

DOI: 10.33184/dokbsu-2026.3.6

Английская терминология в сфере кибербезопасности

М. Е. Букеева*, Т. В. Долгова

Омский государственный технический университет

Россия, 644050 г. Омск, пр. Мира, 11.

**Email: mbuluchevskaya@mail.ru*

Статья посвящена исследованию возникновения терминов в сфере кибербезопасности в английском языке. Авторы рассматривают возможные социокультурные основания при продуцировании данных терминов, а также их концептуальное своеобразие. Отличительной особенностью данных лексических единиц является их переход в другие языки без возможности адекватного перевода (на примере русского и немецкого языков). Таким образом, английская терминология в сфере кибербезопасности рассматривается, во-первых, как сложное гибридное явление, которое для понимания требует специализированных профессиональных знаний, а также владения соответствующими концептами, а во-вторых, выступает безэквивалентной лексикой, в частности в русском и немецком языках.

Ключевые слова: терминология, кибербезопасность, гибридная лексика, концепт, безэквивалентная лексика.

Современный мир уже невозможно представить без Интернета, смартфона, различного рода умных приспособлений и устройств, искусственного интеллекта и глобального информационного пространства. Все мы в той иной мере, вынужденно либо добровольно участвуем в цифровизации. Отметим, что государственная политика в Российской Федерации в сфере развития цифровых технологий шагает в ногу со временем и с 2018 по 2024 гг. была направлена на активное внедрение программы «Цифровая экономика РФ» [1].

В связи с этим определенной интерес для лингвиста представляет изучение лексического своеобразия в сфере компьютерной безопасности. Однако в ходе исследования авторы столкнулись с тенденцией повсеместного внедрения правил кибербезопасности в различных сферах жизни и деятельности людей. Мы видим, что специальная лексика и термины, характерные для рассматриваемой сферы, активно употребляется и вне компьютерной среды.

В статье рассматриваются социокультурные предпосылки, способствующие возникновению концептуальных лексических единиц в сфере кибербезопасности в английском языке, а также нестандартные способы словообразования в этой среде.

Данная тема представляется **актуальной** поскольку возникновение новой лексики в сфере кибербезопасности происходит непрерывно, как правило, в английском языке (в т.ч. в американском варианте английского языка), но специфика данной области такова, что аналогов в других языках указанной новой лексике зачастую не обнаружено. Таким образом широкомасштабная цифровизация с одной стороны и безэквивалентная лексика с другой провоцируют нас становиться активными пользователями заимствованных и зачастую непонятных иностранных терминов.

Цель работы – проанализировать социокультурные предпосылки возникновения новых лексических единиц в сфере кибербезопасности на материале англоязычной лексики, продемонстрировать внедрение узкоспециализированных англицизмов в немецкий и русский языки.

Научная новизна статьи связана с минимальной изученностью рассматриваемых терминов, многие из которых ассимилируются в русском и немецком языках, но никогда не рассматривались с этимологической точки зрения. Кроме того, анализ лексических единиц доказывает, что нет четких правил для образования неологизмов в данной сфере. Исследование отобранного материала свидетельствует о процессах гибридизации, которые происходят на морфологическом, лексическом, концептуальном уровнях. Специфика сферы кибербезопасности такова, что в ней большее значение имеют информативность, метафоричность, языковая экономия и визуальная компактность, нежели привычные нормы языка.

В качестве материала исследования первоначально были отобраны научные статьи на английском языке с сфере кибербезопасности, из которых была сформирована база терминов, актуальных в последнее время [2]. При более детальном рассмотрении авторы заметили использование большого процента отобранной лексики также в русскоязычных научных журналах. Более того, было отмечено, что многие профессиональные выражения уже употребляются в самых разнообразных сферах жизни: на сайте банков, отелей, коммунальных служб и так далее. Как отмечает А. В. Палкова, осуществляется «трансферт специализированной лексики в социально-бытовую сферу» [3, с. 10].

Следует еще раз подчеркнуть, что в русском языке нет аналогов у большинства рассматриваемых слов. Мы видим полное или частичное калькирование, применение транскрипции и транслитерации, либо написание на русском языке заимствованного английского слова. Проанализировав более трехсот лексических единиц, авторы задались вопросом, как человек далекий от сферы компьютерной и информационной безопасности может понять предостережения, в основе которых лежат английские реалии. Так как концепты имеют «национальные особенности содержания и структуры», они могут быть не до конца поняты при переносе в другую культуру [4, с. 22].

В ходе исследования были использованы следующие методы:

1. метод сплошной выборки для сбора материала;
2. контекстуальный анализ для понимания ситуативного использования того или иного слова и выражения;
3. этимологический и структурно-семантический анализ, которые дают возможность понять природу возникновения слова. Особенно продуктивно совместное использование этих методов для понимания процессов словообразования в телескопических единицах;
4. сопоставительный анализ, потребовавшийся для сравнения функционирования рассматриваемой лексики в английском, русском и немецком языках;
5. концептуальный анализ для понимания метафорических образований.

С развитием цифровых технологий увеличивается количество киберугроз и уязвимость информационного поля. Сегодня многие аспекты жизни связаны с цифровыми технологиями: работа государственных учреждений, частных компаний, авиа- и железнодорожного транспорта, больничного сервиса, учебных заведений и это, разумеется, не полный список. Понятие кибербезопасности стало близко обычному человеку, в силу пользования мобильным телефоном, компьютером и различными «умными» устройствами. Развитие технологий влечет за собой и рост преступных проникновений в частное пространство. В рамках данной статьи нас интересует, как происходит «зарождение» новых слов для обозначения способов кибератаки и защиты от них, что способствует закреплению неологизма. Узкая специфика рассматриваемой отрасли обуславливает не просто появление новой лексической единицы, а одновременно – нового термина.

С целью анализа способов словообразования и условий возникновения лексических единиц рассматриваются характерные и актуальные для данной сферы термины.

Прежде всего стоит сказать, что сфера кибербезопасности сравнительно молодая, история ее возникновения и развития берет свое начало в 70-е гг. в США. Так, первый компьютерный вирус, получивший имя Creeper, появился в 1971 г. Это была вредоносная программа, названная в честь антигероя из мультипликационных фильмов, который мог проходить через стены (его имя образовано от английского глагола «сгеер» – ползти, подкрадываться). Это название, которое мы можем характеризовать как концептуальную метафору [5], распространилось по всему миру, но мало кто сможет объяснить его этимологию, т.к. оно непосредственно связано со специфическим объектом американской культуры.

С этого времени происходит нарастание количества угроз в информационно-компьютерном, а позже и цифровом пространстве, и, как следствие, возникают ответные

меры, направленные на обеспечение безопасности. Статистические данные последних нескольких лет непрерывно отображают, что большая часть киберугроз происходит в США, однако в последние три года Россия выходит на второе место в общем рейтинге стран, на которые направлены атаки. Для нашего исследования эта информация имеет важное значение, поскольку этимология большинства английских терминологических единиц не понятна и не очевидна. Исследование практического материала свидетельствует, что англоязычная специализированная лексика в сфере кибербезопасности характеризуется как сложное многомерное явление, возникающая как синтез профессионального знания и коллективного авторского социокультурного опыта. Доказательством данной гипотезы служат такие единицы как: phishing, vishing, smishing, botnet, malware, firewall, spoofing, honey kit и т.д.

Необходимость номинации вызвана прагматическим аспектом, поскольку появившаяся реальность требует наименования. Уникальность нового явления требует нестандартного названия, так может совмещаться компьютерная тематика и обыденная лексика. Большое значение имеет концептуальное авторское восприятие, которое закладывает в неологизм особый смысл.

Слово phishing впервые употребил Эд Стенсел в 1997 г. и по одной из версий оно является результатом морфологической трансформации. Фишинг (phishing) означает «выуживание» данных, в английском языке данный процесс ассоциируется с рыбалкой. Замена морфемы f на ph возможно произошла с учетом существующего языка программистов Нахор, в котором используются непривычные знаки и символы, заменяющие стандартные буквы английского алфавита. Например: Phishing can be fun if you have right bait. Та же фраза, но написанная на языке Нахор: Phi5hiNg c@n 83 fun iF y0U H@V3 tHe RlgH7 8aI7 [6]. Таким образом словообразовательный процесс проходит в несколько этапов, во-первых, возникновение устойчивой ассоциативной связи между двумя процессами – ловлей рыбы и вылавливаем закрытой информации в сети, во-вторых, морфологическое преобразование из-за особенностей сферы функционирования данной лексемы.

Существует вторая версия возникновения термина «phishing» – от сочетания слова phreak (или phreaking) с fishing. В конце 60-х гг. в Америке появляется и развивается телефонное мошенничество, фриками (phreaks) называли людей, которые осуществляли мошенническую деятельность с помощью телефонов. Она соответственно получила имя phreaking. По аналогии с phreaking возникает название fishing, в котором меняется первая буква «f» на буквосочетание «ph».

Обе версии представляют собой нестандартный путь словообразования, результатом которого становится сложный синтезированный неологизм. Процесс формирования

новой лексической единицы проходит на концептуальном, семантическом, лексическом, а также морфологическом уровнях. Это дает основание полагать, что возникает новое гибридное явление, предпосылкой для которого служит социокультурная среда и прагматические цели профессионально-ориентированной аудитории.

Хотим отметить, что слово phishing продолжает свое функционирование теперь и в русском языке, и немецком языках. Одна из особенностей лексических единиц сферы кибербезопасности – отсутствие аналогов для большинства лексем в русском языке. Так, на сайтах банков, государственных учреждений, в научных статьях мы находим употребление слова phishing в его англоязычном варианте. Вероятно, у большинства людей возникает ассоциация с процессом рыбалки, но понять смысл данного термина и объяснить замену морфем – задача сложная. Рассматриваемый термин ассимилировался в русский язык настолько, что встречается его написание кириллицей в текстах, предостерегающих о киберопасности, например: «Как распознать фишинговое письмо и не стать жертвой фишинга» [7]. При переводе слова на русский язык, конечно, теряется часть словообразовательных процессов, поскольку мы видим фишинг и не предполагаем, что в английском языке используется морфема «ph», а не «f».

Аналогичная ситуация прослеживается в немецком языке. Термины из сферы цифровой безопасности активно проникают в повседневную жизнь людей и смешиваются с общеупотребительной лексикой, при этом их объяснение массовой аудитории иногда занимает несколько предложений. Так, на сайте Правительства Германии размещена предостерегающая информация от фишинговых атак в форме электронных писем: Warnung vor Phishingmail im Namen der Bundesregierung, (ср. рус: Предупреждение о фишинговой рассылке от имени Федерального правительства). Данное предупреждение требует дальнейшего детального объяснения сути упомянутого явления только из-за использования лексемы «Phishing». Derzeit werden vermehrt E-Mails im Namen der Bundesregierung verschickt, die NICHT VON DER BUNDESREGIERUNG STAMMEN und betrügerische Absichten beinhalten. Unserem Bürgerservice wurden mehrere solcher Phishing-Angriffe gemeldet (ср. рус.: В настоящее время от имени Федерального Правительства рассылается все больше электронных писем, которые не имеют отношения к Правительству и содержат мошеннические намерения. Нашему центру по работе с населением стало известно о нескольких таких фишинговых атаках).

Wir bitten Sie – seien Sie wachsam, öffnen Sie keine E-Mails, die Ihnen zweifelhaft erscheinen, klicken Sie auf keine Links und öffnen Sie keine Dateianhänge, die in der Mail enthalten sein könnten. Woran Sie Phishing-Mails erkennen. Ср. рус.: Мы просим вас – будьте бдительны, не открывайте сомнительные электронные письма, не переходите по ссылкам и не открывайте вложенные файлы, которые могут быть в письме. Как распознать фишинговые письма [8].

Рассмотренные примеры демонстрируют, как проникает специализированная лексика из сферы кибербезопасности в бытовую сферу в немецком и русском языках, ассимилируется, подстраивается под грамматические правила и нормы языков. Без детального объяснения рядовые «пользователи» компьютера не смогут проследить этимологию слова и понять его значение. Это не единичный случай, а скорее правило для всей англоязычной лексики в сфере кибербезопасности.

Рассмотрим некоторые названия вирусов и вредоносных программ, наиболее известные: Trojans, spyware, adware, worms. Итак, вирусы trojans или «трояны» уже известные многим, впервые были упомянуты в 1974 г. и, очевидно, имеют ассоциативную связь с Троянским конем. Вирус маскируется под безвредное программное обеспечение и наносит урон изнутри. Метафоричность названия отображает специфику действия вируса и активирует соответствующие концепты у специалиста в данной области. Профессионально неподготовленному пользователю сложно установить связь между наименованием вируса и Троянским конем, упомянутом в мифах Древней Греции. В русском языке данная лексическая единица используется как существительное троян или трояны во множественном числе. Вирус «spyware» от англ. «spy» – шпион, «software» – программное обеспечение, устанавливается на компьютер без ведома пользователя и собирает данные. В русском языке мы встречаем наименование этого вируса как «Спайвэр/спайвэры. В немецком языке название данного вируса, также используется в английском варианте, несмотря на то что есть немецкое слово «Spion» – шпион. Например: Die beste Methode zum Entfernen von Spyware ist ein Anti-Spyware-Scanner (ср. рус.: Лучший способ удалить шпионское программное обеспечение – использовать антишпионский сканер) [9]. Примеры демонстрируют нам, что лексема заимствуется в русский и немецкий языки, сохраняет концептуальное значение, но подстраивается под грамматические правила.

Следует упомянуть, что непрерывное развитие сферы кибербезопасности обеспечивает постоянное появление неологизмов, которые, как правило, за счет узкоспециализированной направленности являются терминами. Так, в немецком языке отмечается «присущая неологизмам вариантность морфологических свойств и орфографической фиксации» [10, с. 293].

Значительный пласт лексики в сфере кибербезопасности транспортируется в другие языки из английского языка и американского английского в большей мере, поэтому для понимания этимологии лексических единиц следует учитывать национальную концептосферу данной страны. Однако компьютерная среда является местом пересечения различных сфер деятельности человека, специалистов различного профиля и разных культур, поэтому терминологические единицы могут отличаться гибридным характером. Это свойство непременно отображается на семантическом и морфологическом уровне слова.

Уникальность и концептуальная неповторимость терминов в сфере кибербезопасности, как правило, приводит к переходу данных терминов в другие языки без замены на аналогичные понятия. Это объясняется отсутствием идентичных культурных реалий в других языках (вышеприведенные пример Creeper), громоздкостью конструкции при переводе (phishing и т.д.) и закрепленным образом в сознании пользователей, который теряется при переводе.

Литература

1. Минцифры. Национальная программа «Цифровая экономика Российской Федерации» [электронный ресурс]. URL: <https://digital.gov.ru/target/naczionalnaya-programma-czifrovaya-ekonomika-rossijskoj-federaczii>
2. Journal of Cybersecurity [website]. Oxford University Press. URL: <https://slogix.in/research/journals/journal-of-cybersecurity/>
3. Палкова А. В. Лексический ресурс носителей немецкого языка – пользователей Интернета: автореф. дис. ... М.: МГУ, 2005. 24 с.
4. Антология концептов / под ред. В. И. Карасика, И. А. Стернина. Т. 1. Волгоград: Парадигма, 2005. 352 С.
5. Лакофф Д. Джонсон М. Метафоры, которыми мы живем / пер. с англ. А. Н. Баранова и А. В. Морозовой; под ред. и с предисл. А. Н. Баранова. М.: УРСС, 2004. 252 с.
6. Спецпроекты СберСова. Эволюция живца или как менялся фишинг [электронный ресурс]. URL: <https://sbersova.ru/sections/protection/evolyuciya-zhivca-ili-kak-menyalsya-fishing>
7. Фишинговые письма: как распознать мошенников и защититься. Kaspersky [электронный ресурс]. URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-email>
8. Федеральное правительство (ФРГ) [электронный ресурс]. URL: <https://www.bundesregierung.de/breg-de/service/archiv-bundesregierung/phishing-mail-betrug-2043820>
9. Spyware Entfernung. Avast [website]. URL: <https://www.avast.com/de-de/c-spyware-removal-tool>
10. Буренкова С. В. Problemgerechte Klima-Sprache как инструмент языковой политики Германии на современном этапе // Немецкая филология в Санкт-Петербургском гос. ун-те. 2024. Вып. 14. С. 275–297. URL: <https://doi.org/10.21638/spbu33.2024.114>

English terminology in the field of cybersecurity

M. E. Bukeeva*, T. V. Dolgova

Omsk State Technical University

11 Mira st., 644050 Omsk, Russia.

*Email: mbuluchevskaya@mail.ru**

The article is devoted to the study of the emergence of terms in the field of cybersecurity in English language. The authors consider the possible cognitive foundations for the production of these terms as well as their conceptual uniqueness. A distinctive feature of these lexical units is that they are borrowed by other languages without the use of adequate means of translation (for example in Russian and German). English terminology in the field of cybersecurity is taken, firstly, as a complex hybrid phenomenon that requires specialized professional knowledge and understanding of relevant concept, and, secondly, as words with no direct equivalents in the Russian and German languages.

Keywords: terminology, cybersecurity, hybrid lexis, concept, words with no direct equivalents in other languages.