Литература

1. *Верещагин Е.М., Костомаров В.Г.* Лингвострановедческая теория слова. М.: Русский язык, 1980. 320 с.
2. *Дейкина А.Д., Левушкина О.Н.* Роль лингвокультурологического подхода в методике преподавания русского языка как родного, иностранного и как неродного // Вестник Российского университета дружбы народов. Серия: Вопросы образования: языки и специальность. 2012. № 4. С. 23–27.
3. *Толстой Л.Н.* Полное собрание сочинений: в 90 т. М., 1953.

Literatura

1. *Vereshchagin E.M., Kostomarov V.G.* Lingvostranovedcheskaya teoriya slova. M.: Russkij yazyk, 1980. 320 s.
2. *Dejkina A.D., Levushkina O.N.* Rol' lingvokul'turologicheskogo podkhoda v metodike prepodavaniya russkogo yazyka kak rodnogo, inostrannogo i kak nerodnogo // Vestnik Rossijskogo universiteta druzhby narodov. Seriya: Voprosy obrazovaniya: yazyki i spetsial'nost'. 2012. № 4. S. 23–27.
3. *Tolstoj L.N.* Polnoe sobranie sochinenij: v 90 t. M., 1953.

DOI: 10.25586/RNU.V925X.20.02.P.072 УДК 81'373.46

Л.Я. Долгоновская, И.Н. Новикова

СЕМАНТИЧЕСКИЙ АНАЛИЗ ТЕРМИНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С КОМПОНЕНТОМ ЦВЕТОНАИМЕНОВАНИЯ В АНГЛИЙСКОМ И РУССКОМ ЯЗЫКАХ (СОПОСТАВИТЕЛЬНЫЙ АСПЕКТ)

Посвящено терминологическим единицам из сферы информационной безопасности, в состав которых входят колоронимы, или цветонаименования. Рассмотрена и изучена семантика таких терминов информационной безопасности. Проанализировано, что некоторые термины в английском языке меняют свою семантику в современном языке информационной безопасности. Делается вывод, что представленные колоронимы в составе терминологических единиц облегчают пользователям профессиональной лексики понимание целого ряда понятий из указанной области знания.
Ключевые слова: колороним, цветонаименование, термин, семантический анализ, информационная безопасность, сопоставительный аспект.

L.Ya. Dolgonovskaya, I.N. Novikova

THE SEMANTIC ANALYSIS OF INFORMATION SECURITY TERMS WITH A COLOUR COMPONENT IN THE ENGLISH AND RUSSIAN LANGUAGES (THE COMPARATIVE ASPECT)

Dedicated to terminological units from the field of information security, which include coloronyms, or color names. The semantics of such information security terms are examined and studied. It is analyzed that some terms in English change their semantics in the modern language of information security. It is

© Долгоновская Л.Я., Новикова И.Н., 2020

concluded that the presented coloronyms as part of terminological units make it easier for users of professional vocabulary to understand a number of concepts from the specified field of knowledge.
Keywords: coloronims, terms, semantic analysis, IT security, comparative analysis.

История исследования феномена цветонаименования насчитывает много столетий. Значение цвета как одной из констант культуры, а также его влияние на людей привлекало внимание ученых, начиная с Платона. Понимание цвета в разных культурах имеет свои особенности, связанные с глубинными слоями сознания, и отражает национально-культурную специфику. Проблемы цветообозначений изучались лингвистами, психологами, философами (Р.В. Алимпиева [2], Ю.Д. Апресян [3], Р. Барт [4], Н.Б. Бахилина [5], А.А. Брагина [7], А.П. Василевич [8], Р.М. Фрумкина [17]). Разное отношение к тому или иному цвету отражается в языке посредством идиом, пословиц, поговорок, а также присутствует в качестве составного элемента терминологических единиц.

Цель исследования – провести семантический анализ особенностей терминов информационной безопасности.

Практическая значимость проведенного исследования состоит в том, что полученные результаты могут быть использованы в практике преподавания терминоведения и английского языка для специальных целей.

Объектом исследования послужили терминологические единицы с компонентом цветонаименования в английском и русском языках.

Для достижения поставленной цели были сформулированы следующие задачи:

1) рассмотреть теоретические аспекты исследования цветонаименования;

2) отобрать практический материал;

3) провести семантический и сопоставительный анализ терминов информационной безопасности с компонентом цветонаименования.

Составной частью терминологии являются ее единицы – термины. Термины неразрывно связаны с теми научными концепциями, в которых они используются. Другими словами, термины не могут употребляться вне науки, к терминосферам которой они относятся. Следует заметить, что существует множество подходов к определению понятия термин. В.П. Даниленко, в частности, в своей работе приводит 19 дефиниций из различных научных источников [10]. Мы хотели бы остановиться на некоторых из определений.

К.Я. Авербух рассматривает термин как «элемент терминосистемы, представляющий собой совокупность всех вариантов определенного слова или устойчиво воспроизводимой синтагмы, выражающих специальные понятия определенной области деятельности» [1].

С.В. Гринев-Гриневич дает краткое и емкое определение: «термин – номинативная специальная лексическая единица, принимаемая для точного наименования понятий» [9, с. 30].

Если проанализировать все перечисленные дефиниции термина, то можно выделить некоторые общие черты:

1) термин – слово, относящееся к языку для специальных целей;

2) термин выражает понятие (концепт);

3) каждый термин требует дефиниции;

4) термин существует в системных отношениях с другими терминами. Семантические отношения в любой терминосистеме необходимы для изучения и систематизации терминов. Исследованию значений терминологических единиц посвящено много работ отечественных ученых (О.Н. Блинова [6], Т.Л. Канделаки [12], А.В. Суперанская [16]).

Проведенный анализ и сопоставление отобранных пар терминологических единиц в английском и русском языках позволили выделить следующие семантические особенности:

1. **Whitelist**

Adblocking software usually allows users to "**whitelist**" sites whose ads are not so intrusive or annoying.

В глоссарии терминов информационной безопасности дается следующее определение: *the list of people that you positively want to receive e-mails from* [11]. В "Collins Dictionary" приводится похожее определение: *list of e-mail contacts from whom messages are regarded as acceptable by the user* [20].

Белый список

В «**белый**» **список** сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

Один из способов фильтрации нежелательной почты, белый список содержит перечень разрешенных адресов электронной почты или доменных имен: все сообщения из адресов или доменов белого списка автоматически передаются получателю [19].

Blacklist

The code was written eventually and **the blacklist** was put in place.

A list of persons who are disapproved of or are to be punished or boycotted [22].

A list with negative connotations, eg, it might be a list of those senders that a spam filter will always filter out, or a list of those mobile phones that will be banned from connecting to the mobile phone network [11].

Черный список

Перечень сайтов, программ или других элементов, нежелательных для запуска или посещения [19].

Для более наглядной демонстрации контраста используется дуалистическая пара «черное – белое». Данная пара терминов в области информационной безопасности объединена общим семантическим компонентом «ограничение», который имеет отрицательную коннотацию, на первый взгляд. Однако хотелось бы отметить, что в киберзащите указанное явление может быть рассмотрено в положительном контексте, а именно как отсутствие доступа нежелательным лицам.

2. **Red team**

During a **red team** engagement, highly trained security consultants enact attack scenarios to reveal potential physical, hardware, software and human vulnerabilities.

A professional group organized to emulate a potential attack against an enterprise's cybersecurity defenses. This practice is utilized to detect vulnerabilities and improve protection [21].

An operation which takes four days to identify the vulnerabilities and then crack into each network [22].

Сам термин изначально применялся в англоязычной военной терминологии, где обозначал во время военных учений команду противника (атакующих), в то время как команда защищающихся обозначалась термином *blue team*. При проведении военных учений в США команда противника всегда «красная», в то время как силы США всегда «синие», что достаточно закономерно, так как красный цвет ассоциируется с опасностью, тревогой. С развитием технологий и потребностей надежной защиты информации этот термин перешел в сферу информационной безопасности, где теперь обозначает условную команду «атакующих» или злоумышленников, которые пытаются проникнуть в защищенную систему. Во время таких киберучений специалисты делятся на две команды и отрабатывают возможные варианты проникновения в систему и защиты от таких действий [14].

В настоящее время в русском языке не встречаются термины, зафиксированные в терминологических словарях с похожим

значением, но в то же время в профессиональной среде они широко распространены.

3. **Black-boxtesting**

Black-boxtesting is generally performed on software that is under development.

It is a Software Testing method that analyses the functionality of a software/application without knowing much about the internal structure/design of the item that is being tested and compares the input value with the output value [25].

An approach to testing software in which the tester treats the software as a black box-that is, the testing focuses in the program's functionality rather than on its internal structure [21].

Тестирование методом черного ящика

В рамках **тестирования по методу черного ящика** основной информацией для создания тест-кейсов выступает документация (особенно требования (requirements-based testing 122)) и общий здравый смысл.

Процедура создания и/или выбора тестовых сценариев, основанная на анализе функциональной или нефункциональной спецификации компонента или системы без знания внутренней структуры [15].

У тестировщика либо нет доступа к внутренней структуре и коду приложения, либо недостаточно знаний для их понимания, либо он сознательно не обращается к ним в процессе тестирования [13].

White-box testing

White box testing is testing beyond the user interface and into the nitty-gritty of a system.

A software testing method in which the internal structure/design/implementation of the item being tested is known to the tester [25].

Testing based on an analysis of the internal structure of the component or system [26].

Тестирование белого ящика

Для более глубокого изучения сути **метода белого ящика** рекомендуется ознакомиться с техниками исследования потока управления или потока данных, использования диаграмм состояний.

Процедура разработки или выбора тестовых сценариев на основании анализа внутренней структуры компонента или системы [15].

У тестировщика есть доступ к внутренней структуре и коду приложения, а также достаточно знаний для понимания увиденного [13].

Целесообразно отметить контраст значения терминов *black-boxtesting* и «тестирование методом черного ящика», поскольку при данном виде тестирования пользователь знает особенности структуры тестируемого объекта. Белый цвет, в свою очередь, подчеркивает открытость, доступность. Также терминологическая единица *white-boxtesting* понимается как *glass-boxtesting, transparent-boxtesting* с акцентом на упомянутые свойства.

4. **White hat**

Levy is a so-called "**white hat**" computer hacker who hunts for computer security flaws to help repair them.

A hacker who tests computer systems for possible vulnerabilities so that they can be fixed [22].

A non-criminal hacker [11].

Белый хакер, этичный хакер

Каждая крупная корпорация, имеющая собственную сеть, имеет таких «**белых**» **хакеров** в штате.

Хакеры, основной деятельностью которых является защита компьютерных сетей [18].

В данном термине мы также наблюдаем прозрачность семантики, так как и в английском, и в русском языках белый цвет вызывает положительные ассоциации. Традиционно считается, что данная терминологическая единица, как и представленная ниже ее антонимичная пара (*black hat*),

берет начало из черно-белых фильмов жанра «вестерн», где главный положительный герой носил белую шляпу, а антагонист – черную.

Black hat

We want to bring the fringe elements of the hacking community on board, and steer them away from being "**black hats**" – the malicious hackers responsible for website defacement and security breaches.

A hacker who infiltrates a computer system for malicious purposes (as to disable a website or uncover secret information) [22].

A criminal hacker [11].

Злоумышленник, черная шляпа, хакер

Хакеры проникают в незащищенные компьютеры, оставляя там свои программы-агенты.

Термин, применяемый в хакерской культуре для описания классического киберпреступника, который использует свои знания и навыки для осуществления криминальной деятельности – взлома программ или сайтов, кражи данных, шифрования информации с целью получения выкупа [19].

Хакер, который применяет существующие программы для взлома и использует хорошо известные уязвимости для раскрытия важной информации для личной выгоды или причинения ущерба атакуемым компьютерам или сетям [24].

Контрастность в данном случае проявляется довольно наглядно, так как, в отличие от этичного хакера (*white hat*), «злоумышленник» или «черная шляпа» вызывает у носителей русской культуры нежелательные ассоциации из-за черного цвета, который связан с чем-то плохим, негативным и отрицательным. В данном случае это еще и намекает на темную сторону закона, так как черные шляпы – это прежде всего преступники, на что ясно указывает колороним в выбранном нами термине.

Grey hat

A combination of white hat and black hat [23].

Серая шляпа, серый хакер

Хакер, который имеет те же навыки, что и хакер в белой шляпе, и в большинстве случаев те же намерения, но иногда использует свои знания в не совсем благородных целях [24].

Как следует из колоронима в составе терминологической единицы, серый хакер объединяет в себе черты черного и белого, тем самым балансируя на грани между законом и правонарушениями. В русском языке можно считать уместной ассоциацию с таким понятием, как «серая мораль». Серые хакеры не относятся к абсолютам, выраженным белым и черным цветами, а скорее находятся посередине, объединяя в себе черты одного и другого.

Таким образом, терминология с компонентом цветонаименования в сфере информационной безопасности представляет несомненный интерес для ученых. Для настоящего исследования были отобраны колоронимы с разными компонентами цветонаименования, а именно: красный, белый, черный, серый. Проанализировав терминологические единицы с указанными элементами, целесообразно отметить, что они способствуют пониманию семантики как отдельных терминологических единиц, так и в контексте высказывания (коннотативное значение). В русской и английской культурах закрепились определенные цветовые ассоциации, которые также способствуют облегчению восприятия исследуемого явления. Белый и синий цвета несут положительный оттенок значения, черный и красный цвета – негативный, в то время как серый цвет находится вне данной парадигмы, объединяя в себе черты одного и другого.

Литература

1. *Авербух К.Я.* Общая теория термина: комплексно-вариологический подход: автореф. дис. … д-ра филол. наук. М., 2005. 31 с.
2. *Алимпиева Р.В.* Синонимический микроряд синий – голубой в сопоставлении с польским błekitny – niebieski (к проблеме семантической эволюции лексических эквивалентов родственных языков) // Семантика слова в диахронии: межвузовский тематический сборник научных трудов. Калининград: Калинингр. гос. ун-т., 1987.
3. *Апресян Ю.Д.* Избранные труды. Т. I: Лексическая семантика (синонимические средства языка). 2-е изд., испр. и доп. М.,1995. 472 с.
4. *Барт Р.* Избранные работы: Семиотика: Поэтика / пер. с фр.; сост., общ. ред. и вступ. ст. Г.К. Косикова. М.: Прогресс, 1989. 616 с.
5. *Бахилина Н.Б.* История цветообозначений в русском языке. М., 1975. 286 с.
6. *Блинова О.И.* Лексико-семантическая категория и свойство слова // Русские говоры Сибири: Семантика. Томск, 1995. С. 11–21.
7. *Брагина А.А.* «Цветовые» определения и формирование новых значений слов и словосочетаний // Лексикология и лексикография. М., 1972. С. 73–104.
8. *Василевич А.П.* Этимология цветообозначений как зеркало национально-культурного сознания // Наименования цвета в индоевропейских языках: Системный и исторический анализ / отв. ред. А.П. Василевич. М.: КомКнига, 2007.
9. *Гринев-Гриневич С.В.* Терминоведение. М.: Академия, 2008. 304 с.
10. *Даниленко В.П.* Русская терминология: опыт лингвистического описания. М.: Наука, 1977. 118 с.
11. *Калдер А., Воткинс С.* Термины информационной безопасности, аббревиации и акронимы. [Б. м.], 2007. 102 с.
12. *Канделаки Т.Л.* Значения терминов и системы значений научно-технических терминологий // Проблемы языка науки и техники. М., 1977. С. 12–92.
13. *Куликов С.С.* Тестирование программного обеспечения. Базовый курс. Минск: Четыре четверти, 2017. 312 с.
14. Обзор рынка услуг по оценке киберзащищенности методом Red Team Operations в России и за рубежом // Anti-Malware. URL: https://www.anti-malware.ru/analytics/Market_Analysis/Red-Team-Operations-market-overview (дата обращения: 12.02.2020).
15. Стандартный глоссарий терминов, используемых в тестировании программного обеспечения. URL: https://www.bsuir.by/m/12_100229_1_103512.pdf (дата обращения: 27.03.2020).
16. *Суперанская А.В., Подольская Н.В., Васильева Н.В.* Общая терминология: вопросы теории. М.: Либроком, 2012. 246 с.
17. *Фрумкина Р.М.* Психолингвистика. М., 2001. 320 с.
18. *Шагалова Е.* Самый новейший толковый словарь русского языка XXI века. М.: АСТ, 2011. 416 с.
19. Энциклопедия «Касперского». URL: https://encyclopedia.kaspersky.ru (дата обращения: 12.02.2020).
20. Collins Dictionary. URL: https://www.collinsdictionary.com/ (date of the application: 26.03.2020).
21. Cyber Dictionary. URL: https://cybersecurity.osu.edu/about/glossaries/cyber-dictionary (date of the application: 25.03.2020).
22. Merriam Webster Dictionary. URL: https://www.merriam-webster.com/ (date of the application: 26.03.2020).

23. *Moore R.* Cybercrime: Investigating High-Technology Computer Crime. L.: Routledge, 2010. 298 p.
24. Red Hat Enterprise Linux 4: Руководство по безопасности. URL: http://rhd.ru/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-risk.html (дата обращения: 26.03.2020).
25. Software Testing Fundamentals. URL: http://softwaretestingfundamentals.com/white-box-testing/ (date of the application: 25.03.2020).
26. Standard Glossary of Terms Used in Software Testing. URL: rstqb.org (date of the application: 26.03.2020).

Literatura

1. *Averbukh K.Ya.* Obshchaya teoriya termina: kompleksno-variologicheskij podkhod: avtoref. dis. … d-ra filol. nauk. M., 2005. 31 s.
2. *Alimpieva R.V.* Sinonimicheskij mikroryad sinij – goluboj v sopostavlenii s pol'skim błekitny – niebieski (k probleme semanticheskoj evolyutsii leksicheskikh ekvivalentov rodstvennykh yazykov) // Semantika slova v diakhronii: mezhvuzovskij tematicheskij sbornik nauchnykh trudov. Kaliningrad: Kaliningr. gos. un-t., 1987.
3. *Apresyan Yu.D.* Izbrannye trudy. T. I: Leksicheskaya semantika (sinonimicheskie sredstva yazyka). 2-e izd., ispr. i dop. M.,1995. 472 s.
4. *Bart R.* Izbrannye raboty: Semiotika: Poetika / per. s fr.; sost., obshch. red. i vstup. st. G.K. Kosikova. M.: Progress, 1989. 616 s.
5. *Bakhilina N.B.* Istoriya tsvetooboznachenij v russkom yazyke. M., 1975. 286 s.
6. *Blinova O.I.* Leksiko-semanticheskaya kategoriya i svojstvo slova // Russkie govory Sibiri: Semantika. Tomsk, 1995. S. 11–21.
7. *Bragina A.A.* "Tsvetovye" opredeleniya i formirovanie novykh znachenij slov i slovosochetanij // Leksikologiya i leksikografiya. M., 1972. S. 73–104.
8. *Vasilevich A.P.* Etimologiya tsvetooboznachenij kak zerkalo natsional'no-kul'turnogo soznaniya // Naimenovaniya tsveta v indoevropejskikh yazykakh: Sistemnyj i istoricheskij analiz / otv. red. A.P. Vasilevich. M.: KomKniga, 2007.
9. *Grinev-Grinevich S.V.* Terminovedenie. M.: Akademiya, 2008. 304 s.
10. *Danilenko V.P.* Russkaya terminologiya: opyt lingvisticheskogo opisaniya. M.: Nauka, 1977. 118 s.
11. *Kalder A., Votkins S.* Terminy informatsionnoj bezopasnosti, abbreviatsii i akronimy. [B. m.], 2007. 102 s.
12. *Kandelaki T.L.* Znacheniya terminov i sistemy znachenij nauchno-tekhnicheskikh terminologij // Problemy yazyka nauki i tekhniki. M., 1977. S. 12–92.
13. *Kulikov S.C.* Testirovanie programmnogo obespecheniya. Bazovyj kurs. Minsk: Chetyre chetverti, 2017. 312 s.
14. Obzor rynka uslug po otsenke kiberzashchishchennosti metodom Red Team Operations v Rossii i za rubezhom // Anti-Malware. URL: https://www.anti-malware.ru/analytics/Market_Analysis/Red-Team-Operations-market-overview (data obrashcheniya: 12.02.2020).
15. Standartnyj glossarij terminov, ispol'zuemykh v testirovanii programmnogo obespecheniya. URL: https://www.bsuir.by/m/12_100229_1_103512.pdf (data obrashcheniya: 27.03.2020).
16. *Superanskaya A.V., Podol'skaya N.V., Vasil'eva N.V.* Obshchaya terminologiya: voprosy teorii. M.: Librokom, 2012. 246 s.
17. *Frumkina R.M.* Psikholingvistika. M., 2001. 320 s.

18. *Shagalova E.* Samyj novejshij tolkovyj slovar' russkogo yazyka XXI veka. M.: AST, 2011. 416 s.
19. Entsiklopediya "Kasperskogo". URL: https://encyclopedia.kaspersky.ru (data obrashcheniya: 12.02.2020).
20. Collins Dictionary. URL: https://www.collinsdictionary.com/ (date of the application: 26.03.2020).
21. Cyber Dictionary. URL: https://cybersecurity.osu.edu/about/glossaries/cyber-dictionary (date of the application: 25.03.2020).
22. Merriam Webster Dictionary. URL: https://www.merriam-webster.com/ (date of the application: 26.03.2020).
23. *Moore R.* Cybercrime: Investigating High-Technology Computer Crime. L.: Routledge, 2010. 298 p.
24. Red Hat Enterprise Linux 4: Rukovodstvo po bezopasnosti. URL: http://rhd.ru/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-risk.html (data obrashcheniya: 26.03.2020).
25. Software Testing Fundamentals. URL: http://softwaretestingfundamentals.com/white-box-testing/ (date of the application: 25.03.2020).
26. Standard Glossary of Terms Used in Software Testing. URL: rstqb.org (date of the application: 26.03.2020).

DOI: 10.25586/RNU.V925X.20.02.P.079 УДК 811.111

М.В. Зимина, И.В. Вашунина

КОНЦЕПТ "RUSSIA" В АМЕРИКАНСКОМ ЯЗЫКОВОМ СОЗНАНИИ

Рассматриваются результаты свободного ассоциативного эксперимента на стимул-имя концепта "Russia" с целью выявления актуального содержания данного концепта в американском языковом сознании. Выявлено, что Россия ассоциируется у американцев с различными стереотипами, связанными с природой/климатом, политикой, историей, культурой, географическими названиями. Отрицательные ассоциации в отношении России представлены незначительно. В результате сравнения полученных ассоциаций с представленными в американском тезаурусе сделан вывод о смене образа России у американского народа от образа государства к образу страны и живого народа.
Ключевые слова: концепт, ассоциативный эксперимент, ассоциация, образ России, американское языковое сознание.

M.V. Zimina, I.V. Vashunina

THE CONCEPT OF "RUSSIA" IN THE AMERICAN LINGUISTIC CONSCIOUSNESS

The results of a free associative experiment on the stimulus-name of the "Russia" concept are considered in order to identify the actual content of this concept in the American linguistic consciousness. It has been revealed that among Americans, Russia is associated with various stereotypes related to nature/climate, politics, history, culture, and geographical names. Negative associations with respect to Russia

© Зимина М.В., Вашунина И.В., 2020