приемных родителей; вообще говоря, это язык того окружения, в котором ребенок жил первые годы жизни (например, киргизский или казахский языки тех семей и детских домов, которые в годы войны приняли осиротевших маленьких детей белорусских, украинских или русских родителей). Таким образом, овладение первым языком – это не «природный», а социально-психологический процесс.

В кругу названных измерений человека и социума особое место занимают три признака: язык, этничность (национальность) и конфессионально-вероисповедная принадлежность. Они взаимосвязаны, так что их иногда смешивают (особенно часто определяют этничность, опираясь на признак языка или конфессии). Эти измерения называют в числе главных факторов, создающих своеобразие культуры и ментальности народа, т.е. своеобразие его психического склада, мировосприятия, поведения.

Это один из основополагающих принципов корпорации. Принцип наследственности предполагает, что любой вливающийся в корпорацию индивидуум будет обладать языком и информацией, присущей данной корпорации. Этими инструменты он будет постигать в начале своей жизни и потом передавать по наследству. Если же индивидуум уже обладает информацией и языком другой корпорации, то он будет стремиться передать их корпорации. Однако здесь будет иметь место принцип ассимиляции. Т.е. в корпорации индивидуум приобретет новые инструменты информационного обмена.

Заключение

Корпоративную систему можно рассматривать как систему различных субъектов, между которыми происходят постоянные взаимодействия по обмену формализованными данными, посредством языка и информации. Различные по сложности и функциональным особенностям субъекты системы используют различные ресурсы, но некоторые ресурсы могут одновременно использоваться несколькими субъектами, в результате происходит борьба за ресурсы. Это фактор наличия конкурирующего взаимодействия между компонентами системы за контроль отдельных компонент над однородными общесистемными ресурсами. В процессе развития информационных технологий это привело к обострению вопросов защиты и безопасности информации.

Жизненный цикл корпораций можно сравнить с развитием государства, ведь оно, собственно, и является корпорацией. Изучение исторических процессов может помочь более широко взглянуть на корпоративную теорию.

Литература

1. Осовецкий Л.Г., Немолочнов О.Ф., Твердый Л.В., Беляков Д.А. Основы корпоративной теории информации. – СПб.: СПбГУИТМО, 2004. – 83 с.
2. Берзин Е.А. Оптимальное распределение ресурсов и теория игр. – М.: Радио и связь, 1983. – 216 с.
3. Буч Г., Рамбо Д., Джекобсон А. Язык UML. Руководство пользователя: / Пер. с англ. – М.: ДМК, 2000. – 275 с.
4. Шеннон К. Математическая теория связи. – М.: ИИЛ, 1963. – 207 с.

РЕЖИМ КОММЕРЧЕСКОЙ ТАЙНЫ. ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Е.В. Безгодов
Научный руководитель – к.т.н., доцент А.Г. Карманов

В рамках настоящего исследования рассмотрен вопрос защиты коммерческой тайны: причины повышения потребностей бизнеса в данной сфере; законодательство Российской Федерации в области защиты КТ; связь между требованиями Федерального Закона РФ «О коммерческой тайне» №98-ФЗ и международного стандарта ISO/IEC 27001. Предлагаемая автором схема реализации режима КТ, описанные методики и опыт находят применение при установлении в организации режима коммерческой тайны, его поддержке и применении.

Введение

Конфиденциальной информацией, представляющей определенную ценность, обладают практически все участники рынка. К такой информации относятся не только такие очевидные категории информации, как дорогостоящие технологии, ноу-хау, отчеты о научно-исследовательских и опытно-конструкторских разработках, конфиденциальные данные клиентов, доверенные провайдеру информационных услуг и связи. К ней относятся также внутренние технологии работы любой компании, независимо от того, оформлены ли они документально или же являются просто частью корпоративной культуры; сведения о планах развития компании; информация о структуре и принципах работы корпоративной информационной системы, систем охраны и безопасности; принципы и технологии ценообразования и многие другие категории информации. Любая такая информация, попав в руки конкурентных или недружественных организаций, может быть использована как для получения прибыли, которая могла бы быть получена законным владельцем информации, так и для причинения вреда ее владельцу.

До недавнего времени проблеме информационной безопасности уделяли серьезное внимание немногие коммерческие организации российского рынка. Обусловлено это было, прежде всего, незрелостью большинства компаний и в целом российского частного предпринимательства, начавшего свою новую историю лишь в начале 90-х гг. У незрелой компании, в которой отсутствуют четко описанные бизнес-процессы даже на верхнем уровне, во-первых, «достаточно головной боли и без забот об информационной безопасности», во-вторых, сама задача построения эффективной системы ИБ в таких условиях оказывается неоправданно дорогостоящей в исполнении. Ввиду этих причин до последних лет задачи обеспечения информационной безопасности серьезно ставились и реализовывались только на предприятиях, в силу своего рода деятельности особо чувствительных к уровню информационной безопасности, таких как банки, операторы связи, организации, ведущие научно-исследовательские и опытно-конструкторские разработки, обладающие дорогостоящими уникальными технологиями и пр.

Однако по мере развития частного сектора экономики и рыночных отношений наблюдается тенденция к повышению интереса руководства большинства коммерческих организаций к вопросам обеспечения информационной безопасности. Одновременно с этим повышается и степень готовности самих компаний к организации комплексных систем защиты информации, непосредственно зависящая от зрелости компании.

На фоне такого развития четко прослеживается классификация компаний с точки зрения зрелости обеспечения информационной безопасности, предложенная исследовательской компанией Gartner Group [1]. В рамках этой классификации выделены четыре уровня зрелости.

0 уровень: ИБ в компании никто не занимается; руководство не осознает важности проблем ИБ; финансирование отсутствует; ИБ реализуется штатными средствами опера-

ционных систем, СУБД и приложений; все технические вопросы находятся в зоне ответственности системного администратора.

1 уровень: ИБ в компании рассматривается как чисто техническая проблема; в компании отсутствует политика информационной безопасности; финансирование ведется в рамках общего ИТ-бюджета; ИБ реализуется средствами 0 уровня плюс средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN.

2 уровень: характеризуется появлением организационной составляющей БИ (аудит ИБ, управление рисками, политика и концепция ИБ, регламенты, инструкции и пр.), пониманием важности ИБ со стороны руководства, усилением уровня технической защиты (средства усиленной аутентификации, контентного анализа e-mail- и web-трафика, обнаружения вторжений, анализа защищенности, инфраструктуры открытых ключей). Финансирование ведется в рамках отдельного бюджета.

3 уровень: этот уровень обладает всеми свойствами 2 уровня, плюс на этом уровне ИБ является частью корпоративной культуры; организационно служба ИБ имеет статут самостоятельного подразделения и подчиняется высшему руководству компании; создана группа реагирования на инциденты в области ИБ; внедрено соглашение об уровне услуг (SLA).

По мере перехода компаний с 1 на 2 и с 2 на 3 уровни зрелости становится все более актуальным вопрос об имеющихся в распоряжении этой компании средствах обеспечения ИБ. Стремясь обеспечить конфиденциальность своих данных, компания развивает организационные и технические средства защиты. Однако этих средств оказывается недостаточно для полноценной защиты интересов компании, обладающей важной конфиденциальной информацией, и возникает необходимость в законодательном регулировании отношение с работниками, контрагентами и внешней недружественной конкурентной средой.

Институт КТ является инструментом, позволяющим:

- регулировать отношения участников оборота конфиденциальной информации, представляющей коммерческую ценность;
- требовать владельцу информации охраны ее конфиденциальности от лиц, получивших к ней доступ (законный или незаконный)
- решать конфликты, связанные с разглашением конфиденциальной информации

Законодательство РФ в области защиты коммерческой тайны

Вопросы защиты коммерческой тайны в настоящее время регулируются следующими правовыми актами Российской Федерации:

- Конституция Российской Федерации;
- Федеральный Закон РФ «О коммерческой тайне» №98-ФЗ;
- Гражданский кодекс РФ, Часть 4.

Законодательство РФ в данной области является на данный момент очень «молодым» и недоработанным. Так, например, вступившая в силу с 1 января 2008 г. глава 34 ФЗ РФ «О введении в действие части четвертой Гражданского кодекса Российской Федерации» изменила само понятие коммерческой тайны [2]. Этот факт, а тем более, отсутствие на данный момент в России правоприменительной практики в данной области делают исследования на тему защиты коммерческой тайны особо актуальными.

Методика защиты коммерческой тайны

Федеральным Законом РФ «О коммерческой тайне» №98-ФЗ определены следующие основные условия, необходимые для выполнения режима коммерческой тайны:

- определение перечня информации, составляющей коммерческую тайну;

- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации [3].

Обращаясь к мировому опыту, перенятому недавно и российской системой стандартов, можно увидеть, что задачи, поставленные перед проектом «КТ» в значительной степени перекликаются с технологией построения системы управления информационной безопасностью (СУИБ), предложенной международным стандартом ISO 27001 (ГОСТ ИСО/МЭК 27001)/4/. Этим стандартом предлагаются этапы создания, внедрения, контроля и улучшения СУИБ (табл. 1).

Этап построения СУИБ	Соответствие задачам проекта «КТ»
1.Создание СУИБ	Создание нормативной базы
1.1. Определение области действия и границ СУИБ	Создание концепции СУИБ
1.2. Определение политики СУИБ	Создание политики информационной безопасности
1.3. Оценка рисков организации	
1.3.1. Определение подхода организации к оценке рисков	Определение подхода к составлению перечня информации, составляющей КТ компании
1.3.2. Идентификация рисков	
1.3.2.1. Идентификация активов	Составление перечня информации, составляющей КТ компании
1.3.2.2. Идентификация угроз для активов	Данные работы решено вынести в отдельный проект повышения защищенности корпоративной информационной системы, реализуемый отдельно от проекта «КТ».
1.3.2.3. Идентификация уязвимостей	
1.3.2.4. Идентификация влияния компрометации активов	
1.3.3. Анализ и оценивание рисков	
1.3.3.1. Оценка влияния нарушений безопасности	
1.3.3.2. Оценка вероятности нарушения безопасности	
1.3.3.3. Количественная оценка уровня рисков	
1.3.3.4. Определение допустимости риска	
1.3.4. Определение и выбор вариантов обработки рисков	Построение иерархии разрабатываемых документов
1.3.5. Выбор целей и средств управления для обработки рисков	
1.3.6. Получение одобрения у руководства для предполагаемых остаточных рисков	

1.4. Получение полномочий от руководства	
1.5. Подготовка Положения о применимости	
1.6. Планирование СУИБ	
2.Внедрение и эксплуатация СУИБ	
2.1. Создание плана обработки рисков	Разработка и внедрение основных регламентов, процедур и процессов, обеспечивающих выполнение режима КТ
2.2. Внедрение плана обработки рисков	
2.3. Внедрение средств управления	
2.4. Определение методов измерения эффективности средств управления	
2.5. Внедрение программ повышения квалификации и компетентности	
2.6. Внедрение процедур реагирования на инциденты	Разработка и внедрение Управления инцидентами информационной безопасности, необходимого для нормального функционирования режима КТ
2.7. Управление функционированием СУИБ	
2.8. Управление ресурсами для СУИБ	
3.Мониторинг и анализ СУИБ	Продвижение, исполнение, поддержка и улучшение разработанных регламентов, процедур и процессов.
3.1. Выполнение процедур мониторинга и анализа	
3.2. Анализ эффективности СУИБ	
3.3. Измерение эффективности средств управления	
3.4. Анализ оценок риска	
3.5. Проведение внутренних аудитов СУИБ	
3.6. Анализ СУИБ руководством	
3.7. Корректировка планов безопасности	
3.8. Регистрация действий и событий	
4.Сопровождение и улучшение СУИБ	
4.1. Непрерывное улучшение СУИБ	
4.2. Выполнение корректирующих действий	
4.3. Выполнение превентивных действий	
4.4. Информирование о действиях и улучшениях	
4.5. Проверка действенности улучшений	

Таблица 1. Соответствие между этапами построения СУИБ по стандарту ISO 27001 и основными задачами, решаемыми в рамках проекта «КТ»

Исходя из показанной в табл. 1 проекции стандарта ISO 27001 на требования Федерального Закона РФ «О коммерческой тайне» №98-ФЗ, в ходе исследования построена модель комплекта регламентирующих документов, минимально необходимых для функционирования на предприятии режима коммерческой тайны (рисунок).

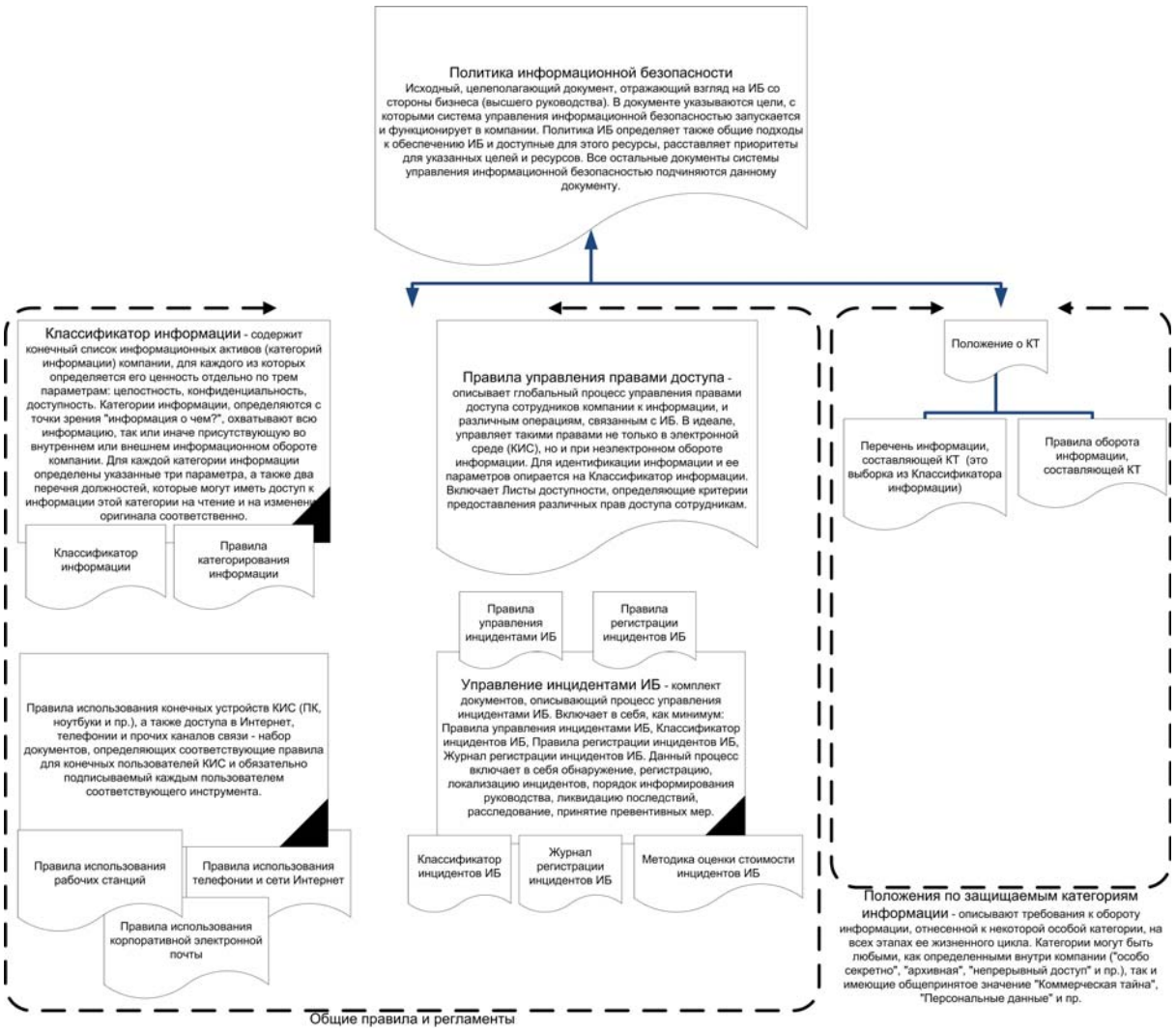


Рисунок. Модель комплекта регламентирующих документов, минимально необходимых для функционирования на предприятии режима коммерческой тайны

Заключение

В исследовании подробно рассмотрен вопрос установления, поддержания и применения на предприятии режима коммерческой тайны с целью защиты конфиденциальной информации. Разработанная в ходе исследования модель комплекта регламентирующих документов, минимально необходимых для функционирования на предприятии режима коммерческой тайны, может успешно применяться при реализации проектов по обеспечению защиты конфиденциальности информации, составляющей коммерческую тайну компании. Особую ценность модель приобретает ввиду отсутствия в открытых источниках подобных разработок, направленных на применение мирового опыта в области защиты информации для выполнения требований Российского законодательства.

Литература

1. Биячуев Т.А. Безопасность корпоративных сетей. – 2004. – 117 с.
2. ФЗ РФ «О введении в действие части четвертой Гражданского кодекса Российской Федерации» №231-ФЗ.
3. ФЗ РФ «О коммерческой тайне» №98-ФЗ.
4. ГОСТ ИСО/МЭК 27001.

ЗАДАЧА ОБЪЕКТНОГО МОДЕЛИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Д.В. Черемушкин
Научный руководитель – к.т.н., доцент А.В. Любимов

В работе представлена постановка задачи объектного моделирования системы управления информационной безопасностью (СУИБ), обоснована ее актуальность и новизна, обозначен подход к ее решению, базирующийся на линейке международных стандартов управления информационной безопасностью ISO/IEC 2700x. Приводятся результаты сравнительного анализа методик и инструментальных средств объектного моделирования, обосновывается их выбор для решения поставленной задачи. На основе анализа стандартов линейки предложена последовательность включения стандартов в модель.

Введение

В современном мире достижение эффективности и экономической выгодности в различных сферах деятельности невозможно без правовой регламентации процессов, составляющих эту деятельность, и обязанностей субъектов, в ней задействованных. Особенную актуальность правила, регламенты и стандарты приобретают в областях, связанных с риском нанесения того или иного ущерба. Одной из таких областей, имеющих в настоящее время важнейшее значение, является управление информационной безопасностью.

Международный опыт в сфере управления информационной безопасностью находит свое отражение в семействе стандартов ISO/IEC 2700x. Эта линейка стандартов описывает вопросы построения и функционирования системы управления информационной безопасностью (СУИБ) в организации и разрабатывается Международной организацией по стандартизации (ИСО, ISO) и Международной электротехнической комиссией (МЭК, IEC). В данную линейку входят как уже принятые, так и находящиеся в разработке стандарты.

(1) ISO/IEC 27000 содержит обзор, состояние, отношения и словарь международных стандартов, составляющих семейство.
(2) ISO/IEC 27001 – сертификационный стандарт – устанавливает требования к созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и улучшению документированной СУИБ в контексте бизнес–рисков организации. Он определяет требования по применению средств управления безопасностью с учетом потребностей отдельных организаций.
(3) ISO/IEC 27002 – переименованный стандарт ISO/IEC 17799:2005 – включает рекомендации по управлению информационной безопасностью, предназначенные для сотрудников, ответственных за создание, внедрение и поддержку мер, обеспечивающих безопасность в организации.
(4) ISO/IEC 27003 предоставляет практическое руководство по руководство по созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и улучшению СУИБ в соответствии с требованиями стандарта ISO/IEC 27001:2005.
(5) ISO/IEC 27004 содержит спецификацию и руководство по использованию методов измерения эффективности СУИБ.
(6) ISO/IEC 27005 предназначен для определения основных факторов информационного риска и подходов к его оценке и обработке.
(7) ISO/IEC 27006 описывает аккредитационные требования к сторонам, проводящим аудит и сертификацию СУИБ.
(8) ISO/IEC 27007 содержит руководство по проведению аудита СУИБ.

Указанное семейство стандартов является развитием британских стандартов BS 7799–1, BS 7799–2 и BS 7799–3, согласованных с положениями серии международных стандартов ISO/IEC 13335.

Каждый стандарт явно или неявно содержит некоторую методологию, т.е. концептуальную модель своей предметной области (содержание и связь основных понятий) в совокупности с моделью постановки проблем и их решения.

Для знания и понимания стандартов, их эффективного практического применения, сравнения и согласования с другими нормативными документами особое значение приобретает формализованное и наглядное представление такой методологии.

В связи со сказанным актуальной задачей является разработка связной системы объектных моделей стандартов линейки ISO/IEC 2700x. Объектом моделирования является общий контекст безопасности организации, описанный в указанном семействе стандартов. Под общим контекстом безопасности понимается совокупность основных принципов, сущностей, процессов и их взаимосвязей, обеспечивающих или непосредственно связанных с обеспечением информационной безопасности. Объектная модель отражает содержание и связь статических (относительно постоянных во времени) понятий предметной области.

Первые отечественные результаты, относящиеся к объектному моделированию стандартов, представлены в работах [1, 2]. В них исследуется возможность объектного моделирования методологии оценки безопасности информационных технологий, основанной на международном стандарте ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий» (Общие Критерии) [3] по методике UML. В рамках указанных исследований были построены: объектная модель общего контекста безопасности (ОКБ) по Общим Критериям (версия 2.2); объектная модель угрозы по Общим Критериям; объектная модель контекста угрозы по Общим Критериям. Накопленный опыт использовался, в том числе, при написании настоящей работы, а разработанные модели могут применяться для сравнения подходов, изложенных в различных линейках международных стандартов в области безопасных информационных технологий.

Для достижения поставленной цели – разработки объектной модели общего контекста безопасности организации в соответствии с семейством международных стандартов ISO/IEC 2700x – необходимо решить следующие задачи:

(1) выбрать методику и инструментарий моделирования;
(2) выбрать стандарт линейки, с общей точки зрения описывающий основное назначение СУИБ, ее место в организации и основные этапы построения и функционирования, рассматриваемый в первую очередь;
(3) определить общие свойства будущей модели – точку зрения, границы и глубину моделирования;
(4) провести анализ и отразить результаты в модели;
(5) дополнять и развивать модель с привлечением других стандартов линейки.

Первые две задачи подробно рассматриваются в настоящей статье.

Основная часть

При выборе методики моделирования к ней предъявлялись следующие требования:

- обязательная стандартизация на международном уровне;
- наличие стандартизованного метода анализа предметной области (желательно);
- наличие в той или иной мере формализованного синтаксиса, имеющего графическое представление;
- наличие системы семантических правил;
- возможность расширения набора элементов языка моделирования и набора графических примитивов;
- наличие инструментальных средств поддержки, доступных непрофессиональному (в области моделирования) пользователю;

- наличие методической поддержки.

В результате сравнительного анализа трех методик объектного моделирования в плане перечисленных требований была выбрана методика UML 1.4/2.0.

В качестве альтернатив рассматривались методики ERD (IDEF1X) и OA (IDEF5). Существенным недостатком первой методики по сравнению с выбранной являются меньшие возможности по представлению отношений между сущностями, а второй – отсутствие средств моделирования процессов. Кроме того, обе эти методики не предусматривают расширение набора элементов и графических примитивов.

Для построения модели по конкретной методике могут использоваться различные инструментальные средства. Выбор инструментального средства моделирования в настоящей работе осуществлялся на основе ряда критериев:

- невысокие требования к ресурсам ПК, приемлемая производительность на ПК 2–3-летней давности;
- удобство использования, доступность непрофессиональному пользователю;
- наличие в открытом доступе наиболее распространенных расширений набора элементов и графических примитивов;
- наличие подробной документации;
- наличие функций формирования отчетов по моделям и возможность настройки таких функций, предпочтительно наличие изменяемых шаблонов отчетов.

С учетом перечисленных критериев были рассмотрены следующие средства UML–моделирования:

- Rational Rose 2000 Enterprise;
- Objecteering/UML;
- Magic Draw;
- Sprax Enterprise Architect;
- Visual UML;
- Case Ace;
- CaseMap;
- Casemaker Totem.

В результате проведенного анализа указанных средств выбор был остановлен на Sprax Enterprise Architect (версия 6.5.0.805) как на наиболее удовлетворяющем всей совокупности критериев кандидате.

Конечной практической целью линейки стандартов ISO/IEC 2700x является построение и сопровождение системы управления информационной безопасностью в конкретных организациях. Наиболее всесторонне этот процесс представлен в стандарте ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements» (русскоязычное название: «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования») [4]. Он был принят в 2005 г. со статусом международного стандарта и описывает спецификацию СУИБ организации, включая обязательные требования к её созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и улучшению, необходимые для сертификации. Поэтому этот стандарт выбран в качестве базового при построении модели. В силу же неопределенности всех понятий методологии в одном стандарте и имеющих место выявленных недоработок стандарта, в ходе работы появилась необходимость использования как других стандартов линейки, так и опосредованных стандартов в областях управления риском, управления качеством и управления экологией:

(a) Проект международного стандарта ISO/IEC 2nd CD 27000:2007 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Основные положения и словарь» (англоязычный оригинал) [5];

(b) Международный стандарт ISO/IEC 17799:2005 «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью» (англоязычный оригинал) [6];
(c) Международный стандарт ISO 9000:2005 «Системы управления качеством – Основные положения и словарь» (англоязычный оригинал) [7];
(d) Международный стандарт ISO 14001:2005 «Системы управления экологией – Требования и руководство по использованию» (англоязычный оригинал) [8];
(e) Государственный стандарт РФ ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения» [9].

Возможность международной сертификация по стандарту ISO/IEC 27001:2005, принятого при построении модели в качестве основного, расширяет сферу применения результирующей модели.

В работе рассматривается англоязычная версия стандарта ISO/IEC 27001:2005, модель также является англоязычной. Причинами такого решения явились следующие обстоятельства.

- ГОСТ Р ИСО/МЭК 27001 — Государственный стандарт РФ, аналогичный международному стандарту ISO/IEC 27001:2005, – на начальный момент только разрабатывался, он должен быть принят в 2008 году. В открытых источниках проект готовящегося Государственного стандарта найти не удалось.
- Доступные русскоязычные версии стандарта характеризуются недостаточно хорошим качеством перевода и вызывают нарекания у ведущих специалистов в данной области.

В будущем предполагается согласовать терминологии международного стандарта ISO/IEC 27001:2005 и готовящегося к принятию ГОСТ Р ИСО/МЭК 27001, что позволит построить аналогичную русскоязычную модель.

Заключение

В рамках работы, описанной в данной статье, были решены следующие задачи:
(1) рассмотрено семейство международных стандартов по управлению информационной безопасностью ISO/IEC 2700x;
(2) обоснована актуальность формализованного представления методологии, содержащейся в указанной линейке стандартов;
(3) проанализированы существующие работы в данной области;
(4) поставлена задача объектного моделирования общего контекста безопасности организации по семейству стандартов ISO/IEC 2700x;
(5) выполнен обзор методик и инструментальных средств моделирования, осуществлен их выбор;
(6) выбран стандарт, рассматриваемый при моделировании в качестве базового.

Литература

1. Любимов А.В. Структурное моделирование угрозы ИТ в контексте методологии Общих Критериев // Труды X-й международной конференции «Теория и технология программирования и защиты информации», Санкт–Петербург, 18 мая 2006 г. – сс. 36–39.
2. Любимов А.В., Зайцев О.Е., Суханов А.В. Подходы к структурному моделированию основных компонентов безопасности ИТ «Общих критериев» // Труды XI-й международной конференции «Теория и технология программирования и защиты информации», Санкт-Петербург, 18 мая 2007 г. – сс. 57–60.

3. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Госстандарт России, Москва, 2002.
4. ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems — Requirements».
5. ISO/IEC 2nd Committee Draft 27000:2007 «Information technology – Security techniques – Information security management systems – Overview and vocabulary».
6. ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management».
7. ISO 9000:2005 «Quality management systems – Fundamentals and vocabulary».
8. ISO 14001:2004 «Environmental management systems – Requirements with guidance for use».
9. ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения».

ПРОЕКТИРОВАНИЕ МЕТОДИКИ ОБУЧЕНИЯ ОСНОВАМ ВИРУСНОГО АНАЛИЗА

В.Д. Стремоухов, А.В. Клейменов, А.А. Калашникова
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В статье рассмотрены основные принципы формирования учебного курса по анализу объектов исполняемого кода на предмет вредоносного функционала на примере методики, разработанной на кафедре БИТ.

Введение

Несмотря на то, что вирусные аналитики, как правило, составляют большую часть штата любой антивирусной компании, часто актуальной является задача обучения основам анализа подозрительных объектов сотрудников АВ-компаний, не связанных напрямую с техническими аспектами исследования вредоносного кода (ведущих аналитиков, маркетологов и т.п.). На нашей кафедре существует антивирусная лаборатория, занимающаяся, в частности, подготовкой описаний вредоносного кода для АВ-компаний, для которой задача начального обучения вирусного аналитика стоит так же остро. В связи с этим по инициативе компании «Лаборатория Касперского» на нашей кафедре был разработан курс «Анализ подозрительных объектов на предмет вредоносного функционала».

Постановка задачи

Задача – создать курс (т.е. методическое пособие + необходимое ПО) для самостоятельного изучения методов вирусного анализа. Целевая аудитория – продвинутые пользователи ПК, имеющие представление о устройстве ОС и ее исполняемых файлов, однако не знакомые с теоретическими основами низкоуровнего программирования и методами реверсивной инженерии.

Основной целью курса является обучение методам определения вредоносности подозрительного объекта. Предполагается, что читатель в достаточной мере обладает навыками работы с ПК и базовыми знаниями об устройстве ОС Windows и исполняемых файлов под эту ОС. В курсе предполагается описать приемы работы с рядом специализированных утилит, в частности с дизассемблером. Однако от читателя не требуется каких-либо специализированных знаний, в том числе знаний языка ассемблера – все необходимые сведения читатель получит в процессе изучения методического пособия.

Следует отметить, что авторы курса не ставили перед собой цели научить читателя подробному анализу объекта с выяснением в точности всего функционала – это задача для технически подготовленного вирусного аналитика (обладающего фундаментальными навыками программирования, дизассемблирования и отладки, знаниями языка ассемблера). Будут показаны лишь способы выяснения функционала в первом приближении. Следует также отметить, что эти методы не дают полной уверенности в обнаружении искомого функционала при его наличии в силу ряда причин, которые будут указаны позднее.

Рассматриваемые типы ВК

В настоящее время ОС семейства Windows являются наиболее распространенными, а потому основной поток вредоносного кода рассчитан именно на работу в этой среде. Это вполне логично, так как основная цель создателей вредоносного кода – извлечение прибыли различными способами, такими как кража, модификация или унич-

тожение ценной информации, вывод из строя информационных ресурсов «вражеской» компании. Кроме того, косвенным следствием распространенности ОС Windows является то, что зачастую с ней работают малоподготовленные в техническом плане люди, неспособные вовремя обнаружить факт заражения компьютера вредоносным кодом, что еще более облегчает работу вирусописателю.

Исходя из сказанного, авторами пособия было принято решение ограничиться рассмотрением исполняемых файлов win32 (32-разрядных ОС семейства Windows), так как в ином случае пришлось бы рассматривать вопросы устройства альтернативных ОС, их исполняемых файлов и т.п. Кроме того, в пособии кратко будет рассмотрены файлы командного интерпретатора (.bat).

Структура методического пособия

Наиболее логичным является, на наш взгляд, построение методического пособия на основе обобщенного алгоритма анализа win32-сэмпла, который выглядит примерно следующим образом:

1. проверка валидности PE,
2. распаковка (если требуется),
3. динамический анализ,
4. статический анализ,
5. исследование в отладчике.

Сразу хотелось бы отметить, что данный алгоритм является неким обобщенным шаблоном, и в зависимости от ситуации те или иные шаги могут не выполняться (как правило, для выяснения функционала несложного сэмпла достаточно одного-двух методов). Именно поэтому, если какие-то последующие главы пособия будут читателю непонятны (курс рассчитан на читателей с разным уровнем технической подготовки), предполагается возможность их пропустить и вернуться к ним, когда за плечами уже будет какой-то опыт анализа исполняемых файлов. Также следует отметить, что метод исследования сэмпла в отладчике в основной части данного пособия рассматриваться не будет, вследствие его сложности и необходимости определенной технической базы (в частности, хорошего знания языка ассемблера), однако ему будет посвящено одно из приложений. Остальным же методам будут посвящены главы основной части методического пособия, после чего, в приложении будут даны несколько примеров полного разбора типовых сэмплов.

Первичный анализ сэмпла

В данной главе будут рассмотрены методы получения начальных сведений об изучаемом объекте и подготовка его к последующим стадиям анализа.

На начальном этапе анализа сэмпла необходимо выяснить несколько важных сведений о нем, а именно:

- является ли он вообще PE-файлом (PE, portable executable – стандарт исполняемых файлов, являющийся на текущий момент основным для win32-систем. Характеризуется наличием PE-заголовка, в котором, в частности, содержатся различные данные о структуре исполняемого файла);
- язык написания и компилятор, использовавшийся при сборке исполняемого файла (если это возможно установить);
- упаковщик/протектор, которым был упакован исполняемый файл, если упаковка производилась.

С большинством этих задач в автоматическом/полуавтоматическом режиме успешно справляются ряд специализированных утилит, работа с которыми рассматривается в данной главе.

Распаковка упакованного файла

Для начала – несколько слов об упаковщиках и протекторах. Принцип работы данных утилит довольно прост: код упаковываемого исполняемого файла обрабатывается определенным алгоритмом («упаковывается»), далее создается новый исполняемый файл, в котором содержится обработанный код исходного файла и код функции-распаковщика. Сначала управление передается на функцию-распаковщик, задача которой – привести код исходного файла к изначальному состоянию, после чего управление передается на так называемую оригинальную точку входа (первую инструкцию оригинального исполняемого файла). Различие между упаковщиками и протекторами – лишь в целях, преследуемых теми и другими: если упаковщики созданы для уменьшения размеров исполняемых файлов, то протекторы созданы для усложнения исследования кода исполняемого файла посредством дизассемблирования.

При исследовании запакованного исполняемого файла его часто распаковывают. Под распаковкой понимают получение оригинального файла (т.е. в таком же виде, в каком он был до упаковки) из запакованного.

Процесс так называемой «ручной распаковки», т.е. распаковки без использования специализированных утилит, довольно сложен и потому рассматриваться здесь не будет. В ознакомительных целях укажем лишь, что он включает 3 основные стадии:

1) поиск так называемых OEP (Original Entry Point – оригинальная точка входа) – наиболее сложная стадия, часто требующая умения логически мыслить и импровизировать. Остальные стадии, как правило, – чисто технические;
2) снятие дампа (образа процесса из оперативной памяти);
3) восстановление таблицы импорта.

Вместе с тем для большинства известных упаковщиков/протекторов имеются утилиты для автоматической распаковки – распаковщики и депротекторы. Здесь следует отметить, что, прежде чем приступить к распаковке, следует сначала определиться, а нужна ли она вообще? К примеру, если вы собираетесь исследовать сэмпл в дизассемблере и/или отладчике, то, конечно, распаковка необходима, в ином случае к сэмплу как правило, относятся как к некоему «черному ящику», а, значит, и его распаковка малоцелесообразна.

Статический анализ

В данной главе рассматриваются основные принципы статического анализа, а также дается ряд теоретических сведений, необходимых при СА.

Понятие статического анализа. Условия, при которых он имеет смысл. В данном пособии под понятием «статический анализ» подразумевается исследование сэмпла в дизассемблере (вообще, понятие статического анализа более широко, так как для некоторых типов исполняемых файлов дизассемблер бессилен, в этом случае на помощь приходят другие утилиты, например, декомпиляторы, однако данная тема выходит за рамки этого методического пособия).

Рассмотрим условия, при которых имеет смысл статический анализ. В общем случае можно выделить 2 наиболее важных условия.

1. Native-code. Целый ряд современных языков программирования (ex.: Visual-Basic, отчасти .Net-семейство, или Java, практически полностью реализовавшая концепцию, заложенную в Oberon от не унимающегося Н. Вирта) реализуют так называемый «виртуальный процессор». Суть концепции в следующем: формируется виртуальный язык программирования низкого уровня со своим набором инструкций и/или API, отличным от ассемблера («виртуальный ассемблер»), под который будут компилироваться программы на одном из языков высокого уровня. Далее, под каждую из необходимых платформ (т.е., по сути, ОС) пишется виртуальная машина (ex.: .NET framework, Java-machine) , транслирующая «на лету» – в процессе выполнения программы – «вир-

туальные» инструкции в реальные. Языки программирования, отличные от вышеописанных (т.е. напрямую компилируемые в машинный код), называют также native-языками. Очевидно, что исследование в обыкновенном дизассемблере чего-либо, кроме native-кода, бесполезно.

2. Необходимость такого анализа. Как правило, динамический анализ довольно трудоемок и требует больших затрат по времени, а потому его целесообразно проводить, если другие методы результата не дали, либо критично выявление именно всего функционала.

Необходимые знания о языке ассемблера и устройстве PE-файла. Не вдаваясь в технические и исторические подробности, сразу следует отметить, что основным форматом исполняемых файлов в ОС семейства win32 является формат PE (portable executable). Общее устройство PE-файла показано в табл. 1.

<table>
<tr><td colspan="2">DOS ”MZ”-заголовок
(IMAGE_DOS_HEADER)</td></tr>
<tr><td>Файловый заголовок
(IMAGE_FILE_HEADER)

Опциональный заголовок
(IMAGE_OPTIONAL_HEADER)</td><td>PE-заголовок
(IMAGE_NT_
HEADERS)</td></tr>
<tr><td colspan="2">Таблица секций
(IMAGE_SECTION_HEADER)</td></tr>
<tr><td>.text</td><td rowspan="5">Секции</td></tr>
<tr><td>.data</td></tr>
<tr><td>.bss</td></tr>
<tr><td>.edata</td></tr>
<tr><td>.idata</td></tr>
</table>

Таблица 1. Структура PE-файла

Основная информация о структуре файла содержится в PE-заголовке и таблице секций. Секции – это «тело» программы. Каждая секция имеет свое назначение. Как правило (хотя и не обязательно), в секции “.text” находится код программы, в секции “.data” – инициализированные данные и т.д. В момент запуска исполняемого файла его содержимое подгружается в оперативную память и управление передается на точку входа, указанную в PE-заголовке.

Взаимодействие программы с ее «внешней средой» (операционной системой) происходит через вызов API-функций. API – основной интерфейс ОС к исполняемой программе; любое действие, которое позволено в системе исполняемой программе, реализуется через последовательный вызов определенных API-функций. Достаточно полные описания API-функций можно найти в Microsoft Developer Network (MSDN). Информация об API-функциях, к которым программа будет обращаться в процессе своей работы (импортируемых API-функциях), содержится в секции импорта (чаще всего .idata) PE-файла.

Авторы пособия не ставили перед собой цели предоставить полный обзор основ языка ассемблера или научить читателя на нем программировать. Мы хотим показать, что можно выяснить о функционале исполняемого файла, исходя из поверхностного изучения дизассемблерного листинга. Общий вид ассемблерной инструкции:

```
команда [операнд[,операнд2...]] [; комментарии]
```

Инструкции разделяются переносом на следующую строку (на каждой строке – только одна инструкция). Естественно, комментарии при ассемблировании исходного кода отбрасываются, однако большинство дизассемблеров пишут в комментариях различные пояснения, облегчающие анализ листинга.

Следует отметить, что существует ряд проблем, препятствующих корректному дизассемблированию исполняемого файла, вследствие чего, в частности, повторно ассемблированный дизассемблерный листинг уже не будет работать, как исходный исполняемый файл (если вообще ассемблируется удачно). Кроме того, при использовании определенных приемов программирования можно добиться того, что большая часть дизассемблерного листинга вообще будет представлять из себя «мусор» (неверно отдизассемблированный код). В этом случае некоторые (так называемые «интерактивные») дизассемблеры предлагают аналитику возможность «подсказать» правильный ход дизассемблирования, однако это требует от аналитика несколько больших познаний в ассемблере, чем предполагает данное методическое пособие. Поэтому, если вы предполагаете, что дизассемблерный листинг исследуемого сэмпла представляет собой «мусор» (основные признаки – малоосмысленный код, отсутствие вызовов API-функций в листинге сэмпла, который по другим признакам активно взаимодействует с ОС), от статического анализа лучше отказаться.

Динамический анализ

Динамический анализ – это метод исследования сэмпла, при котором последний запускается «под присмотром» различного рода следящих программ. Такие программы могут осуществлять слежение за исследуемым процессом в режиме «реального времени» либо анализировать 2 состояния системы – до и после запуска сэмпла.

У динамического анализа есть ряд преимуществ: быстрота анализа, невысокие требования к теоретической подготовке аналитика. Основным недостатком динамического анализа является риск невыяснения части функционала сэмпла, если поведение последнего зависит от параметров «внешней среды» (к примеру, версии ОС, системного времени и т.п.) либо в сэмпле реализованы приемы, противостоящие динамическому анализу.

Заключение

В рамках проекта разработан курс, включающий в себя методическое пособие и специальное ПО, упрощающее процесс вирусного анализа, в частности, экспертную систему соответствия подозрительных последовательностей вызовов API-функций определенным типам вредоносного функционала. В курсе представлены основные методы анализа сэмпла на предмет вредоносного функционала. Хотелось бы отметить несколько общих моментов.

Во-первых, если Вы хотите всерьез заниматься анализом исполняемых файлов, Вы в первую очередь должны понять, что в данном процессе не существует шаблонов. Все представленные алгоритмы – лишь примерные. Очень редко можно сказать «если Вы проделали то-то и получили то-то, то сэмпл относится к такому-то типу вредоносного кода». Одни и те же действия могут быть совершенно обыкновенным функционалом, а могут быть вредоносными. Не существует «вредоносных» API-функций – одна и та же функция может быть использована как в легальных, так и во вредоносных целях. При анализе необходимо подключать логику.

Во-вторых, авторы курса не ставили перед собой цели рассказать читателю всю теорию по каждому рассматриваемому вопросу, обучить работе с каждой упоминаемой утилитой, привести большое количество справок и спецификаций. Как известно, лучший способ получения данных знаний – практический опыт. Приступая к анализу, следует запастись справочниками и терпением. Если Вы видите, что сэмпл, к примеру, модифицирует

тот или иной системный файл или ключ реестра, имеет смысл посмотреть в Интернете назначение этого файла/ключа – это поможет Вам сделать заключение о цели, которую преследовал программист. При статическом анализе (особенно небольших сэмплов) необходимо читать в MSDN назначение ВСЕХ неизвестных API-функций – со временем Вы научитесь отделять «важные» вызовы от тех, которые можно пропустить. Если Вы собираетесь использовать статический анализ, имеет смысл постепенно изучать основы языка ассемблера.

Литература

1. Касперский Е. Вирусы и средства борьбы с ними – М., 2005.
2. Крис Касперски. Образ мышления – дизассемблер IDA – М.: СОЛОН-Р, 2001.
3. Крис Касперски. Техника сетевых атак. – М.: СОЛОН-Р, 2001.
4. Хакер. Спец-выпуск [anti]cracking. – 2005. – №57.

ПРИМЕНЕНИЕ АППАРАТА КУБИЧЕСКИХ ПОКРЫТИЙ ДЛЯ ГАРАНТИРОВАННОГО ОБНАРУЖЕНИЯ НДВ

И.А. Ларионов
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Рассматриваются графо-аналитические модели программ. Предлагается новый подход к верификации программ на основе алгебро-топологических свойств кубических покрытий, построенных по графо-аналитическим моделям.

Введение

В настоящее время для повышения эффективности делопроизводства в государственных учреждениях, качественной организации бизнес-процессов предприятий и обеспечения их конкурентоспособности на рынке требуется все более интенсивное внедрение и использование узкоспециализированного программного обеспечения. Соответственно, возрастают и требования к качеству программных изделий, что заставляет производителей уделять большое внимание как технологическому процессу разработки, так и вопросам тестирования и верификации своих продуктов. Поэтому эффективный анализ программ на предмет соответствия спецификации, отсутствия недекларированных возможностей (НДВ), является актуальной проблемой.

Предложенный в статье метод позволяет перейти от программного кода к математическим моделям высокого уровня и исследовать их с помощью аппарата кубических покрытий.

Метод

Проектирование программного продукта можно представить в виде некоторого технологического процесса, состоящего в переходе от технического задания к системе программ или, в частном случае, к одной программе (P), реализуемых в заданной вычислительной среде. Так как все команды конкретного процессора делятся на две категории – команды обработки данных (обработка десятичных знаков, сдвиги, пересылки, арифметические команды) и команды, регулирующие последовательность управления (вызовы процедур, команды возврата, условные и безусловные переходы), – то программа P, в свою очередь, может быть представлена в виде булева графа $BG(P)$, который содержит линейные и условные вершины. Линейная вершина содержит одну точку входа и одну точку выхода, в ней происходит вычисление некоторой переменной на безальтернативной основе, которое впоследствии реализуется в виде последовательности операторов (машинных операций в исполнительных командах). Условная вершина имеет одну точку входа и две точки выхода, задающие адреса ветвления в зависимости от выполнения или невыполнения условия, задаваемого в вершине. Каждый возможный путь l выполнения программы P соответствует некоторому пути на графе $BG(P)$, соединяющему начальную и конечную вершины [1].

Пример. В качестве примера рассмотрим булев граф программы, реализующей некоторую простую интервальную формулу.

Пусть задана интервальная формула

$$r = \begin{cases} LFR1, \text{ при } x \le k_1 \text{ или } x \ge k_2; \\ LFR2, \text{ при } k_1 < x < k_2. \end{cases}$$

Переменная r вычисляется по линейным формулам $LFR1$ и $LFR2$ в зависимости от значений переменной x, диапазон значений которой разбит на три интервала константами k_1 и k_2.

Видно, что условия вычисления *r* по формуле *LFR1* или *LFR2* заданы в избыточной форме, и с учетом перестановок существует восемь вариантов их последовательного вычисления. Поэтому существует и несколько различных программных реализаций. Закодируем условия: $x \le k_1$ как a, $x > k_1$ как $\overline{a}$, $x \ge k_2$ как b, $x < k_2$ как $\overline{b}$. На рисунке приведен булев граф одной из реализаций.

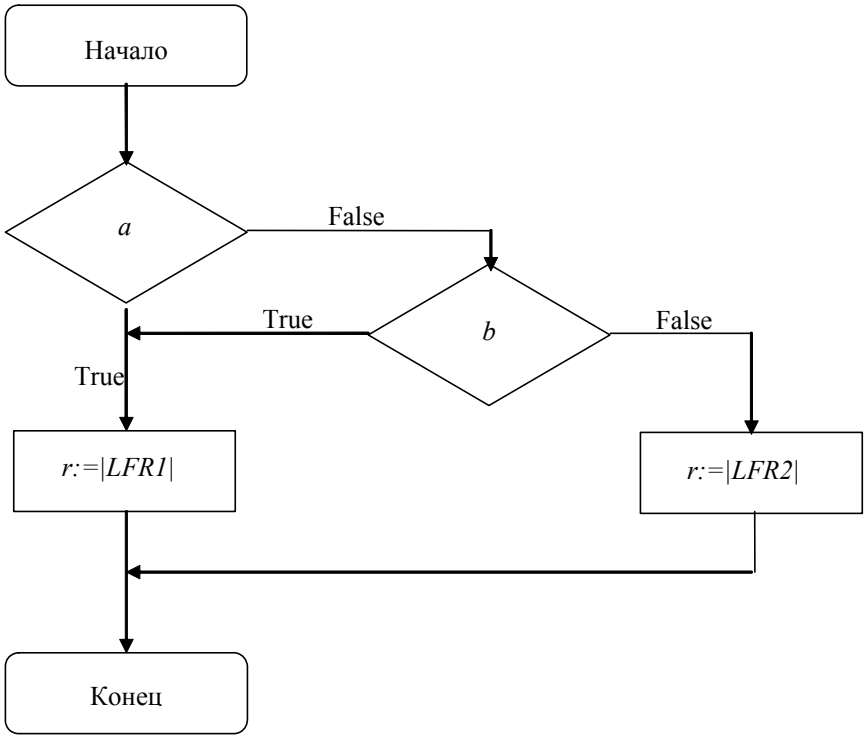


Рисунок. Булев граф одной из реализаций интервальной формулы

Итак, для программы *P* в машинных кодах, закодировав условия-предикаты булевыми переменными, можно построить её булев граф *BG(P)*. Каждый путь *l* на графе *BG(P)* можно задать логическими переменными, которые описывают условия его прохождения и принимают значения 1 или 0 в зависимости от истинности или ложности выражений в условных вершинах. Таким образом, можно построить кубическое покрытие $C(P)=\{c_1, c_2,...,c_m\}$, где каждый куб c_j представляет собой набор условий, определяющих путь l_j на графе *BG(P)*. Координаты куба c_j могут принимать значения 0, 1 или x, где 0 соответствует значению *False* (невыполнению условия), 1 – значению *True* (выполнению условия), а x – неопределенному значению, т.е. неопределенному условию, которое может быть произвольно доопределено как в 0, так и в 1.

Покрытия *C(P)* и кубы c_j соответствуют определению покрытий в исчислении кубических комплексов, поэтому к ним применимы алгебро-топологические операции пересечения (∩), вычитания (#) и звездчатого произведения (*) [2].

Операция # вычитания двух кубов $a = (a_1, a_2, ..., a_n)$ и $b = (b_1, b_2, ..., b_n)$ осуществляется по следующим правилам:

$$a \# b = \begin{cases} \varnothing, \text{ если } a_i \# b_i = z \text{ для всех } i; \\ a, \text{ если } a_i \# b_i = y \text{ для хотя бы одного } i; \\ \left\{ \bigcup_i (a_1, a_2, ..., a_{i-1}, p, a_{i+1}, ..., a_n) \right\} \text{ для всех } i \text{ таких, что } a_i \# b_i = p,\ p \in \{0,1\}. \end{cases}$$

Здесь z и y – вспомогательные величины, определяемые из таблицы значений операции # на элементах кубов.

a_i \ b_i	0	1	x
0	z	y	z
1	y	z	z
x	1	0	z

Таблица. Значения операции # на элементах кубов

Например, для рассмотренной нами ранее реализации P интервальной формулы (см. пример 1) кубическое покрытие $C(P)$ имеет следующий вид:

$$C(P) = \begin{pmatrix} a & b & r \\ 1 & x & LFR1 \\ 0 & 1 & LFR1 \\ 0 & 0 & LFR2 \end{pmatrix}.$$

С помощью операции # можно определить эквивалентность покрытий $C(P1)$ и $C(P2)$, а, следовательно, и программ $P1$ и $P2$ между собой. Более подробно, если для программ $P1$ и $P2$, имеющих одну и ту же спецификацию, верны равенства

$C(P1) \# C(P2) = \emptyset$ и $C(P2) \# C(P1) = \emptyset$,

то покрытия признаются эквивалентными, а программы – реализующими одно и то же, т.е. верифицированными относительно друг друга. Если же хотя бы одно из этих равенств неверно, то у программ есть участки, где они функционируют по-разному [3].

Заключение

Предложенное использование графо-аналитических моделей программ и кубических покрытий, построенных на их основе и объединяющих в себе булевы функции, переменные и алгебраические выражения, позволяет перейти от анализа программ к анализу математических моделей. Это дает возможность построения автоматизированных систем для решения задач верификации, тестирования, поиска не декларированных возможностей и обеспечения антивирусной безопасности.

Литература

1. Зыков А.Г., Немолочнов О.Ф., Поляков В.И., Сидоров А.В. Структурирование программ и вычислительных процессов на множество линейных и условных вершин // Научно-технический вестник СПбГИТМО (ТУ). – 2005. – Выпуск 19. Программирование, управление и информационные технологии / Гл. ред. В.Н. Васильев. – С. 207–212.
2. Немолочнов О.Ф., Зыков А.Г., Поляков В.И. Кубические покрытия логических условий вычислительных процессов и программ // Научно-технический вестник СПбГИТМО (ТУ). – 2004. – Выпуск 14. Информационные технологии, вычислительные и управляющие системы / Гл. ред. В.Н. Васильев. – С. 225–233.
3. Лаздин А.В., Немолочнов О.Ф. Метод построения графа функциональной программы для решения задач верификации и тестирования // Научно-технический вестник СПбГИТМО (ТУ). – 2002. – Выпуск 6. Информационные, вычислительные и управляющие системы / Гл. ред. В.Н. Васильев. – С. 109–111.

ФУНКЦИОНАЛЬНОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ПО СЕМЕЙСТВУ СТАНДАРТОВ ISO/IEC 2700X

С. В. Шустиков, Н. В. Андреева
Научный руководитель – к.т.н., доцент А. В. Любимов

В рамках настоящего исследования проведен системный анализ системы управления информационной безопасности, описанной семейством международных стандартов ISO/IEC 2700x. Для проведения анализа текста стандарта и построения функциональной модели системы использована методология SADT. Полученная модель находит применение при разработке и внедрении систем управления информационной безопасностью.

Введение

В настоящее время функционирование практически всех процессов в организации в той или иной степени зависит от наличия у сотрудников оперативного доступа к полной и достоверной информации.

Можно выделить три основных свойства информации:

- доступность – свойство быть доступной и используемой со стороны авторизованной стороны [1];
- целостность – свойство сохранения точность и полноту активов [1];
- конфиденциальность – свойство информации не быть доступной или раскрытой неавторизованными лицами, сторонами или процессами [1].

Информационной безопасностью организации является обеспечение указанных свойств информации [2]. Следует учитывать, что это не разовое мероприятие, не продукт однократной деятельности. Безопасность – это процесс [3]. Для достижения оптимального уровня защищенности информационных ресурсов организация управляет этим непрерывным процессом обеспечения доступности, целостности и конфиденциальности информации через документированную систему управляющих процессов и процедур, именуемую системой управления информационной безопасностью (СУИБ).

Принципы построения СУИБ, ее описание и требования к ней изложены в международном стандарте ISO/IEC 27001:2005 [4].

СУИБ базируется на двух основных принципах:

- циклический процессный подход, базирующийся на цикле Деминга;
- подход к защите информации на основе управления рисками.

Цикл Деминга, также известный как PDCA-цикл, представляет собой модель непрерывного улучшения качества [5], которая широко распространена в мире и описана в международном стандарте системы менеджмента качества (СМК) ISO 9001:2000 [6].

Подход к защите информации, основанный на управлении рисками обеспечивает адекватность и полноту защиты информации, так как он позволяет сконцентрировать внимание на наиболее актуальных угрозах и соизмерять стоимость внедряемых средств защиты со стоимостью защищаемой информации.

Внедрение СУИБ в организации заключается в разработке процессов, процедур и инструкций, структурированных и описанных в руководящих документах, в соответствии с требованиями международного стандарта ISO/IEC 27001:2005.

Практический опыт показывает, что для успешного внедрения СУИБ в организации весьма целесообразно использовать формальную модель основных процессов СУИБ. Для разработки и внедрения процессов в организациях в настоящее время широко применяется методология структурного анализа и проектирования SADT (Structured Analysis and Design Technique) [7]. Данная методология подразумевает построение функциональной модели процесса в виде диаграмм в нотации IDEF0, IDEF3

или DFD. В результате сравнительного анализа нотаций выбор был сделан в пользу нотации DFD.

Идея применения методов структурного моделирования для анализа стандартов была выдвинута и реализована в [8] для ISO 9001. В [9] она впервые была применена к стандарту ИБ, конкретно – к Общим Критериям. Наиболее полно она изложена в [10].

Постановка задачи

Целью настоящего исследования является построение функциональной SADT-модели СУИБ по семейству стандартов ISO/IEC 2700x.

Цель модели – наиболее точно описать процессы СУИБ в соответствии с требованиями международного стандарта ISO/IEC 27001:2005 в рамках выбранной методологии моделирования. Точка зрения на объект моделирования – СУИБ – руководителя подразделения, ответственного за обеспечение информационной безопасности организации (CISO).

Для построения функциональной модели используется программное средство построения SADT-диаграмм бизнес-процессов Computer Associates BPwin 4.0. Данное средство положительно зарекомендовало себя как инструмент для построения функциональных моделей бизнес-процессов и широко применяется организациями с этой целью [11]. Это дает дополнительные преимущества, так как само средство распространено в среде бизнес-аналитиков и его формат файла данных (.bp1) не требует дополнительной адаптации.

Методы исследования

Система управления информационной безопасностью (СУИБ) определена в международном стандарте ISO/IEC 27001:2005 как часть всеобщей системы управления, основанной на подходе анализа бизнес-рисков, необходимой для создания, внедрения, функционирования, мониторинга, пересмотра, поддержания и усовершенствования информационной безопасности. Система управления включает организационную структуру, политики, планируемые действия, обязанности и ответственность, практики, процедуры, процессы и ресурсы [2].

Здесь и далее под бизнес-процессами организации будет пониматься основная деятельность организации, независимо от ее вида. Под бизнес-рисками понимаются риски, связанные с осуществлением данной деятельности. СУИБ рассматривает риск информационной безопасности, т.е. сочетание вероятности события, влияющего на обеспечение доступности, целостности и конфиденциальности информационных активов организации, и последствий такого события.

СУИБ основана на цикле Деминга, также известном как цикл PDCA или спираль непрерывного улучшения. Цикл состоит из четырех стадий – Планруй (Plan), Делай (Do), Проверяй (Check), Улучшай (Act). Суть этих стадий заключается в следующем:

- Планируй (Plan) – планирование действий и изменений наперед, анализ и прогнозирование результатов;
- Делай (Do) – выполнение плана, принятие мер в контролируемых условиях;
- Проверяй (Check) – изучение результатов действий;
- Улучшай (Act) – принятие мер по улучшению процессов.

Планирование СУИБ – это понимание требований организации к информационной безопасности и необходимости разработки политики и целей информационной безопасности.

Внедрение и управление мерами по защите информации имеет своей целью управление рисками организации в области информационной безопасности в контексте общего управления бизнес-рисками.

Мониторинг и анализ производительности и эффективности СУИБ проводится для выявления несоответствий протекающих процессов и выполняющихся процедур заявленным в ходе разработки.

Непрерывное улучшение процессов СУИБ, основанное на объективных измерениях, необходимо для оперативного устранения несоответствий и обработки новых рисков.

Для успешного решения поставленной задачи функционального моделирования СУИБ методология моделирования должна включать следующие составляющие и обладать следующими возможностями:

- стандартизованный метод;
- в той или иной мере формализованный синтаксис (формальный язык), имеющий графическое представление;
- возможность построения и отображения иерархий с достаточно высокой степенью вложенности;
- доступный инструментарий.

Для функционального моделирования СУИБ в настоящем исследовании была выбрана популярная методология структурного анализа и проектирования SADT (Structured Analysis and Design Technique) [7], полностью удовлетворяющая поставленным требованиям и практически не имеющая конкуренции. Действительно, SADT – это методология, разработанная специально для того, чтобы облегчить описание и понимание искусственных систем, попадающих в разряд средней сложности.

С точки зрения SADT модель может быть сосредоточена либо на функциях системы, либо на ее объектах. SADT-модели, ориентированные на функции, принято называть функциональными моделями; функциональная модель представляет с требуемой степенью детализации систему функций, которые отражают свои взаимоотношения через объекты системы.

К модели SADT предъявляются следующие требования:

- модель имеет единственного субъекта;
- у модели может быть только одна точка зрения.

SADT-модель состоит из SADT-диаграмм. Диаграмма является основным рабочим элементом при создании модели. Диаграммы структурируются по принципу декомпозиции диаграммы вышележащего уровня диаграммами нижележащего уровня.

Каждая SADT-диаграмма содержит прямоугольные блоки и дуги. Блоки изображают процессы моделируемой системы. Дуги связывают блоки вместе и отображают взаимодействия и взаимосвязи между ними [7].

Диаграммы SADT-модели могут быть описаны в одной из нотаций: IDEF0, IDEF3, DFD. Что касается нотаций моделирования, допускаемых методикой SADT, то сравнительный анализ возможных кандидатов – IDEF0, IDEF3 и DFD – достаточно однозначно рекомендует последний.

Действительно, метод IDEF0 моделирования бизнес-процессов фокусируется на высокоуровневом представлении операций и на факторах, которые контролируют эти операции. Контролирующие факторы включают правила, согласно которым происходит выполнение заданий (такие как международные или государственные регулятивные нормы, или другие ограничения со стороны собственных бизнес-правил организации), а также механизмы, необходимые для выполнения заданий (включая рабочий персонал, оборудование и другие ресурсы). В рассматриваемой задаче все перечисленные контролирующие факторы очевидны, а операции, наоборот, должны представлять-

ся на весьма низком уровне – вплоть до элементов или даже шагов действий. Поэтому метод IDEF0 не является правильным выбором.

Такой же вывод (но по другим причинам) можно сделать и в отношении метода IDEF3, который фокусируется на бизнес-логике выполнения операций и на принятии решений, относящихся к выполнению определенной операции, а также на том, каким образом осуществляется синхронизация процессов. В рассматриваемой задаче эти вопросы не имеют существенного значения, в первую очередь благодаря отдельным последовательно используемым процессам цикла PDCA, которые функционируют в рамках СУИБ. В то же время метод IDEF3 практически лишен средств описания данных (документов, свидетельств, результатов действий), которые являются важнейшими компонентами процесса разработки и поддержки СУИБ.

Таким образом, наилучшим выбором в задаче функционального моделирования СУИБ является метод DFD. Он фокусируется именно на операциях обработки данных, необходимых для проведения операций или создаваемых какими-либо операциями, данных для субъектов или организаций, которые либо предоставляют, либо получают данные, и потоках данных между различными действиями, видами или подвидами действий или операциями, а также между операциями и вовлеченными хранилищами данных.

Построение функциональной модели начинается с контекстной диаграммы (A-0 в терминах SADT), после чего процессы моделируемой системы подвергаются декомпозиции до заданного уровня детализации.

Для построения функциональной модели требуется выделить структурные элементы системы – процессы и ресурсы, через которые осуществляется их взаимосвязь, пользуясь единственным источником информации о моделируемой системе – текстами международных стандартов семейства ISO/IEC 2700x, в первую очередь – текстом международного стандарта ISO/IEC 27001:2005.

Основная стратегия моделирования заключается в максимально возможном приближении модели к тексту стандарта.

Наиболее актуальным, с точки зрения информативности по элементам системы, является раздел 4.2 международного стандарта ISO/IEC 27001:2005, описывающий непосредственно процессы СУИБ.

Выделение процессов СУИБ происходит в соответствии со структурой текста стандарта:

- раздел 4.2.1 - Establish the ISMS – процесс планирования СУИБ;
- раздел 4.2.2 - Implement and operate the ISMS – процесс внедрения и управления СУИБ;
- раздел 4.2.3 - Monitor and review the ISMS – процесс мониторинга и анализа СУИБ;
- раздел 4.2.4 - Maintain and improve the ISMS – процесс сопровождения и улучшения СУИБ.

Помимо этого, были выделены еще два основных процесса, не входящих в цикл PDCA, с точки зрения стандарта ISO/IEC 27001:2005, но имеющих большое значение для СУИБ, позволяющее выделить их наравне с четырьмя основными процессами:

- процесс управления документацией СУИБ, описанный в разделе 4.3 стандарта ISO/IEC 27001:2005;
- процесс ответственности руководства организации, описанный в разделе 5 стандарта ISO/IEC 27001:2005.

С точки зрения цикла PDCA эти процессы являются вспомогательными и логично вписываются в структуру цикла. Процесс управления документацией СУИБ должен иметь связи со всеми остальными процессами СУИБ, и с этой точки зрения его логично поместить в центр «колеса Деминга», связав «спицами колеса» с каждым из четырех процессов цикла PDCA.

Процесс ответственности руководства организации демонстрирует двойственную сущность руководства организации. С точки зрения процесса руководство является функциональной частью СУИБ, выполняющей свои непосредственные обязанности в рамках СУИБ. В то же время, с точки зрения цикла PDCA руководство является внешней сущностью, предъявляющей свои требования к СУИБ и получающей на выходе СУИБ определенные результаты.

Ресурсы, благодаря которым осуществляется взаимосвязь процессов СУИБ, выделяются при помощи следующего алгоритма:

- в определении процесса или уточняющем тексте ищутся сказуемые, описывающие данные, используемые процессом – являющиеся его входами или выходами; эти данные являются ресурсами;
- в тексте стандарта ищутся все сведения, относящиеся к выделенной сущности; на основе анализа этих сведений строится поток данных между процессами.

Данные, полученные на выходе одного процесса, могут быть использованы на входе нескольких процессов, такая ситуация отображается на диаграмме ветвлением ресурса. Или иначе – данные, полученные на выходе нескольких процессов, могут быть составными элементами другой сущности-ресурса, используемой на входе других процессов; такая ситуация отображается на диаграмме слиянием ресурсов.

В рамках построения функциональной модели СУИБ были выделены внешние сущности, в контексте которых функционирует СУИБ. Вешние сущности являются источниками входных ресурсов для процессов СУИБ и потребителями выходных ресурсов процессов СУИБ.

В соответствии с методологией SADT и выбранной нотацией построена функциональная модель, которая представляет собой иерархию DFD диаграмм, описывающих потоки данных между процессами. Каждая диаграмма модели получена путем детализации процесса, принадлежащего диаграмме более высокого уровня. Этот исходный процесс декомпозировался на несколько подпроцессов в соответствии с описанием данного процесса в международном стандарте ISO/IEC 27001:2005. Во избежание ошибок при переводе терминов, в процессе разработки модели использовался язык оригинала международного стандарта – английский. На рисунке представлена одна из диаграмм модели – диаграмма A0.

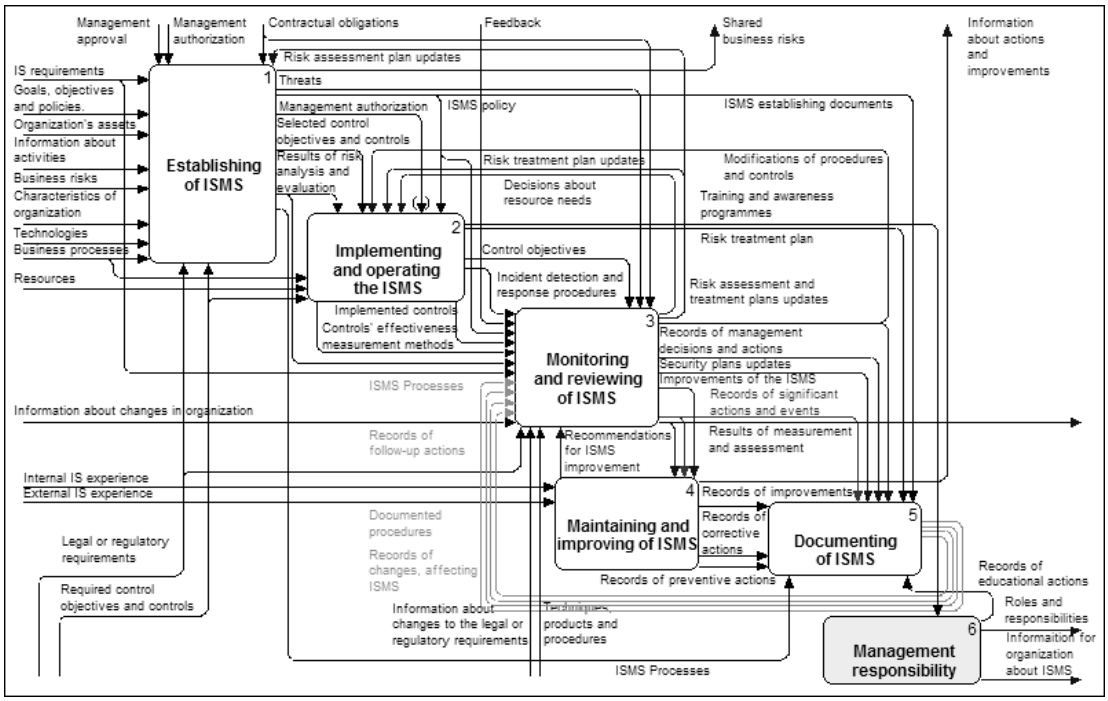


Рисунок. Диаграмма A0 функциональной модели СУИБ

Результаты

Графические диаграммы функциональной модели обладают рядом качеств, которые позволяют применять их в процессе построения СУИБ, а именно:

- методология SADT проста в понимании, и построенная с ее помощью модель дает наглядное представление всех процессов СУИБ и их взаимосвязи через ресурсы, что дает возможность использовать модель в процессе обучения специалистов;
- представление процессов СУИБ в виде диаграмм позволяет описать их с заданной степенью детализации, а также адаптировать их к условиям конкретной организации, что немаловажно в процессе создания СУИБ;
- при проведении анализа и построении модели существующей СУИБ можно использовать модель СУИБ, построенную по международному стандарту ISO/IEC 27001:2005, в качестве эталонной, что позволит легко выявить необходимые изменения для приведения существующей СУИБ в соответствие с данным международным стандартом; это позволяет применять модель для аудита СУИБ;
- модель СУИБ, построенную с использованием методологии SADT, можно достаточно быстро модернизировать при обновлении международного стандарта;
- функциональную модель СУИБ, построенную по международному стандарту ISO/IEC 27001:2005, можно использовать совместно с функциональными моделями процессов, регламентированных иными руководящими документами и стандартами в области информационной безопасности, если таковые распространяются на организацию, для создания гибридной СУИБ, соответствующей нескольким стандартам, в результате чего устраняются нормативные риски.

Заключение

Рассмотрен объект моделирования – система управления информационной безопасностью организации по семейству стандартов ISO/IEC 2700x и методология построения функциональной модели – SADT. Доказана актуальность и новизна задачи функционального моделирования системы управления информационной безопасностью. Для построения диаграмм SADT-модели выбрана нотация DFD. Рассмотрен процесс выделения структурных элементов системы – процессов, ресурсов и внешних сущностей – из источника информации о ней – текста международного стандарта ISO/IEC 27001:2005

Задача функционального моделирования системы управления информационной безопасности организации по семейству международных стандартов ISO/IEC 2700x решена, цель исследования достигнута в полном объеме.

Литература

1. ISO/IEC 13335-1:2004 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
2. ISO/IEC 27002:2005 «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью».
3. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб: Питер, 2003. – 368 с.: ил.
4. ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования».

5. Deming Cycle // 12manage. Management communities. Сообщество по электронному обучению в области менеджмента. – Режим доступа: http://www.12manage.com/methods_demingcycle.html
6. ISO 9001:2000 «Системы менеджмента качества. Требования».
7. Марка Д.А., МакГоуэн К. Методология структурного анализа и проектирования SADT. – Электронная библиотека, 1999. – Режим доступа: http://www.interface.ru/fset.asp?Url=/case/sadt0.htm.
8. Любимов А.В. Модели процессов СМК по стандарту ISO 9001:2000. Препринт кафедры Распределенных вычислений и компьютерных сетей. – СПб: СПбГТУ, 2004.
9. Любимов А.В., Зайцев О.Е., Суханов А.В. Подходы к структурному моделированию основных компонентов безопасности ИТ «Общих критериев» // Труды 11-й международной конференции «Теория и технология программирования и защиты информации.» Санкт - Петербург, 18 мая 2007 г. – С. 57–60.
10. Любимов А.В. Структурное моделирование стандартов информационной безопасности // Материалы V Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2007)», Санкт - Петербург, 23-25 октября 2007 г. – С. 57–58.
11. Маклаков С.В. Моделирование бизнес-процессов с AllFusion Process Modeler (BPwin 4.1). – М.: ДИАЛОГ-МИФИ, 2004 – 240 с.

МЕТОД СТАТИЧЕСКОГО АНАЛИЗА ПО ТОКЕНАМ УПРОЩЕННОГО ЯЗЫКА

А.И. Галанов, Д.Б. Арефьев, В.Л.Верещагин
Научный руководитель – д.т.н., профессор А.А. Молдовян

Исследуется метод статического анализа исходных текстов, выполняемого по результатам разбора текстов при помощи упрощенной грамматики языка.

Введение

Материал данной статьи описывает один из базовых этапов поиска уязвимостей в программах. Существуют различные подходы к контролю уязвимостей и программных закладок. Одни специалисты считают, что наиболее эффективна ручная обработка текстов, другие же создают специальные анализаторы, которые могут работать по совершенно различным принципам. Например, анализаторы могут получать необходимые сведения из отладочной информации или осуществлять поиск конструкций языка непосредственно в тексте программы. Одному из вариантов анализа самого текста программы посвящена эта статья.

Статический анализ предназначен для исследования исходного текста программы на соответствие стандартам программирования, на наличие дефектов и уязвимостей, в частности, программных закладок. Требования к статическому анализу формируются в соответствии с задачей (альфа-тестирование, сертификация и т.п.). В данной статье не будем выходить за границы требований, сформированных в руководящем документе (РД[1]). Среди основных требований можно выделить следующие:

1) определение функциональных объектов (функций, процедур) и связей между ними;
2) определение линейных участков и связей между ними.

Подход к выполнению данных требований должен предоставить достаточно точные сведения, что выполнить без синтаксического разбора текста весьма сложно. Такой разбор требует составления грамматики языка и выполнения предварительного лексического анализа. В целях сокращения трудоемкости в исследовании был применен метод упрощенной грамматики языка, т.е. в грамматику вошли только те правила, которые были использованы в исходных текстах. Является ли такой подход корректным, предстоит исследовать в этой работе: если сформированной упрощенной грамматики достаточно для разбора, то и результаты, полученные в результате статического анализа, должны совпадать с полученными ранее другим методом (ручной анализ либо анализ на основе отладочной информации компилятора). Другой задачей исследований является проверка эффективности самого метода статического анализа.

Идея упрощенной грамматики языка используется в таких сканерах безопасности, как «ITS4» [2]. Сканер является инструментом, разработанным американскими исследователями, и успешно выполняет поиск таких ошибок, как переполнения буфера, утечка памяти, ошибки в работе механизма указателей, ошибки инициализации создаваемых объектов и др. Но результаты анализа не соответствуют требованиям РД. Кроме «ITS4», существуют специализированные анализаторы (удовлетворяющие этим требованиям), которые являются разработками испытательных лабораторий, таких как «ЦБИ», «НФ ФГУП НИИ «Вектор» СЦПС «Спектр», «М-Стандарт» и др. Среди инструментов с известными (из публикаций) алгоритмами можно найти использование полной грамматики языка, что, безусловно, имеет более высокий прикладной уровень, но оказывается более трудоемким в процессе составлении и отладки грамматики.

[1] см. документ [1]

В исследовании был использован язык ANSI C (99) по причинам широкого применения языка в российской промышленности и относительной простоты синтаксиса.

Постановка задачи

Метод статического анализа исходных текстов представляет собой совокупность приемов и операций теоретического и практического характера, направленных на достижение безопасности и корректности выполнения конечного программного обеспечения. Характерной особенностью статического анализа в сфере информационной безопасности является определение наличия уязвимостей, в том числе и программных закладок, в исходных тестах без запуска исследуемой программы. В российских нормативных документах подобный статический анализ описан в документе [1] и имеет четкие требования к результатам его выполнения. При постановке задачи исследования будем исходить из требований руководящего документа. Но при этом будем иметь в виду возможность расширения требований, связанную с недостаточностью базовых требований при контроле уязвимостей.

Приемы анализа, используемые в рассматриваемом методе, требуют обязательной автоматизации, иначе время, затраченное на анализ, может оказаться сравнимым со временем, потраченным на разработку предмета исследования. В связи с этим такие приемы необходимо применять не столько к исходному тексту программ, сколько к их некоторому промежуточному виду, понятному для программы-анализатора. Промежуточный вид – это массив токенов и последовательностей вывода. Массив токенов формируется на стадии лексического анализа, а последовательность вывода – во время синтаксического анализа исходных текстов. Как уже было сказано во введении, в разных анализаторах используются разные подходы, упрощающие разбор исходных текстов. В данной статье рассматривается возможность использования упрощенной грамматики языка при синтаксическом разборе исходных текстов. Такая грамматика включает только те порождающие правила, которые используются для вывода цепочек, существующих в исследуемых исходных текстах. Совокупность цепочек, выведенных при помощи всех правил упрощенной грамматики, является языком, который представляет собой подмножество исходного языка – того языка, на котором написана исследуемая программа. Фактически мощность языка, таким образом, упрощается, и возможно его тоже определить как упрощенный язык.

В теории компиляции токен представляется как логическая единица, формируемая по результатам лексического анализа и содержащая в себе информацию о типе лексемы и ссылку на лексему [3]. Для компиляции исходного текста данной информации вполне достаточно, а для статического анализа необходимо иметь дополнительную информацию, такую как смещение лексемы в файле относительно начала, длина, и пр. В результате токен приобретает некоторое расширенное определение как логическая единица, содержащая сведения о конкретной лексеме.

В результате на вход статического анализатора попадает массив таких токенов и последовательность правил вывода упрощенного языка. Необходимо определить возможность использования такого подхода, в частности, достаточность входных данных для реализации приемов, которые должны предоставить на выходе информацию в соответствии с требованиями руководящего документа.

Методы исследований

Как уже было сказано выше, приемы анализа требуют автоматизации. В рамках исследования необходимо создать инструмент, который будет получать на входе некоторое представление исходных текстов, а на выходе выдавать информацию, являю-

щуюся результатом статического анализа. После сопоставления полученных результатов с действительным положением дел, можно будет сделать вывод о применимости представленного метода при статическом анализе.

Перед тем, как рассмотреть концептуальную схему работы статического анализатора, целесообразно определить его местоположение в составе специального комплекса контроля уязвимостей и программных закладок. На рис. 1 представлена схема, отображающая основные взаимосвязи модулей комплекса.

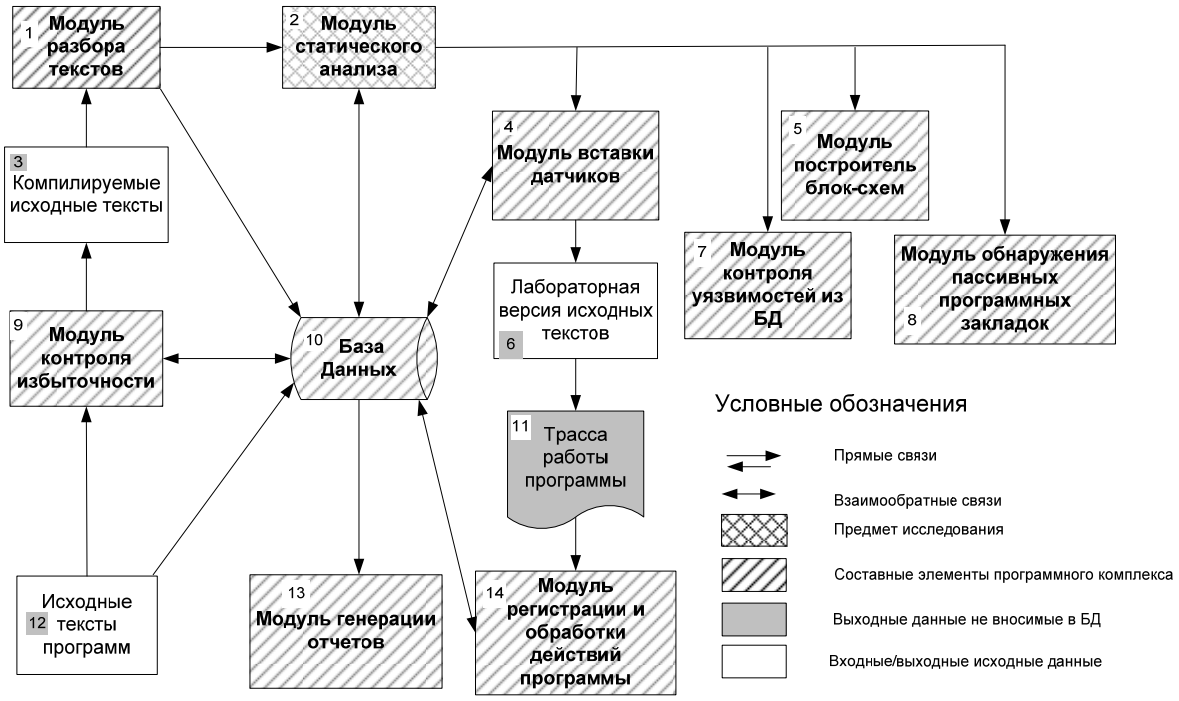


Рис. 1. Упрощенная схема комплекса контроля уязвимостей

Некоторые принципы взаимодействия модулей целесообразно рассмотреть ниже. Исходные тексты (см. № 12 на рис. 1) исследуются на наличие избыточности в модуле № 9 (см. рис. 1). Те файлы, которые были отобраны как «используемые», участвуют в дальнейшем анализе, а избыточные файлы помечаются в базе данных (БД, см. № 10 на рис. 1). Файлы попадают на вход модуля разбора исходных текстов (см. № 1 на рис. 1). Модуль разбора исходных текстов играет основополагающую роль. Алгоритм модуля преобразует исходные тексты к такому виду, который можно использовать для статического и динамического анализов. Информация о файлах сохраняется после разбора в БД, после чего используется на стадии статического анализа (см. № 2 на рис. 1). Именно методы, применяемые в данном модуле, исследуются в данной статье. Статический анализ предназначен для исследования исходного текста программы на соответствие стандартам программирования, на наличие дефектов и уязвимостей, в частности, программных закладок. Подготовка к динамическому анализу реализуется в модуле вставки датчиков (см. № 4 на рис. 1). Датчики вставляются в каждый линейный участок, информация о которых хранится в БД, заполненной после разбора исходных текстов. Версия исходных текстов проекта со вставленными датчиками называется лабораторной (см. № 6 на рис. 1). Последовательность сработавших датчиков формирует «трассу» программы (см. № 11 на рис. 1), которая затем попадает на вход модуля динамического анализа (см. № 14 на рис. 1). Блок № 13 (см. рис. 1) формирует отчеты по результатам статического и динамического анализа (список функций, связей, переменных, и т.п.). В блоках №№ 5, 7, 8 (см. рис. 1) показаны некоторые модули, теоретически входящие в процесс статического анализа, но фактически реализованные как отдельные

программные модули. Среди них, соответственно, «Модуль построителя блок-схем», «Модуль контроля уязвимостей из БД» и «Модуль обнаружения пассивных программных закладок».

Рассмотрим взаимодействие модуль статического анализа с модулем разбора исходных текстов более подробно. На рис. 2 штриховой линией выделены в логические группы компоненты программных модулей: статического анализа и разбора исходных текстов. Остальные условные обозначения соответствуют перечню на рис. 1.

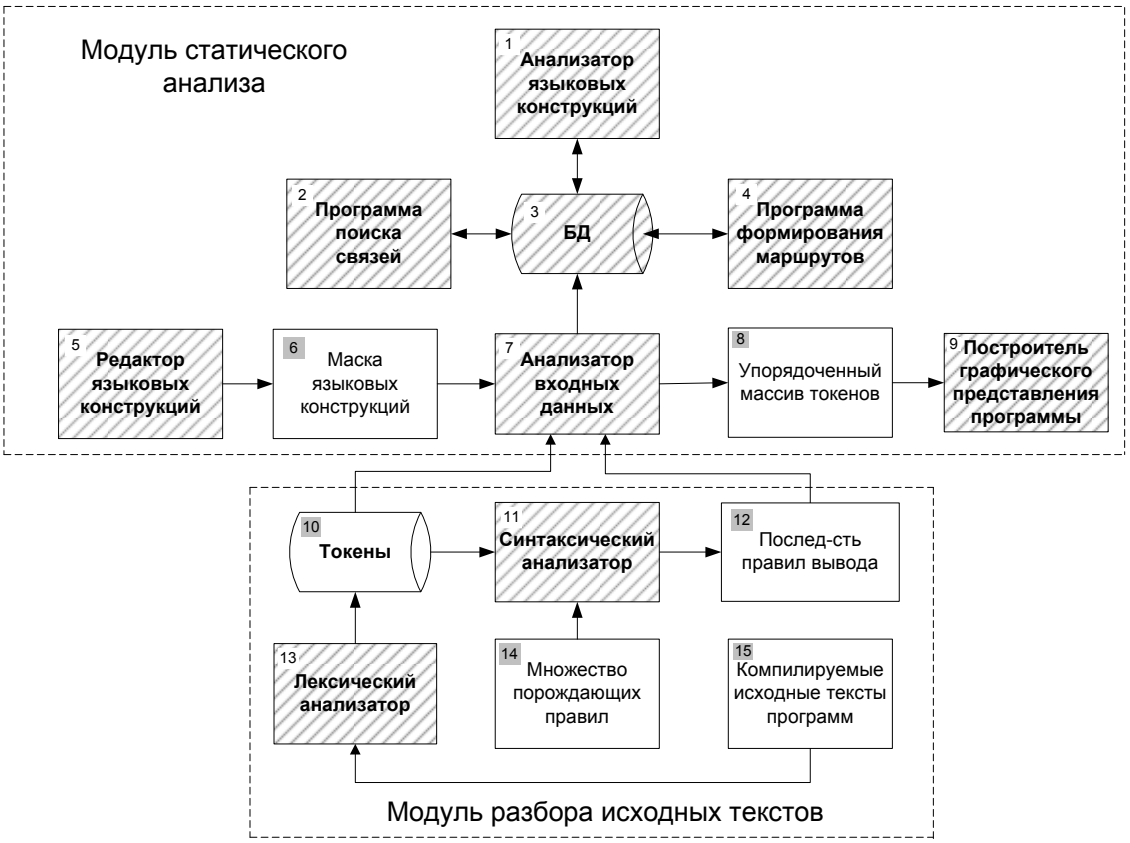


Рис. 2. Схема взаимодействия модулей

Исходные тексты (см. № 15 на рис. 2), которые не являются избыточными и собираются в проект, попадают на вход лексического анализатора (см. № 13 на рис. 2). В результате лексического разбора исходные тексты представляются в виде множества лексем (см. № 10 на рис. 2) с соответствующими им атрибутами – токенов. Множество порождающих правил вместе с лексемами формируют грамматику языка, которая используется при синтаксическом анализе. В результате работы синтаксического анализатора формируется множество правил вывода, используемых в исходных текстах. Лексемы и правила вывода подаются на вход модуля статического анализатора. Его первоочередная задача – это отобрать среди потока токенов такие, в которых есть необходимость при дальнейшем анализе. Например, одно из требований руководящего документа предписывает сформировать список функций. Для этого в массиве токенов необходимо выделить те, которые содержат сведения о функциях. Среди них: имя, тип, аргументы, расположение и др. информация. Какие именно языковые конструкции необходимо распознавать в массиве токенов, определяется с помощью фильтра (см. № 6 на рис. 2), задаваемого с помощью специального редактора (см. № 5 на рис. 2). Редактор играет важнейшую роль при статическом анализе, так как он предоставляет гибкость этому инструменту – с помощью редактора возможно менять требования к отбору информации, детализируя или укрупняя ее. Кроме того, редактор позволяет выби-

рать конструкции для различных языков программирования. На основе маски для правил анализатор входных данных (см. № 7 на рис. 2) находит в массиве токенов необходимую информацию и заполняет БД (см. № 3 на рис. 2 и № 10 на рис. 1). На этом этапе в БД попадают сведения о функциях, переменных и линейных участках. Формируемая структура БД показана на рис. 3.

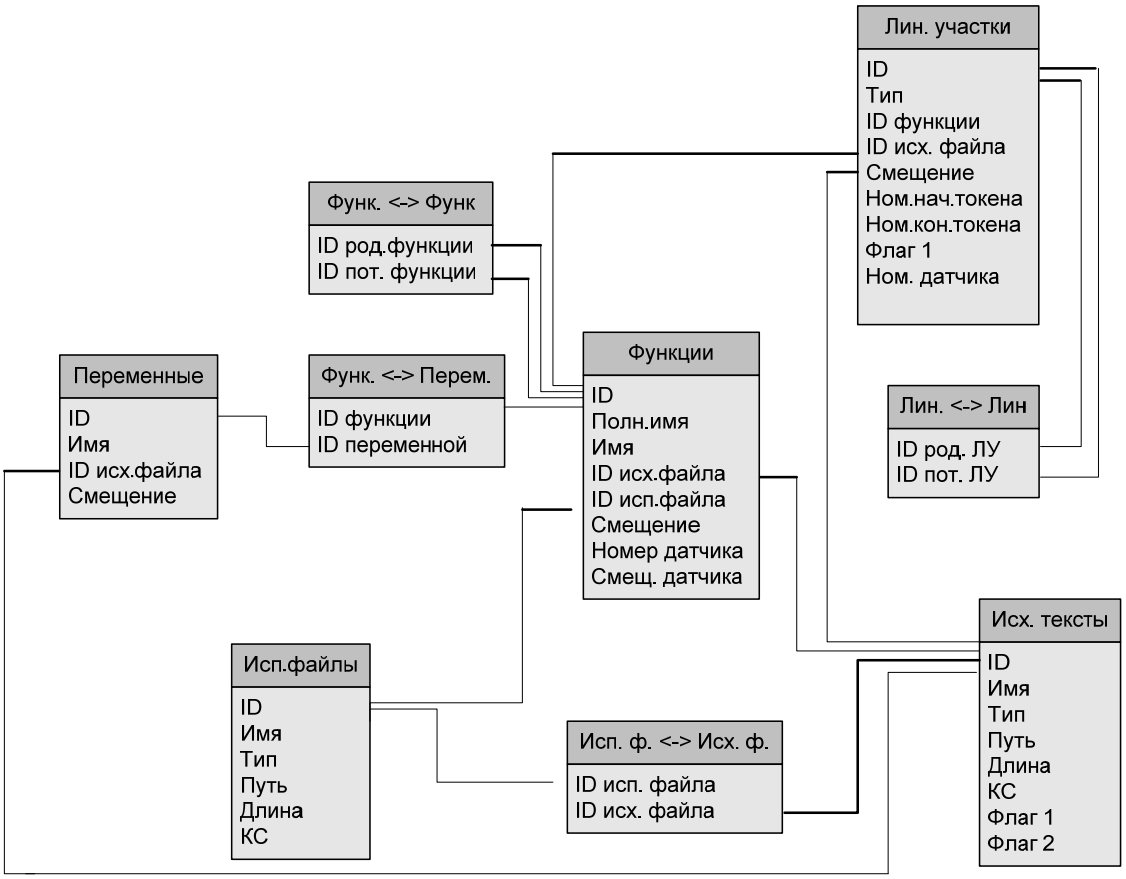


Рис. 3. Структура связей БД

«Анализатор входных данных» формирует три таблицы в БД: таблица переменных, таблица функций и таблица линейных участков. После того, как таблицы сформированы и заполнены, по полученной информации находятся связи (см. № 2 на рис. 2). Эти связи оформляются в виде таблиц, что можно видеть на рис. 3. Дополняет базу данных «Анализатор языковых конструкций», формирующий дополнительную информацию, которая, например, необходима для подготовки исходных текстов к динамическому анализу (см. №№ 4, 6, 11, 14 на рис. 1). «Программа формирования маршрутов» (см. №4 на рис. 2) выполняет требование руководящего документа, строя последовательности вызовов функций. Данная программа может оказаться полезной на стадии динамического анализа, и основная ее концепция заключается в обращении к списку связей во время анализа последовательности вызовов, полученной по результатам работы исследуемой программы.

«Построитель графического представления программы» (см. № 9 на рис. 2) не использует БД, а получает данные прямо от «Анализатора входных данных». Т.е. входные токены, упорядочиваются в соответствии с последовательностью правил вывода и сохраняются в отдельном массиве, к которому может обращаться любая другая программа комплекса, представленного на рис. 1.

Сведения, представленные на рис. 3, раскрывается более подробно в табл. 1 и 2.

Наименование таблицы в БД	Поясняющие сведения
Исх. тексты	Исходные тексты, которые непосредственно подлежат статическому анализу. Таблица заполняется на начальной стадии формирования проекта[2], до начала работы модуля контроля избыточности (см. №9 на рис. 1)
Исп. файлы	Исполняемые файлы, которые получаются в результате компиляции и сборки исходных текстов. Таблица заполняется на начальной стадии формирования проекта, до начала работы модуля контроля избыточности (см. №9 на рис. 1)
Переменные	Таблица содержит сведения о переменных, используемых в проекте. Таблица заполняется по результатам статического анализа. В результате работы анализатора входных данных
Функции	Таблица содержит сведения о функциях, используемых в проекте. Таблица заполняется по результатам статического анализа
Лин. участки	Линейные участки. Таблица содержит сведения о линейных участках (ЛУ), используемых в проекте. Таблица заполняется по результатам статического анализа
Исп.ф. <–> Исх.ф.	Связь между исполняемыми и исходными файлами. Таблица заполняется на начальной стадии формирования проекта, в процессе работы модуля контроля избыточности (см. № 9 на рис. 1)
Функ. <–>Перем.	Связь между функциями и переменными. Таблица заполняется по результатам статического анализа, в процессе работы программы поиска связей.
Функ. <–> Функ.	Связь между функциями и переменными. Таблица заполняется по результатам статического анализа, в процессе работы программы поиска связей.
Лин. <–> Лин.	Связь между линейными участками. Таблица заполняется по результатам статического анализа, в процессе работы программы поиска связей.

Таблица 1. Сведения о таблицах БД

Наименование поля в таблице БД	Поясняющие сведения
Таблица «Исп. файлы»	
ID	Уникальный идентификационный номер исполняемого файла для учета в БД.
Имя	Имя исполняемого файла (без пути и расширения).
Тип	Тип исполняемого файла (расширение)
Путь	Путь к файлу от каталога проекта
Длина	Длина файла в байтах
КС	Контрольная сумма файла
Таблица «Исх. файлы»	
ID	Уникальный идентификационный номер исходного файла, для учета в БД.

[2] В данном случае под проектом понимается совокупность сведений, формируемых специальным комплексом контроля уязвимостей и программных закладок, о котором шла речь в подразделе «Постановка задачи»

Наименование поля в таблице БД	Поясняющие сведения
Имя	Имя исходного файла (без пути и расширения).
Тип	Тип исполняемого файла (расширение)
Путь	Путь к файлу от каталога проекта
Длина	Длина файла в байтах
КС	Контрольная сумма файла
Флаг 1	Флаг №1 определяет избыточность файла
Флаг 2	Флаг №2 определяет включение в тело исходного файла маркера, контролирующего избыточность
Таблица «Функции»	
ID	Уникальный идентификационный номер функции, для учета в БД
Полн. имя	Полное имя функции содержит сведения о типе, аргументах и названии
Имя	Короткое имя – название функции
ID исх. файла	Уникальный идентификационный номер исходного файла, в котором располагается функция.
ID исп. файла	Уникальный идентификационный номер исполняемого файла, в котором располагается функция.
Смещение	Смещение в байтах от начала файла до начала функции
Номер датчика	Номер датчика, вставленного программой «Модуль вставки датчиков» (см. № 4 на рис. 1)
Смещ. Датчика	Смещение в байтах от начала файла до начала датчика
Таблица «Переменные»	
ID	Уникальный идентификационный номер переменной, для учета в БД.
Имя	Имя переменной
ID исх. файла	Уникальный идентификационный номер исходного файла, в котором располагается переменная.
Смещение	Смещение в байтах от начала файла до начала переменной
Таблица «Лин. Участки»	
ID	Уникальный идентификационный номер линейного участка, для учета в БД.
Тип	Тип линейного участка
ID функции	Уникальный идентификационный номер функции, в которой располагается ЛУ
ID исх. файлов	Уникальный идентификационный номер исполняемого файла, в которой располагается ЛУ
Смещение	Смещение в байтах от начала файла до начала линейного участка
Ном. нач. токена	Номер начального токена в линейном участке
Ном. кон. Токена	Номер конечного токена в линейном участке

Наименование поля в таблице БД	Поясняющие сведения
Флаг 1	Флаг, определяющий такую особенность синтаксиса, как фигурные скобки. В некоторых конструкциях целесообразно добавлять скобки для вставки дополнительного кода. Необходимость вставки определяется этим флагом
Ном. датчика	Номер датчика, вставленного в линейный участок. Поле заполняется после работы программы «Модуль вставки датчиков» (см. № 4 на рис. 1)
Таблица «Исп.ф. <–> Исх.ф.»	
ID исп. файла	Уникальный идентификационный номер исполняемого файла
ID исх. файла	Уникальный идентификационный номер исходного файла
Таблица «Функ. <–>Перем.»	
ID функции	Уникальный идентификационный номер функции
ID переменной	Уникальный идентификационный номер переменной
Таблица «Функ. <–> Функ»	
ID род. функции	Уникальный идентификационный номер родительской функции
ID пот. функции	Уникальный идентификационный номер потомственной функции.
Таблица «Лин. <–> Лин.»	
ID род. ЛУ	Уникальный идентификационный номер родительского линейного участка
ID пот. ЛУ	Уникальный идентификационный номер потомственного линейного участка

Таблица 2. Расшифровка полей в таблицах

Данные, приведенные в таблицах БД, позволяют сформировать необходимые отчеты, а все дополнительные способы анализа наиболее удобно реализовывать исходя из упорядоченного массива токенов.

Эксперимент, проводимый при исследовании предложенного метода анализа, заключается в следующем. Цель – определить корректность выполнения статического анализа исходных текстов по упрощенной грамматике языка. Файлы с исходными текстами подаются на вход анализатора, над ними производятся лексический, синтаксический и статический анализы, в результате чего в БД сохраняется информация[3], приведенная в табл. 1 и табл..2. Среди этой информации имеются сведения о функциях, линейных участках, переменных и связях между ними. Критерием правильности выполнения анализа исходных текстов является соответствие списка функций, линейных участков и переменных действительному состоянию в исходных текстах. Исходными условиями следует считать нижеперечисленные:

- 1539 исходных файлов, написанных на языке ANSI C (99);
- все файлы компилируются и собираются в конечные исполняемые файлы;
- в исходных текстах отсутствуют правила не учтенные в грамматике
- компилятор «Watcom C 10.6»;

[3] В соответствии с требованиями РД

- среда компиляции – операционная система реального времени «QNX» версии 4.25;
- среда анализа – MS Windows XP (SP2) + драйвер поддержки файловой системы «ext2»;

Методика проверки заключается в следующем. Для всех 1539 файлов производится синтаксический и затем статический анализы. В результате формируется БД со списком функций, переменных и линейных участков. Для контроля формируем список файлов, которые будут проверены вручную. Из всех файлов выбираем такие, которые содержат максимальное число неповторяющихся порождающих правил. Из этих файлов формируем группу, которая суммарно содержит все порождающие правила упрощенной грамматики. Для сформированного списка файлов проводится ручной анализ, который сравнивается с результатами статического. В том случае, если результаты совпадают, считается что к данным исходным текстам метод был применен корректно. Проверенные файлы удаляются из общего списка, и формируется новая группа для проверки. Общее количество таких проверок равно трем. По результатам делается вывод о корректности работы метода анализа на основе упрощенной грамматики языка.

Вторая часть проверки заключается в контроле модулей статического анализа, основанных на информации из массива токенов. К таким модулям относятся «Программа контроля наличия заданных конструкций» и «Построитель графического представления программы». Первая программа, при определенном подходе, может быть реализована вне рамок предлагаемой концепции, например, путем составления списка функций типа «Delete» и поиском их в самом тексте. Более сложные варианты требуют синтаксического разбора, но такой подход целесообразно рассмотреть [4] отдельно, и в рамках этого исследования он проводиться не будет. «Построитель графического представления программы» представляет наиболее интересную инженерную задачу, в связи с чем проведем проверку именно на данном алгоритме. Проверка заключается в следующем: программа-построитель формирует для выбранных файлов (см. первую часть методики проверки) графическое представление. При построении используется информация не из БД, а из упорядоченного множества токенов. Это связано с тем, что в БД нет достаточных сведений. Результаты построения должны быть вручную сопоставлены с исходными текстами, по которым они были построены. Если соответствие существует, то считается, что построение выполнено корректно. В ином случае будем считать, что такой конкретный способ требует коррекции либо полной замены.

Результаты исследований

Результаты исследования, в частности, проведенного эксперимента, целесообразно разложить на два основных этапа. Первый – это анализ исходных текстов, второй – это выполнение ручного контроля полученных результатов.

Результаты, полученные на первом этапе, были записаны в БД в виде таблиц (формат таблиц см. в табл. 1 и табл. 2) и в специальное хранилище, в котором содержится упорядоченный массив токенов. БД содержит таблицы, содержащие все заданные в таблицах сведения. Ручной анализ показал, что при автоматическом подходе были верно заполнены поля таблиц БД. Вторая часть эксперимента показала, что построение блок схем было выполнено корректно для каждого отдельного файла с исходным текстом.

На основании полученных результатов можно сделать следующие выводы:

1) использование упрощенной грамматики языка формирует данные, применимые для статического анализа;
2) предложенный метод статического анализа на основе упрощенной грамматики языка представил точные данные о структуре проекта;
3) предложенный метод удобно использовать для расширенных требований, предъявляемых к статическому анализу.

К недостаткам данного подхода проверки можно отнести индукционный подход доказательства. В связи с тем, что полностью исходные тексты проверить вручную не представляется возможным, целесообразно найти эталонный вариант контроля функций, переменных и линейных участков и разработать автоматизированное средство сравнения полученных результатов. В качестве такого эталонного варианта анализа может быть использован, например, компилятор и его отладочная информация. Кроме того, исследования показали, что применяемые способы анализа требуют расширения, так как выполнение текущих формальных требований не решает задачи обеспечения безопасности ПО.

Заключение

Проведенные исследования позволил сформировать представление о достоинствах и недостатках метода статического анализа исходных текстов, основанного на использовании упрощенной грамматики языка. Упрощенная грамматика определяется на основе множества правил вывода конечных цепочек языка, характерных только для тех исходных текстов, которые исследуются. За счет такого подхода процесс формирования полной грамматики языка упрощается пропорционально мощности схемы грамматики. Исследования показали, что метод позволяет корректно получать все требуемые сведения. Среди достоинств метода следует отметить следующие:

1) гибкость (можно одними и теми же инструментами исследовать программы, написанные на различных языках программирования);
2) корректность (анализ производится с необходимой точностью);
3) масштабируемость (статический анализ может быть дополнен необходимыми методами контроля без изменения существующих концепций).

К недостаткам такого подхода следует отнести прикладные качества – метод возможно использовать при достаточном уровне знаний, касающихся теории компиляции и программирования. Другой недостаток – низкая эффективность рассмотренных способов при контроле уязвимостей программ

Литература

1. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по 3 уровню контроля, Гостехкомиссия России (в настоящее время ФСТЭК), Москва, 1999 г.
2. J. Viega et al.. ITS4: A Static Vulnerability Scanner for C and C++ Code. Ann. Computer Security Applications Conf. (ACSAC), Applied Computer Security Assoc., 2000.
3. Санкт-Петербургский Государственный Электротехнический Университет им. Ульянова (Ленина) [Электронный ресурс]/ Кафедра ВТ, Фомичев В.С. Теория автоматов, СПб: СПбГЭТУ, 2007 – Режим доступа: http://www.eltech.ru/misc/LGA_2007_FINAL/Allpage/Section6/part_6.1_.html, свободный. – Яз. рус.
4. Арефьев Д.Б., Солодянников А.В. Обнаружение программных закладок и недекларированных возможностей посредством анализа ошибок программирования. / V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23-25 октября 2007г.: Материалы конференции. – СПб: СПОИСУ, 2007. – 153 с.
5. Ахо А.В., Сети Р., Ульман Д. Компиляторы: принципы, технологии и инструменты. – М: Издательский дом «Вильямс», 2003.

6. Котенко Д.А. Контроль избыточности исходных файлов программ на основе вставки программных датчиков. / V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23-25 октября 2007 г.: Материалы конференции. – СПб: СПОИСУ, 2007. – 153 с.
7. Арефьев Д.Б., Солодянников А.В. Обнаружение программных закладок и недекларированных возможностей посредством анализа ошибок программирования. / V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23-25 октября 2007 г.: Материалы конференции. – СПб: СПОИСУ, 2007. – 153 с.
8. Дастин Э., Рэшка Д., Пол Д. Автоматизированное тестирование программного обеспечения. Внедрение, управление и эксплуатация. – М.: «Лори», 2003.
9. Калбертсон Р., Браун К., Кобб Г.. Быстрое тестирование. – М.: Издательский дом «Вильямс», 2002. – 384с.
10. Грицанов А.А. Новейший философский словарь. – Мн: В.М.Скакун, 1999.
11. Котенко Д.А., Солодянников А.В. Метод использования формальных грамматик языков программирования при проведении сертификационных испытаний на отсутствие недекларированных возможностей. / V Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23-25 октября 2007 г.: Материалы конференции. – СПб: СПОИСУ, 2007. – 153 с.
12. Верещагин В.Л., Солодяннков А.В. Анализатор исходного текста, основанный на обработке отладочной информации. / V Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23-25 октября 2007 г.: Материалы конференции. – СПб: СПОИСУ, 2007. – 153 с.
13. Ховард М., Лебланк Д. Защищенный код \ Пер.с англ. – 2-е изд.. испр. – М.: Издательско-торговый дом «Русская Редакция», 2005. – 704 с.
14. Верещагин В.Л., Солодяннков А.В. Использование отладочной информации компилятора для контроля недекларированных возможностей. / X Санкт-Петербургская международная конференция «Региональная информатика-2006» (РИ-2006). – Санкт-Петербург, 24–26 октября 2006 г.: Материалы конференции. – СПб: СПОИСУ, 2007.

МЕТОД ГРАФИЧЕСКОГО ПРЕДСТАВЛЕНИЯ АЛГОРИТМА ПРИ КОНТРОЛЕ УЯЗВИМОСТЕЙ ПРОГРАММЫ

В.Л. Верещагин, Д.Б. Арефьев, А.И. Галанов
Научный руководитель – д.т.н., профессор А.А. Молдовян

Статья содержит исследования метода графического представления алгоритма программы. Проводится контроль выполнения требований руководящего документа и оценивается прикладной уровень метода при исследованиях безопасности программного кода.

Введение

Вопросы, рассмотренные в этой работе, имеют практическое значение для тех исследователей, которые занимаются поиском уязвимостей в исходных текстах программы. В числе уязвимостей можно рассматривать программные закладки и так называемые недекларированные возможности.

Одной из важных задач при исследовании программ являются представление исходного текста, наиболее удобное для понимания. Существует достаточное количество таких форм преставления, в числе которых есть и блок-схемы, и UML-диаграммы, и даже просто исходный текст как таковой. В большинстве случаев подобные графические представления позволяют обрисовать некоторый уровень абстракции, на котором воспринимается алгоритм программы. Чтобы перейти от верхнего уровня абстракции к самому нижнему (уровню конкретного кода), обычно требуется сформировать соответствующее число блок-схем, диаграмм и т.п. Исходя из этого, возникает задача: найти такой способ графического представления, который бы позволил соединить в себе различные уровни абстракции, т.е. можно было бы на одной схеме увидеть и общую концепцию работы программы, и конкретные участки программного кода, которые, например, с точки зрения безопасности могут быть оценены как потенциальные уязвимости.

Актуальность задачи можно определить, исходя из следующих видов деятельности, проводимой на территории РФ. Работа в области сертификации программного обеспечения (ПО) включает в себя «анализ алгоритма на основе блок-схем, диаграмм и т.п.» [1]. Работа со свободным программным обеспечением (СПО) [2] включает в себя исследование архитектуры по исходному тексту программы, для чего могут быть полезны и различные уровни графического представления. Наконец, графическое представление может облегчить задачу исследования, редактирования и понимания существующих исходных текстов.

В настоящий момент рынок представлен самыми различными видами построителей блок-схем, диаграмм и графических представлений для ПО. Среди них есть инструменты, используемые на стадии проектирования, например, средства визуального моделирования («Telelogic Rhapsody», «Rational Rose»), средства построения структурных диаграмм, блок-схем и диаграмм последовательностей (« Micrografx FlowCharter»). В этих программах решается вопрос графического представления программ за счет того, что диаграммы формируются на стадии проектирования, а не на стадии статического анализа[1]. Среди российских производителей выделяется компания «Интерстрон», разработчик компилятора для C++, и «Центр безопасности информации», известный своим анализатором исходных тестов «АИСТ». «Интерстрон» строит UML-диаграммы по исходным текстам, а «АИСТ» выдает блок-схемы в виде bmp-файла. Кроме перечисленных средств, существует достаточно большое количество программ, выполняющих построение различных вариантов представления кода, среди них «IDA Pro», «Understand for C++» и др.

[1] Понятие статического анализа введено в документе [1]

Графическое представление, рассмотренное в данной статье, строится с помощью редактора «MS Visio». Альтернатива существующим построителям блок-схем заключается в прикладном уровне абстракции. Абстракция представлена на уровне функций и линейных участков конкретного Си-файла. Строится дерево связей, от которого можно переходить к конкретным участкам программы, не обращаясь к исходному тексту программы. Такой вариант представления генерируется автоматически и предоставляет исследователю возможность последовательно переходить (в любом направлении) между уровнем функций и уровнем операторов.

Постановка задачи

Проектирование архитектуры ПО принято начинать с документации. Программная и конструкторская документация предполагает формирование концепции ПО до момента кодирования. В российских стандартах существует ряд документов, которые могут содержать алгоритмы программы и описания к ним. Считается[2], что если взять исходные тексты и построить по ним блок-схемы, то можно, интерпретировав их, произвести сравнительный анализ с алгоритмами, записанным в документе «Пояснительная записка» [3]. Трудно представить, какой ресурс (как временной, так и человеческий) должен быть задействован для того, чтобы произвести этот анализ в действительности. Сложности связаны и с тем, что не учтены возможные отклонения от предписанного хода разработки. Например, множество программных продуктов разрабатывается на основе технического задания, даже без параллельного формирования документации. В результате необходимый комплект документов формируется на основе имеющихся исходных текстов и обычно имеет весьма произвольный характер, так как существует другая группа особенностей, связанная именно с разработкой документации. Среди этих особенностей можно выделить тот факт, что разработчиком документации часто является самый невостребованный специалист на предприятии. Он же – человек, который имеет наименьшие представления о том, как работает программная система. Такой подход к формированию документации не оставляет шансов для успешного сравнения сформированных блок-схем с алгоритмом, описанным в документации.

Наиболее развитые компании (обычно зарубежные) используют для преодоления этой сложности средства визуального моделирования, что позволяет сначала представить алгоритм программы на бумаге, а затем его перевести в программный код. Допустим, что программный код никак не отклоняется от того алгоритма, который был представлен до начала кодирования. В таком случае оба вида построенных диаграмм теоретически должны отражать одну и ту же ситуацию в программном коде. Но на самом деле этого, вероятнее всего, не произойдет. Даже блок-схемы одного и того исходного текста могут иметь различный уровень представления (от верхнего – уровня технического задания, до нижнего – уровня операторов), что в результате не позволит сделать вывод о соответствии. Чтобы проконтролировать работоспособность системы и соответствие заложенной в нее архитектуре, выполняется набор тестов, проверяющий различные уровни проекта (от программного кода до общей архитектуры, представленной в виде диаграмм)

В рамках сказанного графическое представление, построенное по исходным тестам, может граничить с неэффективностью применения на практике. Но в силу того, что данное требование является обязательным при выполнении сертификационных исследований на наличие недекларированных возможностей, постараемся найти грани полезности графического представления.

[2] См документ [1]

Процесс понимания исходных текстов во многих случаях затруднен плохой структуризацией кода, смешанным стилем написания и т.п. Представление таких текстов в каком-либо более стандартном виде с графическим отображением связей может позволить более эффективно «читать» тексты и тем самым помогать при исследовании чужого исходного кода. Важнейшая задача исследователя безопасности кода – сформировать представление о работе программы по ее исходным текстам. Различные языки, имя отличный от других языков синтаксис, не упрощают работу исследователя – перестройка даже с одного знакомого языка на другой знакомый язык бывает достаточно длительной. Но допустим, что все исходные тексты можно представить в некотором универсальном виде, таком, например, как блок-схема или диаграмма. При таком представлении программы важно иметь возможность переходить от главных блоков к составляющим блокам, а далее к исходным кодам.

В данной статье рассматривается метод графического построения, который позволяет выделить в исходном тексте функции и линейные участки, найти их взаимосвязи и представить алгоритм программы в соответствующих блоках. Задача исследования – оценить корректность и эффективность данного подхода.

Методы исследований

Оценка полученного графического представления производится путем выявления соответствия информации, отраженной на блок-схеме, с информацией, представленной в исходном коде. Для этого необходимо сформировать инструмент, который в соответствии с методом будет строить графические изображения, и инструмент, который будет выявлять функции, линейные участки и связи между ними. Второй инструмент будет использоваться для проверки графических данных.

Перед тем как рассмотреть эти два инструмента, важно представить их положение в составе специального комплекса контроля уязвимостей и программных закладок. На рис. 1 представлена схема, отображающая основные взаимосвязи модулей комплекса.

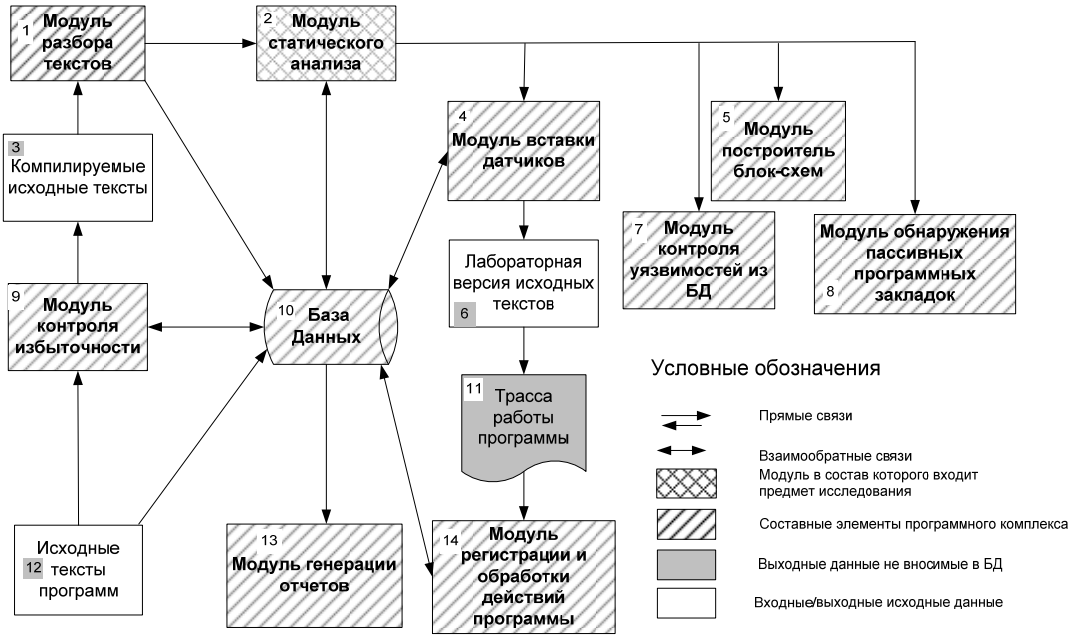


Рис. 1. Упрощенная схема комплекса контроля уязвимостей

Некоторые принципы взаимодействия модулей целесообразно рассмотреть ниже. Исходные тексты (см. № 12 на рис. 1) исследуются на наличие избыточности в модуле

№ 9 (см. рис. 1). Те файлы, которые были отобраны как «используемые», участвуют в дальнейшем анализе, а избыточные файлы помечаются в базе данных (БД, см. № 10 на рис. 1). Файлы попадают на вход модуля разбора исходных текстов (см. № 1 на рис. 1). Модуль разбора исходных текстов играет основополагающую роль. Алгоритм модуля преобразует исходные тексты к такому виду, который возможно использовать для статического и динамического анализов. Информация о файлах сохраняется после разбора в БД, после чего используется на стадии статического анализа (см. № 2 на рис. 1). Именно методы, применяемые в данном модуле, исследуются в данной статье. Статический анализ предназначен для исследования исходного текста программы на соответствие стандартам программирования, на наличие дефектов и уязвимостей, в частности, программных закладок. Подготовка к динамическому анализу реализуется в модуле вставки датчиков (см. № 4 на рис. 1). Датчики вставляются в каждый линейный участок, информация о которых хранится в БД, заполненной после разбора исходных текстов. Версия исходных текстов проекта со вставленными датчиками называется лабораторной (см. № 6 на рис. 1). Последовательность сработавших датчиков формирует «трассу» программы (см. № 11 на рис. 1), которая затем попадает на вход модуля динамического анализа (см. № 14 на рис. 1). Блок № 13 (см. рис. 1) формирует отчеты по результатам статического и динамического анализа (список функций, связей, переменных, и т.п.). В блоках №№ 5, 7, 8 (см. рис. 1) показаны некоторые модули, теоретически входящие в процесс статического анализа, но фактически реализованы, как отдельные программные модули. Среди них, соответственно, «Модуль построителя блок-схем», «Модуль контроля уязвимостей из БД» и «Модуль обнаружения пассивных программных закладок».

Рассмотрим более подробно модуль статического анализа, в состав которого входят и построитель графического представления программы, и программа формирования информации о функциях, линейных участках и связях между ними.

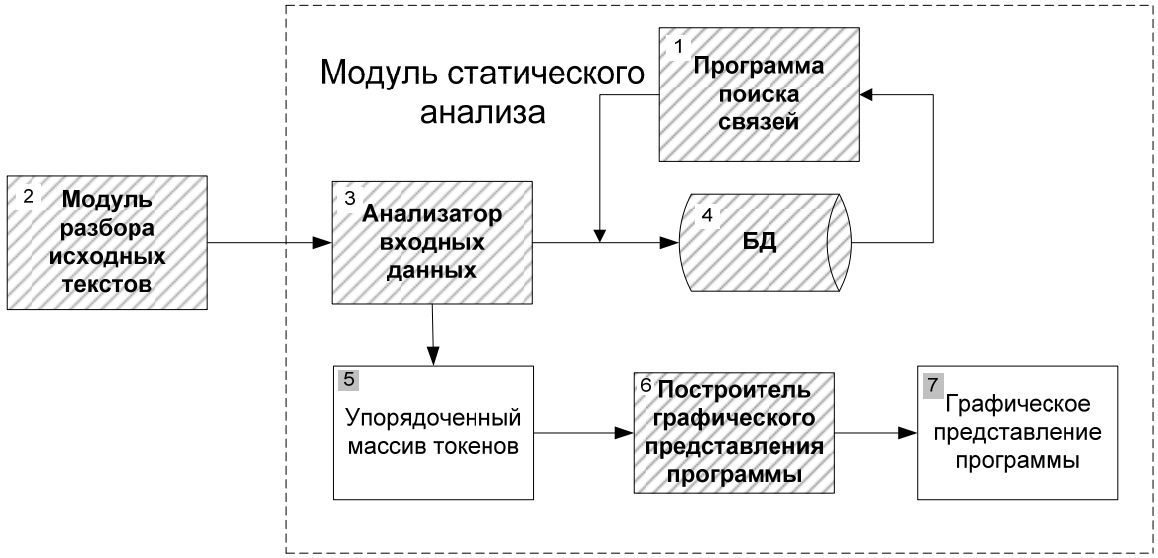


Рис. 2. Упрощенная схема работа модуля статического анализа

Исходные тексты, которые не являются избыточными и собираются в проект, попадают на вход лексического анализатора. В результате лексического разбора (см. № 2 на рис. 2) исходные тексты представляются в виде множества лексем с соответствующими им атрибутами – токенов. Множество порождающих правил вместе с лексемами формируют грамматику языка, которая используется при синтаксическом анализе. В результате работы синтаксического анализатора формируется множество правил выво-

да, используемых в исходных текстах. Лексемы и правила вывода подаются на вход (см. № 3 на рис. 2) модуля статического анализатора. Его первоочередная задача – это отобрать среди потока токенов такие, которые необходимы для дальнейшего использования. Например, одно из требований руководящего документа предписывает сформировать список функций, то в массиве токенов необходимо выделить те, которые содержат сведения о функциях. Среди них: имя, тип, аргументы, расположение и др. информация. Какие именно языковые конструкции необходимо распознавать в массиве токенов, определяется с помощью фильтра, задаваемого с помощью специального редактора. Редактор играет важнейшую роль при статическом анализе, так как он предоставляет гибкость этому инструменту – с помощью редактора можно менять требования к отбору информации, детализируя или укрупняя ее. Кроме того, редактор позволяет выбирать конструкции для различных языков программирования. На основе маски для правил анализатор входных данных (см. № 3 на рис. 2) находит в массиве токенов необходимую информацию и заполняет БД (см. № 4 на рис. 2 и № 10 на рис. 1). На этом этапе в БД попадают сведения о функциях, переменных и линейных участках. Программа поиска связей (см. № 1 на рис. 2) получает информацию из БД и на ее основе создает новые таблицы – таблицы связей. Построитель графического представления программы (см. № 6 на рис. 2) работает независимо от БД, напрямую с упорядоченным массивом токенов (см. № 5 на рис. 2). Построитель получает на вход токены, определяет по ним комбинации лексем и ставит им в соответствие графические объекты (см. № 7 на рис. 2).

Обобщенная схема работы программы построителя показана на рис. 3.

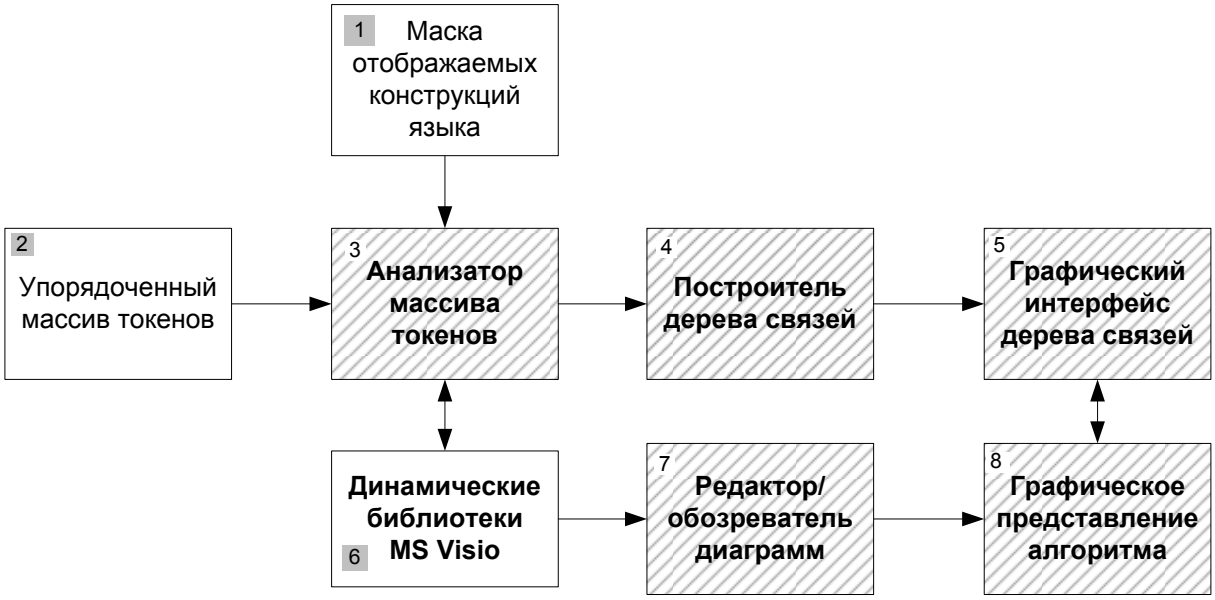


Рис. 3. Схема программы-построителя

Упорядоченный массив токенов (см. № 2 на рис. 3) приходит на вход (см. № 3 на рис. 3) программы-построителя, где разбирается на языковые конструкции, которые необходимо отразить в графическом виде. Например, к этим конструкциям относятся функции, линейные участки и пр. Список необходимых для отбора правил задается с помощью маски (см. № 1 на рис. 3), которая формируется исследователем при помощи специального редактора. Те конструкции, которые были отобраны в результате работы анализатора массива токенов (см. № 3 на рис. 3), обрабатываются с помощью динамических библиотек программы MS Visio, в результате чего для каждой конструкции определяется графический объект. Графическому объекту задаются определенные харак-

теристики, например, для линейного участка этими характеристиками являются смещение от начала файла первого токена и смещение от начала файла последнего токена. Эта информация позволяет определить, какие размеры должен принимать графический объект в развернутом виде, чтобы отразить входящие в его состав другие линейные участки. Редактор/обозреватель диаграмм (см. № 7 на рис. 3) получает на вход всю информацию о графическом представлении и после обработки выдает в специальном окне графическое представление алгоритма (см. № 8 на рис. 3). Данное представление может быть отредактировано сразу после построения. Другая ветвь программы формирует рядом с построенным изображением управляющее дерево, которое позволяет раскрывать и собрать представленные линейные участки. Данное дерево формируется с помощью специальной подпрограммы «Построитель дерева связей» (см. № 4 на рис. 3), в результате работы которой пользователю предоставляется дружественный интерфейс управления (см. № 5 на рис. 3).

Методика проверки корректности и эффективности данного подхода заключается в следующем. Полученные графические результаты соотносятся с исходными текстами и данными, собранными в БД. Формат представления БД показан на рис. 4. Более подробное описание содержимого БД можно увидеть в таблице. Проводится ручной анализ соответствия между графическим представлением алгоритма, с одной стороны, и сведений, содержащихся в исходных текстах и БД, с другой стороны.

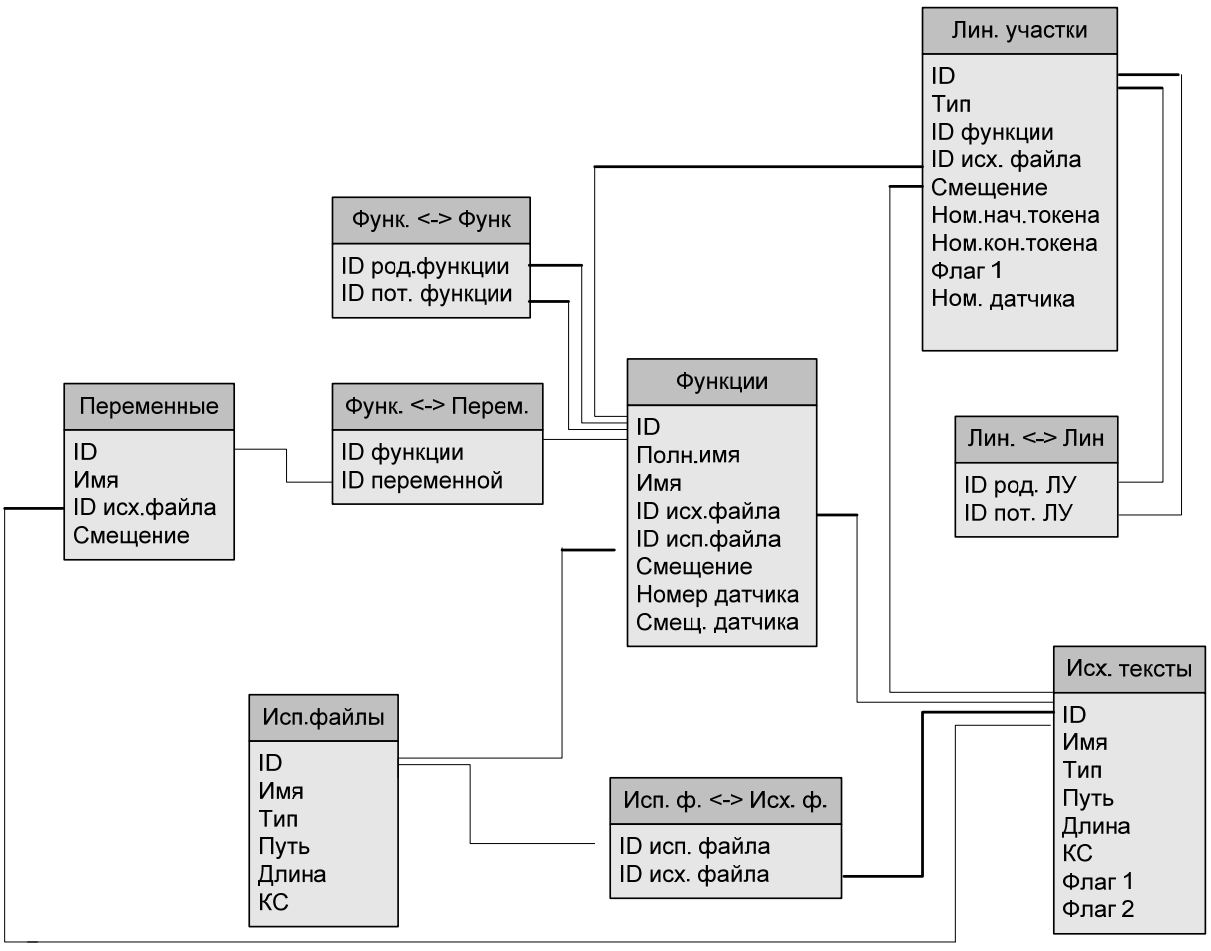


Рис. 4. Структура связей БД

Наименование таблицы в БД	Поясняющие сведения
Исх. тексты	Исходные тексты, которые непосредственно подлежат статическому анализу. Таблица заполняется на начальной стадии формирования проекта[3], до начала работы модуля контроля избыточности (см. №9 на рис. 1)
Исп. файлы	Исполняемые файлы, которые получаются в результате компиляции и сборки исходных текстов. Таблица заполняется на начальной стадии формирования проекта, до начала работы модуля контроля избыточности (см. №9 на рис. 1)
Переменные	Таблица содержит сведения о переменных, используемых в проекте. Таблица заполняется по результатам статического анализа. В результате работы анализатора входных данных
Функции	Таблица содержит сведения о функциях, используемых в проекте. Таблица заполняется по результатам статического анализа
Лин. участки	Линейные участки . Таблица содержит сведения о линейных участках (ЛУ), используемых в проекте. Таблица заполняется по результатам статического анализа
Исп.ф. <–> Исх.ф.	Связь между исполняемыми и исходными файлами. Таблица заполняется на начальной стадии формирования проекта, в процессе работы модуля контроля избыточности (см. №9 на рис. 1)
Функ. <–>Перем.	Связь между функциями и переменными. Таблица заполняется по результатам статического анализа, в процессе работы программы поиска связей.
Функ. <–> Функ.	Связь между функциями и переменными. Таблица заполняется по результатам статического анализа, в процессе работы программы поиска связей.
Лин. <–> Лин.	Связь между линейными участками. Таблица заполняется по результатам статического анализа, в процессе работы программы поиска связей.

Таблица. Сведения о таблицах БД

Результаты исследований

Ручной анализ показал, что метод обладает достаточной точностью, потенциалом к детализации графического представления и практической применимостью при исследовании исходных текстов в рамках безопасности. К недостаткам стоит отнести отсутствие взаимосвязи между отдельными файлами исходного текста: с точки зрения прикладного значения метода необходимо графическое представление формировать на уровне одного или группы исполняемых файлов.

Заключение

Статья содержит исследования, выполненные для метода графического представления исходных текстов. Данный метод включает в себя способы построения графической структуры текста на основе информации, полученной в результате лексического и

[3] В данном случае под проектом понимается совокупность сведений, формируемых специальным комплексом контроля уязвимостей и программных закладок, о котором шла речь в подразделе «Постановка задачи»

синтаксического разборов исходного текста. Метод включает способы отображения текста в графическом виде, являющиеся альтернативным для блок-схем.

Исследования показали, что подобный способ может быть применим для реализации требований руководящего документа [1] и при определенной доработке использоваться при исследовании плохо документированных исходных текстов, например текстов свободного программного обеспечения.

Литература

1. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по 3 уровню контроля, Гостехкомиссия России (в настоящее время ФСТЭК), Москва, 1999.
2. «Концепция развития разработки и использования свободного программного обеспечения в Российской Федерации», Министерство информатизации и связи, 12 марта 2008 г.
3. ГОСТ 19.404-79. ЕСПД. Пояснительная записка. Требования к содержанию и оформлению, Москва, 1979.
4. Котенко Д.А., Солодянников А.В. Метод использования формальных грамматик языков программирования при проведении сертификационных испытаний на отсутствие недекларированных возможностей. / V Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23–25 октября 2007 г.: Материалы конференции. – СПб: СПОИСУ, 2007. – 153 с.
5. Верещагин В.Л., Солодяннков А.В. Анализатор исходного текста, основанный на обработке отладочной информации. / V Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23-25 октября 2007 г.: Материалы конференции. – СПб: СПОИСУ, 2007. – 153 с.
6. J. Viega et al. ITS4: A Static Vulnerability Scanner for C and C++ Code. Ann. Computer Security Applications Conf. (ACSAC), Applied Computer Security Assoc., 2000.
7. Котенко Д.А. Контроль избыточности исходных файлов программ на основе вставки программных датчиков. / V Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)». Санкт-Петербург, 23–25 октября 2007 г.: Материалы конференции. – СПб: СПОИСУ, 2007. – 153 с.
8. Ховард М., Лебланк Д. Защищенный код \ Пер. с англ. – 2-е изд.. испр. – М.: Издательско-торговый дом «Русская Редакция», 2005. – 704 с.
9. Ахо А.В., Сети Р., Ульман Д. Компиляторы: принципы, технологии и инструменты. – М: Издательский дом «Вильямс», 2003.
10. Дастин Э., Рэшка Д., Пол Д. Автоматизированное тестирование программного обеспечения. Внедрение, управление и эксплуатация. – М: «Лори», 2003.
11. Калбертсон Р., Браун К., Кобб Г. Быстрое тестирование. – М.: Издательский дом «Вильямс», 2002. – 384с.

К ПРЕДСТАВЛЕНИЮ ЗНАНИЙ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

И.А. Коробовский, П.А. Пугач
Научный руководитель – д.т.н., профессор Г.Ф. Нестерук

В работе рассмотрены вопросы представления знаний, программной поддержки методологии мониторинга безопасности ИС и компьютерного моделирования интеллектуальных средств в составе адаптивных классификаторов для средств МБ ИС.

Введение

Создание перспективных систем защиты информации (СЗИ) в последнее время отождествляют с активным использованием интеллектуальных средств, таких как экспертные системы (ЭС), системы нечеткой логики (НЛ), нейронные сети (НС), реализующих в СЗИ эволюционные свойства адаптации, самоорганизации, обучения, возможности наследования и представления опыта экспертов информационной безопасности (ИБ) в виде доступной для анализа системы нечетких правил If-Then [1, 2].

Актуально исследование адаптивных средств классификации угроз безопасности информационных систем (ИС), построенных с учетом биоподобных механизмов ЭС, НЛ и НС. Рассмотрим формы представления знаний экспертов ИБ, используя системы правил ЭС, нечеткое представление информации в НЛ и способность к адаптации информационных полей НС.

«Нечеткое» представление знаний

«Нечеткое» представление знаний базируется на [1, 3]:

- преобразовании исходных значений данных (в заданном диапазоне значений) в *значения истинности* высказываний о принадлежности этих значений некоторой функции (например, «большая величина» *L* или «малая величина» *S*);
- *принципе обощения*, согласно которому основные положения и математический аппарат «четкой» логики переносятся на случай «нечеткого» представления информации.

Например, текущее значение нечеткой переменной x_0 (признак атаки) сопоставляется с двумя функциями принадлежности, которые каждому значению нечеткой переменной ставят в соответствие значение истинности двух взаимно противоположных (комплементарных) высказываний (рис. 1):

- значение признака атаки «большое» – кривая *L* (истинность 0,2),
- значение признака атаки «малое» – кривая *S* (истинность 0,8).

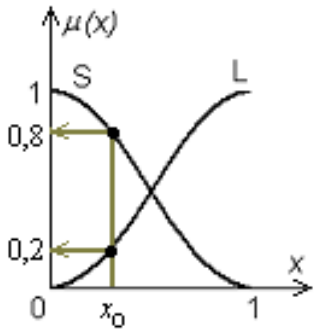


Рис. 1. Комплементарная пара функций принадлежности

Если совокупность признаков атаки представить вектором, то конкретному значению каждой нечеткой координаты вектора (на отрезке области определения) будут соответствовать значения ординат (истинности) функций принадлежности *S* (small) и *L* (large), которые в сумме дают 1. Согласно принципу распространения, значения истинности комплементарных высказываний могут обрабатываться в соответствии с этапами логического вывода [4].

Например, пусть знания экспертов ИБ о классификации угрозы *Y* по вектору признаков атаки *X*, образованному из трех нечетких координат x_2, x_1, x_0, представлены в таблице.

x_2	x_1	x_0	*Y*
S	S	S	S
S	S	L	S
S	L	S	L
S	L	L	L
L	S	S	L
L	S	L	S
L	L	S	L
L	L	L	S

Таблица. Представление знаний

Представления знаний в экспертных системах

Функция *Y* задана на всех наборах значений вектора атаки и может быть описана *конъюнктивной* (по «единицам») или *дизъюнктивной* (по «нулям») системой правил логического вывода [2, 4].

Рассмотрим, например, представление знаний экспертов ИБ (табл. 1) в виде конъюнктивных правил (аналог представления знаний в совершенной дизъюнктивной нормальной форме – ДНФ):

- формируют правила (rules) по числу конъюнктивных термов в ДНФ (числу значений *L* в столбце *Y*);
- значениям координат вектора атаки x_i (i = 0, 1, 2) присваивают значения из строк таблицы, соответствующих значению *L* в столбце *Y* (или значениям переменных x_i из соответствующих конъюнктивных термов ДНФ).

Rule1: If (x_2 is *S* AND x_1 is *L* AND x_0 is *S*) Then *Y* is *L*
Rule2: If (x_2 is *S* AND x_1 is *L* AND x_0 is *L*) Then *Y* is *L*
Rule3: If (x_2 is *L* AND x_1 is *S* AND x_0 is *S*) Then *Y* is *L*
Rule4: If (x_2 is *L* AND x_1 is *L* AND x_0 is *S*) Then *Y* is *L*

Представление знаний в виде структуры нечеткой НС

Логическая структура знаний ЭС преобразуется в информационное поле нечеткой НС [5] в соответствии с этапами логического вывода [1, 2].

Первый этап – формирование взаимно противоположных высказываний (соответствует операции «приведение к нечеткости» нечеткого логического вывода). Например:

- x_2 is *L* – высказывание «значение признака атаки x_2 «большое»,
- x_2 is *S* – высказывание «значение признака атаки x_2 «малое»,

реализуется входным узлом нечеткой НС (рис. 2), формирующим комплементарную пару функций принадлежности *S* и *L* (рис. 1).

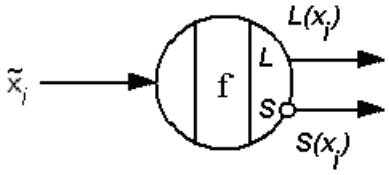


Рис. 2. Входной узел нечеткой НС

Второй этап – логический вывод – соответствует реализации отдельных правил If – Then экспертной системы формальным нейроном (ФН) MIN. ФН MIN (рис. 3) от нечетких аргументов реализует логическую операцию нечеткой конъюнкции $Y = \mu(x_n) \cdot \ldots \cdot \mu(x_0) = \min(\mu(x_n), \ldots, \mu(x_0))$.

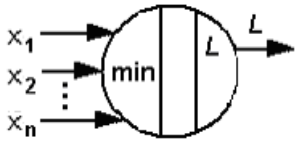


Рис. 3. Формальный нейрон MIN

Третий этап – композиция – соответствует объединению правил с одинаковыми заключениями (частью Then) и реализуется ФН MAX (рис. 4).

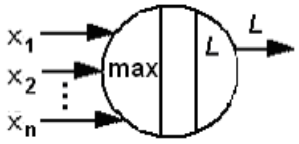


Рис. 4. Формальный нейрон MAX

ФН MAX от нечетких аргументов реализует логическую операцию нечеткой дизъюнкции $Y = \mu(x_n) + \ldots + \mu(x_0) = \max(\mu(x_n), \ldots, \mu(x_0))$.

Нечеткая НС реализует конъюнктивную систему правил нечеткого логического вывода в соответствии с вышеперечисленными этапами (рис. 5).

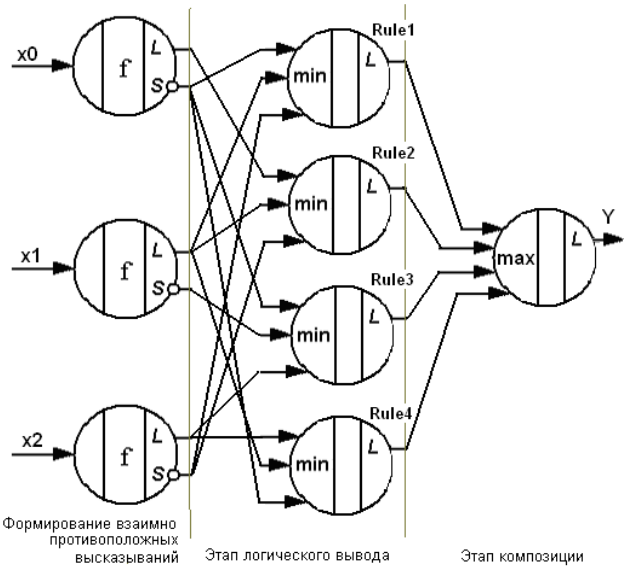


Рис. 5. Нечеткая нейронная сеть

Сети теории адаптивного резонанса

Сети теории адаптивного резонанса или классификаторы Карпентера-Гроссберга (Adaptive Resonance Theory Network, ART) также применяются для кластеризации многомерных векторов, но обладают рядом особенностей. Главным их свойством является адаптация – процесс обучения сети и ее эксплуатации не разделяются. Сети ART реализуют потоковые алгоритмы кластеризации (без предварительного накопления обучающей выборки) с изменяемым количеством кластеров.

Алгоритм обучения нейронной сети ART1 можно описать следующим образом.

Первый входной вектор считается эталоном первого кластера. Следующий входной вектор сравнивается с эталоном первого кластера. Считается, что он принадлежит этому кластеру, если расстояние до эталона в некоторой метрике меньше заданного порога. При этом координаты эталона корректируются по определенному правилу. В противном случае второй вектор становится эталоном второго кластера. Данный процесс повторяется для всех последующих входных векторов. Число кластеров, таким образом, постепенно растет в зависимости от заданной величины порога и используемой метрики.

Если в качестве координат входных векторов использовать признаки атаки, то координаты выходного вектора, определяемые активным в данный момент кластером, соответствуют классифицируемым угрозам.

Представление знаний экспертной системы в ART-сети

Можно провести аналогию между структурой нечеткой НС и сетей адаптивного резонанса. Так, структура ART-сети соответствует этапам нечеткого логического вывода, а отдельные правила базы знаний экспертной системы – формируемым кластерам. Этапу формирования взаимно противоположных высказываний соответствует первый, входной слой нейронов. На вход НС подаются нормированные (в диапазоне [0;1]) значения в прямом и инверсном виде, т.е. используется комплементарное представление информации.

Этапу логического вывода соответствует скрытый слой ART-сети, в котором формируются кластеры, а этапу композиции – выходной слой, объединяющий выходы нейронов ряда кластеров, ассоциированных с одной угрозой.

Заключение

База знаний экспертной системы с учетом специфики нечеткого представления данных однозначно отражается в структуре нечеткой НС или ART-сети, но, в отличие от ЭС, знания экспертов ИБ могут быть автоматически скорректированы в процессе обучения межнейронных связей НС на достоверном множестве пар векторов $\{X,Y\}$. Анализ весов связей между ФН (после обучения НС) позволяет устранить противоречивость знаний экспертов ИБ, которая может присутствовать в исходной базе знаний ЭС.

В ART-сетях за счет использования нечетких операций min и max в процессе идентификации входных векторов достигается высокая скорость решения задачи классификации угроз, а инкрементное обучение (адаптация весов только активного кластера) позволяет в режиме, близком к реальному, корректировать базу знаний, представленную динамичной структурой ART-сети. Отсюда следует, что сети адаптивного резонанса могут применяться в более широком классе задач, чем нечеткие НС.

Литература

1. Negnevitsky M. Artificial intelligence: a guide to intelligent systems. Addison-Wesley, 2002.
2. Нестерук Г.Ф., Осовецкий Л.Г., Харченко А.Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов. (Иммунология систем информационных технологий). – СПб.: Изд-во СПбГУЭФ, 2003.
3. Zadeh L.A., Kacprzyk J. Fuzzy Logic for the Management of Uncertainty. – NY: John Wiley. 1992.
4. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. – 2-е изд., стереотип. – М.: Горячая линия – Телеком, 2002.
5. Нестерук Ф.Г., Молдовян А.А., Нестерук Л.Г., Нестерук Г.Ф. Квазилогические нейронечеткие сети для решения задач классификации в системах защиты информации // Вопросы защиты информации». – 2007. – № 1. – С. 23–31.
6. Горбань А.Н. Обучение нейронных сетей. – М.: СП ПараГраф, 1991.

ПРОГРАММНЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

М.В. Григорьева
Научный руководитель – к.т.н., доцент М.А. Вус
(Санкт-Петербургский институт информатики и информатизации РАН)

Данная работа посвящена разработке алгоритма генерации псевдослучайных чисел (далее ПСЧ) с применением скоростного программного алгоритма криптографического преобразования, созданию программной реализации алгоритма для применения в составе программных средств защиты информации и оценке качества выдаваемых последовательностей ПСЧ.

Введение

Важным элементом построения любой защищенной компьютерной системы, независимо от ее сложности и назначения, являются программные и программно–аппаратные средства генерации псевдослучайных чисел (ПСЧ). Генерация случайных (непредсказуемых) чисел – одна из главных трудностей при реализации любой системы безопасности, в частности криптографической системы. Случайные числа – числа, которые нельзя выработать, используя определенный алгоритм. Но можно создать последовательность чисел, которая будет приближать многие свойства случайных чисел – последовательность ПСЧ. Эти числа являются *псевдо*случайными, поскольку между ними есть детерминированная связь.

Ранее не раз решалась задача создания генераторов ПСЧ, но наибольшее распространение получили простые арифметические генераторы, характеризующиеся быстродействием, но обратимостью, малой длиной периода и в связи с этим невозможностью применения в системах ЗИ. Таким образом, актуальной задачей является развитие теории генераторов ПСЧ, в том числе создание новых алгоритмов генерации ПСЧ, отвечающих требованию применимости в системах ЗИ. В связи с этим цель работы – разработать и реализовать программно-ориентированный алгоритм генерации ПСЧ с применением скоростного программного алгоритма криптографического преобразования. Разработанный алгоритм генерации должен отвечать требованиям непредсказуемости, высокого быстродействия, эффективной и безопасной программной реализации, стойкости к атакам на основе известных, а также специально подобранных текстов, иметь хорошие статистические и периодические свойства.

1. Описание работы

Введем понятия последовательности ПСЧ, генератора ПСЧ и программных шифров.

Последовательность псевдослучайных чисел – последовательность, элементы которой генерируются с помощью каких–либо алгоритмов и подчиняются заданному распределению. *Генератор псевдослучайных чисел* – алгоритм, генерирующий последовательность псевдослучайных чисел. Этот же термин часто используется для описания генераторов псевдослучайных бит, а также различных поточных шифров. *Программные шифры* — это системы шифрования, которые используют операции над компьютерными единицами обработки данных и учитывают специфику обработки данных в вычислительных системах, что дает возможность при программных реализациях этих систем шифрования получать высокие скорости шифрования [1].

1.1. Алгоритм генерации

Для достижения поставленной цели были решены следующие задачи: выполнен обзор области применения генераторов ПСЧ и наиболее перспективных семейств алгоритмов генерации ПСЧ, изучены скоростные программные шифры.

Для генерации ПСЧ было решено использовать алгоритм на основе пароля (**E**), а именно, скоростной программный алгоритм шифрования «СПЕКТР-F» [2]. При разработке данного алгоритма шифрования предполагалось, что основной областью его использования будет обеспечение внутреннего шифрования в компьютерных системах и применение в составе СЗИ НСД, сохраняющих высокую производительность компьютерных систем [3]. Принятие таких решений позволяет выполнить требования, предъявляемые к алгоритму генерации.

Схема разработанного алгоритма генерации ПСЧ представлена на рис. 1.

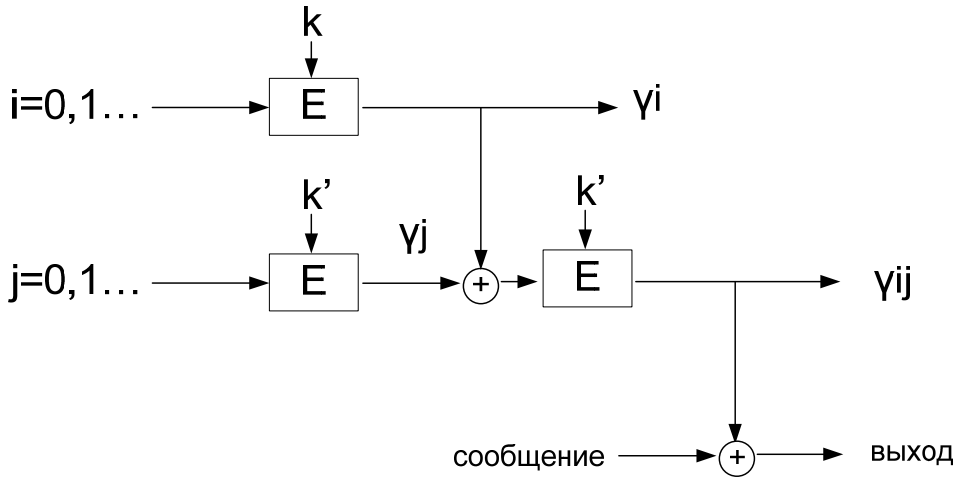


Рис. 1. Алгоритм генерации ПСЧ

Обозначения, используемые на схеме алгоритма генерации ПСЧ:

- **i, j** – начальные множества значений, над которыми осуществляется преобразование;
- **E** – алгоритм шифрования «СПЕКТР-F»;
- **k, k'** – расширенные ключи шифрования, применяемые при шифровании в алгоритме «СПЕКТР-F»;
- γ_i, γ_j – выходные векторы преобразований;
- $\oplus$ – поразрядное сложение по модулю 2.

На вход алгоритму генерации подаются:

- числа (от i_{n1} **до** i_{n2} и от j_{n3} **до** j_{n4}), заданные пользователем, по которым формируются выходные векторы преобразований (γ_I и γ_j);
- начальное множество значений, над которым осуществляются преобразования;
- пароль пользователя, по которому формируется расширенный ключ шифрования или, в случае использования фиксированного расширенного ключа, который используется при вычислении параметров алгоритма «СПЕКТР-F».

В зависимости от того, ввел ли пользователь граничные значения только для параметра i или для параметров i и j, выполняется соответственно один или два цикла преобразований.

Если заданы граничные значения только для параметра i:

- для каждого значения вектора γ_I и каждого блока сообщения выполняется операция XOR;
- полученный блок подается в качестве начального множества значений для алгоритма шифрования **E**.

Если заданы граничные значения для параметров i и j:

- для каждого значения вектора γ_I и текущего значения γ_j выполняется операция XOR;
- полученный блок подается в качестве начального множества значений для алгоритма шифрования **E**;

– для полученного блока и блока сообщения выполняется операция XOR;
– полученный блок подается в качестве начального множества значений для алгоритма шифрования **E**.

Эти действия выполняются в цикле до тех пор, пока значение параметра j не станет равно заданному граничному значению.

1.2. Ограничения алгоритма

Если количество значений конечного вектора преобразований меньше количества блоков сообщения, то заново вычисляются γ. Это может произойти, если оператор неверно задал диапазон значений параметров i и j. В таком случае статистические свойства алгоритма снижаются.

Для эффективной работы алгоритма оператор должен установить значения параметров i и j с учетом величины начального множества значений, над которым будут осуществляться преобразования.

1.3. Программная реализация

Реализовывать алгоритм генерации ПСЧ было решено модульно. Структуру программы генерации ПСЧ можно графически представить в виде модулей (рис. 2).

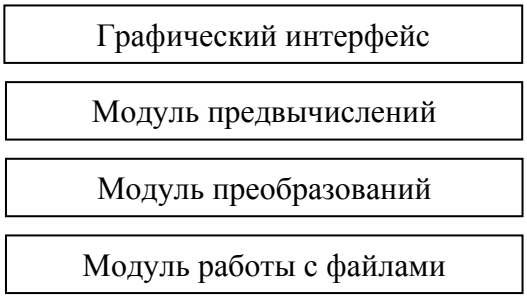


Рис. 2. Модульная структура программы

Программа «Vector-f», интерфейс которой представлен на рис. 3, представляет собой приложение Windows, разработанное в среде «Microsoft Visual Studio 6.0» на языке программирования C++, построенное с использованием библиотеки MFC (Microsoft Foundation Classes – библиотека базовых классов «Microsoft»).

Разработанная программа реализует следующие функции:
– генерация расширенного ключа шифрования;
– реализация алгоритма шифрования дискового пространства «СПЕКТР-F»;
– генерация псевдослучайных чисел;
– шифрование блоков данных по заданным пользователем параметрам;
– дешифрование блоков данных по заданным пользователем параметрам.

При выборе ключа расширенного типа программа произведет генерацию расширенного ключа по введенному пользователю паролю и специализированной подстановочной таблице. Данный ключ будет использоваться в криптографическом алгоритме. При выборе ключа фиксированного типа в алгоритме будет использоваться ключ, зафиксированный в коде программы, а введенный пользователем пароль будет использоваться для вычисления параметров криптографического алгоритма.

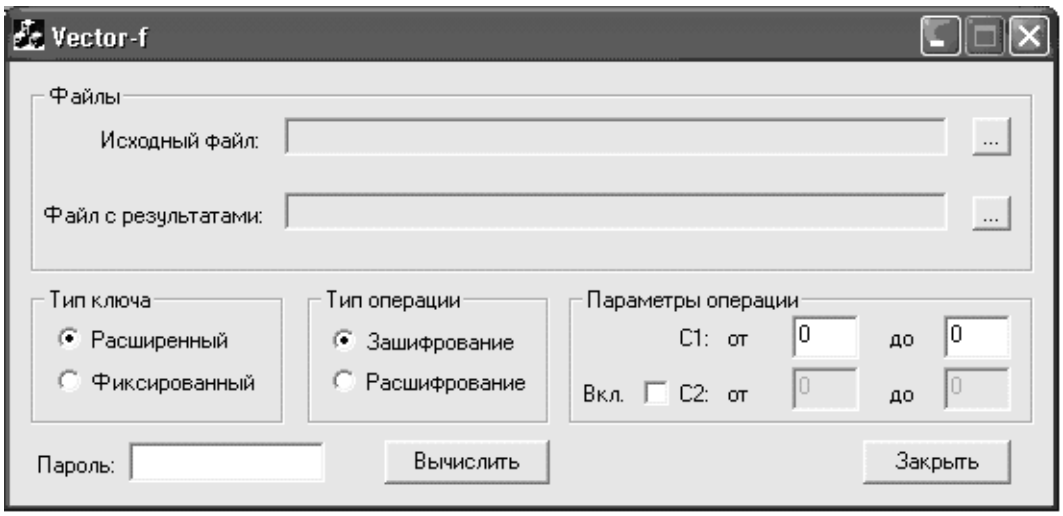


Рис. 3. Главное окно программы

2. Анализ статистических свойств генерируемых последовательностей

Исследование проводилось традиционно используемым методом тестирования. В настоящей работе для исследования последовательностей ПСЧ применяются две группы тестов.

- *Графические тесты.* При этом статистические свойства последовательностей отображаются в виде графических зависимостей, по виду которых делают выводы о свойствах исследуемой последовательности.
- *Оценочные тесты.* При этом статистические свойства последовательностей определяются числовыми характеристиками. На основе оценочных критериев делаются заключения о степени близости свойств анализируемой и истинно случайной последовательностей.

Тестирование разработанной автором программы «Vector-f» проводилось с помощью «ПКСТ-П» – модуля тестирования поточных шифров, разработанного в НФ ФГУП НИИ «Вектор» – СЦПС «Спектр». Модуль тестирования включает в себя следующие тесты: проверка частот появления битов 0 и 1, кумулятивный тест, спектральный тест, тест серий, посимвольная проверка, покерный тест, автокорреляционный тест, геометрический тест [4]. На случайность исследуется гаммирующая последовательность на выходе алгоритма при случайном ключе.

В отличие от графических тестов (в данной работе применялся только графический тест распределения на плоскости), где результаты интерпретируются пользователями, вследствие чего возможны субъективные различия в трактовке результатов, оценочные тесты характеризуются тем, что они выдают численную характеристику, которая позволяет однозначно сказать, пройден тест или нет. Последовательность успешно прошла оценочные тесты. Результат прохождения графического теста представлен на рис. 4.

Вывод: между элементами последовательности отсутствуют зависимости, точки на поле расположены хаотично.

По результатам описанных выше проведенных исследований с большой долей уверенности можно сделать вывод, что генерируемая последовательность ПСЧ отвечает требованию случайности.

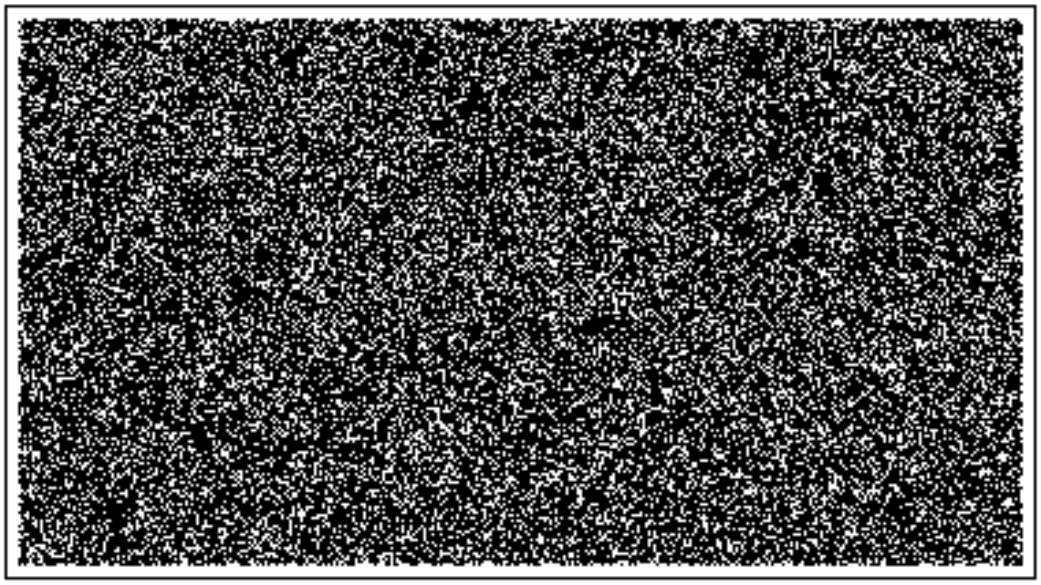


Рис. 4. Результаты теста распределения на плоскости

2.1. Оценка скорости генерации

Оценка скорости генерации последовательности ПСЧ проводится для оценки применимости данной программы в современных системах ЗИ, требующих быстродействия. В данной работе оценка проводилась при использовании расширенного ключа шифрования и параметрах операции C1 от 2 до 256. Характеристики компьютера: процессор Pentuim 1400 MHz, 588 МГц; 248 Мб ОЗУ. Результаты оценки скорости генерации приведены в таблице.

Входной блок данных, Мбайт	68,1	155
Время, с.	15,1	38,2
Скорость, Мбайт/с	4,5	4,1

Таблица 1. Скорость генерации последовательности ПСЧ

Вывод: средняя скорость генерации – 4,3 Мбайт/с.

В данной работе эксперимент носил тестовый характер, так как при написании программы задача достижения максимального быстродействия не ставилась. Естественно полагать, что скорость генерации может быть существенно повышена за счет уменьшения буферизации данных при осуществлении преобразований типов данных.

Заключение

Генераторы ПСЧ – важные элементы построения любой защищенной компьютерной системы. Поэтому создание новых алгоритмов генерации ПСЧ, сочетающих в себе непредсказуемость, высокое быстродействие, эффективную и безопасную программную реализацию – актуальная и экономически эффективная задача.

Разработанный и реализованный алгоритм генерации является криптостойким и характеризуется хорошими статистическими и периодическими свойствами, поэтому может применяться в криптографических системах защиты информации.

В результате выполнения работы:

– выполнен обзор скоростных программных шифров и статистических тестов для оценки качества псевдослучайных последовательностей;

– разработан оригинальный алгоритм генерации псевдослучайных чисел с применением скоростного программного алгоритма криптографического преобразования «СПЕКТР-F»;
– создан пример программной реализации алгоритма для применения в составе программных средств защиты информации;
– проведена отладка программы;
– разработана подробная пользовательская документация;
– выполнен анализ свойств программной реализации: проведена оценка скорости генерации и качества выдаваемых псевдослучайных последовательностей с использованием методов статистического тестирования, реализованных в разработанном в НФ ФГУП НИИ «Вектор» – СЦПС «Спектр» программном комплексе.

Литература

1. Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. – СПб: БХВ-Петербург, 2004.
2. Бодров А.В., Молдовян Н.А., Молдовян П.А. Повышение производительности программных шифров с большим размером блока данных. – СПб: Специализированный центр программных систем «СПЕКТР», 2006.
3. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры. – СПб: БХВ-Петербург, 2002. – 496 с.: ил.
4. Башков И.О., Гортинская Л.В. Исследование статистических свойств блочного шифра EAGLE-128. – СПб: НФ ФГУП НИИ «Вектор» – СЦПС «Спектр», 2006.

МЕТОД ДИНАМИЧЕСКОГО ПОСТРОЕНИЯ ТОПОЛОГИИ СЕТИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОБНАРУЖЕНИЯ УГРОЗ БЕЗОПАСНОСТИ

М.Ю. Будько

Научный руководитель – к.т.н., доцент Г.П. Жигулин

Рассматривается метод динамического построения топологии сети. В качестве исходных данных используется статистика загрузки интерфейсов сетевых устройств, собранная с помощью протокола SNMP.

Введение

В настоящее время широкое распространение получили сети передачи данных, построенные с использованием технологии Ethernet. Несмотря на то, что физическая топология таких сетей представляет собой дерево, достаточно большие сегменты могут быть объединены на втором уровне модели OSI. Это приводит к возникновению угроз безопасности, связанных с использованием широковещательных и групповых адресов для организации штормов в сети. В связи с этим возникает задача динамического анализа потоков данных с целью обнаружения источников дестабилизирующего воздействия на сеть и определения области поражения. При ее решении возникла необходимость предварительного построения топологии сети, в связи с чем и был разработан соответствующий метод. Одним из его возможных применений является автоматизация процесса документирования структуры крупных сетей. Кроме того, для упрощения процедур устранения неисправностей, проектирования и управления сетью решается задача наглядного представления сетевой инфраструктуры.

В настоящее время используются следующие методы построения топологии распределенных сетей передачи данных:

(1) вручную, посредством документирования структуры сети;
(2) с использованием международного стандарта IEEE 802.1AB [1] (Link Layer Discovery Protocol);
(3) с использованием фирменных протоколов, таких как EDP (Extreme Discovery Protocol) компании Extreme Networks, CDP (Cisco Discovery Protocol) компании Cisco Systems, NDP (Nortel Discovery Protocol) компании Nortel Networks;
(4) с использованием универсальных методов, анализирующих адресные таблицы коммутаторов или счетчики количества пропущенных пакетов или байтов.

Недостатки ручного метода документирования структуры сети состоят в неудобстве использования. Протокол 802.1AB мало распространен и не поддерживается большинством сетевого оборудования. Сфера применения фирменных протоколов ограничивается оборудованием конкретного производителя. Соответственно, в настоящее время наиболее удобными являются универсальные методы, ориентированные на использование некоторых общих закономерностей в работе сети для построения сетевой топологии [2].

Среди недостатков универсальных методов можно выделить их невысокую точность и сложность применения. Как правило, все они рассчитаны на использовании информации, запрашиваемой по протоколу SNMP. Следовательно, для их функционирования необходимо поддерживать актуальный список всех устройств в сети. Также постоянные запросы могут «отвлекать» устройства от выполнения их основных функций и, следовательно, приводить к снижению быстродействия некоторых узлов.

Для устранения ряда существующих недостатков универсальных методов предложены следующие улучшения:

(1) для получения статистической информации о функционировании устройств в сети используются сведения из общей системы мониторинга сети, и не требуется дополнительный опрос устройств;

(2) автоматическое, на основе данных системы мониторинга составление списка устройств в сети;
(3) обеспечение возможности построения топологии сети по состоянию на заданную дату и отслеживание изменений в топологии в течение времени;
(4) обеспечение автоматического определения уровней иерархии устройств в сети с выделением периферийных, промежуточных и центральных узлов;
(5) обеспечение независимости метода построения топологии сети от используемой системы мониторинга и программно-аппаратных платформ.

Основная часть

Одна из задач, которую предстояло решить, состояла в обеспечении высокой достоверности обнаружения связей между устройствами. Природа этой проблемы состоит в том, что устройства опрашиваются не синхронно, т.е. существует разница во времени между запросом статистики у первого и последнего устройства в списке мониторинга. Известно только, что максимальный интервал времени задержки равен 300 с. Приложение RRDtool для снижения влияния задержки при опросе устройств интерполирует данные до того момента, когда начался опрос первого устройства.

Это приводит к несоответствию показаний статистики для двух портов, даже если весь трафик с одного из них поступает на вход другого. Соответственно показания, считанные из базы данных, являются функцией от реальных значений:

$$y(t) = f(t) + \varepsilon,$$

где $t = (t_1, t_2, \ldots, t_n)$ – вектор значений временных меток, во время которых инициируется процесс опроса устройств, $\Delta t = (t_i - t_{i+1})$ – период опроса устройств, n – количество значений в выборке; $y = y(t_1, t_2, \ldots, t_n)$ – вектор показаний трафика на порту, сохраненных в системе мониторинга; $f = f(t_1, t_2, \ldots, t_n)$ – реальные значения трафика на порту; $\varepsilon = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ – вектор случайных компонент, образовавшихся вследствие несинхронного опроса устройств и последующей интерполяции данных.

В общем виде задача определения связей между устройствами состоит в поиске наиболее близких последовательностей интенсивностей трафика среди множества портов других устройств:

$$\mathrm{Y} = \begin{Bmatrix} y_1 = y_1(t_1, t_2, \ldots, t_n) \\ y_2 = y_2(t_1, t_2, \ldots, t_n) \\ \vdots \\ y_k = y_k(t_1, t_2, \ldots, t_n) \end{Bmatrix},$$

где Y – множество значений показаний статистики по всем портам, y_i – вектор показаний трафика на порту i, k – количество портов в сети, n – объем анализируемой выборки.

Одним из вариантов решения задачи поиска похожих последовательностей является представление ее в виде задачи нахождения нормы в k-мерном арифметическом пространстве, т.е. отклонений между векторами из множества Y:

$$\left\| y_i - y_j \right\| = \min.$$

Векторы, разница отклонений между которыми будет минимальной и не превысит некоторого порогового значения, будут относиться к связанным портам. В качестве меры похожести можно использовать следующий критерий:

$$s_{ab} = \sum_{i=1}^{n} \left| y_a(i) - y_b(i) \right|^p,$$

где s_{ab} – коэффициент, определяющий близость между значениями трафика на портах a и b, $y_a(i)$ – значение отсчета с номером i на порту a, $y_b(i)$ – значение отсчета с номером i на порту b, n – количество отсчетов, используемых для определения связей между устройствами, p – показатель, определяющий степень влияния выбросов в выборке.

При p=1 получаем сумму абсолютных значений остаточных разностей, которую Лаплас предложил использовать для поиска нормы отклонений наблюдаемых и расчетных значений, при p=2 – сумму квадратов отклонений, которую предложили Гаусс и Лежандр для применения в методе наименьших квадратов. Увеличение значения p влияет на степень учета отклонений сравниваемых значений. Например, при p=2 наличие выбросов в сравниваемых выборках может ухудшить значение коэффициента s по сравнению с p=1.

Для применения на практике следует несколько модифицировать последнюю формулу, чтобы получать не абсолютные, а относительные значения при расчете s:

$$s_{ab} = \sqrt[p]{\frac{1}{n}\sum_{i=1}^{n}\left|\frac{y_a(i) - y_b(i)}{\max(y_a(i), y_b(i))}\right|^p}.$$

В этом случае вычисляется сумма долей, которую занимают отклонения от максимального из отсчетов. Это также позволяет ввести универсальное пороговое значение s^*, при котором связь между устройствами будет считаться обнаруженной:

$$\begin{cases} s_{ab} = \min \\ s_{ab} < s^* \end{cases}.$$

Определение значения p, которое бы приводило к наиболее достоверным результатам, возможно экспериментальным путем. Однако уже при p=1 в реальной сети были получены достаточно точные сведения о связях между устройствами.

Одним из вариантов решения задачи поиска похожих последовательностей может являться использование коэффициента корреляции. Например, стандартного коэффициента корреляции Пирсона, характеризующего степень линейной зависимости или непараметрического коэффициента корреляции, например, коэффициента ранговой корреляции Кендалла. Коэффициент корреляции Пирсона определяется как:

$$\rho = \frac{\operatorname{cov}(X,Y)}{\sqrt{DX \times DY}},$$

где $\operatorname{cov}(X,Y) = M[(X - MX)\times(Y - MY)]$ – ковариация двумерного распределения случайного вектора (X, Y); MX и DX – математическое ожидание и дисперсия случайной величины X.

Для применения к двумерной выборке объемом n вычисляем выборочный коэффициент корреляции:

$$r = \frac{\overline{\operatorname{cov}}(X,Y)}{S_X S_Y} = \frac{\sum_{i=1}^{n}\left(x_i - \frac{1}{n}\sum_{i=1}^{n}x_i\right)\times\left(y_i - \frac{1}{n}\sum_{i=1}^{n}y_i\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i - \frac{1}{n}\sum_{i=1}^{n}x_i\right)^2 \times \sum_{i=1}^{n}\left(y_i - \frac{1}{n}\sum_{i=1}^{n}y_i\right)^2}},$$

где $\overline{\operatorname{cov}}(X,Y) = \frac{1}{n}\sum_{i=1}^{n}\left(x_i - \frac{1}{n}\sum_{i=1}^{n}x_i\right)\times\left(y_i - \frac{1}{n}\sum_{i=1}^{n}y_i\right)$ – выборочная ковариация;

$S_X = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_i - \frac{1}{n}\sum_{i=1}^{n}x_i\right)^2}$ и $S_Y = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(y_i - \frac{1}{n}\sum_{i=1}^{n}y_i\right)^2}$ – выборочные оценки дисперсий.

Коэффициент корреляции Кендалла вычисляем по формуле [4]:

$$r_K = \frac{2}{n(n-1)} \sum_{i=1}^{n} \sum_{j=i+1}^{n} sign\left(q_{(j)} - q_{(i)}\right),$$

где $sign(x) = \begin{cases} -1, x < 0 \\ 0, x = 0 \\ +1, x > 0 \end{cases}$ – знаковая функция; $q_{(i)}$ – ранговые статистики, вычисленные путем построения вариационных рядов значений x_i и y_i, присвоения им рангов r_i и q_i и дальнейшего упорядочивания по возрастанию рангов r_i.

Выделим преимущества использования рангового коэффициента корреляции Кендалла по сравнению с коэффициентом корреляции Пирсона для решения задачи поиска похожих последовательностей:

– коэффициент корреляции Кендалла характеризует степень произвольной нелинейной зависимости между переменными величинами;
– он не зависит от распределения исследуемых выборок;
– он менее чувствителен к выбросам;
– он дает более точные результаты на малых выборках.

При реализации и разработке программного обеспечения для обнаружения связей между устройствами предусмотрена возможность выбора критерия, на основании которого следует строить топологию сети. Это также дало возможность провести исследование точности работы различных подходов к поиску похожих последовательностей.

Были проведены испытания, в ходе которых оценивалась степень надежности обнаружения связей между устройствами и доля ошибочно обнаруженных связей. При этом использовалось четыре критерия:

(1) коэффициент, вычисленный на основе сумм абсолютных значений остаточных разностей;
(2) коэффициент, использующий сумму квадратов отклонений;
(3) выборочный коэффициент корреляции Пирсона;
(4) выборочный ранговый коэффициент корреляции Кендалла.

Результаты приведены на рис. 1 и рис. 2.

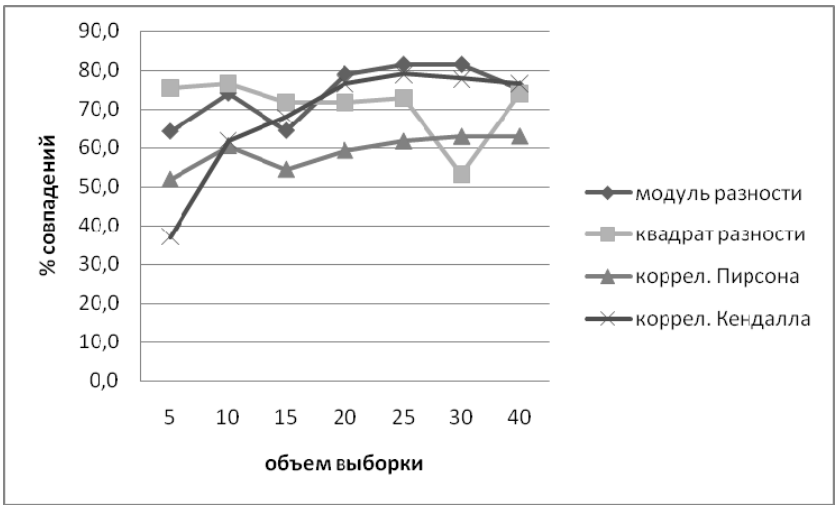


Рис. 1. Степень совпадения с реальной топологией

Можно сделать вывод о том, что наиболее точными оказались коэффициент, вычисленный на основе сумм абсолютных значений остаточных разностей, и коэффициент корреляции Кендалла. Наихудшие результаты показал коэффициент корреляции Пирсона. По количеству ошибочно обнаруженных связей лучше всех был коэффициент

корреляции Кендалла. Однако он может показывать хорошие результаты только при объеме выборки от 10. Таким образом, при объеме выборки до десяти значений целесообразней использовать коэффициент, вычисляющий модуль разности отсчетов, а при большем – коэффициент корреляции Кендалла.

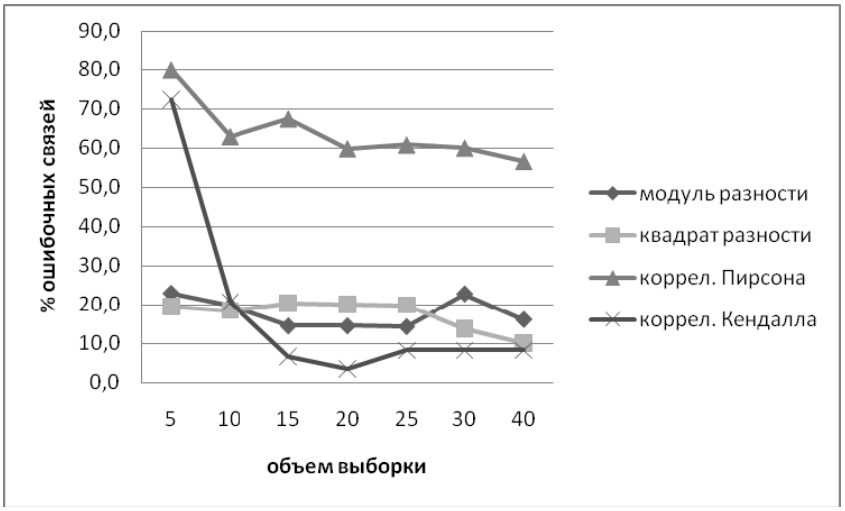


Рис. 2. Ошибочно обнаруженные связи

Рис. 3. Блок-схема алгоритма динамического построения структуры сети

Испытания проводились на основе разработанной программы построения топологии сети. Для ее применения достаточно указать каталог для хранения файлов статистики (файлов в формате RRD), IP-адрес и параметры учетной записи для подключения к серверу мониторинга сети и дату, на которую необходимо строить дерево. После этого программа в автоматическом режиме проведет анализ файлов базы данных статистики и определит названия устройств, связи между ними, номера портов, посредством которых они соединяются, центральное устройство, которое будет находиться на вершине дерева, а также сохранит построенное дерево в специальном формате в виде текстового файла и построит в графическом режиме дерево сети.

Блок-схема алгоритма представлена на рис. 3.

Заключение

В настоящей работе разработаны и реализованы:

- метод динамического построения топологии сети,
- алгоритмы и программное обеспечение, которое в автоматическом режиме проводит анализ файлов базы данных статистики и строит топологию сети.

Определен наиболее точный критерий для обнаружения связей между устройствами. Преимущество предлагаемого метода состоит в том, что для его применения не требуется сохранять и накапливать информацию об используемом сетевом оборудовании и схемах его включения. Достаточно просто указать каталог для хранения файлов статистики, IP-адрес, параметры учетной записи для подключения к серверу мониторинга сети и дату, на которую необходимо строить структуру сети.

Литература

1. IEEE, “802.1AB. IEEE Standard for Local and metropolitan area networks. Station and Media Access Control Connectivity Discovery”. – New York, 2005.
2. Пат. 5,926,462 USA, МКИ^{6} H04L 12/28. Method of determining topology of a network of objects which compares the similarity of the traffic sequences/volumes of a pair of devices. David Schenkel, Michael Slavitch, Nicholas Dawes, 16.11.1995, 20.07.1999.
3. Казиев В.М. Введение в математику и информатику. – СПб: БИНОМ. Лаборатория знаний; Интернет-университет информационных технологий – ИНТУИТ.ру, 2007. – 304 с.
4. Минько А.А. Статистический анализ в MS Excel. – М.: Издательский дом «Вильямс», 2004. – 448 с.

РАЗРАБОТКА МЕТОДИКИ СРАВНИТЕЛЬНОГО ТЕСТИРОВАНИЯ АНТИВИРУСНЫХ ПРОДУКТОВ

А.А. Калашникова, Д.А. Калинин, А.В. Клейменов, В.Д. Стремоухов, А.А. Янковская
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В настоящее время существует большое количество методик сравнения антивирусных продуктов, но, по мнению автора, они не в полной степени соответствуют всем необходимым критериям. Поэтому целью исследования является разработка открытой и универсальной методологии, позволяющей получить максимально объективные и достоверные результаты.

Введение

В настоящее время нет недостатка в информации о тестировании антивирусов (www.anti-malware.ru, www.antivirus.ru/AntiVirPS.html, www.virusbtn.com, www.av-comparatives.org и пр.). Причем, сколько тестирований, столько и выводов. Практически любой антивирус может стать по итогам тестирования самым лучшим. Результаты тестирований и присваиваемые рейтинги по этим результатам зачастую имеют противоположные оценки. Причина этих расхождений – не в неточности или обмане пользователей, а в различных условиях проведения и критериях выбора лучшего антивируса.

Целью данного исследования является разработка методики сравнительного тестирования антивирусных продуктов, которая имела бы следующие качества:

- адекватность;
- открытость, т.е. чтобы тестирование по ней можно было бы повторить кому угодно с получением таких же результатов;
- универсальность, т.е. должна охватывать наиболее важные критерии, в соответствии со спецификой тестируемых продуктов;
- носить технический характер, т.е. отвечать на вопрос, насколько хорошо тот или иной продукт будет защищать компьютер от вредоносного кода, не затрагивая вопросы юзабилити, дополнительных функций и т.п.

Основными задачами данного исследования являются исследование существующих методик, формирование списка критериев, выбор продуктов тестирования, проведение эксперимента.

Существующие методологии

Характер компьютерных угроз постоянно меняется, и по мере того, как они становятся все более изощренными, уже ни одна технология не может гарантировать 100% защиты. Хотя пользователи сами вынуждены решать, какие средства применять, задачу выбора им существенно упрощают независимые тестирования продуктов, проводимые специализированными агентствами.

Установка антивирусного программного обеспечения сегодня обязательна для всех пользователей ПК, обеспокоенных проблемой безопасности данных. Выбирая тот или иной продукт, они стремятся сделать защиту максимально надежной. А подробную информацию о рассматриваемых антивирусных средствах могут получить из отчетов по результатам тестирований [1].

Исследование надежности антивирусов в основном сводится к проверке эффективности ПО в реальных условиях. Однако подходы к проведению тестирования могут различаться. В антивирусной индустрии существует и вполне научный, признанный всеми основными игроками подход к тестированию антивирусного ПО. Базируется он на деятельности некоммерческой организации WildList (www.wildlist.org), которая сама тестированиями не занимается, а предоставляет тестерам вирусные базы.

«Дикие» вирусы. WildList (www.wildlist.org) – международная организация, созданная для сбора и обобщения информации о вирусах, атакующих компьютеры пользователей по всему миру. Основное понятие, используемое в проекте WildList – это термин «дикий вирус» («In the Wild», или сокращенно ITW).

«Дикие вирусы» – это вирусы, свободно распространяющиеся по Всемирной сети и периодически атакующие компьютеры пользователей. Списки «диких вирусов» составляются каждый месяц и предоставляются для тестирований антивирусов независимым исследовательским агентствам.

Список «диких вирусов» включает только те вирусы, которые, во-первых, обнаружены более чем двумя респондентами более чем в двух различных местах (сообщившие о вирусе специалисты должны принадлежать к разным компаниям и обнаружить вирус различными способами, т.е. обнаружение одним антивирусом не считается явным доказательством его «дикости»), во-вторых, являются реальными malware, самораспространяющимися и несущими вред либо представляющими угрозу информационной безопасности пользователей.

Сама организация WildList лишь собирает и анализирует информацию о вредоносных программах. Тестированием антивирусного ПО, отталкиваясь от списка «In The Wild», занимаются такие компании, как ICSA Labs, West Coast Labs и Virus Bulletin. Надо заметить, что абсолютно все известные производители антивирусного ПО тестируют свои продукты в этих исследовательских компаниях. Сегодня такие испытания стали единственным общепризнанным инструментом, позволяющим сделать объективный вывод об эффективности того или иного антивируса. Формат предоставления данных исследователями обычно позволяет хронологически проследить надежность каждого продукта от версии к версии и от платформы к платформе [2].

Сертификация ICSA. ICSA (www.icsalabs.com) – International Computer Security Association (Международная компьютерная ассоциация по защите) – начала свою деятельность в 1992 г. В тестированиях, проводимых ICSA Labs, используется вредоносный код как из собственной «коллекции», так и из списка «In The Wild». По результатам исследований продуктам выдается сертификат ICSA – его удостаиваются те антивирусы, которые способны обнаружить 100% вирусов из списка «In The Wild», выпущенного за месяц до испытаний, и не менее 90% из вирусов собственной коллекции ICSA. Дополнительно антивирусы проверяются на наличие ложных срабатываний. Сертификацию ICSA способно пройти большинство существующих на рынке антивирусов. Данный сертификат есть практически у всех более-менее известных продуктов.

West Coast Labs/ Checkmark. West Coast Labs (www.check-mark.com**)** – один из мировых лидеров в области тестирования ПО для защиты от угроз. По результатам испытаний в West Coast Labs антивирусным продуктам выдается сертификат CheckMark.

В рамках сертификации CheckMark продукты тестируются по категориям. Сегодня это 4 типа испытаний и, соответственно, 4 типа сертификатов:

- Anti-Virus Level 1. Испытываемый продукт должен распознать все вирусы из списка «In The Wild», выпущенного за два месяца до даты тестирования.
- Anti-Virus Level 2. Антивирус, получивший этот сертификат, должен не только обнаружить, но и вылечить систему от всех вирусов, найденных в Level 1.
- Trojan. Проверяется возможность антивируса бороться с вредоносным кодом категории «трояны». Тестирование проводится на базе образцов, отобранных специалистами West Coast Labs.
- Spyware. Антивирусы тестируются на способность противостоять «шпионским программам» (spyware). Тестирование проводится на базе образцов, отобранных специалистами West Coast Labs.

Сертификатами Anti-Virus Level 1 и Anti-Virus Level 2 обладает очень большое количество антивирусов. Прежде всего, это говорит о том, что большинству антивиру-

сов не составляет труда обнаружить и обезвредить вирусы из списка «In The Wild», выпущенного за 2 месяца до даты тестирования. Список антивирусного ПО, имеющего сертификат CheckMark категории «Trojan», существенно короче – пройти это тестирование оказывается для многих компаний уже сложнее. А сертификатами CheckMark в категории «Spyware» обладает совсем небольшое количество продуктов.

Британский «бюллетень». Virus Bulletin (www.virusbulletin.com) – наиболее известный и авторитетный в мире британский журнал, посвященный антивирусам. Тестирования, которые проводятся журналом Virus Bulletin, также основываются на списке вирусов «ln The Wild». Успешно прошедшие испытания продукты получают награду «VB100%». Тестирования проводятся регулярно, несколько раз в год для разных платформ.

Особенность Virus Bulletin – в том, что в испытаниях используется список, выпущенный лишь за две недели до даты испытаний. Параллельно при этом антивирус тестируется на заведомо чистых от вирусов файлах – на наличие ложных срабатываний. Компании, предоставившие свой продукт для тестирования, никогда заведомо не знают, пройдет ли их антивирус испытания успешно. В отличие от других исследователей, Virus Bulletin обязательно информирует своих читателей не только об успехах, но также и о неудачах антивирусных программ. В последнем случае они получают специальный значок, свидетельствующий о том, что антивирус тест не прошел.

Важная особенность методики Virus Bulletin состоит в том, что награда VB100% присуждается продукту не обязательно в случае обнаружения им 100% угроз: допускается возможность пропустить некоторый процент вредоносных программ. Например, если антивирус нашел 98%, то награду он все равно получит. Сегодня многие производители антивирусного ПО заявляют, что смогут гарантированно обнаружить угрозу через один или два часа после ее появления. Но, как показывают тестирования Virus Bulletin, огромное количество вирусов пропускается и через 2 недели после их обнаружения.

В последнее время антивирусная индустрия сталкивается с необходимостью противостоять не только уже обнаруженным вирусам, но также и еще не известным угрозам. Чтобы оценить надежность защиты от еще не существующих угроз, требуются особые методики тестирования. Традиционные испытания здесь бессильны, так как в них исследуется способность антивируса противостоять угрозам, которые уже обнаружены и включены в вирусную базу.

С одной стороны, можно просто попробовать отключить у тестируемого антивирусного продукта сигнатурные базы и посмотреть, как он без них сможет обнаружить вирусы из актуального списка «In The Wild». Но этот путь не приведет к получению полезного и значимого результата: сама технология работы антивирусных программ не предполагает отключения сигнатурных баз. Антивирус с отключенными сигнатурными базами – уже совсем другой продукт, тестировать который не имеет смысла.

С другой стороны, способность антивируса противостоять еще не существующим угрозам можно проверить, используя в тестировании актуальную вирусную базу, но испытывая антивирус с сигнатурной базой, скажем, полугодовой давности. Ведь те вирусы, которые есть в актуальном списке ITW, полгода назад еще не существовали. Продукту, таким образом, придется противостоять несуществующим угрозам. Ресурс Андреаса Клименти www.av-comparatives.org специализируется именно на таких тестированиях. На сайте можно познакомиться с результатами ретроспективных тестов, которые могут оказаться не только полезны при выборе антивируса, но и просто любопытны.

На сайте Virus Bulletin говорится: «Если какой-либо антивирус не прошел наш тест, то это еще не значит, что он неэффективен. Он неэффективен только в руках неподготовленного пользователя. Специалист же сможет его использовать совершенно

по-иному». Один из выводов, который можно сделать после изучения разных методик тестирования и результатов испытаний, состоит в том, что, к сожалению, сегодня ни один продукт не способен гарантировать 100%-защиту от связанных с вредоносным кодом угроз. Однако полное представление о существующей опасности и правильный выбор методов защиты способны свести возможность заражения к минимуму [3].

Разрабатываемая методика

Были выбраны следующие критерии:

- уровень детектирования вирусной коллекции,
- уровень детектирования «in the wild»,
- процент ложных срабатываний,
- эвристический анализ,
- эмуляция,
- лечение активного заражения.

Из них наиболее критичными являются:

- уровень детектирования «коллекции»,
- уровень детектирования «In The Wild»,
- процент ложных срабатываний,
- эвристический анализ.

1) Уровень детектирования вирусной коллекции. В каждом тестируемом антивирусе запускается сканирование по требованию каталога с огромным количеством вирусных экземпляров («коллекция»). Уровень детектирования определяется процентным соотношением количества вредоносных объектов к общему числу проверенных файлов.

2) Уровень детектирования «In The Wild». Данный критерий подразумевает проверку образцов взятых из списка in the wild. Данный параметр определяется отношением обнаруженных вредоносных объектов к общему количеству объектов.

3) Процент ложных срабатываний (false-alarms). Проверяется на коллекции с большим количеством файлов, не относящихся к вредоносным, затем считается количество ложных срабатываний и высчитывается отношение количества ложных срабатываний к общему количеству файлов.

4) Эвристический анализ. Это метод работы антивирусной программы, основанный на сигнатурах и эвристике, он призван улучшить способность сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда сигнатура совпадает с телом неизвестной программы не на 100 %, но в подозрительной программе налицо более общие признаки вируса. Данная технология, однако, применяется в современных программах очень осторожно, так как может повысить количество ложных срабатываний [4].

У всех антивирусов необходимо отключить функцию обновления, т.е. заморозить антивирусные базы данных на дату начала теста.

Сканирование ITW-образцов. Сканирование по требованию производится с максимально возможными настройками: включение эвристики (максимальный уровень), проверка всех файлов, обнаружение всех типов вредоносных и потенциально опасных программ.

5) Эмулятор. Эвристические методы нацелены на исследование файла, который не опознается сигнатурным сканером в качестве подозрительного или вредоносного. Их задача состоит в обнаружении еще не известных антивирусной компании вредоносных программ. Эвристических технологий достаточно много, среди них можно выделить основные.

- Сигнатурный метод. Основан на поиске характерных для вредоносной программы фрагментов кода и (или) констант.

- Эмулятор. Как следует из названия, его задачей является эмуляция выполнения изучаемой программы. Качество эмуляции может быть разным – от примитивной эмуляции команд без эмуляции API функций до почти идеальной эмуляции работы программы в операционной системе. Хороший эмулятор является очень мощным инструментом для выявления новых видов malware, однако он уязвим перед специальными методиками защиты – так называемыми антиэмуляторами.
- Эмулятор и сигнатурный анализ. Также возможно использование одновременно двух вышеперечисленных эвристических технологий для детектирования еще не известных видов вредоносных программ, когда возможности эмулятора дополняются поиском в объекте специфических фрагментов кода [5].

Для сравнительного тестирования необходимо отбирать только те антивирусные программы, которые содержат в себе хоть какой-то эмулятор. Специально для данного антивирусного сравнения должны быть подготовлены тестовые образцы (мини-программы), моделирующие поведение вредоносных программ. К каждому образцу следует подготовить краткое описание. В тестовых образцах используются только тривиальные методы, доступные каждому начинающему программисту.

6) Лечение активного заражения. Данное тестирование заключается в изучении способностей антивирусных программ в лечении активного заражения, когда вредоносная программа уже была ранее запущена и установлена на компьютере и более того, может препятствовать детектированию и удалению со стороны различных антивирусных продуктов. Если вредоносный код не детектируется автоматически антивирусным монитором, то инициируется проверка по требованию каталога (или нескольких каталогов), где должны были быть расположены файлы вредоносной программы. Для каждого отобранного семпла вредоносной программы выделялась своя чистая виртуальная машина. После попытки установки какого-либо антивируса и лечения заражения, машина откатывалась в первоначальное состояние.

Для проведения тестирования антивирусов на лечение активного заражения экспертной группой Anti-Malware.ru отбирались вредоносные программы по следующим критериям:

1. детектирование родительского файла всеми участвующими в тесте антивирусами;
2. способность маскировать свое присутствие;
3. способность противодействовать обнаружению со стороны антивируса;
4. способность восстанавливаться в случае удаления некоторых компонент;
5. распространенность и известность.

В отборе вредоносных программ для теста отдавался приоритет наиболее сложным семплам, которые больше удовлетворяют приведенным выше критериям. Стоит отметить, что критически важным параметром для отбора вредоносных программ для теста было детектирование их со стороны всех участвовавших в тесте антивирусов. Все используемые в тесте вредоносные программы были собраные экспертами Anti-Malware.ru во время распространения в Интернет (In The Wild). Каждый отобранный экземпляр вредоносной программы проверялся на работоспособность и установку на тестовой системе [6].

Методология теста антивирусов на статическое сканирование

Тест проводился на специально подготовленном стенде под управлением VMware Workstation 6.0. Для каждого антивирусного продукта клонировалась «чистая» виртуальная машина с операционной системой Microsoft Windows XP SP2. В тестировании участвовали следующие антивирусные программы:

1. Avira Antivir Personal Edition Premium 7.0,
2. DrWeb 4.44,

3. Eset Nod32 Antivirus 3.0,
4. Kaspersky Anti-Virus 7.0,
5. McAfee VirusScan Enterprise 8.5,
6. Norton Anti-Virus 15.5,
7. Trend Micro Antivirus 16.0.

При установке антивирусов производились все рекомендуемые программой действия (перезагрузка системы, обновление и т.д.). Настройки антивирусов не изменялись и оставались установленными по умолчанию.

Шаги проведения тестирования:

1. включение виртуальной машины;
2. проверка коллекции отобранных вредоносных программ сканером по требованию;
3. подсчет детектируемых файлов.

Для каждой антивирусной программы выделялась отдельная чистая виртуальная машина. Сканировалась коллекция записанная на внешнем жестком диске.

В каждом тестируемом антивирусе запускалась задача сканирования по требованию каталога с огромным количеством вирусных экземпляров. Тестовая база вирусов насчитывала 64446. Коллекция сформирована путем поиска в Интернете и системы honeypot. Вирусы в коллекции не повторяются. Все вирусные экземпляры были распакованы (не было файлов zip, rar, ace и т.д.). Также все тестируемые программы на момент тестирования имели актуальные версии с обновленными базами данных.

Результаты сравнительного тестирования

Отобранные 7 антивирусов показали следующие результаты по обнаружению вредоносных программ:

1. Avira Antivir Personal Edition Premium 7.0 – 61,82%;
2. DrWeb 4.44 – 69,17%;
3. Eset Nod32 Antivirus 3.0 – 60,57%;
4. Kaspersky Anti-Virus 7.0 – 61,38%;
5. McAfee VirusScan Enterprise 8.5 – 96,07%;
6. Norton Anti-Virus 15.5 – 43,84%;
7. Trend Micro Antivirus 16.0 – 87,34%.

Наименование	Всего	Вирусов	%	Позиция в рейтинге
McAFee	65169	62605	96,07	1
TrendMicro	64450	56291	87,34	2
DrWeb	86190	59621	69,17	3
Avira	76919	47552	61,82	4
Kaspersky	109490	67205	61,38	5
Eset	84295	51059	60,57	6
Symantec	84427	37015	43,84	7

Таблица. Результаты тестирования антивирусных продуктов

Заключение

В ходе работы был проведен сравнительный анализ наиболее популярных существующих методик тестирования антивирусного ПО. Была разработана собственная

методика, учитывающая все недостатки предыдущих и обладающая рядом преимуществ, в первую очередь полной открытостью, адекватностью и универсальностью. Также на основе разработанной методологии было проведено сравнительное тестирование антивирусов наиболее крупных компаний в данной области IT-сферы.

Литература

1. Касперский Е. Вирусы и средства борьбы с ними. – М., 2005.
2. Сравнение антивирусов. – Режим доступа: http://svk.sanet.ru/articles/AntivirusDiffs/antivirusdiffs.htm
3. Опыт использования антивирусных программ. – Режим доступа: http://ambernic.nm.ru/antivir2.html
4. Andreas Clementi Anti-virus Comparative №5. On-demand detection of malicious software. – Режим доступа: http://ambernic.nm.ru/antivir2.html
5. Сравнение различных антивирусов на основе вероятностной оценки их качества. – Режим доступа: http://www.antivirus.ru/VirAnalizC.html
6. Сравнения средств защиты от вредоносных программ. – Режим доступа: http://www.anti-malware.ru/index.phtml?part=compare

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ПАССИВНОГО СБОРА СТАТИСТИКИ ОБ ИНФИЦИРОВАНИИ ВРЕДОНОСНЫМ КОДОМ

А.А. Калашникова, Д.А. Калинин, А.В. Клейменов
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Полнота и актуальность сигнатурных баз антивирусных продуктов – наиболее критичный параметр с точки зрения обеспечиваемой ими защищенности. В этой ситуации антивирусным компаниям приходится использовать все возможности по сбору образцов вредоносного кода (ВК). В данном исследовании проектируется модель системы пассивного сбора статистики об инфицировании ВК (honeypot) на основе анализа недостатков и требований, предъявляемых к подобным системам, производится оценка возможности реализации подобной системы на основе существующих программных решений.

Введение

Сегодня вопрос сбора статистики о распределении различных образцов вредоносного кода по регионам, частота инфицирования отдельными образцами, а также сбор in-the-wild образцов стоит наиболее острым образом [1]. С этой целью антивирусные компании создают honeynet – сети распределенных honeypot, систем пассивного сбора статистики об атаках и инфицировании вредоносным кодом, самих образцов ВК. Также подобные системы используются различными компаниями в комплексе с другими средствами обеспечения сетевой безопасности для предупреждения атак (в том числе вирусных) на ресурсы корпоративных компьютерных сетей, борьбу с внутренними угрозами, защиты от спама [2].

Для решения подобных задач существует множество как открытых, так и коммерческих программных решений, предоставляющих различный инструментарий в зависимости от решаемых ими задач, организации, принципов работы. Однако у подобных систем существует ряд фундаментальных недостатков, влияние которых не позволяет использовать их наиболее эффективным образом.

Подобное состояние вопроса и послужило доказательством необходимости проектирования системы, использующей все плюсы вышеназванной технологии, с учетом поставленных для нее задач, выявленных в ходе исследования требований и попыткой минимизировать отрицательное влияние недостатков технологии.

Основы и классификация honeypot систем

Использовать систему-приманку для исследования безопасности различных систем, поиска уязвимостей и изучения действий злоумышленников, пытающихся ее взломать, было предложено довольно давно. Со временем подобные системы получили свое неповторимое название – honeypot (англ. горшочек меда). Сейчас системы honeypot и сети honeynet распространены довольно широко. Существует множество проектов, решающих различные задачи с использованием сетей honeynet.

Идея использовать honeypot для сбора именно актуальных образцов ВК не получила такого широкого распространения, хотя ее потенциал очень велик. По сути дела, honeypot – это система (основанная на реальной или эмулируемой), реализующая некий функционал, позволяющий злоумышленникам взломать ее и неким способом использовать в своих целях. Та степень функциональности, которую подобная система предоставляет в соответствии с заявленной для нее платформой, операционной системой (ОС) и набором неких сервисов для злоумышленника (как реального, так и некой программы), называется интерактивностью.

Основные возможности honeypot можно охарактеризовать так:

(1) сбор малых объемов информации высокой значимости. В отличие от обычных систем сбора статистики, honeypot система собирает только информацию о реальных попытках взлома и атаках, причем реальных, а не ложных. К тому же владелец системы сам решает, какого характера воздействия необходимо регистрировать;
(2) получение информации об атаках, основанных на ранее неизвестных уязвимостях, для их изучения, своевременного устранения и соответственного обновления других систем безопасности, таких как фаейерволы, межсетевые экраны, систем обнаружения вторжения;
(3) сбор инструментов, использованных злоумышленником для использования уязвимостей системы (эксплойты) или образцов ВК.

При этом организация таких систем не требует больших затрат ресурсов, а выгода от их использования становится очевидной в довольно короткие сроки [2].

Классификация систем honeypot может проводиться по различным параметрам, но степень интерактивности, пожалуй, является наиболее важным, так как влияет на то, какие возможности инфицирования будут доступны, на какие типы ВК будут направлены, уязвимости каких платформ и ОС будет охватывать.

С точки зрения интерактивности системы honeypot принято делить на две группы:
(1) низко-интерактивные (low-interaction) honeypot эмулируют различные сервисы, приложения и ОС. К ним можно отнести следующие продукты honeyd (http://www.honeyd.org/), nepenthes (http://www.mwcollect.org/), honeytrap (honeytrap.mwcollect.org). Их легче установить и настроить, но и объем собираемой информации значительно меньше, однако важно понимать, что это не всегда является минусом;
(2) высоко-интерактивные (high-interaction) honeypot основаны на предоставлении уязвимостей реальных сервисов, приложений, ОС на реальных компьютерных системах. Собирают больше информации, однако их установка и обслуживание занимает больше времени.

Недостатки honeypot

Несмотря на явные преимущества применения систем honeypot, существует ряд фундаментальных недостатков:
(1) ограниченная область видения – honeypot осуществляют мониторинг деятельности, которая направлена только против них;
(2) возможность раскрытия honeypot – не так критично с точки зрения сбора образцов ВК, в меньшей мере подвержены honeypot низкой степени интерактивности;
(3) риск взлома honeypot и использование его злоумышленниками в своих целях (например, для рассылки спама или атаки различных узлов сети, участие в бот-сетях и т.п.) – в меньшей мере подвержены honeypot низкой степени интерактивности [3].

Также в связи с решаемой проблемой недостатком является:
(1) ограниченный тип предоставляемых уязвимостей: ему подвержены оба типа систем honeypot, так как различный ВК рассчитан не только на различные уязвимости сервисов и приложений, но также и на платформы, ОС, и даже версии установленных для них обновлений;
(2) безопасность самой системы honeypot от загружаемых или внедряющихся образцов ВК [4].

Задачи, решаемые системой

Пассивный сбор статистики об инфицировании ВК. При успешном использовании ВК предоставляемого функционала (инфицировании системы) этот факт фиксиру-

ется, после чего вся сопутствующая информация передается на сервер для дальнейшей обработки. В случае неудачи должны быть зафиксированы ее причины (отсутствие уязвимости в списке имеющегося функционала системы, отсутствие уязвимости для данной конфигурации системы). Таким образом, для этой задачи сбору и передачи подлежит следующая информация:

(1) реквизиты системы honeypot (так речь идет о сборе статистики то предполагается использовании сети honeynet на основе проектируемой системы) – к ним относится расположение системы;
(2) информация об успешной атаке (инфицировании) или неудаче – дата и время, использованные уязвимости, текущие параметры конфигурации системы.

Сбор образцов ВК. Все образцы ВК, тем или иным образом попавшие в систему, сохраняются в ней так, чтобы исключить возможность их исполнения, нарушения работы системы, взаимного влияния. В дальнейшем они передаются на сервер для их анализа дальнейшей классификации.

Анализ и обработка полученной информации. Вся собранная информация обрабатывается и сохраняется в специальной базе данных. На ее основе составляются отчеты о частоте инфицирования различными образцами ВК, о распределении различных образцов ВК по регионам и т.д. Образцы вредоносного кода же исследуются на вредоносный функционал, к примеру, с использованием так называемых сервисов sandbox (песочница), которые запускают ВК в некой специальной среде и регистрируют всю его вредоносную активность, впоследствии предоставляя отчет. В данном исследовании вопрос анализа собранного ВК является вторичным и подробно не рассматривается.

Требования к проектируемой системе

Исходя из решаемых задач и необходимости снижения влияния как фундаментальных, так и выявленных недостатков, проектируемая система должна отвечать следующим требованиям:

(1) расширяемость, модульная организация – система должна быть легко расширяема для внедрения новых уязвимостей (в том числе для различных платформ и ОС), новых возможностей по сбору и анализу ВК, дополнительному или служебному функционалу, что обеспечивает удобную и эффективную с ней работу, получение правдивой и актуальной информации. Модульная организация – наиболее адекватный способ организации подобной системы, так как позволяет легко конфигурировать систему под различные условия, делает ее более гибкой и универсальной, применимой к возможному расширению спектра решаемых задач;
(2) наличие виртуальной среды для хранения образцов ВК, защита от возможности их исполнения и взаимного влияния – одно из наиболее важных условий, так как от этого зависит функционирование всей системы;
(3) организация в соответствии с принципами клиент\сервер – необходим центр, куда поступала бы и где обрабатывалась бы вся собираемая информация. Также подобный централизованный узел необходим для управления всеми контролируемыми системами honeypot, их удаленного конфигурирования;
(4) обеспечение активности – по исследованиям различных антивирусных компаний, наибольшее количество ВК принадлежит к классу троянских программ, на втором месте выступают черви. В соответствии со способами проникновения данных типов ВК в систему была выявлена необходимость в обеспечении различного вида сетевой активности системой (посещение различных сайтов, использование почтовых клиентов, использование различных обменных сетей, irc-протокола) [5];

(5) защищенный канал между honeypot и сервером – вся информация между honeypot системой и сервером должна передаваться по защищенному каналу, во избежание ее перехвата и использования злоумышленниками;
(6) ограничение исходящего трафика – необходимо для пресечения возможного использования системы злоумышленниками в преступных целях.

Модель спроектированной системы

На основе поставленных задач и с учетом выявленных требований была построена модель системы, которая представлена на рисунке.

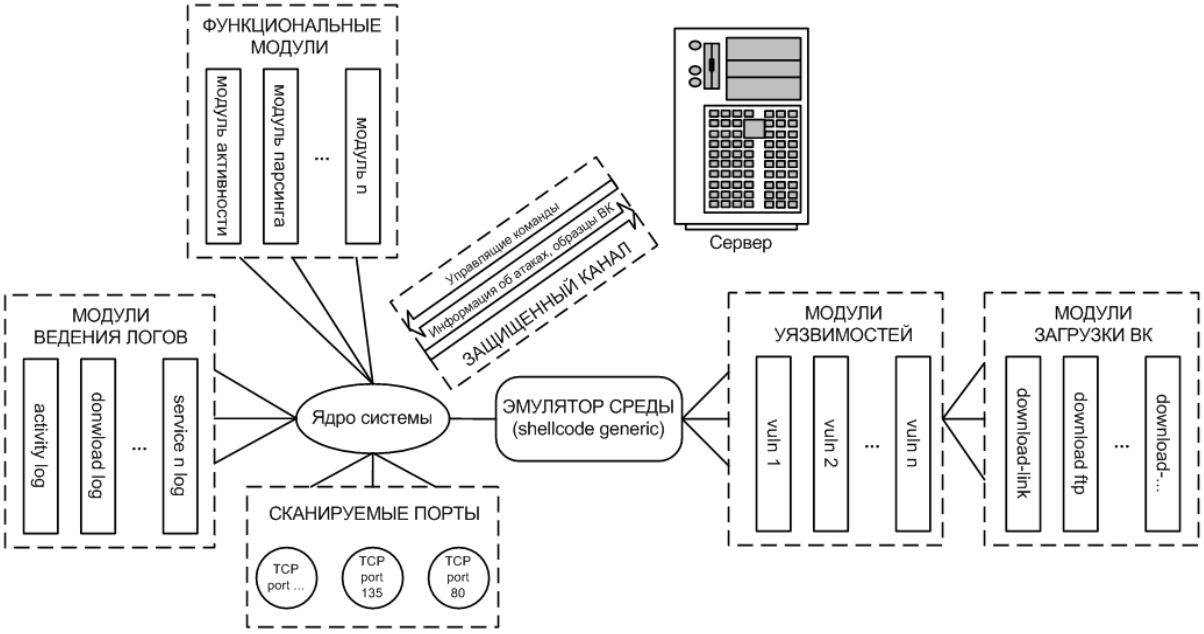


Рисунок. Модель спроектированной системы honeypot

Возможность реализации на основе существующих программных решений

Для оценки возможности реализации на основе существующих программных решений были выбраны 3 приложения: honeyd (http://www.honeyd.org/), nepenthes platform (http://www.mwcollect.org/), specter (http://www.specter.com), одно из которых является коммерческим (specter) [6]. Системы honeypot с высокой степенью интерактивности не рассматривались, так как они не отвечают требованию расширяемости и модульности.

Так как подробное сравнение этих продуктов потребовало бы написания отдельной статьи, в таблице приводится лишь соответствие рассматриваемых продуктов поставленным к системе требованиям.

Подводя итоги оценки, очевидно, что платформа Nepenthes отвечает всем поставленным требованиям и, кроме того, обладает наиболее богатым потенциалом и функциональными возможностями по сравнению с остальными. Кроме того, она в своих свойствах сочетает достоинства низко-интерактивных и высоко-интерактивных систем honeypot (при номинальном отношении к системам низкого уровня интерактивности), что и позволяет ей отвечать всем требованиям. Соответственно, платформа Nepenthes выбрана для дальнейшей реализации спроектированной системы [last].

Требования/Продукты	Specter	Nepenthes platform	Honeyd
расширяемость, модульная организация	+	+	+
наличие виртуальной среды для хранения образцов ВК, защита от исполнения, и взаимного влияния	-	+	-
организация в соответствии с принципами клиент\сервер	+	+	+
обеспечение активности	-	+	потенциально да
защищенный канал между honeypot и сервером	+	+	потенциально да
ограничение исходящего трафика	+	+	+

Таблица. Соответствие продуктов поставленным требованиям

Заключение

В результате исследования были проанализированы фундаментальные недостатки систем honeypot, выделены требования к проектируемой системе. Была спроектирована система пассивного сбора статистики об инфицировании ВК с учетом минимизации недостатков и в соответствии с поставленными требованиями. Произведена оценка возможности реализации модели спроектированной системы с помощью существующих программных решений на примере трех систем honeypot.

Непосредственная реализация будет выполнена в ходе дальнейшей работы.

Литература

1. Касперский Е. Вирусы и средства борьбы с ними – М., 2005
2. The Honeynet Project . – Режим доступа: http://www.honeynet.org
3. Developments of the Honeyd Virtual Honeypot. – Режим доступа: http://www.honeyd.org/
4. Nepenthes – finest collection. – Режим доступа: http://nepenthes.mwcollect.org
5. Лаборатория Касперского. – Режим доступа: http://www.viruslist.com/ru/analysis
6. Specter: Коммерческое Honeypot-решение для Windows. – Режим доступа: http://www.securitylab.ru/analytics/216274.php

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ МОДЕЛИ НА ОСНОВЕ ПОСТРОЕНИЯ ЦЕПЕЙ МАРКОВА ПРИ ПОИСКЕ СХОЖИХ ОБРАЗЦОВ ВРЕДОНОСНЫХ ПРОГРАММ

А.В. Клеймёнов, В.Д. Стремоухов
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Главной тенденцией в распространении вредоносного ПО становится криминализация Интернета. Это приводит к появлению схожих образцов вредоносного кода (ВК), в которые вносятся незначительные изменения лишь для сокрытия от новых записей в базах антивирусов. Кластеризация данных объектов может существенно повысить эффективность работы вирусных аналитиков. В данном исследовании приводятся теоретические основы построения модели поиска схожих вредоносных программ и экспериментальная проверка ее реализации на практике.

Введение

Изначально большинство вредоносных программ создавалось людьми, желающими проверить свои знания и практические навыки в области программирования. Поэтому при создании ВК использовались преимущественно языки низкого уровня: ассемблер, намного реже C. Однако времена изменились, и в настоящее время абсолютное большинство вредоносных программ создается с целью извлечения выгоды. В результате, по оценке Виталия Камлюка, 96% вредоносного кода является инструментом криминального бизнеса, направленного на кражу информации, рассылку спама, шантаж и атаки на ресурсы конкурентов [1]. Этому в немалой степени способствует ощущение собственной безопасности, связанное с тем, что доказать причастность того или иного человека к созданию вредоносного кода крайне тяжело. Согласно статистическим данным, очень малое количество подобных преступлений раскрывается ввиду того, что автора не могут своевременно выявить, и, в случае опасности, он успевает избавиться от улик [2].

Целью исследования является разработка универсального алгоритма определения автора конкретной вредоносной программы, основанного на формальной математической модели последовательности байтов кода как реализации цепи А.А. Маркова.

Теоретическое обоснование модели

Обозначим через A множество различных вариантов байтов. Пусть заданы n классов C_i, где i = 0, ..., n–1. В каждом классе C_i находятся последовательности $f_{i,j}$ O A, где j = 1, ..., m_i, т.е.

$$C_i = \{ f_{i,j} \mid j = 1,j,m_i\} \quad (1)$$

Наша задача состоит в том, чтобы отнести x ∩ A к одному из классов C_i.

Предположим, что последовательности байтов $f_{i,j}$ являются реализациями цепи Маркова с переходной матрицей P^i. Построим оценку P^i. Обозначим через $h_{i,j,kl}$ число переходов букв k–l в фрагменте $f_{i,j}$, положим

$$h_{i,kl} = \Sigma_j h_{i,j,kl} \qquad h_{i,k} = \Sigma_l h_{i,kl} \quad (2, 3)$$

Положим

$$P^i_{kl} = h_{i,kl}/h_{i,k} \quad (4)$$

Обозначим через Z_i множество таких упорядоченных пар (k,l), что $P^i_{kl} > 0$.

Предположим, что x также является реализацией цепи Маркова с матрицей переходных вероятностей P^q , где q – неизвестный параметр, который принимает одно из значений 1, ..., n.

Обозначим через $n_{k,l}$ число переходов k → l в x. Пусть также

$$n_k = \Sigma_l n_{k,l} \quad (5)$$

Обозначим через

$$L_i(x) = - \sum_{(k,l)} n_{k,l} \times \ln(n_{k,l} / (P^i_{kl} \times n_k)), \quad (6)$$

где сумма берется по парам $(k,l) \cap Z_i$. Грубо говоря, $L_i(x)$ равно минус логарифму вероятности x при условии, что x – реализация цепи Маркова с матрицей переходных вероятностей P^i. Назовем t(x) оценкой максимального правдоподобия для неизвестного параметра q [3, 4]:

$$t(x) = \mathrm{argmin}_{i = 0,\ldots,n-1} L_i(x). \quad (7)$$

Для проведения эксперимента были отобраны образцы вредоносных программ, с максимально высокой степенью вероятности созданных одним автором. Затем их объединили в группы по данному критерию. Важным условием для получения достоверных результатов является то, что все образцы должны быть написаны на одном языке программирования и созданы по возможности с использованием одного компилятора, чтобы уменьшить погрешность производимых вычислений.

Общие положения эксперимента

Цель эксперимента – проверка эффективности прикладного применения модели на основе использования цепей Маркова для анализа стиля написания различных программ.

Одна задача практически всегда может решаться несколькими путями. При написании программ выбор реализуемого алгоритма играет очень важную роль. От него зависит скорость, функциональность и надежность готовой программы. Использование определенных приемов программирования накладывает на код отпечаток его создателя.

Кроме того, огромную роль играет инструментарий, используемый автором. Различные компиляторы одного и того же языка программирования по-разному преобразуют программный код в машинный. Это достигается за счет использования различных алгоритмов оптимизации и интерпретации. Таким образом, компиляторы также оказывают свое влияние на структуру конечного исполняемого модуля. Данные особенности образуют в совокупности уникальный стиль, который может интерпретироваться как «почерк» программирования.

С целью проверки рассматриваемой модели на основе построения цепей Маркова была создана специальная программа. Основной функцией программы является поиск и отбор среди множества вредоносных программ, существующих в настоящий момент, образцов, имеющих схожий стиль написания.

Общий стиль указывает на 2 возможных варианта:

1) программы схожи по методу создания и выполняемым функциям,
2) код был написан одним человеком или группой людей.

В первом случае полученные данные позволяют заранее с большой долей вероятности утверждать, какие функции заложены в данную вредоносную программу, при условии, что известны функции схожих с ней вредоносных программ. Во втором случае полученная информация может быть неоценима для нахождения автора данной вредоносной программы, поскольку становится возможным построение круга подозреваемых.

Для проведения эксперимента необходимо некоторое количество вредоносных программ, с максимально большой долей вероятности принадлежащих одному автору. С целью их нахождения была создана программа, которая просканировала вирусную коллекцию кафедры БИТ университета СПбГУ ИТМО и выделила все частные e-mail’ы, повторяющиеся в нескольких различных ВК (рис. 1, 2). Затем вручную были отобраны образцы, созданные под одну платформу и на одном языке программирования. С целью повышения точности исследования предпочтение отдавалось ВК, создан-

ным при помощи одного компилятора. Данная мера точности является достаточной для того, чтобы считать, что данные программы написаны одним автором.

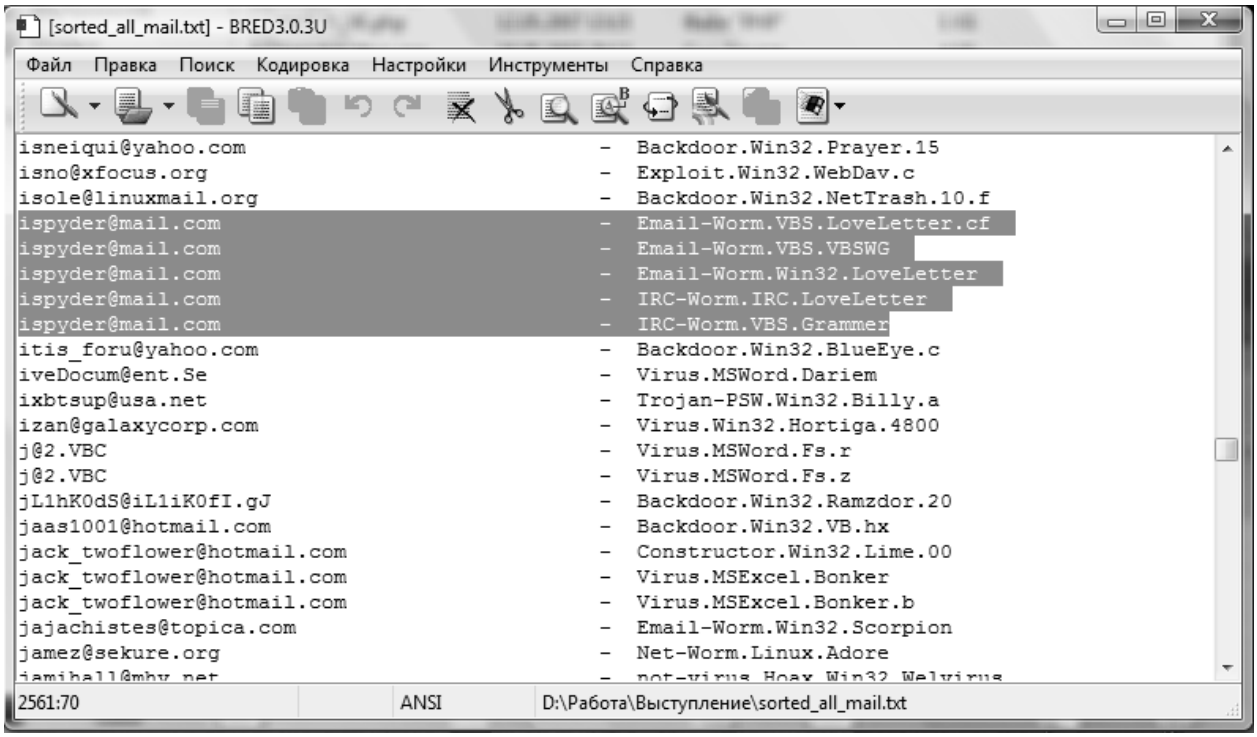


Рис. 1. Результат поиска ВК, принадлежащих одному автору

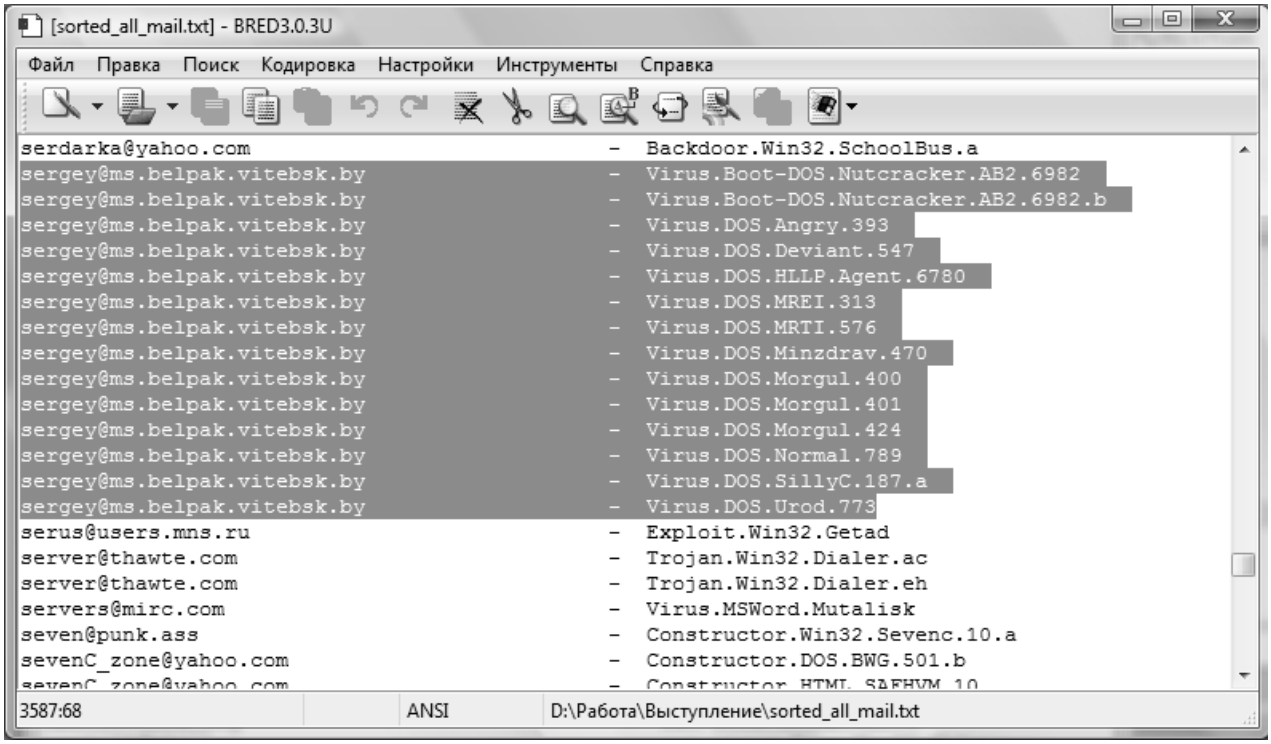


Рис. 2. Результат поиска ВК, принадлежащих одному автору

Для проведения эксперимента из группы вредоносных программ, созданных одним автором, отбирается один образец. Затем с помощью специально написанной программы сканируется вирусная коллекция с сайта ***.org. В ходе сканирования анали-

зируются только образцы, написанные под одну платформу, при этом отбор производится по маске в названии. Название вредоносных программ взято по классификации Лаборатории Касперского. В результате мы получаем список максимум из 10 программ, схожих по стилю написания с выбранным образцом. Эффективность модели можно оценить по тому, сколько программ, написанных этим же автором, было найдено в результате вычислений.

В ходе эксперимента анализировалась эффективность модели в случае применения к макровирусам, вредоносным программам под win32, как наиболее распространенным представителям вредоносного кода. Также было проведено дополнительное исследование вредоносного кода, созданного под операционную систему DOS.

Результаты исследований

Оценка эффективности для макровирусов, базирующихся на MSWord. В группу вредоносных программ, созданных одним автором, включены:

1) Virus.MSWord.Groovie.b,
2) Virus.MSWord.Melissa.bc,
3) Virus.MSWord.Nail.b,
4) Virus.MSWord.Natas.

В исходном коде данных образцов содержится значительное количество общих строк, доказывающих, что данные ВК имеют общего автора. Примеры:

manioc@innocent.com
szulevs@matavnet.hu

Кроме того, вредоносные программы содержат общие строки:

www.111sexstreet.com/private/sex02.html
www.Shockingpink.com/members/tina1.html
www.ultimatexxx.com/members42488/ L:tyle
www.18hardcore.com/secure/enter2.htm L:p
www.adultpleasures.com/members/ l:llll p
www.allasians1.com/membersonly/gallery/

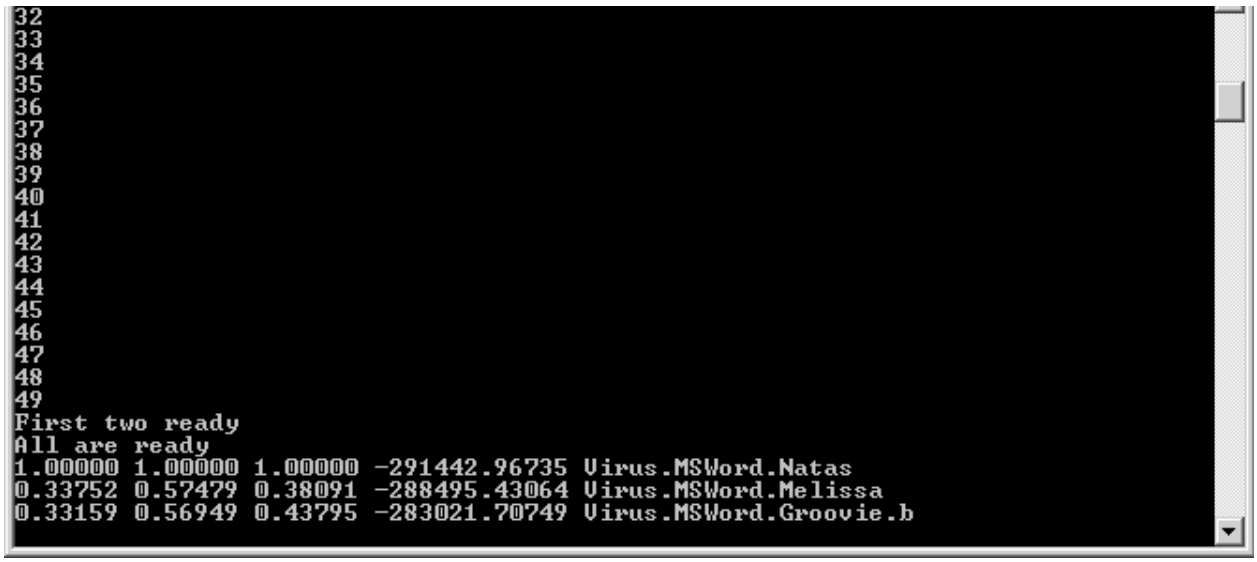


Рис. 3. Результат поиска макровирусов, базирующихся на MSWord

В результате работы исследуемая программа смогла вычислить 2 другие программы, достоверно созданные данным автором.

Оценка эффективности для вредоносных программ, созданных под платформу Win32. В группу вредоносных программ, созданных одним автором, включены:

1) Backdoor.Win32.HackTack.120.a
2) Backdoor.Win32.MoonPie.10
3) Backdoor.Win32.Y3KRat.15.b

В исходном коде данных образцов обнаружена общая строка:
www.dev-soft.comuFont.ColorclBlackFon

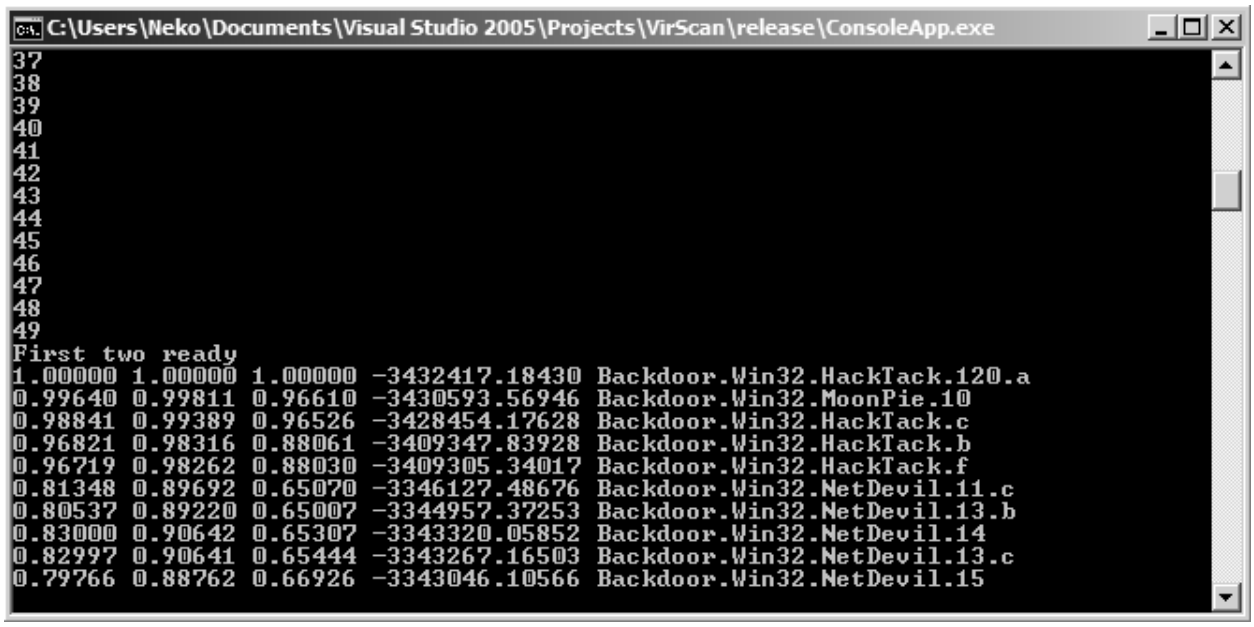


Рис. 4. Результат поиска ВК, базирующихся на Win32

В результате работы программы были найдены модификации анализируемого образца и еще одна программа, предположительно созданная данным программистом.

В ходе проверки программного кода вручную было выяснено, что серия вредоносных программ Backdoor.Win32.NetDevil также была создана данным автором. Доказательством является наличие во всех данных образцах общего e-mail'а

info@netmastersllc.com.

Таким образом, исследуемая утилита, реализующая модель на основе построения цепей Маркова, смогла зафиксировать образец, изначально даже не учтенный при обработке статистики.

Оценка эффективности для вредоносных программ, созданных под DOS. В группу вредоносных программ, созданных одним автором, включены:

1) Virus.DOS.Angry.393,
2) Virus.DOS.Deviant.547,
3) Virus.DOS.Minzdrav.470,
4) Virus.DOS.Morgul.400,
5) Virus.DOS.MREI.313,
6) Virus.DOS.MRTI.576,
7) Virus.DOS.Normal.789,
8) Virus.DOS.SillyC.187.a.

В исходном коде данных образцов был обнаружен общий e-mail:
sergey@ms.belpak.vitebsk.by

В результате вычислений из 10 найденных образцов вредоносных программ лишь один не принадлежит данному автору – **Virus.DOS.Asbo.335**.

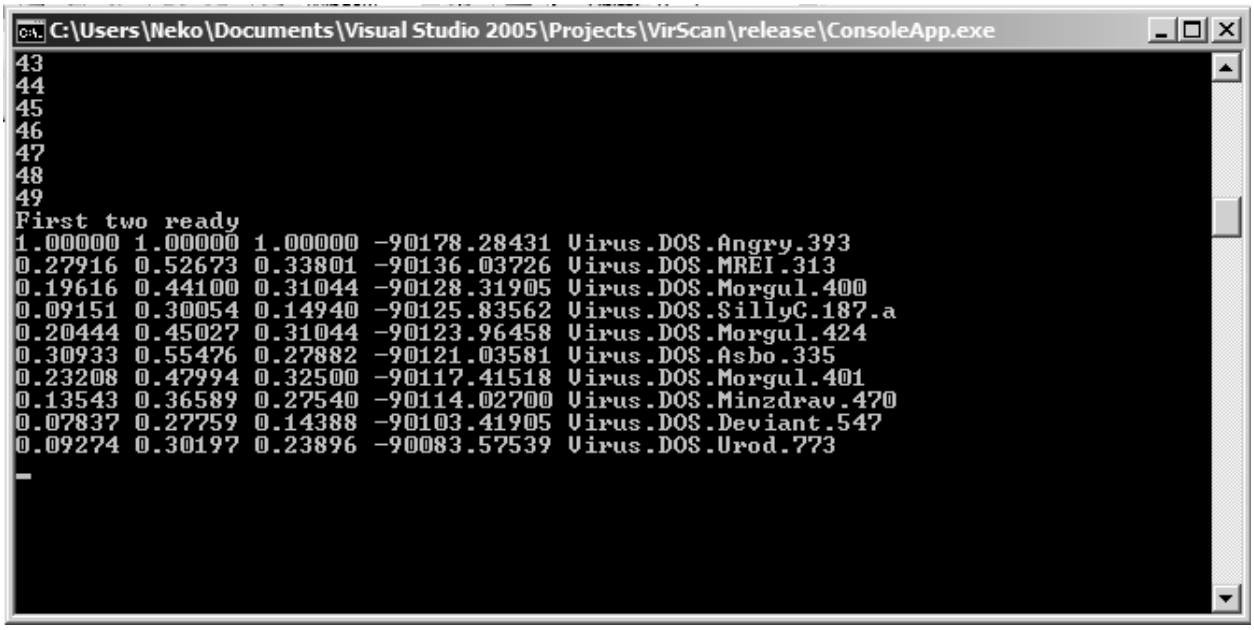


Рис. 5. Результат поиска ВК, базирующихся на DOS

Выделим преимущества предложенного метода.

- Оценка степени сходства каждого образца с исследуемым кодом.
- Применение нескольких различных алгоритмов, использование которых позволяет получить большую точность результатов.
- Значительные возможности для повышения эффективности за счет выделения различных анализируемых участков программного кода и диапазонов переходов байт.
- Реализация возможности расположения выбранных образцов по принципу их сходства с исследуемым кодом.

Заключение

Несмотря на спорность многих теоретических моментов в применении марковской модели для поиска схожих образцов исполняемого кода, серия экспериментов подтверждает эффективность ее применения на практике. Но, несмотря на довольно высокую точность определения общего авторства образцов ВК указанными алгоритмами, она не является достаточной, чтобы установленное ими заключение было неоспоримым доказательством. Анализ образцов исполняемого кода на предмет общего авторства имеет смысл только в случае, когда они написаны на одном языке и собраны одним и тем же компилятором. Примером практической реализации модели является разработка на ее основе дополнительного инструмента вирусного аналитика при детектировании подозрительных объектов. Данная программа позволит существенно ускорить поиск схожих образцов ВК в вирусной коллекции.

Литература

1. Шпунт Я. Угрозы в области информационной безопасности. – Режим доступа: http://www.crime-research.ru/analytics/threat07/
2. http://www.osnovi-bezopasnost.ru/about/clause/283/239726/
3. Хмелёв Д.В. Распознавание автора текста с использованием цепей А.А. Маркова //
4. Вестн. МГУ. – Сер. 9, Филология. – 2000. – № 02. – С. 115–126.
5. Кукушкина О.В., Поликарпов А.А., Хмелёв Д.В. Определение авторства текста с использованием буквенной и грамматической информации // Проблемы передачи информации. – 2001. – Т.37. – Вып.2 (апрель-июнь). – С. 96–108.

АДАПТИРУЕМАЯ МОДЕЛЬ ПОИСКА СХОЖИХ ОБРАЗЦОВ ВРЕДОНОСНОГО КОДА С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВЫХ СРЕДСТВ

А.В. Клеймёнов, В.Д. Стремоухов
Научный руководитель – д.т.н., профессор Г.Ф. Нестерук

Современное информационное общество все чаще сталкивается с проблемой распространения вредоносного кода (ВК). В борьбе с ним задействованы государственные структуры и коммерческие компании, занимающиеся проектированием программных и аппаратных СЗИ. В данном исследовании разрабатывается модель, позволяющая осуществлять автоматизированный поиск схожих образцов ВК и выбирать из конкретных подозреваемых наиболее вероятных авторов.

Введение

Борьба с вредоносным кодом является одной из наиболее приоритетных задач в современной информационной индустрии. В настоящее время отмечается резкое увеличение количества вирусных угроз. По данным «Лаборатории Касперского», в 2006 г. было зафиксировано появление 169 000 новых вредоносных программ, в 2007 г. данное значение увеличилось до 472 000 [1].

Согласно отчету CSI/FBI, в 2007 году потери от вирусов заняли второе место, уступив лишь потерям от финансового мошенничества [2].

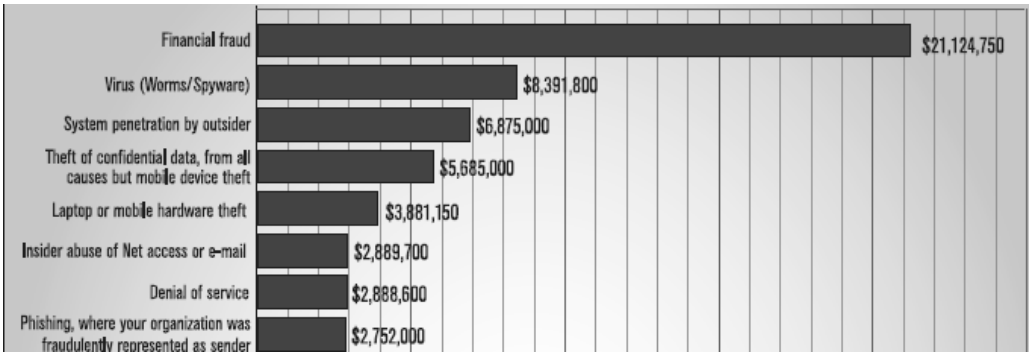


Рис. 1. CSI/FBI Computer Crime and Security Survey 2007

Целью данного исследования является реализация модели, позволяющей делать оценку сходства образцов вредоносного кода, построенной на основе применения сетей теории адаптивного резонанса (ART) [3–5].

Данная разработка позволит вирусным аналитикам затрачивать существенно меньше времени на анализ отдельного образца, поскольку более оперативно будут выявлены черты сходства анализируемого файла с детектированными ранее. За счет этого увеличится производительность и эффективность их работы. Модель способна успешно разрешать задачи разделения объектов на группы. Это позволит после соответствующего обучения осуществлять определение принадлежности исследуемого образца вредоносного кода одному из подозреваемых авторов.

Исследование проводится с использованием нейронной сети семейства ART-FANNC. Данный тип нейронных сетей выбран, поскольку он относится к классу обучающихся с учителем, и с высокой степенью точности решает задачи классификации объектов [1, 6, 7]. В следующей работе будет проведен практический эксперимент с использованием свободно распространяемой программной библиотеки FANNC, реализующей данный тип сетей, построенных на основе реализации метода обратного распространения ошибки.

Краткая теория используемых НС

Сети теории адаптивного резонанса [3–5] (Adaptive Resonance Theory Network, ART) применяются для кластеризации многомерных векторов. Главная особенность сетей ART – процесс обучения и эксплуатации НС не разделяются, т.е. сети ART представляют собой потоковые алгоритмы кластеризации с заранее не оговоренным числом кластеров.

Сеть FANNC предназначена для решения классификационных задач методом однопроходного инкрементного обучения. При появлении новых входных векторов не переобучают все категории НС. Сеть дообучают, вызывая либо изменение весов связи (параметрическая пластичность), либо локальную модификацию НС (структурная пластичность) путем добавления одного или двух нейронов (узлов) и соответствующих связей к уже существующей сети.

FANNC состоит из четырех слоев (рис. 1), в которой функция активации нейронов скрытых слоев представлена сигмоидой, а связи с гауссовыми весами соединяют узлы входного слоя с нейронами второго слоя НС. FANNC использует нейроны второго слоя для внутренней классификации входного вектора, а нейроны третьего слоя для внутренней классификации выходного вектора. Модификация связей между этими слоями осуществляется по методу обучения с учителем.

За исключением межнейронных связей между узлами первого и второго слоя, все связи – двунаправленные. Обратные связи передают ответные сигналы для реализации резонанса и соревнования нейронов и равны 1.

В начальный момент времени НС состоит только из входного и выходного слоев, число узлов в которых равно, соответственно, числу компонентов входного и выходного векторов. Число узлов в скрытых слоях равно нулю. При представлении новых данных FANNC добавляет нейроны в скрытые слои НС.

При представлении первого вектора FANNC добавляет два взаимосвязанных нейрона – один во второй и один в третий скрытые слои НС, веса прямых и обратных связей между которыми равны 1. Нейрон третьего слоя соединен со всеми выходными нейронами прямыми связями с весами, равными соответствующим компонентам выходного вектора, а веса обратных связей равны 1. Нейрон второго слоя соединен со всеми нейронами входного слоя с помощью гауссовых связей. Координаты центра образованного кластера (классификационной категории) равны соответствующим значениям компонентов входного вектора, а радиус кластера устанавливается в значение по умолчанию.

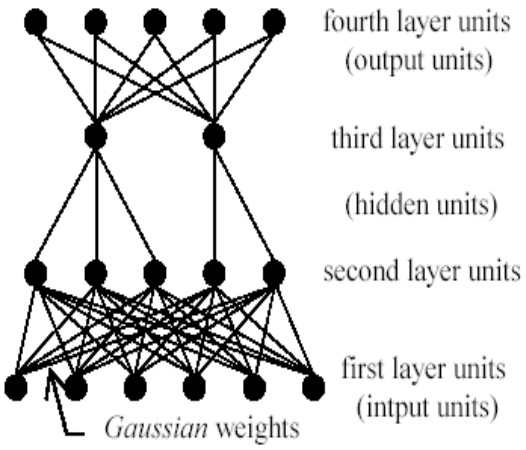


Рис. 2. Сеть FANNC

Входной вектор $A_k = (a_k^1, a_k^2, ..., a_k^n)$, k=1, 2, …, m, k – индекс входного вектора, образован из n координат. Входное значение для нейрона j второго слоя от нейрона i первого слоя равно

$$bIn_{ij} = e^{-(\frac{a_i^k - \theta_{ij}}{\alpha_{ij}})^2},$$

где θ_{ij} и α_{ij} – соответственно, центр и радиус кластера гауссова веса, соединяющего нейрон i с нейроном j.

Так как динамические свойства гауссова веса полностью определяются параметрами центра и радиуса кластера, то знания, получаемые во время обучения, могут быть запомнены в информационном поле НС путем модификации этих двух параметров [4].

Решаемые задачи

Поиск схожих с исследуемым файлом образцов ВК. Данная задача базируется на методе классификации произвольных объектов. Первоначально имеется один образец и массив объектов аналогичной природы. На его основе создаются 2 группы. В одну включаются объекты, имеющие черты сходства с рассматриваемым образцом, в другую – не имеющие. В качестве объектов в данном случае выступает вредоносный код.

Для реализации данной задачи предлагается использовать сеть FANNC**.** Исходные данные преобразуются к виду, в котором их можно подать на входы сети. В исследовании рассматривается аналоговая нейронная сеть, использующая информацию в форме действительных чисел. Каждая запись в файле данных называется обучающей парой или обучающим вектором. Обучающий вектор содержит по одному значению на каждый вход сети. При обучении на входы сети идут присутствующие и отсутствующие признаки образца, при использовании – только присутствующие [9].

При обучении сети предлагаются различные образцы с указанием того, к какому классу они относятся. Образец, как правило, представляется как вектор из его признаков. При этом совокупность всех признаков должна однозначно определять класс, к которому относится образец. По окончании обучения сети можно предъявлять неизвестные ей ранее образы и получать от нее ответ о принадлежности к определенному классу. Топология такой сети характеризуется тем, что количество нейронов в выходном слое равно количеству определяемых классов. При этом устанавливается соответствие между выходом нейронной сети и классом, который он представляет [7, 8].

С целью проверки модели необходим набор образцов ВК, созданных тем же автором, что и исследуемый файл. Поиск данных образцов осуществлялся по следующему алгоритму:

1) В образце выявляются признаки, характеризующие автора. В данном случае в качестве искомых признаков выступают почтовый ящик создателя ВК и его ник.
2) В коде образцов ВК вирусной коллекции кафедры СПбГУ ИТМО БИТ осуществляется поиск данных признаков. Поиск осуществляется специально созданной программой, одновременно выполняющей функции кластеризации найденных файлов.
3) Над найденными образцами выполняется полная проверка на степень сходства с исследуемым образцом. Признаками сходства служат:
   а) язык программирования
   б) используемый компилятор
   в) наличие характеризующих одинаковых блоков кода в сегменте данных

В результате проведенных действий можно утверждать, что найденные образцы ВК с максимальной вероятностью созданы одним автором, следовательно, имеют черты сходства.

Для создания обучающих пар взяты присутствующие и отсутствующие признаки рассматриваемого ВК. В качестве признаков, подаваемых на входы нейронной сети, выступают следующие характеристики файла:

1) Степень сходства сжимаемости
   - заголовка,
   - секции кода,
   - секции данных.
2) Частоты встречаемости последовательностей байт, реализующих команды:
   - условного перехода,
   - безусловного перехода,
   - циклов,
   - обнуления регистра EAX,
   - передача данных парой команд lods/stos.

В данном случае рассматривается частота встречаемости опкодов данных команд на единицу объема информации, содержащейся в сегменте кода образца.

На основе данных значений создается обучающая выборка, по которой осуществляется обучение сети FANNC. После этого сеть становится пригодной для выделения групп схожих с исследуемым объектом образцов ВК. Оценка эффективности модели определяется, исходя из количества истинно схожих ВК, выделенных обученной НС из группы посторонних файлов.

Выбор автора конкретного вредоносного кода из группы подозреваемых на основе анализа их программных разработок. Данная задача решается методом классификации объектов. Обозначим через А множество объектов. Пусть заданы n классов C_i, где $i = 0, ..., n\text{-}1$. В качестве классов в нашем случае выступают программисты, подозреваемые в создании данного ВК. Также задается пустой класс, который не ставится в соответствие какому-либо человеку. Он необходим для выделения файлов, не принадлежащих ни одному из подозреваемых авторов. Наша задача состоит в том, чтобы отнести объект $x \in A$ к одному из классов C_i

Для создания обучающих выборок используются программные разработки подозреваемых авторов. С целью повышения эффективности вычислений необходимо, чтобы все программы были написаны на одном языке программирования и собраны с помощью одного компилятора, сходного с использованным при создании образца.

В качестве признаков файлов, подаваемых на вход НС, выступают характеристики файла, используемые в предыдущем исследовании. На выходе располагаются подозреваемые авторы. Задача нейронной сети – после соответствующего обучения на образцах каждого из авторов верно распределять другие созданные ими программы.

С целью проверки эффективности модели после завершения разработки ее программной реализации будет проведен практический эксперимент. Из каждой группы образцов ВК, найденных в результате реализации действий, описанных в предыдущей задаче, выбирается произвольный объект. Остальные объединяются в группу, на основе которых происходит обучение НС. Оценка эффективности модели определяется, исходя из количества верно соотнесенных с истинными авторами образцов ВК.

Интерес также представляет задача кластеризации вредоносных объектов. Под кластеризацией понимается разбиение множества входных сигналов на классы, притом, что ни количество, ни признаки классов заранее не известны. После обучения такая сеть способна определять, к какому классу относится входной сигнал. Сеть также может сигнализировать о том, что входной сигнал не относится ни к одному из выделенных классов – это является признаком новых, отсутствующих в обучающей выборке, данных. Таким образом, подобная сеть *может выявлять новые, неизвестные ранее классы сигналов*. Соответствие между классами, выделенными сетью, и классами, существующими в предметной области, устанавливается человеком [7].

Развитие данного алгоритма позволит создать программу, разбивающую все вредоносные объекты на классы, обусловленные спецификой их кода и, как следствие, выполняемыми функциями. Это существенно повысит эффективность труда вирусных аналитиков, поскольку позволит сразу работать со схожими образцами и скорее выявлять их вредоносный потенциал по методу аналогий.

Данное направление будет подробно рассмотрено в следующих публикациях.

Заключение

В исследовании приводятся основные теоретические аспекты разработки модели поиска схожих образцов ВК с использованием НС. К ее преимуществам относятся широкая сфера применения и возможность дальнейшего наращивания эффективности за счет выделения различных диапазонов рассматриваемых байт, а также отдельных участков сканируемого кода. Производительность данной модели на практике будет оценена в серии последующих экспериментов.

Литература

1. Чем ответит Россия на киберугрозы? – Режим доступа: http://www.cnews.ru/reviews/index.shtml?2008/02/12/287829
2. Computer Security Institute. – Режим доступа: http://www.gocsi.com
3. Carpenter G.A., Grossberg S., Reynolds J.H. ARTMAP: Supervised real-time learning and classification of nonstationary data by a self-organizing neural network. // Neural Networks. – 1991. – №4. –P. 565–588.
4. Zhou Z., Chen S., Chen Z. FANNC: A Fast Adaptive Neural Network Classifier. // Knowledge and Information Systems. – 2000. – №2. – P. 115–129.
5. Carpenter G. A., Grossberg S., Rosen D. B. Fuzzy ART: Fast stable learning and categorization of analog patterns by an adaptive resonance system. // Neural Networks. – 1991. – №4. – P. 759–771.
6. Нестерук Ф.Г., Молдовян А.А., Нестерук Г.Ф., Нестерук Л.Г. Квазилогические нейронечеткие сети для решения задачи классификации в системах защиты информациии // Вопросы защиты информации. – 2007. – № 1. – С. 23 – 31.
7. 2007 CSI/FBI Computer Crime and Security Survey
8. Искусственная_нейронная_сеть – Режим доступа: http://ru.wikipedia.org/wiki/Искусственная_нейронная_сеть
9. Обучение_с_учителем – Режим доступа: http://ru.wikipedia.org/wiki/Обучение_с_учителем
10. Нейронные сети. – Режим доступа: http://www.intuit.ru/department/ds/neuronnets/

НАШИ АВТОРЫ

Аверкин Антон Нилович – студент кафедры компьютерной фотоники
Агеев Александр Юрьевич – студент кафедры информационных систем
Андреева Наталья Викторовна – аспирант кафедры безопасных информационных технологий
Антонов Олег Николаевич – студент кафедры компьютерной фотоники
Арефьев Дмитрий Борисович – аспирант кафедры безопасных информационных технологий
Ахмадеева Алина Альбертовна – студент кафедры технологий профессионального обучения
Безгодов Евгений Викторович – аспирант кафедры безопасных информационных технологий
Береговой Михаил Викторович – аспирант кафедры безопасных информационных технологий
Будько Михаил Юрьевич – аспирант кафедры мониторинга и прогнозирования чрезвычайных ситуаций
Булгакова Вера Геннадьевна – студент кафедры фотоники и оптоинформатики
Верещагин Владимир Леонидович – аспирант кафедры безопасных информационных технологий
Волынский Максим Александрович – студент кафедры компьютерной фотоники
Галанов Алексей Игоревич – аспирант кафедры безопасных информационных технологий
Головков Иван Викторович – аспирант кафедры безопасных информационных технологий
Гордеева Наталья Олеговна – аспирант кафедры технологий профессионального обучения
Григорьева Мария Владимировна – аспирант кафедры безопасных информационных технологий
Громова Юлия Александровна – студент кафедры фотоники и оптоинформатики
Гусарова Дарья Алексеевна – аспирант кафедры безопасных информационных технологий
Дементьева Юлия Сергеевна – аспирант кафедры лазерных технологий и экологического приборостроения
Дроздов Аркадий Анатольевич – студент кафедры фотоники и оптоинформатики
Дроздова Дарья Валентиновна – ассистент кафедры технологий профессионального обучения
Дудина Татьяна Федоровна – аспирант кафедры компьютерной фотоники
Журкин Игорь Валерьевич – студент кафедры технологий профессионального обучения
Задорожная Екатерина Ивановна – студент кафедры фотоники и оптоинформатики
Захаревич Мария Вячеславовна – студент кафедры технологий профессионального обучения
Зеленская Ольга Витальевна – аспирант кафедры технологий профессионального обучения
Златов Андрей Сергеевич – студент кафедры оптоинформационных технологий и материалов
Иващук Ирина Юрьевна – аспирант кафедры безопасных информационных технологий

Калашникова Алиса Александровна – студент кафедры безопасных информационных технологий
Калинин Даниил Алексеевич – студент кафедры безопасных информационных технологий
Киреев Дмитрий Геннадьевич – студент кафедры технологий профессионального обучения
Киселёв Станислав Сергеевич – студент кафедры оптоинформационных технологий и материалов
Клеймёнов Алексей Владимирович – студент кафедры безопасных информационных технологий
Козьмина Евгения Андреевна – студентка кафедры технологий профессионального обучения
Кононенко Михаил Евгеньевич – студент кафедры фотоники и оптоинформатики
Коробовский Илья Андреевич – студент кафедры безопасных информационных технологий
Костин Игорь Алексеевич – студент факультета среднего профессионального образования
Котелкова Галина Олеговна – аспирант кафедры технологий профессионального обучения
Котенко Денис Алексеевич – аспирант кафедры безопасных информационных технологий
Котов Владимир Владимирович – студент факультета среднего профессионального образования
Кувшинов Виктор Андреевич – студент факультета среднего профессионального образования
Кузьмин Кирилл Андреевич – студент кафедры технологий профессионального обучения
Кулешов Антон Анатольевич – студент кафедры фотоники и оптоинформатики
Ларионов Илья Андреевич – аспирант кафедры безопасных информационных технологий
Левин Петр Вадимович – студент кафедры технологий профессионального обучения
Лесничий Василий Валерьевич – студент кафедры фотоники и оптоинформатики
Малов Андрей Михайлович – аспирант кафедры компьютерной фотоники
Новиков Василий Викторович – студент факультета среднего профессионального образования
Павлова Анна Алексеевна – аспирант кафедры технологий профессионального обучения
Пантась Ярослав Сергеевич – студент кафедры оптического материаловедения
Пишко Анна Юрьевна – аспирант кафедры экологического приборостроения и мониторинга
Поршнев Ярослав Игоревич – аспирант кафедры физики
Потапов Алексей Сергеевич – докторант кафедры компьютерной фотоники
Пугач Павел Александрович – студент кафедры безопасных информационных технологий
Разумовский Андрей Владимирович – аспирант кафедры безопасных информационных технологий
Сандуленко Александр Витальевич – соискатель кафедры оптического материаловедения
Спивак Антон Игоревич – аспирант кафедры безопасных информационных технологий
Степанова Екатерина Владимировна – студент кафедры компьютерной фотоники

Стремоухов Всеволод Дмитриевич – студент кафедры безопасных информационных технологий
Янковская Анастасия Александровна – студент кафедры безопасных информационных технологий
Сугракшиева Мария Гамбуцириновна – кафедра оптического материаловедения
Сулейманов Данис Фанисович – аспирант кафедры физики
Тишкин Виталий Олегович – студент кафедры фотоники и оптоинформатики
Торшенко Юлия Александровна – аспирант кафедры безопасных информационных технологий
Царев Михаил Николаевич – студент кафедры компьютерных технологий
Царев Федор Николаевич – студент кафедры компьютерных технологий
Цыпкин Антон Николаевич – студент кафедры фотоники и оптоинформатики
Черемушкин Дмитрий Владимирович – аспирант кафедры безопасных информационных технологий
Шекланова Елизавета Борисовна – студент кафедры компьютерной фотоники
Шустиков Сергей Вячеславович – аспирант кафедры безопасных информационных технологий

СОДЕРЖАНИЕ

Научно-технический вестник СПбГУ ИТМО. Выпуск 52. **ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ** / Главный редактор д.т.н., проф. В.О. Никифоров. – СПб: СПбГУ ИТМО, 2008. – 312 с.

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК СПбГУ ИТМО
Выпуск 52
ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Главный редактор
доктор технических наук, профессор
В.О. Никифоров
Дизайн обложки В.А. Петров, А.А. Колокольников
Редакционно-издательский отдел СПбГУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99.
Подписано в печать 10.04.08.
Заказ 1192. Тираж 100 экз.