УДК 811.111

СЕМАНТИЧЕСКИЙ АНАЛИЗ АНГЛИЙСКИХ ТЕРМИНОВ-ФРАЗЕОЛОГИЗМОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.Я. Долгоновская

Московский городской педагогический университет, Москва

dolgonovskaya@list.ru

Поступила в редакцию 29.09.2017

Исследуются характерные признаки терминов-фразеологизмов, проводится этимологический и семантический анализ. Выявлены особенности функционирования данных терминов, а также приведены примеры на английском языке из специализированной литературы.

Ключевые слова: термины-фразеологизмы, семантический анализ терминов, информационная безопасность.

Терминология в области информационной безопасности представляет собой довольно обширное поле для лингвистических исследований. Во многом это обусловлено тем, что терминологический запас данной области знаний пополняется постоянно в связи с развитием информационных технологий и необходимостью описания новых методов и явлений. Следует отметить, что терминологический словарь информационной безопасности также расширяется благодаря развитию таких смежных дисциплин, как информатика, кибернетика и криптография, поскольку их термины используются при описании многих аспектов безопасности компьютерных систем.

Термины-фразеологизмы (иногда их еще называют составными терминами) представляют особый интерес для исследователей ввиду их широкого употребления на практике и сложности для понимания неспециалистами. Следует упомянуть, что значение терминов-фразеологизмов, как и фразеологизмов в лингвистике, не является суммой значений составляющих их терминоэлементов. По мнению К.Я. Авербуха, «…большая часть единиц номинации не может быть в собственном смысле охарактеризована как лексическая единица, так как содержит в своем составе более одной словесной позиции ... и это никак не продвинет нас в определении их статуса как единицы описания, ибо принципы описания фразеологизмов существенно отличаются от сложившихся традиций описания единиц номинации» [1]. В связи с этим, при описании таких терминологических единиц мы опирались на их семантику, но не обходили вниманием и форму внешнего выражения слова. Мы согласны с точкой зрения, выраженной в статье об упорядочении современной терминологии: «Поскольку терминосистема является открытой и постоянно пополняющейся в силу необходимости отражения новых замеченных свойств и сторон объекта новыми монолексемными и полилексемными терминами, при моделировании этой системы желательно оказывать предпочтение мотивированным терминам, имеющим прозрачную смысловую структуру» [2].

Для нашего анализа мы старались подобрать такие термины, которые имели непрозрачную смысловую структуру и потому могли представлять сложность для понимания и перевода. Например, такой термин-фразеологизм как *evil twin* (разновидность атаки в беспроводных сетях, заключающаяся в создании точки доступа, которая копирует оригинальную и безопасную точку с целью получения доступа к конфиденциальной информации). *Злой двойник* пришел из общеупотребительной лексики, где он встречается в сфере литературы и кино, обозначая антипод главного героя, схожий с ним внешне, но отличный от него по характеру. **Cybercriminals build evil twin hotspots to allow them to both eavesdrop on network traffic and insert themselves into the data conversation between the victims and their destination servers* [3].

Термин *honeypot,* очевидно, прошел процесс терминологизации из предметно-бытовой лексики, где обозначал ёмкость с мёдом. В сфере информационной безопасности он стал термином-фразеологизмом, описывающим *ресурс-приманку* для злоумышленников, цель которого привлечь их внимание и заставить совершить взлом. Данные о такой атаке впоследствии анализируются и применяются для защиты информационных ресурсов от последующих взломов. Таким образом, при образовании этого термина-фразеологизма мы видим пример метафорического переноса на основании сходства свойств предметов: в данном контексте это свойство мёда притягивать к себе насекомых, так же как ресурс-приманка будет

притягивать злоумышленников. **Honeypots can also be described as being either low interaction or high interaction, a distinction based on the level of activity that the honeypot allows an attacker* [4].

Некоторые слова, хорошо знакомые многим, часто подвергаются процессу терминологизации, поскольку «языковая деятельность объясняется разумной целесообразностью» [5]. Другими словами, специалистам проще использовать известные и понятные людям слова в новом контексте, нежели придумывать и затем внедрять в терминологию новые терминологические единицы. Так произошло и со словом *zombie*, пришедшим из поп-культуры. В сфере информационной безопасности это слово превратилось в термин, который обозначает компьютер в сети, зараженный вирусом и используемый третьими лицами для рассылки спама или перенаправления трафика. Таким образом, компьютер-зомби, как и фантастический персонаж с телеэкрана, выполняет команды злоумышленника, который завладел доступом к этому компьютеру.

**There are millions of zombie computers in the world, about one-fourth of them located in the United States [6].*

В таких дисциплинах, как логика и теория вероятностей, известен «парадокс дней рождения». Суть его в том, что в группе из 23 испытуемых велика вероятность (более 50%) совпадения дней рождения хотя бы у двух человек. По аналогии с данным парадоксом метод криптоанализа, заключающийся в переборе открытых текстов для взлома шифра, получил название *birthday attack*. Злоумышленник, опираясь на статистические данные, пытается соотнести открытые тексты, зная, что вероятность обнаружить уязвимость для взлома крайне велика.

**Although methods of preventing Birthday Attacks have already been invented1, it is interesting to discuss the Birthday Attack since we can observe how often simple mathematical ideas may be applied to be used as a form of a cyberattack* [7].

Zero day attack – это те уязвимости системы или программы, которые производители ПО не сумели ликвидировать в срок. Сам термин предполагает, что у производителей не было дней, чтобы обнаружить и устранить эти уязвимости. Кроме того, *zero day attack* описывает уязвимости, для устранения которых еще не выпустили обновления, то есть они остаются до этого момента потенциально опасными.

**Zero-day attacks occur because of a zero-day vulnerability window that exists between the time a threat is discovered and the time a security patch is released* [8].

В профессиональной среде информационной безопасности распространен термин-фразеологизм *logic bomb*. Это особая программа, которая запускается при определенных условиях с целью хищения или искажения информации. Прилагательное «логический» в данном случае не имеет отношения к логике как таковой, а указывает на применяемый в информатике, а также во многих языках программирования тип данных. Логический тип данных, или булев тип, может принимать два значения, иногда называемых истиной (true) и ложью (false). Исполнение программы напрямую зависит от того, какое значение было принято. Иначе говоря, *логическая бомба* может быть незаметна пользователю, когда, например, тип данных принимает значение true, однако как только значение меняется на false, бомба «активируется». **The logic bomb dictated the date and time the malware would begin erasing data from machines to coordinate the destruction across multiple victims* [9].

Термины-фразеологизмы, описывающие людей, которые имеют прямое отношение к информационной безопасности и, по сути, обеспечивают её, также представляют интерес для терминологов. Например, такая антонимичная пара как *white hat* и *black hat*. *Белая шляпа*, или *этичный хакер*, это прежде всего специалист в области информационной безопасности, который использует свои навыки на благо людям и тестирует уязвимые системы. Прямо противоположен ему термин *черная шляпа*, хакер, который взламывает защищенные системы для личной выгоды. Оба термина пришли из поп-культуры, а именно из вестернов, где положительный персонаж носил белую шляпу, а отрицательный – черную. Позднее, по аналогии с этими двумя терминами, появляется третий термин *gray hat* для описания хакера, который работает с правительством и спецслужбами, то есть, по сути, находится посередине между белой и черной шляпами. **White hats disclose vulnerabilities to software vendors so they can be fixed; black hats use or sell them to other criminals to conduct crimes; gray hats disclose or sell them to governments to be used for hacks against adversaries and criminal suspects* [10].

Часто употребляется в профессиональной сфере такой термин, как *backdoor*. Основной целью *бэкдора* является получение несанкционированного доступа к конфиденциальной информации. Разработчик, создающий бэкдор, намеренно оставляет лазейку в программном коде, чтобы в дальнейшем можно было удаленно управлять компьютером жертвы или получать с него закрытую информацию. Отсюда видна связь с черным ходом в дом, предназначенным для служебных нужд. **PoisonTap "in-*

stalls a web-based backdoor in HTTP cache for hundreds of thousands of domains and it works even when a computer is password-protected," Kamkar said [11].

На основании проведенного анализа терминов-фразеологизмов можно установить, что терминология информационной безопасности тесно связана с логикой, статистикой, информатикой (из которой, по сути, эта сфера и возникла). Кроме того, большое влияние на образование новых терминов оказывают поп-культура (*zombie computers, white hats, evil twin*) и обиходная сфера общения (*honeypot, backdoor*). Данная область знания располагает большим объемом практического материала, часть которого была проанализирована в этой статье для наглядности. Проведенный анализ может быть впоследствии дополнен новыми терминами-фразеологизмами, которые постоянно входят в употребление в сфере обеспечения информационной безопасности.

Список литературы

1. Авербух К.Я. Средства специальной номинации и проблема их описания в словарях разных типов // Вестник ННГУ. 2015. № 3. С. 237–241.

2. Скуратов И.В., Сорокина Э.А. К вопросу об упорядочении современной терминологии и условий создания терминосистем (на материале французского и русского языков) // Вестник Московского государственного областного университета. Сер.: Лингвистика. 2016. № 2. С. 173.

3. http://www.techrepublic.com/article/minimizing-the-threats-of-public-wi-fi-and-avoiding-evil-twins/ (дата обращения: 23.09.2017).

4. https://www.computerworld.com/article/2573345/security0/honeypots--the-sweet-spot-in-network-security.html (дата обращения: 23.09.2017).

5. Авербух К.Я. Общая теория термина. М.: МГОУ, 2006. С. 55.

6. https://www.britannica.com/technology/zombie-computer (дата обращения: 23.09.2017).

7. http://www.pumj.org/docs/Issue1/Article_3.pdf (дата обращения: 23.09.2017).

8. https://www.symantec.com/connect/blogs/guide-zero-day-exploits (дата обращения: 23.09.2017).

9. https://www.wired.com/2013/03/logic-bomb-south-korea-attack/ (дата обращения: 23.09.2017).

10. https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/ (дата обращения: 23.09.2017).

11. https://www.computerworld.com/article/3142131/security/hacker-can-backdoor-your-computer-and-router-in-30-seconds-with-5-poisontap-device.html (дата обращения: 23.09.2017).

SEMANTIC ANALYSIS OF ENGLISH INFORMATION SECURITY IDIOMATIC TERMS

L.Ya. Dolgonovskaya

The article examines distinctive features of idiomatic terms and provides etymological and semantic analysis of these terms. The author has studied the peculiarities of usage of such terms and has provided examples from specialized literature in English.

Keywords: idiomatic terms, semantic analysis, information security.

Refertnces

1. Averbuh K.Ya. Sredstva special'noj nominacii i problema ih opisaniya v slovaryah raznyh tipov // Vestnik NNGU. 2015. № 3. S. 237–241.

2. Skuratov I.V., Sorokina Eh.A. K voprosu ob uporyadochenii sovremennoj terminologii i uslovij sozdaniya terminosistem (na materiale francuzskogo i russkogo yazykov) // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Ser.: Lingvistika. 2016. № 2. S. 173.

3. http://www.techrepublic.com/article/minimizing-the-threats-of-public-wi-fi-and-avoiding-evil-twins/ (data obrashcheniya: 23.09.2017).

4. https://www.computerworld.com/article/2573345/security0/honeypots--the-sweet-spot-in-network-security.html (data obrashcheniya: 23.09.2017).

5. Averbuh K.Ya. Obshchaya teoriya termina. M.: MGOU, 2006. S. 55.

6. https://www.britannica.com/technology/zombie-computer (data obrashcheniya: 23.09.2017).

7. http://www.pumj.org/docs/Issue1/Article_3.pdf (data obrashcheniya: 23.09.2017).

8. https://www.symantec.com/connect/blogs/guide-zero-day-exploits (data obrashcheniya: 23.09.2017).

9. https://www.wired.com/2013/03/logic-bomb-south-korea-attack/ (data obrashcheniya: 23.09.2017).

10. https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/ (data obrashcheniya: 23.09.2017).

11. https://www.computerworld.com/article/3142131/security/hacker-can-backdoor-your-computer-and-router-in-30-seconds-with-5-poisontap-device.html (data obrashcheniya: 23.09.2017).