УДК 81`11
Науч. спец. 10.02.20
DOI: 10.36809/2309-9380-2021-31-101-106

Диана Ильдаровна Имамгаязова
Башкирский государственный университет, соискатель кафедры современного русского языкознания, Уфа, Россия
e-mail: diana.imamgaiazova@gmail.com

Лексико-словообразовательные значения фрейма «malware» в медиатекстах на русском и английском языках

Аннотация. В статье рассматривается структура фрейма «malware» на материале текстов русскоязычных и англоязычных средств массовой информации (СМИ). С целью выявления взаимосвязи между глубинным и внешним уровнем фрейма проводится анализ лексико-словообразовательных значений (ЛСЗ) и пропозициональных схем, через которые актуализируются стереотипные знания о характере и действии вредоносных программ. Результаты исследования демонстрируют, что в англоязычных медиафрейм «malware» сопоставим по структуре с фреймом «болезнь»: слоты «симптомы», «способы заражения», «пораженные органы/системы» и т. д. заполняются специфическими лексическими единицами, активно используются неологизмы для отсылки к конвенциональным знаниям. В то же время в русскоязычных медиа основные ЛСЗ группируются вокруг субфрейма «компьютерный вирус», широко используются заимствование и калькирование, что приводит к смешению понятий в концептосфере «вредоносные программы».

Ключевые слова: медиафрейм, субфрейм, когнитивная модель, вредоносное ПО, когнитивная лингвистика.

Diana I. Imamgayazova
Bashkir State University, Degree-Seeking Student of the Department of Modern Russian Linguistics, Ufa, Russia
e-mail: diana.imamgaiazova@gmail.com

Lexical and Derivational Meanings of “Malware” Frame in Russian and Engish-Language Media Texts

Abstract. The article examines the structure of the “malware” frame based on the texts of the Russian and English-language media. In order to identify the relationship between the deep and external levels of the frame, an analysis of lexical and derivational meanings and propositional schemes is carried out, through which stereotyped knowledge about the nature and action of malicious programs is actualized. The research results demonstrate that in English-language media the malware frame is comparable in structure to the “disease” frame: slots “symptoms”, “methods of infection”, “affected organs/systems”, etc. are filled with specific lexical units, neologisms are actively used to refer to conventional knowledge. At the same time, in the Russian-language media, the main lexical and derivational meanings are grouped around the “computer virus” subframe, borrowing and calquing are widely used, which leads to a confusion of concepts in the concept sphere of “malware”.

Keywords: media frame, subframe, cognitive model, malware, cognitive linguistic.

Введение (Introduction)

Появление и трансформация медиафреймов отражает изменения в социально-коммуникативном пространстве, происходящие под влиянием информатизации экономики и социальных отношений. Формальные и содержательные характеристики современного медиадискурса, с одной стороны, зависят от распространения новых информационных технологий, с другой стороны, в значительной степени определяют восприятие и адаптацию технологий аудиторией СМИ.

Новые явления и понятия из области информационно-коммуникационных технологий (ИКТ) находят отражение в медиафреймах и впоследствии закрепляются в разговорном языке. Для терминов ИКТ, не получивших частотного упоминания в медиатекстах, употребление ограничено сферой профессиональной коммуникации или дискурсом отдельных сообществ. В настоящем исследовании концептосфера «информационная безопасность» рассматривается на материале русскоязычных и англоязычных массмедиа, что позволяет изучить процессы фрейминга новых понятий, актуальные для широких групп носителей данных языков.

Обращение к анализу фрейма «malware» / «вредоносная программа» обусловлено **целью** изучить структуру и содержание фрейма с позиций когнитивно-дискурсивного подхода. Для выявления взаимосвязи мыслительных операций и языковых единиц применяются методы фреймового моделирования, анализ лексико-словообразовательных моделей

и пропозициональных схем в медиатекстах о вредоносных программах / компьютерных вирусах.

В основе эмпирического исследования лежит гипотеза о схожести стереотипных знаний о кибербезопасности в глобальном медиадискурсе, что позволяет сопоставить материалы СМИ на русском и английском языках. Актуальность исследования обусловлена тем, что выбранный подход позволяет рассмотреть как глубинный уровень фрейма (уровень абстрактных структур / когнитивных моделей), так и его внешний уровень (языковые единицы). Данное направление востребовано как в современной когнитивной лингвистике, так и в междисциплинарных исследованиях, рассматривающих медиатексты в контексте политических, социальных и культурных процессов.

Теория фреймов берет свое начало в работах М. Минского, общие свойства и структуру фреймов исследуют О. В. Гусельникова, М. С. Белозерова, Т. В. Перуцкая и Е. В. Платонова. Эмпирические исследования концептосферы «malware» представлены работами А. А. Шиповской, Е. В. Исаевой и Р. Кроуфорда. Выводы в данной статье опираются на работы предшественников, а также результаты собственного исследования.

Методы (Methods)

В эмпирическую базу исследования входят материалы корпуса текстов англоязычных СМИ Corpus NOW (News on the Web / Новости в Сети Интернет), объём которого превышает 9 млрд слов из онлайн-газет, журналов и новостных порталов. Для анализа русскоязычных СМИ за аналогичный период времени проведен сбор первичных данных с использованием семантического поиска на платформе Google News (более 40 тыс. индексируемых источников).

Основные методы исследования эмпирического материала в работе — метод анализа фреймов и лексико-словообразовательный анализ.

Понятие фрейма введено М. Минским для структурирования и упорядочивания информации, входящей в базы данных в рамках теории искусственного интеллекта [1]. В широком смысле фрейм характеризуют как структуру, систему представления иерархических связей различных элементов. О. В. Гусельникова выделяет в содержании фрейма различные формы знаний о мире: статичные элементы, динамические сценарии, фиксацию одного момента в последовательности событий и семантические знания [2].

М. С. Белозерова и Т. В. Перуцкая представляют фрейм в виде сети, состоящей из вершинных узлов, которая наполняется объективной информацией по отношению к любой ситуации [3]. На нижних уровнях — слотах — содержатся дифференциальные характеристики и данные, которые уточняют структуру фрейма и актуализируют заключенную в нем информацию. Фреймирование осуществляется при наличии трех обязательных компонентов: создателя — субъекта, создаваемого — объекта и предиката — действия создания.

Метод анализа фреймов востребован в различных научных направлениях: от психологии до теории ИКТ. Е. В. Платонова приводит ряд специальных определений фрейма, характерных для отдельных дисциплин: «Фрейм — набор предположений об устройстве формального языка для выражения знаний, в качестве альтернативы для семантических сетей, или для исчисления предикатов; набор сущностей, по предположению исследователя, существующих в описываемом мире (метафизическая интерпретация понятия); ...организация представлений, хранимых в памяти (человека и/или компьютера) плюс организация процессов обработки и логического вывода, оперирующих над этим хранилищем...» [4, с. 199]

В качестве основных подходов к анализу фреймов можно выделить социокоммуникативный и лингвистический. В первом случае фрейм предстает как каркасная информационная структура, которая содержит данные о представлении тех или иных ситуаций, а во втором является одним из вариантов когнитивной модели — центрального элемента теории когнитивной лингвистики. В настоящем исследовании анализ фреймов используется для выявления универсальных когнитивных моделей, которые структурируют знания о вредоносных программах на основе стереотипных представлений.

По М. Минскому, основная часть терминалов большинства фреймов заполнена субфреймами, в результате чего образуются системы фреймов и семейства взаимосвязанных фреймов [1, с. 35–109]. О. В. Гусельникова выделяет во фреймовой структуре субфреймы — «...уровни, представляющие собой набор тематически единых признаков, — являются цепочками иерархически расположенных слотов» [2, с. 145]. В свою очередь, субфреймы состоят из слотов, объединенных по тематическому признаку. Каждый слот — это та или иная форма вербального выражения когнитивных признаков, причем один и тот же признак может быть частью сразу нескольких слотов.

Таким образом, фреймы и субфреймы встраиваются в уровневые иерархические системы представления знаний. Фреймы — базовые элементы лингвистической картины мира, определяющие тот или иной аспект репрезентации социальной реальности. Субфреймы — это тематические составляющие когнитивной модели, участвующие в формировании горизонтальной структуры фреймов. Слоты, составляющие субфреймы, выражаются в фактически существующих в информационном пространстве лексемах, относящихся к признакам фреймов.

В отечественной лингвистике достаточно подробно изучены концепты «Интернет», «сетевая культура» и «информационные технологии». Несколько исследований посвящены непосредственно концепту «компьютерный вирус». Так, А. А. Шиповская рассматривает сетевые юмористические тексты и пути репрезентации в них категории «вирус» [5].

Изучая концепт «вирус» на примере сетевого фольклора, автор выделяет его основные содержательные характеристики: 1) вредоносный характер; 2) отрицательное отношение общества к компьютерным вирусам и их создателям; 3) заражение через использование программного обеспечения, кажущегося безопасным; 4) способность перехватывать управление компьютером, удалять, похищать данные и рассылать нежелательную информацию, блокировать доступ в Интернет, нарушить работу программного обеспе-

чения и аппаратную часть компьютера; 5) основной источник вирусов — развлекательные ресурсы; 6) популярность темы вирусов в сетевом фольклоре и массовый характер прецедентных текстов [5, с. 125–126].

По результатам исследования А. А. Шиповская приходит к выводу, что концепт «компьютерный вирус» выстраивается на основе связи с существующими общими концептами национальной картины мира и других глобальных когнитивных моделей. В частности, наименование *троян* подчеркивает диверсионные свойства вирусов, *червь* — способность выводить системы из строя, а *зомби-вирус* — функцию несанкционированной рассылки сообщений [5, с. 128].

Исследуя лексемы концептосферы «вирус», Е. В. Исаева прибегает к методу трехмерного метафорического моделирования концепта «virus» на основе данных корпуса современного американского английского языка [6]. Исследовательница выделяет, наряду с социальным и биологическим/медицинским, компьютерный институциональный дискурс. В фокусе исследования находятся метафоры, используемые для характеризации концепта «вирус»: объект, агент, заболевание, заражение, инфекция, эпидемия, преступление и т. д. В совместном исследовании с Р. Кроуфордом Е. В. Исаева рассматривает концепт «вирус» также с позиции теории фреймов. По итогам изучения англоязычных медиатекстов авторы выделяют «центральные» субфреймы концепта «вирус»: «agent», характеризующий активность вируса и скрытый характер угрозы, и «patient», характеризующий пользователей зараженных компьютеров как жертв [7].

В настоящей работе проведено фреймовое моделирование и сопоставление лексико-словообразовательных значений, используемых для наименования вредоносных программ в русскоязычных и англоязычных медиатекстах. Это сочетание методов позволяет изучить глубинный уровень фрейм-структуры (пропозициональные схемы и уровень слотов) наряду с лексико-словообразовательными значениями конкретных словоформ, которые составляют поверхностный уровень фрейма.

Результаты и обсуждение (Results and Discussions)

В англоязычных медиатекстах фрейм «malware» / «вредоносная программа» реализуется посредством следующих лексико-словообразовательных значений (ЛСЗ):

1. ЛСЗ «вредоносные программы по способу их распространения»: *malicious adware / malvertising* — рекламное приложение, распространяющее вредоносный код; *phising email* — рассылка вредоносных программ через электронную почту; *malicious Web / mobile application* — вредоносные приложения в веб- и мобильной среде; *malicious USB devices* — USB-устройства, зараженные вредоносными программами. К примеру:

− *The **hidden adware** was also **injecting adverts** on to browsers* (BBC, 19.04.2019) — *Скрытое рекламное ПО также внедряло рекламу в браузеры* (здесь и далее перевод наш. — *Д. И.*).

− *The body of the **phising email** asked users to download a **malicious file*** (Fox Business, 14.04.2020) — *В теле фишингового письма пользователям предлагалось загрузить вредоносный файл.*

− ***A malicious USB** wall charger that could **deploy malware** on iOS devices* (ZDNet, 14.11.2019) — *Вредоносное зарядное устройство USB, которое может развертывать вредоносное ПО на устройствах iOS.*

Пропозициональная структура: объект — предикат — средство.

2. ЛСЗ «вредоносные программы по цели воздействия»: ransomware («программа-вымогатель») — вредоносная программа, нарушающая работу устройства и требующая оплаты за восстановление функциональности или данных; *spyware* («программа-шпион») — вредоносная программа для несанкционированного сбора / передачи данных; *stalkerware* («программа-сталкер») — вредоносная программа для несанкционированной слежки; *hijackware* («программа-угонщик») — вредоносная программа, изменяющая стартовые настройки в браузерах; *phising apps* («фишинг-приложения») — вредоносная программа для сбора персональных данных, в особенности платежных систем; *mining malware* — вредоносная программа, использующая мощности зараженного устройства для майнинга данных; *DDoS-malware* («Distributed Denial of Service», распределенная кибератака типа «отказ в обслуживании») — вредоносная программа, используемая для организации кибератаки такого типа. К примеру:

− *The company experienced **a ransomware attack** by one of the most active **ransomware malware*** (Forbes, 29.11.2020) — *Компания подверглась атаке вымогателей, использующих одну из самых активных вредоносных программ-вымогателей.*

− *Use of **'stalkerware' apps** that allow abusers **to spy on partners** soar by 93 % in pandemic* (Independent, 21.04.2021) — *Использование приложений-преследователей, которые позволяют лицам, нарушающим права других, шпионить за окружающими, в условиях пандемии возросло на 93 %.*

− *Most Docker **servers are infected** with **cryptocurrency-mining malware*** (ZDNet, 26.06.2020) — *Большинство серверов Docker заражены вредоносным ПО для майнинга криптовалюты.*

Пропозициональная структура: объект 1 — предикат — объект 2 — цель.

3. ЛСЗ «вредоносные программы по сходству с другим объектом»: *trojan* («троян») — вредоносная программа, скрытая под видом легитимного программного продукта; *worm* («червь») — вредоносная программа, проникающая на устройство через уязвимые компоненты других программ; *virus* («вирус») — вредоносная программа, проникающая на устройство в результате контакта с «зараженным» устройством / системой и обладающая свойством не проявлять себя до заданного момента; *bot / botnet* («бот» / «сеть ботов») — устройство и сеть устройств, находящаяся под несанкционированным контролем, полученным с помощью вредоносных программ. К примеру:

− ***Banking trojans** (...) have been **hiding under** the layers of COVID-19 related information* (Financial Express, 15.04.2020) — *Банковские трояны (...) скрываются под несколькими уровнями информации, связанной с COVID-19.*

− *WhatsApp* ***worm malware is infecting*** *contact list of users* (India Times, 30.01.2021) — *Вредоносный червь, разработанный под приложение WhatsApp, заражает список контактов пользователей.*

− *Microsoft has taken legal steps to dismantle* ***one of the world's largest botnets*** (Washington Post, 13.10.2020) — *Microsoft предприняла юридические шаги к тому, чтобы один из крупнейших в мире ботнетов лишился оборудования.*

Пропозициональная структура: объект 1 — предикат — объект 2.

4. ЛСЗ «устройство или система, пораженная вредоносной программой»: *MacOS/Windows malware* — вредоносная программа, нарушающая работу операционных систем MacOS/Windows; *browser malware* — вредоносная программа, нарушающая работу браузера; *iOS/Android malware* — вредоносная программа, нарушающая работу мобильных устройств с операционной системой iOS или Android; *rootkit malware* — вредоносная программа, нарушающая работу программных средств набора руткит; *BIOS malware* — вредоносная программа, влияющая на систему BIOS (basic input / output system, «базовая система ввода-вывода»). К примеру:

− *Adrozek is* ***browser-modifying malware****. When it infects a system it* ***injects itself into the victim's browsers*** (Forbes, 11.12.2020) — *Adrozek — это вредоносная программа, модифицирующая браузер. Когда она заражает систему, она внедряется в браузеры жертв.*

− ***Mac malware*** *developers have* ***jumped on*** *a recently disclosed* ***MacOS Gatekeeper*** *vulnerability* (ZDNet, 25.07.2019) — *Разработчики вредоносных программ для устройств Mac воспользовались недавно обнаруженной уязвимостью MacOS Gatekeeper.*

− *The official Google Play Store is the biggest* ***spreader of Android malware*** (Daily Express, 23.10.2020) — *Официальный магазин приложений Google Play — это крупнейший распространитель вредоносных программ для Android.*

Пропозициональная структура: объект — предикат — место.

5. ЛСЗ «вредоносные программы по признакам воздействия»: *freezing malware* — вредоносная программа, замедляющая работу устройства; *BSOD malware* — вредоносная программа, имитирующая появление BSOD (blue screen of death, «синий экран смерти»), информирующего о критической ошибке в системах Windows; *pop-up malware* — вредоносная программа, вызывающая запуск всплывающего окна. К примеру:

− *They (online criminals) forward documents which* ***include file-freezing malware*** (BBC, 05.01.2017) — *Они (онлайн-преступники) пересылают документы, которые содержат вредоносную программу, замораживающую файлы.*

− *Microsoft Warns That* ***A Fake BSoD Malware*** *Called Hicurdismos Is Spreading* (Forbes, 31.10.2017) — *Microsoft предупреждает о распространении вредоносной программы под названием Hicurdismos, которая имитирует критическую ошибку BSoD.*

− *Google Play Store removes gaming* ***apps with pop-up porn malware*** *(*India Express, 15.01.2018) — *Магазин Google Play удаляет игровые приложения с вредоносными программами, содержащими всплывающие окна с порнографией.*

Пропозициональная структура: объект — предикат — результат.

Лексико-словообразовательные значения фрейма «вредоносная программа» в англоязычных СМИ сопоставимы со структурой фрейма «болезнь», состоящего из схожих слотов: симптомы, способы заражения, пораженные органы/системы и т. д. Это позволяет авторам медиатекстов задействовать конвенциональные знания аудитории о биологических организмах и их болезнях при описании механизмов вредоносных программ, делая материал более понятным и удобным для восприятия.

В русскоязычных медиатекстах о вредоносных программах можно отметить меньшее разнообразие лексико-словообразовательных значений, прочно вошедших в дискурс СМИ, и высокую долю заимствований из английского языка. Многие деривативы относятся к субфрейму «вирус», который соответствует одному из видов вредоносных программ. Лишь немногие русскоязычные авторы обращаются к метафрейму «вредоносная программа», используя англицизмы или авторские неологизмы (*зловред, зловредный код*) для характеристики таких программ.

Лексико-словообразовательные значения и пропозициональные структуры (суб)фрейма «компьютерный вирус» в русскоязычных СМИ представлены следующими группами.

1. ЛСЗ «способ распространения вируса»: *вредоносные рассылки; рекламный вирус, браузерный вирус, почтовый вирус*:

− *Аналитики назвали самые популярные у мошенников* ***вредоносные рассылки*** (РБК, 18.10.2020).

− *При использовании таких приложений есть риск подхватить* ***рекламный вирус*** (Российская газета, 12.03.2021).

− ***Браузерный вирус*** *стал фаворитом хакеров в сентябре (*ИА Прайм, 09.10.2020).

Пропозициональная структура: объект — предикат — признак.

2. ЛСЗ «вирусы по цели воздействия»: *вирус-шпион, вирус-вымогатель, вирус-шифровальщик / шифровальщик*:

− ***Вирус-вымогатель*** *грозит пользователю смартфона полицией* (РИА Новости, 13.10.2020).

− *Чтобы заблокировать сервисы Garmin,* ***хакеры использовали шифровальщика-вымогателя*** (Российская газета, 20.11.2020).

− *Кто внедрил* ***вирус-шпион*** *в сети российских госорганов* (Lenta.ru, 30.06.2017).

Пропозициональная структура: объект 1 — предикат — объект 2.

3. ЛСЗ «устройство или система, пораженные вирусом»: *компьютерный вирус, мобильный вирус, Android-вирус, вредоносное мобильное приложение / ПО*:

− *Хакеры из FancyBear создали новый* ***компьютерный вирус*** (ИА Регнум, 13.08.2020).

− *На клиентов «Сбербанка» охотится опасный* ***Android-вирус*** (Ведомости, 05.04.2018).

− *Скачивание приложений из официальных магазинов снизит вероятность установки* ***вредоносного мобильного ПО*** (Gazeta.Ru, 15.01.2021).

Пропозициональная структура: объект 1 — предикат — признак.

4. ЛСЗ «вредоносные программы / вирусы по сходству с другим объектом»: *программа-вредитель; зловред / зловредный код; зомби-устройство / зомби-сеть*:

− *Вирусы — малая часть огромного мира* ***программ-вредителей*** (Российская газета, 20.11.2020).

− ***Зловредный код*** *запускает скрытую рекламу на устройствах* (Известия, 25.02.2019).

− ***Зомби-сети*** *превратились в эффективный способ заработка киберпреступников* (Lenta.ru, 28.06.2018).

Пропозициональная структура: объект 1 — предикат — объект 2.

В статьях русскоязычных СМИ о вредоносных программах активно используется заимствованная лексика: *фишинг, скрипт, софт, ботнет, троян, руткит* и др. Заполнение слотов фрейма «компьютерный вирус» с помощью англицизмов и кальки приводит к смешению понятий и не позволяет читателям, которые не владеют английским языком, выделить мотивационный признак наименования. К примеру:

− *В сети был выявлен* ***банковский троян*** *удаленного доступа* (Gazeta.Ru, 15.01.2021).

− *ФБР удалила* ***вредоносные скрипты*** *с сотен серверных компьютеров* (Forbes, 14.04.2020).

− *Россияне оказались частыми жертвами* ***шпионского софта*** (Ведомости, 04.10.2019).

Третья группа ЛСЗ в русскоязычных статьях наиболее продуктивна по количеству деривативов, что связано с укоренившейся в дискурсе СМИ метафорой «*компьютерный вирус = эпидемия*». Метафора порождает производные значения: *компьютерные эпидемии, неизлечимый мобильный вирус, заразились примерно 9000 машин*. Остальные группы ЛСЗ в целом соотносятся с англоязычными аналогами, но включают в себя меньшее число деривативов. Пропозициональные схемы, организующие слоты фрейма «malware», также отличаются большей вариативностью, нежели схема фрейма «вредоносная программа».

Субфрейм «компьютерный вирус» подчеркивает такие характеристики вредоносных программ, как заразность, высокая скорость и большой масштаб распространения (*широко распространившийся вирус*, *заразил тысячи компьютеров*). Метафора «вирус = живой организм» способствует заполнению слотов фрейма, отсылающих к биологической и соматической сфере (*родился новый червь*, *наплодить копии*, *сеть была парализована*).

Лексико-словообразовательные значения, используемые по признаку сходства компьютерного вируса с другим объектом, чаще всего заимствованы из английского языка. При калькировании языковых единиц (например, *троян, руткит*) частично утрачиваются их семантические связи. Например, субфрейм «trojan malware» сохраняет метафорическую связь с мифологемой «троянский конь», которая способствует считыванию значения термина — вредоносное ПО, скрытое под видом легитимного. Аналогично «rootkit malware» отсылает к значению «root» («корень, коренной») и транслирует имплицитное значение воздействия программы на базовый элемент системы — это конвенциональное знание доступно даже тем пользователям и читателям СМИ, которые не являются экспертами в информационных технологиях.

Ряд авторов из русскоязычных СМИ предпринимали попытки ввести неологизмы, характеризующие вредоносные программы. Специфическими для русскоязычного медиадискурса выступают субфреймы «зловредная программа / зловред», «вирус-вредитель» и «зомби-компьютер». Данные наименования подчеркивают такие характеристики вредоносных программ, как ущерб, негативные последствия запуска и вредительский характер, но не конкретизируют цели воздействия. Выявленные в англоязычных медиатекстах субфреймы точнее указывают на цели, характер и проявления воздействия.

Лексико-словообразовательные значения в структуре фрейма «malware» в англоязычных медиатекстах в высокой степени дифференцированы. Rootkit script, «worm», «trojan», «virus» — это отдельные родовые понятия, которые не смешиваются ни в текстах специализированных изданий, ни в медиатекстах, предназначенных для широкой аудитории.

Заключение (Conclusions)

В настоящем исследовании проведено сравнение структурных и содержательных компонентов медиафрейма «malware» / «вредоносная программа». В структурном плане представления фрейма в англоязычных и русскоязычных СМИ во многом схожи, что подтверждает гипотезу об универсальном характере когнитивных моделей, лежащих в основе понятия об информационной безопасности. В частности, в обоих случаях выделяются тематические субфреймы, уточняющие функции, свойства и характер воздействия вредоносных программ.

Концептуальное содержание фреймов изучается путем выявления групп лексико-словообразовательных значений и пропозициональных схем, используемых для описания вредоносных программ. На языковом материале выделены особенности фрейма, характерные для англоязычного и русскоязычного медиадискурса. В частности, в англоязычных СМИ для фрейминга вредоносных программ задействованы различные группы ЛСЗ, которые используются для наименования болезней: симптомы, способы распространения, пораженные органы/системы. В русскоязычных СМИ эти группы ЛСЗ представлены меньшим числом деривативов.

Для медиафрейма «malware» наиболее продуктивной группой ЛСЗ выступает «цель воздействия», которая активно пополняется авторскими неологизмами: *ransomware, spyware, stalkerware, hijakware* и др. Также у этой группы значений наиболее развернутая пропозициональная схема. В русскоязычных СМИ неологизмы чаще создаются по принципу сходства вредоносного ПО с иными объектами *(зомби-сеть, зловредный код)*, из-за чего понятие вредоносной программы в медиатекстах носит более абстрактный характер. Использование заимствованной лексики и кальки препятствует разворачиванию пропозиции.

Фреймовое моделирование объединяет концепции когнитивной лингвистики и теории информационных систем. Использование данного метода в анализе медиатекстов позволяет систематизировать анализ языковых единиц разного уровня и сопоставить их с мыслительными моделями, определяющими понимание текста.

Библиографический список

1. Минский М. Фреймы для представления знаний / пер. с англ. О. Н. Гринбаума. М. : Энергия, 1979. 152 с.

2. Гусельникова О. В. Терминологический аппарат структуры фрейма // Вестн. Челяб. гос. пед. ун-та. 2010. № 9. С. 137–149.

3. Белозерова М. С., Перуцкая Т. В. Субфрейм «производство» в структуре фрейма «намеренное создание объектов действительности» в современном английском языке // Современные подходы к изучению единиц языка и речи и вопросы лингводидактики. Белгород : Политерра, 2012. С. 29–32.

4. Платонова Е. В. Соотношение фрейма с содержательной структурой языковых выражений на примере фрейма «добродетель» // Симбирский научный вестник. 2012. № 2. С. 199–201.

5. Шиповская А. А. Репрезентация категории «Вирус» в прецедентных текстах юмористических жанров русскоязычной сетевой культуры // Современное общество и власть. 2017. № 4. С. 121–131.

6. Исаева Е. В. Модели метафоры в дискурсе компьютерной безопасности : автореф. дис. … канд. филол. наук. Пермь, 2013. 20 с.

7. Isaeva E. V., Crawford R. Semantic Framing of Computer Viruses: the Study of Semantic Roles' Distribution // Вестн. Перм. ун-та. Российская и зарубежная филология. 2019. Т. 11, вып. 1. С. 5–13. DOI: 10.17072/2073-6681-2019-1-5-13

References

Belozerova M. S., Perutskaya T. V. (2012) Subfreim "proizvodstvo" v strukture freima "namerennoe sozdanie ob"ektov deistvitel'nosti" v sovremennom angliiskom yazyke [Subframe "Production" in the Structure of the Frame "Intentional Creation of Objects of Reality" in the Modern English Language]*, *Sovremennye podkhody k izucheniyu edinits yazyka i rechi i voprosy lingvodidaktiki [Modern Approaches to the Study of Language and Speech Units and Questions of Linguodidactics]*.* Belgorod, Politerra Publ., pp. 29–32. (in Russian)

Gusel'nikova O. V. (2010) Terminologicheskii apparat struktury freima [Frame Structure Terminology], *Vestnik Chelyabinskogo gosudarstvennogo pedagogicheskogo universiteta [Bulletin of Chelyabinsk State Pedagogical University],* no. 9, pp. 137–149. (in Russian)

Isaeva E. V. (2013) *Modeli metafory v diskurse komp'yuternoi bezopasnosti [Metaphor Models in Computer Security Discourse]*,* Cand. philol. sci. diss. Abstr. Perm, 20 p. (in Russian)

Isaeva E. V., Crawford R. (2019) Semantic Framing of Computer Viruses: the Study of Semantic Roles' Distribution, *Vestnik Permskogo universiteta. Rossiiskaya i zarubezhnaya filologiya [Perm University Herald. Russian and Foreign Philology],* vol. 11, issue 1, pp. 5–13, doi: 10.17072/2073-6681-2019-1-5-13 (in English)

Minsky M. (1979) *[A Framework for Representing Knowledge].* Moscow, Ehnergiya Publ., 152 p. (in Russian)

Platonova E. V. (2012) Sootnoshenie freima s soderzhatel'noi strukturoi yazykovykh vyrazhenii na primere freima "dobrodetel' " [Correlation of Frame with Informative Structure of Language Expressions (Frame «Virtue» Case Study)], *Simbirskii nauchnyi vestnik [Simbirsk Scientific Bulletin]*,* no. 2, pp. 199–201. (in Russian)

Shipovskaya A. A. (2017) Reprezentatsiya kategorii "Virus" v pretsedentnykh tekstakh yumoristicheskikh zhanrov russkoyazychnoi setevoi kul'tury [Representation of the Category "Virus" in Precedent Texts of Humorous Genres of Russian-Language Network Culture], *Sovremennoe obshchestvo i vlast' [Contemporary Society and Government],* no. 4, pp. 121–131. (in Russian)

* Перевод названий источников выполнен автором статьи / Translated by author of the article.