

2. Гак В. Г. Сравнительная типология французского и русского языков. М., 1977.
3. Даль В. И. Толковый словарь живого великорусского языка: В 4-х т. – СПб., 1863-1866
4. Карасик В.И. Языковой круг: личность, концепты, дискурс / В.И. Карасик. – Волгоград: Перемена, 2002.
5. Фреге Г. Логика и логическая семантика: Сборник научных трудов / М.: Аспект Пресс, 2000, 512 с.
6. Larousse Dictionnaire de la langue française, Paris : Editions Larousse 2010

*Глазырина А.И.
УрГПУ, г. Екатеринбург, Россия*

**КОМПОНЕНТНЫЙ АНАЛИЗ СПЕЦИАЛЬНЫХ ЕДИНИЦ
С СУФФИКСОМ *-WARE* ПРЕДМЕТНОЙ ОБЛАСТИ
«ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ»
(НА МАТЕРИАЛЕ АНГЛИЙСКОГО И РУССКОГО
КОМПЬЮТЕРНЫХ ПОДЪЯЗЫКОВ)**

Abstract. The article is dedicated to the comparative componential analysis of special units of English and Russian computer sublanguages (LSP) with suffix *-ware* which constitute the subject subfield «Malware».

Лингвистика XXI, прирастая новыми знаниями из смежных и «отдаленных» наук, все чаще оглядывается назад, на достижения предыдущих веков. Ориентиром в сегодняшних исследованиях по лингвистической семантике все так же остается метод компонентного анализа, разработанный в 50-е года XX века. В частности, еще Эмиль Бенвенист призывал ученых «анализировать язык в рамках его собственных формальных элементов» [Бенвенист 1997: 23].

В конце XX столетия компонентный анализ перестал быть лишь приемом системно-структурного метода (см. трактовку С.В. Черновой процедуры компонентного анализа в качестве приема), превратившись действительно в метод лингвистического исследования, поскольку стал применяться и в других лингвистических парадигмах (см. работы А. М. Кузнецова, Е.Г. Беляевской и др.).

Настоящая статья посвящена сопоставительному анализу специальных единиц английского и русского компьютерного подъязыка с суффиксом *-ware* предметной подобласти «Malware (вредоносное ПО (программное обеспечение))» [АРСОЛ; АРТСТС].

На сегодняшний день под компьютерным подъязыком все чаще понимают триаду компьютерный термин – профессионализм – жаргонизм. В статье предпринимается попытка ответить на следующие вопросы: остались ли «чистые» лингвистические

методы? Что представляет компонентный анализ терминологического значения?

Возможно ли четко сформулировать (дать наименование) семам компьютерного подъязыка даже на материале этой предметной подобласти?

Суффикс *-ware* обозначает тип программного обеспечения, компьютерных программ [OD 2005] и является крайне продуктивным для образования терминов и специальных единиц в английском компьютерном подъязыке.

Исходя из принципа определения концептосферы исследуемой предметной области, следует различать предметную подобласть «Компьютерные программы» и предметную подобласть «Программное обеспечение» (см. данные на сайте www.glossary.ru).

В английском компьютерном подъязыке насчитывается 87 однокомпонентных специальных единиц с суффиксом *-ware*.

Наиболее полный список, 73 единицы (84 %), содержится в Википедии (Wikipedia): *abandonware, adware, annoyware, badware (bad software), baitware, beerware, begware, betaware, bloatware, brochureware, careware, charityware, crapware, crimeware, crippleware, crudware, cyberware, demoware, donationware, dreamware, dribbleware, emailware, fatware, firmware, foistware, fraudware, freeware, fritterware, garbageware, greenware, greyware (grayware), groupware, guiltware, hijackware, liveware, malware, meatware, middleware, moralityware, muffinware, nagware, otherware, parasiteware, payware, postcardware, prayerware, ransomware, riskware, rogueware, scareware, scamware, shareware, shelfware, shitware, shovelware, spyware, stealware, testware, trackware, trialware, vaporware, wetware, warez*.

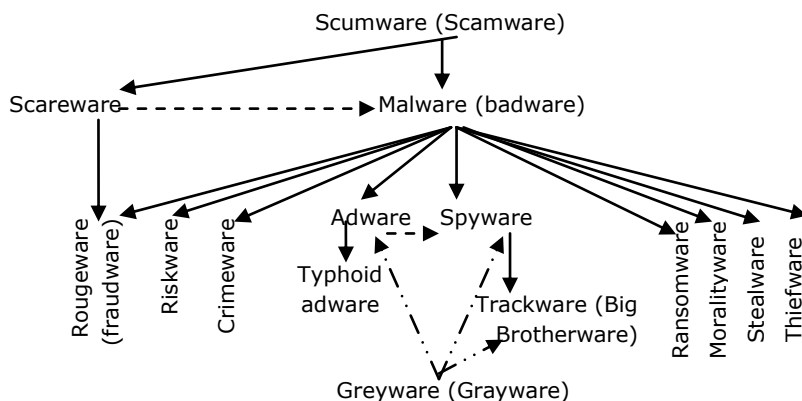
16 % содержатся в других источниках (14 единиц): *bannerware, Big Brotherware, coasterware, comfortware, dicware, giftware, hostware, psychedellicware, rightware, romware, teamware, teachware, telesoftware*.

В нашу предметную подобласть также входят 2 двухкомпонентные специальные единицы – *Big Brotherware* (аллюзия к роману Дж. Оруэлла «1984» представляется очевидной, русский эквивалент отсутствует) и *typhoid adware* («тифозный» бесплатный программный продукт с размещенной в нём рекламой [Здесь и далее перевод мой. - А.Г.]).

Энциклопедия Википедия (Wikipedia), один из ярчайших примеров реализации проекта Web 2.0, предлагает следующую классификацию Scumware (Scamware) («жульнического» программного обеспечения) [<http://blog.immunet.com/blog/tag/scamware>]: *scareware* (русский эквивалент в настоящее время отсутствует, образуя лакуну) и *malware* (вредоносное ПО).

Группа Scumware (Scamware) представлена 19 единицами. Представим взаимосвязи данных единиц на рисунке 1. Пунктиром обозначены отношения гипонимии, стрелка указывает на гипероним.

Рисунок 1



Перейдем к описанию данных, приведенных на рисунке 1.

Группа Malware включает подгруппу «Malware for profit (вредоносное ПО для получения выгоды)», куда входят такие единицы, как *adware*, *ransomware* (программа-вымогатель), *scareware*, *spyware* (шпионское (шпиониющее) ПО) [АРТСТС].

Группа Scareware не содержит подгрупп. Данная группа входит в качестве подгруппы в группу Malware.

Подгруппа содержит лишь две синонимичные специальные единицы – *fraudware* и *rougeware*¹.

Подгруппы Adware, Spyware и Trackware (ПО отслеживания предпочтений) [АРТСТС] объединены в группу Greyware (Grayware). Под специальной единицей *greyware* (*grayware*) обычно понимается «"серое" ПО, вредоносные программы, попадающие в "серую зону" между обычным ПО и вирусами. К этой категории относятся такие опасные и/или надоедливые программы², как *adware*, *spyware*, *trackware* и многие другие» [АРТСТС]. Подгруппа Spyware включает Trackware.

Подгруппа Adware (тж. *advertising-supported software*, зачастую имеет в виду «dishonest adware» (мошеннический бесплатный программный продукт с размещенной в нём рекламой [<http://en.wikipedia.org/wiki/Malware>]) включает подвид *typhoid adware*.

Особняком стоят такие подгруппы, как Riskware (потенциально опасное ПО, потенциально опасные (невирусные) приложения) [АРТСТС], Crimeware (мошенническое ПО) [<http://translate.google.ru>],

¹ *rougeware* - мошенническое ПО [<http://translate.google.ru>].

² В рамках данной статьи мы намеренно не рассматриваем группу *adware* (надоедливые условно-бесплатные программы) в виду ее многочисленности.

Moralityware (русский эквивалент отсутствует)³, Ransomware (программа-вымогатель) [<http://ru.wikipedia.org/wiki/Ransomware>], Stealware (компьютерные воры) [<http://shelbydap.wgz.cz/babylon>] и Thiefware (русский эквивалент отсутствует). Возможно, их можно объединить в подгруппу под названием privacy-invasive software (ПО, нарушающее конфиденциальность информации) [http://en.wikipedia.org/wiki/Privacy-invasive_software].

В результате компонентного анализа специальных единиц предметной области «Вредоносное программное обеспечение» было выявлено 78 сем, которые подразделяются на четыре неравномерные группы. Перечислим их в таблице 1.

Таблица 1

№	Группа сем	Номера сем
1	Нейтральные семы	2, 6, 8, 15, 34, 46, 53, 57, 60, 61, 62, 63, 65, 66, 67, 74
2	Семы, относящиеся к рекламной деятельности	5, 10, 11, 14, 58 ⁴ , 68
3	Семы, описывающие действия негативного характера, направленные на пользователя или компьютерную систему	1, 7, 9, 13, 17, 18, 19, 20, 21, 22, 27, 28, 29, 30, 31, 33, 36, 37, 39, 40, 43, 44, 45, 47, 48, 49, 50, 51, 52, 54, 55, 56, 58, 59, 64, 69, 71, 72, 73, 77, 78
4	Семы, описывающие действия потенциально негативного характера, направленные на пользователя или компьютерную систему	16, 24, 75, 76
5	Семы, описывающие отрицательные характеристики	3, 4, 12, 23, 25, 26, 32, 35, 38, 41, 42, 70

Целесообразно в самом начале перечислить те специальные единицы, до сих пор не имеющих зафиксированных определений: *Big Brotherware, fraudware, scamware, scamware, thiefware, trackware*.

Перейдем к единицам, имеющим определения, зафиксированные в специальных толковых словарях и энциклопедических изданиях. Начнем с понятия *rogueware*: «*a form of Internet fraud using computer malware (malicious software) that deceives or misleads users*

³ См. пример <http://www.eweek.com/c/a/Security/KoranSpouting-Trojan-Is-First-Example-of-Moralityware/>.

⁴ Сема 'Получение прибыли разработчиками данной программы за счет демонстрации рекламных сообщений' может быть одновременно отнесена как ко второй, так и к третьей группе сем.

into paying for fake or simulated removal of malware or that installs other malware» [http://en.wikipedia.org/wiki/Rogue_security_software]: (форма Интернет-мошенничества с использованием вредоносного программного обеспечения, которая обманывает пользователя или вводит его в заблуждение, в результате которого последний оплачивает поддельное/мнимое удаление вредоносного ПО или устанавливает другое вредоносное ПО). Русскоязычные определения даже не в специальных толковых словарях пока отсутствуют.

Как показывает компонентный анализ, несмотря на наличие суффикса *-ware*, данная специальная единица обозначает не вид программного обеспечения, а вид (категорию) преступления.

Единица *crimeware* была намеренно создана Питером Кэссиди (Peter Cassidy), генеральным секретарем Антифишинговой рабочей группы (Anti-Phishing Working Group, APWG) и имеет следующее определение: «a class of malware designed specifically to automate cybercrime» (ПО, разработанное специально для автоматизации сетевых преступлений) [<http://en.wikipedia.org/wiki/Crimeware>]. В русскоязычной Википедии *crimeware* определяется следующим образом: «класс вредоносных программ, специально созданный для автоматизации финансовых преступлений» [http://ru.wikipedia.org/wiki/DBвредоносная_программа].

В русскоязычном определении преступные намерения ограничены сферой финансов.

Несомненную опасность, особенно для пользователей русскоязычных сайтов на территории бывшего Советского Союза, представляет *ransomware* [<http://ru.wikipedia.org/wiki/Ransomware>].

В широком смысле под *ransomware* понимают «software that is released as open source only in exchange for payment» (ПО, предоставляющее исходный код только за вознаграждение) [<http://en.wikipedia.org/wiki/Ransomware>]; в узком – «computer malware which holds a computer system, or the data it contains, hostage against its user by demanding a ransom for its restoration» (вид вредоносного ПО, блокирующего компьютерную систему и данные от пользователя, требуя взамен выкуп за восстановление системы) [[http://en.wikipedia.org/wiki/Ransomware_\(malware\)](http://en.wikipedia.org/wiki/Ransomware_(malware))]. Русскоязычные определения даже не в специальных толковых словарях пока отсутствуют.

Под *stealware* имеют в виду «a type of software that effectively transfers money owed to a website owner to a third party» (вид ПО, эффективно переводящего деньги, предназначенные владельцу сайта, третьей стороне) [<http://en.wikipedia.org/wiki/Stealware>]. В статье англоязычной Википедии, посвященной шпионскому (шпионящему) ПО, находим следующее определение *stealware*: «diverts the payment of affiliate marketing revenues from the legitimate affiliate to the spyware vendor» (направляет платежи легальной дочерней структуры продавцу шпионского ПО) [<http://en.wikipedia.org/wiki/Spyware>].

Таблица 2

Сема	Энциклопедии	Wiki 2012 (stealware)	Wiki 2012 (spyware)
'Вредоносное ПО' (8) ⁵		+	-
'Незаконный перевод денег третьей стороне' (33)		+	+
'Платежи легальной дочерней структуры' (53)		-	+

Две семы (8, 53) относятся к нейтральным, сема 'Незаконный перевод денег третьей стороне' (3) – к третьей, самой многочисленной группе сем. Русские определения отсутствуют, определение, данное в статье-гиперониме, конкретизирует «третью сторону» (*the payment of affiliate marketing revenues from the legitimate affiliate*).

Moralityware есть ни что иное, как «*a subset of malware which infects a PC with the intention of imposing morality upon the user (for example, by blocking pornographic websites)*» (вредоносное ПО, заражающее персональный компьютер и пытающееся навязать пользователю моральные принципы (например, блокируя порнографические сайты) [<http://en.wikipedia.org/wiki/Moralityware>]).

Русскоязычные определения данной единицы отсутствуют даже в неспециальных толковых словарях.

Таблица 3

Сема	Единица компьютерного подъязыка				
	<i>crimeware</i>	<i>stealware</i>	<i>ransomware</i>	<i>rogueware</i>	<i>moralityware</i>
'Вредоносное ПО' (8)	+	+	+	-	+
'Преступные намерения в сфере финансов' (62)	+	+	-	-	-
'Автоматизация преступных намерений в сети Интернет' (1)	+	+	-	-	-
'Перевод денежных средств третьей стороне' (47)	-	+	-	-	-
'Заражение компьютера' (18)	-	-	-	-	+
'Навязывание нравственного поведения' (24)	-	-	-	-	+

⁵ В круглых указан номер семы в алфавитном всех 78 рассматриваемых в данной статье сем.

'Восстановление компьютерной системы после уплаты выкупа'(7)	-	-	+	-	-
'Удержание компьютерной системы или хранящихся в ней данных в качестве «заложников»'(77)	-	-	+	-	-
'Форма Интернет-мошенничества'(78)	-	-	-	+	-
'С использованием вредоносного ПО'(69)	-	-	-	+	-
'Обман или введение в заблуждение с целью оплаты поддельного/мнимого удаления вредоносного ПО или установка другого вредоносного ПО'(40)	-	-	-	+	-

Две семы (8, 62) относятся к нейтральным, сема 'Навязывание нравственного поведения' (24) – к семам, описывающим действия потенциально негативного характера, направленные на пользователя или компьютерную систему, подавляющее большинство (1, 7, 18, 40, 47, 69, 77, 78) – к семам, описывающим действия негативного характера, направленные на пользователя или компьютерную систему.

Особняком стоит понятие *riskware*, которое по своей сути является потенциально опасным ПО. Обратимся к определению *riskware*, которое также содержит описание, включающее его существенные признаки: «*computer software, which actually was not programmed and intended as malware, but has security critical functions. These functions can be used to start or stop computer processes or computer services. Riskware can also be defined as potentially dangerous software*» (ПО, изначально разработанное не как зловредное, но являющееся критическими для безопасности. Эти функции могут использоваться для запуска или остановки работы компьютера. Невирусные приложения можно также определить как потенциально опасное ПО) [<http://en.wikipedia.org/wiki/Riskware>]. Приведем русскоязычное определение, взятое из специализированного словаря: «программное обеспечение, которое при некоторых условиях может стать чревато потенциальными опасностями (рискованным) для безопасности системы (FTP, IRC, MIRC, проху, утилиты дистанционного администрирования и т. д.)» [АРТСТС].

Таблица 4

Сема	Словари/ энциклопедии	Wiki 2012	АРТСТС
'Потенциально опасное ПО'(60)		+	+
'Запуск работы компьютера'(17)		+	-
'Приостановление работы компьютера'(64)		+	-
'Некоторые условия'(34)		-	+

Половина сем (34, 60) принадлежит нейтральным семам, вторая половина – к семам, описывающим действия негативного характера, направленные на пользователя или компьютерную систему.

Перейдем к определениям более широких совокупностей: *greyware* (*grayware*), *adware*, *spyware*, *scareware*, *malware* (*badware*) и *scumware* (*scamware*).

Greyware (*grayware*) представляет собой пограничное явление между обычным ПО и вирусами [АРТСТС] и подразумевает «*applications that behave in a manner that is annoying or undesirable, and yet less serious or troublesome than malware*» (приложения, раздражающие пользователя или работающие в нежелательном/неподходящем/неудобном режиме и одновременно представляющие меньшую опасность и причиняющие меньший вред безопасности компьютерной системы, чем вредоносное ПО) [<http://en.wikipedia.org/wiki/Greyware#Grayware>]. Принято считать, что именно «серое» ПО является гиперонимом для *adware* и *spyware*.

Приведем определения *Greyware* (*grayware*) в русскоязычных специальных словарях: «вредоносные программы (*malware*), попадающие в "серую зону" между обычным ПО и вирусами. К этой категории относятся такие опасные и/или надоедливые программы, как *adware*, *spyware*, *trackware* и многие другие [АРТСТС].

Таблица 5

Сема	Словари/ энциклопедии	Wiki 2012	АРТСТ С
'Программное обеспечение'(65)		+	+
'Приложение'(63)		+	-
'Программы'(66)		-	+
'Меньшая степень вредоносности'(23)		+	-
'Большая степень вредоносности'(4)		-	+
'Надоедливость'(25)		+	+
'Нежелательность'(32)		+	-
'Неподходящий пользователю режим работы'(36)		+	-
'Неудобство'(38)		+	-
'Опасность'(42)		-	+

Большая часть установленных сем (5 единиц – 4, 23, 32, 38, 42) относится к семам, описывающим отрицательные характеристики; 3 семы (63, 65, 66) принадлежат к нейтральным, одной семой представлены третья (1) и четвертая (24) группы.

Проследим эволюцию понятия *spyware*. Изначально (см. Стив Гибсон, 2000 [там же]) под шпионским (шпионящим) ПО понималось «*any software which employs a user's Internet connection in the background (the so-called 'backchannel') without their knowledge or*

explicit permission» (любое ПО, использующее обратный канал связи (при подключении пользователя к Интернету) без ведома пользователя или его явного согласия) [http://en.wikipedia.org/wiki/Privacy-invasive_software]. Далее понятие шпионящего ПО стало обрабатываться новыми характеристиками – возникли такие его синонимы, как *thiefware*, *scumware*, *trackware* и *badware* [там же]. Тем не менее, все, входящие в группу шпионящего ПО, имеют две классифицирующие семы, различающиеся различной степенью градуальности: 'степень согласия пользователя', 'уровень негативного влияния на пользователя и компьютерную систему' [там же].

Коалиция по борьбе со шпионским и рекламным ПО (Anti-Spyware Coalition, ASC) выделяет два уровня в определении шпионящего ПО: в узком смысле под ним понимают «*a term for tracking software deployed without adequate notice, consent, or control for the user*» (термин для ПО слежения, примененного без соответствующего уведомления, согласия, надзора пользователя). В широком смысле мы имеем дело с комбинацией определения и описания: «*technologies deployed without appropriate user consent and/or implemented in ways that impair user control over: 1) Material changes that affect their user experience, privacy, or system security; 2) Use of their system resources, including what programs are installed on their computers; and/or 3) Collection, use, and distribution of their personal or other sensitive information*» (технологии, использованные без соответствующего согласия пользователя и/или приводимые в исполнение способами, негативно влияющими на контроль со стороны пользователя над: 1) существенными переменами, отражающимися на его пользовательском опыте, частной жизни или безопасности работы системы; 2) использованием системных ресурсов, включая установленные программы; и/или 3) сбором, использованием и распространением личных данных или другой конфиденциальной информации пользователя) [там же].

Сравним определения *spyware* в англоязычных словарях и Википедии, расположив их в хронологической последовательности: 1) «*software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive*» (ПО, позволяющее пользователю получать конфиденциальную информацию о действиях компьютерной системы другого пользователя путем тайной передачи данных с жесткого диска пользователя) [OD 2005]; 2) «*software that self-installs on computers and tracks the user's Internet use, mainly for marketing purposes*» (самоустанавливающееся ПО, следящее за действиями пользователя в Интернете, в основном в целях маркетинга) [OAD 2005]; 3) «*software installed via the internet on a computer without the user's knowledge and used to send information about the user to another computer*» (ПО, установленное на компьютер пользователя в режиме реального времени без его согласия и используемое для отправки информации о действиях пользователя другому компьютеру) [Collins 2006]; 4) «*computer software that secretly records information about which websites you visit*» (компьютерное ПО, в тайне

записывающее информацию о сайтах, посещаемых пользователем) [CollinsCobuild 2008].

Приведем определения *sruware* в русскоязычных словарях. Отметим, что специальная единица *sruware* с пометой *информ.* содержится уже в словаре общей лексики: «передает данные с жесткого диска компьютера пользователю на другом компьютере» [АПСОЛ 2008]. Приведем также определение *sruware*, содержащееся в специальном толковом словаре: «ПО, предназначенное для слежения за действиями пользователя на компьютере. Перехватывает его почтовую переписку, вводимую им информацию, пароли и команды» [АРТСТС].

Проведем сравнительный компонентный анализ данных определений в таблице 6.

Таблица 6

Словари/ энциклопедии	OD 2005	OA D 2005	Coll ins 2006	Coll ins Cobuild 2008	Wik i 2012	AP СО Л 2008	AP ТСТ С
Сема							
'Компьютерное программное обеспечение, предназначенное для осуществления скрытой от пользователя деятельности'(22)	+	+	+	+	+	-	-
'Самоинсталлируемость (самоустанавливаемость)' (70)	-	+	-	-	-	-	-
'Получение секретной информации о действиях компьютерной системы'(59)	+	-	-	-	+	-	-
'Секретное перемещение данных с жесткого (магнитного) диска'(73)	+	-	-	-	-	+	-
'Слежение за действиями пользователя в Интернете преимущественно в маркетинговых целях'(75)	-	+	-	-	-	-	-
'Слежение за действиями пользователя во время работы на компьютере'(76)	-	-	-	-	-	-	+
'Работа в режиме реального времени (он-лайн, в режиме подключения к сети Интернет)' (67)	-	-	+	-	-	-	-

'Пересылка пользовательских данных другому компьютеру'(48)	-	-	+	-	+	+	-
'Запись информации о посещенных пользователем сайтов'(16)	-	-	-	+	-	-	-
'Потеря и/или отсутствие контроля со стороны пользователя'(61)	-	-	-	-	+	-	-
'Негативное влияние на безопасность работы системы'(29)	-	-	-	-	+	-	-
'Негативное влияние на пользовательский опыт'(30)	-	-	-	-	+	-	-
'Негативное влияние на частную жизнь пользователя'(31)	-	-	-	-	+	-	-
'Использование личных данных или другой конфиденциальной информации пользователя'(20)	-	-	-	-	+	-	-
'Использование системных ресурсов компьютера пользователя, включая установленные программы'(21)	-	-	-	-	+	-	-
'Отсутствие надзора пользователя за работой ПО'(43)	-	-	-	-	+	-	-
'Отсутствие согласия пользователя на работе ПО'(44)	-	-	-	-	+	-	-
'Отсутствие уведомление пользователя о работе ПО'(45)	-	-	-	-	+	-	-
'Перехват почтовой переписки'	-	-	-	-	-	-	+
'Перехват вводимой пользователем информации'(49)	-	-	-	-	-	-	+
'Перехват команд'(50)	-	-	-	-	-	-	+
'Перехват паролей'(51)	-	-	-	-	-	-	+

Более 70% принадлежат семам, описывающим действия негативного характера, направленные на пользователя или компьютерную систему (20, 21, 22, 29, 30, 31, 43, 44, 45, 48, 49, 50, 51, 59, 73), 14% – семам, описывающим действия потенциально негативного характера, направленные на пользователя или компьютерную систему (16, 75, 76), 7% - нейтральные семы (61, 67), группа сем описывающих отрицательные характеристики, немногочисленна – всего лишь 1 сема (70).

Приведем определения специальной единицы *adware* в хронологическом порядке: «*adjunct software that displays advertising while the program it is attached to is running*» (добавочное ПО, демонстрирующее встроенные в программу рекламные сообщения во время его работы) [OAD 2005]; «1) *a type of computer software that collects information about a user's browsing patterns in order to display relevant advertisements in his or her Web browser*; 2) *computer software that is given to a user with advertisements already embedded*» (1) тип компьютерного ПО, собирающего информацию о просмотре, поиске и организации доступа пользователя к ресурсам сети в целях демонстрации в браузере пользователя рекламных сообщений, относящихся именно к этому пользователю; 2) компьютерное ПО, доступное пользователю с уже встроенными рекламными сообщениями) [Collins 2006]; «*any software package which automatically plays, displays, or downloads advertisements to a computer*» (любой пакет ПО, автоматически проигрывающий, демонстрирующий, загружающий на компьютер рекламные сообщения) [Wiki 2012].

Что касается определений в русскоязычных словарях, то мы обнаружили определение лишь в Большом англо-русском словаре по экономике и менеджменту: «*компьютерная программа, которая помимо своей основной функции демонстрирует пользователю рекламные объявления; показ рекламы часто является основным источником дохода для разработчиков таких программ*» [БАРСЭМ 2008].

Таблица 7

Сема \ Словари/ энциклопедии	ОА D 20 05	Col lins 20 06	Wi ki 20 12	БА РС ЭМ
'Программное обеспечение'(65)	+	+	+	+
'Пакет ПО'(46)	-	-	+	-
'Автоматизированность'(2)	-	-	+	-
'Добавочность/несущественность'(12)	+	-	-	+
'Демонстрация рекламы'(11)	+	+	-	+
'Загрузка рекламы из Интернета в компьютерную систему'(14)	-	-	+	-
'Во время работы основной программы'(6)	+	-	-	-
'Сбор информации о просмотре, поиске и организации доступа пользователя к ресур-	-	+	-	-

сам сети'(71)				
'Релевантность демонстрируемой рекламы'(68)	-	+	-	-
'Демонстрация рекламных сообщений в браузере'(10)	-	+	-	-
'Вложенность рекламных сообщений в программу'(5)	-	+	-	-
'Получение прибыли разработчиками данной программы за счет демонстрации рекламных сообщений'(58)	-	-	-	+

Две трети сем являются нейтральными (2, 6, 46, 65) и семами, описывающими действия потенциально негативного характера, направленные на пользователя или компьютерную систему (5, 10, 11, 14, 68).

Семы третьей (58, 71) и пятой групп (12) составляют одну треть сем в компонентном составе лексического значения специальной единицы *adware*.

Adware включает *typhoid adware* – «*a new potential type of computer security threat identified by researchers from the University of Calgary which does not require the affected computer to have adware installed in order to display advertisements on this computer*» (новый потенциальный тип угрозы компьютерной безопасности, выделяемое исследователями университета г. Калгари (Канада), демонстрирующий рекламные объявления на компьютере пользователя, не требуя при этом предварительной установки) [http://en.wikipedia.org/wiki/Typhoid_adware].

Перечислим определения специальной единицы *scareware*: «*comprises several classes of scam software with malicious payloads, or of limited or no benefit, that are sold to consumers via certain unethical marketing practices*» (включает несколько классов «жульнического» ПО, содержащего злонамеренные просьбы об оплате, или ПО с ограниченными возможностями, а также не представляющие никакой пользы, продаваемые потребителям в ходе неэтичной маркетинговой деятельности) [<http://en.wikipedia.org/wiki/Scareware>]; «*malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection*» (вредоносные компьютерные программы, разработанные с целью обманным путем склонить пользователя к покупке и загрузке ненужного и потенциально опасного ПО, например, поддельное антивирусное ПО)[OD 2010]; «*a term used to describe software that scares the users into purchasing the full program. A good example of scareware is a program claiming it's an [anti-virus](#) or other security protection program and that it's found dozens of potential threats on the computer, which in reality are either non-existent or not really a threat to the user or his or her computer* (термин, использующийся для описания такого типа ПО, которое путем запугивания заставляет пользователей покупать полную

версию программы. Хорошим примером подобного ПО служит программа, позиционирующая себя как антивирусное ПО или программа, обеспечивающая защиту компьютера. Данная программа находит десятки потенциальных угроз в компьютерной системе, которые в действительности либо не существуют, либо не представляют угрозы пользователю или его/ее компьютеру) [<http://www.computerhope.com/jargon/s/scareware.htm>].

Таблица 8

Сема	Словари/ энциклопедии	Wik i 201 2	OD 201 0	CH 201 2
‘Вредоносное ПО’(8)		-	+	-
‘Жульничество’(13)		+	-	+
‘Злонамеренные просьбы об оплате’(19)		+	-	-
‘Ограниченные возможности’(41)		+	-	+
‘Бесполезность’(3)		+	-	-
‘Неэтичная маркетинговая деятельность’(39)		+	-	-
‘Ненужность’(35)		-	+	+
‘Покупка’(57)		-	+	+
‘Загрузка’(15)		-	+	-
‘Потенциально опасное ПО’(60)		-	+	-
‘Подделка’(55)		-	+	-
‘Покупка полной версии программы в результате запугивания пользователя’(56)		-	-	+

Группы сем единицы *scareware* представлены достаточно равномерно: нейтральные семы (8, 15, 57, 60); семы, описывающие действия негативного характера, направленные на пользователя или компьютерную систему (13, 19, 39, 55, 56); семы, описывающие отрицательные характеристики (3, 35, 41).

Специальная единица *malware*, с одной стороны, признается большинством специалистов наиболее общим и является гиперонимом для специальной единицы *scareware*, с другой стороны, вместе со *scareware* входит в гипероним *scumware* (*scamware*). Иногда в качестве синонима *malware* приводят *badware* – «*software that has been installed on a computer without a user’s knowledge or control*» (ПО, установленное без ведома пользователя или не под надзором пользователя) [OD 2010].

Википедия автоматически перенаправляет со статей *badware* и *scumware* на страницу со статьей *malware*.

Приведем англоязычные определения *malware* в хронологической последовательности: «*software that is intended to damage or disable computers and computer systems*» (ПО, предназначенное для

повреждение или нарушения работы компьютеров и компьютерных систем) [OAD 2005]; «malicious software, such as a virus, which is specifically designed to disrupt or damage a computer system» (вредоносное ПО (например, вирусы), разработанное специально для повреждения или нарушения работы компьютерной системы) [OD 2005]; «a computer program designed specifically to damage or disrupt a system, such as a virus» (компьютерная программа, разработанная специально для повреждения или нарушения системы (например, вирусы)) [Collins 2006]; «software (or script or code) designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems» (ПО (скрипт (программа на макроязыке) или код), разработанное для нарушения работы компьютера, сбора конфиденциальной информации или получения несанкционированного доступа к компьютерным системам) [Wiki 2012]; «malicious software, such as a virus, which is specifically designed to disrupt or damage a computer system» (вредоносное ПО (например, вирусы), специально разработанное с целью повреждения или нарушения работы компьютера) [OD 2010]. Приведем определения из русскоязычных словарей: «информ.; (от malicious + software) вредоносное ПО, способное нанести ущерб или вывести из строя информационно-вычислительную систему; например, вирус» [АРСОЛ 2008]; «любая программа, действующая против интересов пользователя или владельца компьютерной системы. К нему относятся все виды вирусов, "черви", троянцы, шпионящее ПО и т. п.» [АРТСТС].

Таблица 9

Словари/ энциклопедии Сема	OA D 20 05	OD 20 05	Col lin s 20 06	AP TC TC	AP CO Л 20 08	Wi ki 20 12	OD 20 10
'Программное обеспечение'(65)	+	+	+	+	+	+	+
'Намеренная вредоносность'(26)	-	+	+	+	+	-	
'Повреждение компьютеров и/или компьютерных систем'(54)	+	+	+	-	-	-	+
'Нарушение работы компьютеров и/или компьютерных систем'(28)	+	+	+	-	+	+	+
'Скрипт/код'(74)	-	-	-	-	-	+	-
'Сбор конфиденциальной информации'(72)	-	-	-	-	-	+	-
'Несанкционированный доступ к компьютерным системам'(37)	-	-	-	-	-	+	-

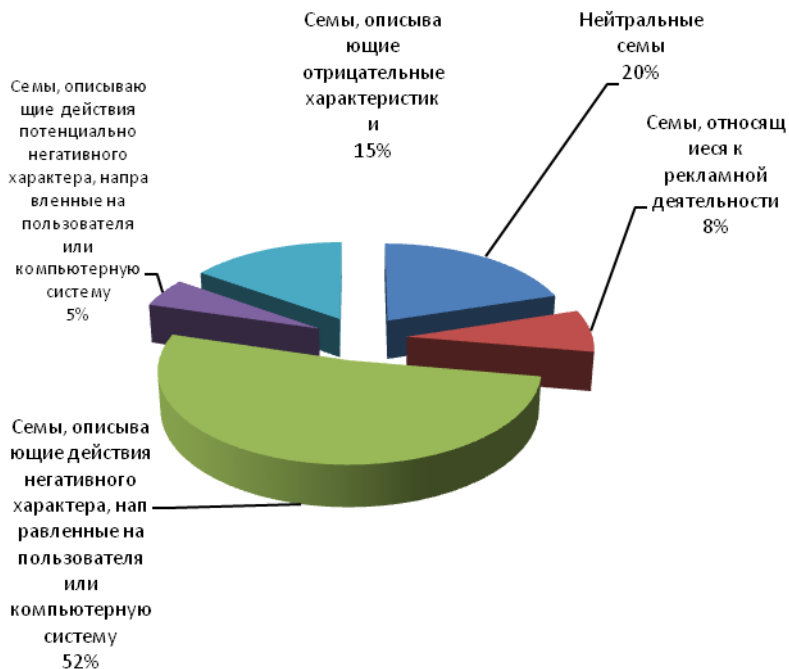
'Нанесение ущерба'(27)	-	-	-	-	+	-	-
'Действие, направленное против интересов пользователя/владельца компьютерной системы'(9)	-	-	-	-	+	-	-

Две трети сем являются семами, описывающими действия потенциально негативного характера, направленные на пользователя или компьютерную систему (9, 27, 28, 37, 54, 72).

Нейтральные семы (65, 74) и семы, описывающие отрицательные характеристики (26), составляют одну треть.

Таким образом, представим количественное соотношение всех пяти групп сем в диаграмме 1.

Диаграмма 1



Проанализировав 11 специальных единиц и их определения, можно утверждать, что более половины единиц (*crimeware, moralityware, ransomware, rogueware, scareware, stealware*) не имеют зафиксированных в терминологии определений, 2 единицы (*greyware (grayware), stealware*) имеют определения в англоязычной Википедии и

англо-русском толковом словаре терминов и сокращений по вычислительной технике, Интернету и программированию под редакцией Э.М. Пройдакова и Л.А. Теплицкого [АРТСТС].

Наиболее представлены в словарях *malware* и *spyware* (5 английский источников и 2 русских): данные единицы представлены как в специальном словаре под редакцией Э.М. Пройдакова и Л.А. Теплицкого [АРТСТС], так и в англо-русском словаре общей лексики, подготовленным лексикографической группой отдела прикладной лингвистики компании АВВУУ [АРСОЛ].

Специальная единица *adware* представлена в трех англоязычных источниках и 1 русскоязычном – большом англо-русском словаре по экономике и менеджменту [БАРСЭМ].

Подводя итоги исследования группы *Scumware* (*Scamware*), отметим неустойчивый характер данной терминологии (данный факт напрямую подтверждается несовпадением ни одного определения даже в словарях, выпущенных одним издательством в один год (за исключением определения специальной единицы *malware* в OD 2005 и OD 2010 (определения полностью идентичны) и Collins 2006); наличие большого числа лакун среди русскоязычных эквивалентов; сложные парадигматические отношения внутри групп и подгрупп (гипонимии (квазисинонимии) и синонимии); присутствие всех трех типов специальной лексики, указанных в начале статьи (компьютерный термин – профессионализм – жаргонизм; несомненную пользу компонентного анализа при корректировке концептосферы исследуемой предметной подобласти (например, некоторые специальные единицы вообще не относятся к заявленной группе (см. *greyware*), *riskware*, *rogueware*)).

Итак, ответим на поставленные в начале статьи вопросы. Да, «чистые» лингвистические методы остались, но интерпретация результатов анализа носит все более синтезирующий характер, требуя обобщений на более высоком уровне, привлекая данные не только «внутренней» лингвистики.

Компонентный анализ специальных единиц носит более сложный по сравнению с анализом единиц общего словаря характер в силу того факта, что термин представляет собой единицу специального знания. Затруднительной, но потенциально достижимой, является возможность четкой формулировки (наименования) сем компьютерного подъязыка даже на материале анализируемой предметной области.

Несомненно, полученный материал требует последующего осмысления в русле теории языковых контактов (контактной лингвистики), а другие предметные области такого нового объекта изучения, как компьютерный подъязык, ожидают последующего исследования с помощью проверенных временем методов.

Именно проверенный инструментарий исследования и новый материал способны выявить много нового и интересного, а также помочь тем исследователям, кому не безразлична судьба языка в общем и судьба специальных подъязыков в частности.

Библиография

1. АРСОЛ – Англо-русский словарь общей лексики [Электронный ресурс]: подгот. по печ. изд. – М.: «Русский язык-Медиа», 2004. – 1 электрон. опт. диск (CD-ROM).
2. АРТСТС – Пройдаков, Э.М. Англо-русский толковый словарь по вычислительной технике, Интернету и программированию [Электронный ресурс]: подгот. по печ. изд. – М.: Русская редакция, 2004. – 1 электрон. опт. диск (CD-ROM).
3. БАРСЭМ 2008 – Большой англо-русский словарь по экономике и менеджменту [Электронный ресурс]: АБВУУ, 2008; ООО «Экономикус», 2008. – 1 электрон. опт. диск (CD-ROM).
4. Бенвенист Э. Взгляд на развитие лингвистики // Общая лингвистика. – М., 1997. – С. 21–32.
5. CH 2012 – Computer Hope Computer Dictionary – 2012 [Электронный ресурс]. – URL: <http://www.computerhope.com/jargon/s/scareware.htm> (дата обращения: 17.01.2012).
6. Collins 2006 – Collins English Dictionary [Электронный ресурс]: подгот. по 8-ому печ. изд. – London: Collins, 2006. – 1 электрон. опт. диск (CD-ROM).
7. Collins Cobuild 2008 – Collins Cobuild Advanced Learner's English Dictionary [Электронный ресурс]: подгот. по 5-ому печ. изд. – London: Collins, 2005. – 1 электрон. опт. диск (CD-ROM).
8. OAD 2005–New Oxford American Dictionary [Электронный ресурс]: подгот. по 2-ому печ. изд. – Oxford: Oxford University Press, 2005. – 1 электрон. опт. диск (CD-ROM).
9. OD 2005–Oxford Dictionary of English [Электронный ресурс]: подгот. по 2-ому печ. изд. – Oxford: Oxford University Press, 2005. – 1 электрон. опт. диск (CD-ROM).
10. OD 2010 – Oxford Dictionaries. April 2010. Oxford Dictionaries. April 2010. Oxford University Press. – 2010 [Электронный ресурс]. URL: <http://oxforddictionaries.com/definition/badware> (дата обращения: 19.01.2012).

*Гукетлова Ф.Н., Бербекова Ф.А.
Кабардино-Балкарский государственный университет, г. Нальчик,
Россия*

КРАСОТА БРОВЕЙ КАК НОМИНАЦИЯ КОНЦЕПТА «КРАСОТА» НА МАТЕРИАЛЕ КАБАРДИНО-ЧЕРКЕССКОГО, РУССКОГО И ФРАН- ЦУЗСКОГО ЯЗЫКОВ

Abstract. The article studies the concept «beauty». The object of this work is find out ethnoculture specific nature of concept “beauty” in Cabardian, Russian and French languages world-views. The tasks of our article are find out universal and specific in function of concept “beauty” and find out