

RU

## Милитарная метафора в англоязычном научно-популярном дискурсе по кибербезопасности: семантический, когнитивный, прагматический аспекты

Савченко А. А.

**Аннотация.** Цель исследования – выявление особенностей функционирования милитарных метафор в английских научно-популярных текстах, посвященных проблемам кибербезопасности. В статье рассматриваются номинации, метафорически используемые со значением «нападения» / «обороны»; определяются наиболее частотные метафоры; выделяются оригинальные метафоры; дается обоснование для метафорического переноса; анализируются контексты их употребления в семантическом, когнитивном и прагматическом аспектах. Научная новизна работы заключается в установлении наиболее значимых образов, репрезентирующих метафорическую модель «Виртуальное пространство – это война» в англоязычных научно-популярных текстах по кибербезопасности с использованием методов современной дескриптивной лингвистики. В результате установлено, что в англоязычном научно-популярном дискурсе метафорическая модель войны обладает большим потенциалом в интерпретации киберугроз и мер, направленных на их предотвращение. В анализируемых текстах она представлена фреймами «Военные действия», «Оружие и военный арсенал», «Участники военных действий и воинские подразделения», «Начало войны и ее итоги», «Воинские символы и атрибуты». В прагматическом аспекте использование милитарных метафор связано с необходимостью отобразить всю серьезность киберугроз, вызвать определенный эмоциональный отклик у целевой аудитории и таким образом мотивировать ее соблюдать правила кибербезопасности.

EN

## Military metaphor in English-language popular science discourse on cybersecurity: Semantic, cognitive and pragmatic aspects

Savchenko A. A.

**Abstract.** The study is aimed at revealing the peculiarities of military metaphor functioning in the English-language popular science texts on cybersecurity. The article considers the metaphor notions “attack” and “defence”, identifies the most frequent metaphors, highlights original metaphors, provides justification for metaphorical transfer and analyses the contexts of their usage in semantic, cognitive, and pragmatic aspects. The scientific novelty of the study lies in identifying the most significant images representing the metaphorical model “Virtual Space is War” in English-language popular science texts on cybersecurity using methods of contemporary descriptive linguistics. As a result, it has been determined that in the English-language popular scientific discourse, the metaphorical model of war has great potential for interpreting cyber threats and measures aimed at their prevention. In the analysed texts, it is represented by the following frames: “Military Actions”, “Weapons and Military Arsenal”, “Participants in Military Operations and Military Units”, “The Beginning of War and Its Outcome” and “Military Symbols and Attributes”. From a pragmatic perspective, the use of military metaphors is associated with the need to reflect the seriousness of cyber threats, evoke a specific emotional response from the target audience and thus motivate them to comply with cybersecurity rules.

### Введение

Актуальность нашего исследования обусловлена растущим интересом лингвистов к изучению метафоры в когнитивном аспекте. Исследователи отмечают, что метафора является не столько ярким тропом, сколько основной «ментальной операцией», позволяющей определенным образом структурировать окружающий мир путем объединения различных понятийных сфер. В связи с этим особый интерес представляют метафорические

модели, так как именно они являются «средством постижения, рубрикации, представления и оценки какого-то фрагмента действительности, в котором отражается национальное, социальное и личностное самосознание при помощи сценариев, фреймов и слотов, относящихся к совершенно иной понятийной области» (Чудинов, 2001, с. 48), а наблюдения за функционированием метафор признаются важным источником информации о человеческом мышлении.

Выбор тематики текстов также не случаен. Развитие новых технологий, цифровизация требуют как от обычных пользователей, так и от специалистов в данной сфере осведомленности о потенциальных угрозах и рисках в киберпространстве, чем объясняется достаточно большое число публикаций по этой теме.

Поставленная цель предполагает решение следующих задач:

- 1) раскрыть содержание понятия «милитарная/военная метафора» и установить лексические единицы, включенные в процесс метафоризации;
- 2) в исследуемом материале выявить наиболее частотные милитарные метафоры и фреймы;
- 3) выделить оригинальные метафоры и определить основания для метафорического переноса с учетом создаваемого ими эмоционального фона.

Для решения данных задач использовались следующие методы исследования: метод сплошной выборки – для сбора иллюстративного материала, лингвостилистический и контекстологический анализ текста – для выявления особенностей функционирования милитарных метафор в исследуемом дискурсе, метод метафорического моделирования – при описании фреймов и слотов, метод количественного и процентного подсчета – при определении пропорционального соотношения милитарных метафор разных фреймов.

Материалом для исследования послужили аутентичные статьи, посвященные актуальным проблемам кибер- и информационной безопасности, опубликованные на британских и американских новостных сайтах технологической направленности The Register (<https://www.theregister.com>), CNET (<https://www.cnet.com/tech/services-and-software>); в электронных англоязычных изданиях Infosecurity Magazine (<https://www.infosecurity-magazine.com>), Communications of the ACM (<https://arxiv.org/pdf/1407.5225.pdf>), New Scientist (<https://www.newscientist.com>), MIT Technology Review (<https://www.technologyreview.com>); на сайтах профессиональных обществ, сообществ и организаций IEEE UIT Computer Society (<https://www.computer.org/>), CSO Online (<https://www.csoonline.com>), Prey Project (<https://preyproject.com>), TechTarget (<https://www.techtarget.com>), StealthLabs (<https://www.stealthlabs.com>), а также на сайтах англоязычной прессы и новостных каналов в разделах «Технологии» и «Кибербезопасность», таких как CNBC (<https://www.cnbc.com>), CNN (<https://edition.cnn.com>), The Guardian (<https://www.theguardian.com>), The New York Times (<https://www.nytimes.com>), BBC (<https://www.bbc.com>), на интернет-портале Yahoo! (<https://www.yahoo.com/>), поисковой интернет-платформе Semantic Scholar (<https://www.semanticscholar.org/>). Иллюстративный корпус составляет 374 контекста употребления. Объем проанализированного материала – более 60 статей.

В качестве справочного материала были задействованы следующие словари: Безопасность пользователей в сети Интернет. Глоссарий. URL: <https://safe-surf.ru/glossary/>; Большая Российская энциклопедия. 2004-2017. URL: <https://old.bigenc.ru/>; Merriam-Webster Dictionary. URL: <https://www.merriam-webster.com/>; TechTarget Network. URL: <https://www.techtarget.com/whatis/definition/island-hopping-attack>.

Теоретической базой исследования послужили труды отечественных и зарубежных ученых, среди которых представлены работы, посвященные изучению метафоры в когнитивном аспекте (Лакофф, Джонсон, 2004; Будаев, Чудинов, 2007), метафорическому моделированию и дескрипторной теории метафоры (Баранов, 2004; 2014; Баранов, Михайлова, Шипова, 2006; Чудинов, 2001), милитарной метафоре в политическом (Крышталева, 2019; Чудинов, 2001) и спортивном (Кудрин, 2011; Мальшева, 2009) дискурсах.

Практическая значимость данного исследования заключается в том, что результаты работы могут быть использованы в курсах по стилистике, когнитивной лингвистике, лингвокультурологии.

## Обсуждение и результаты

### Содержание понятия «милитарная/военная метафора»

Идея противоборства присуща человеческому обществу на протяжении всей истории, что, несомненно, находит свое отражение в языке. Военная метафора является архетипичной, ее образы понятны представителям различных культур и поколений. Именно поэтому она широко используется в различных дискурсах, включая политический, медицинский, экономический и т. д. В этом смысле англоязычные научно-популярные тексты по кибербезопасности не являются исключением. Действия злоумышленников и меры противодействия компьютерным угрозам часто представляются в военных терминах, а киберпространство описывается как поле битвы. Таким образом, в соответствии с подходом метафорического моделирования, предложенным А. П. Чудиновым, А. Н. Барановым, виртуальное пространство может быть представлено в виде метафорической модели «Виртуальное пространство – это война», а языковые единицы из сферы источника «Война», репрезентирующие ее, классифицированы как милитарные метафоры.

Вслед за В. Е. Крышталевой к милитарным метафорам мы относим «номинации, в которых есть признаки военного действия в форме противостояния (“свой” – “чужой”, т. е. враг) с использованием оружия» (2019, с. 81). В анализируемом материале они представлены следующими существительными и глаголами: *ambush* – засада, *arms* – оружие, *army* – армия, *attack* – атака, атаковать, *attacker* – атакующий, *battle* – битва, сражаться,

*beat* – победить, *bomb* – бомба, *bulletproof* – пуленепробиваемый, *campaign* – кампания, *combat* – бороться, сражаться, *colonize* – колонизировать, *conquer* – завоевать, *counterintelligence* – контрразведка, *crusade* – участвовать в крестовом походе, *defender* – защитник, *defense* – оборона, *demobilize* – демобилизовать, *deploy* – развертывать, *deployment* – развертывание, *espionage* – шпионаж, *fight* – сражаться, сражение, *fleet* – флот, *guard* – охранять, *intelligence* – разведка, *intrusion* – вторжение, *raid* – налет, *siege* – осада, *storm* – штурм, *surrender* – капитуляция, *target* – направлять удар, *victory* – победа, *weapon* – оружие, *weaponize* – вооружать, *weaponry* – оружие, объединенными в такие понятийные сферы или фреймы, как «Военные действия», «Оружие и военный арсенал», «Участники военных действий и воинские подразделения», «Начало войны и ее итоги», «Воинские символы и атрибуты», количественное и процентное соотношение которых показано на рисунке (Рис. 1).

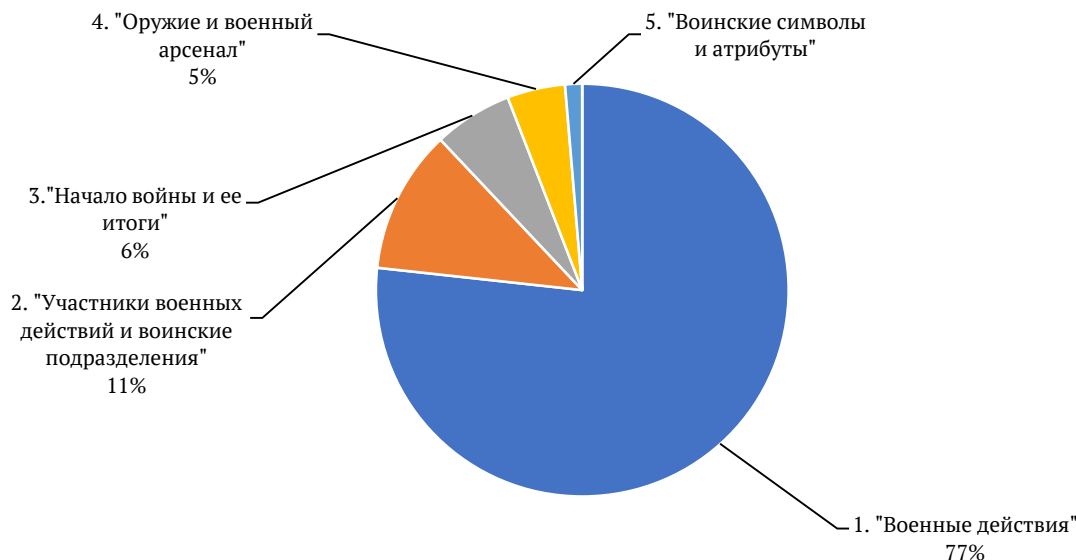


Рисунок 1. Количественное и процентное распределение военных метафор по фреймам

#### Фрейм «Военные действия»

По нашим наблюдениям, наиболее многочисленной группой являются метафоры, репрезентирующие различные действия злоумышленников и специалистов в сфере кибербезопасности (всего 287 контекстов употребления). К ним относятся как метафоры «нападения» (19 номинаций) со стороны киберпреступников, мошенников, хакеров и т. п., так и метафоры «обороны» (17 номинаций), описывающие либо ответные меры, либо шаги, направленные на предотвращение подобных действий.

Метафора «нападения» актуализируется глаголами *attack* (5 – здесь и далее указывается количество контекстов употребления в анализируемом материале) – атаковать, *crusade* (1) – участвовать в крестовом походе, *demobilize* (1) – демобилизовать, *target* (26) – направлять удар; существительными *ambush* (1) – засада, *attack* (133) – атака, *battle* (1) – битва, *campaign* (26) – кампания, операция, *espionage* (1) – шпионаж, *intervention* (1) – интервенция, *intrusion* (2) – вторжение, *island hopping* (1) – прыжки по островам, *raid* (1) – налет, *siege* (1) – осада, *storm* (1) – штурм, *strategy* (1) – стратегия; прилагательным *invasive* (1) – захватнический.

Метафора «обороны» представлена глаголами *battle* (2) – сражаться, *beat* (1) – отбивать, *bulletproof* (1) – делать пуленепробиваемым, *combat* (11) – сражаться, *deploy* (5) – размещать, развертывать, *detect* (16) – обнаруживать, *fight* (5) – сражаться, *guard* (2) – охранять, *protect* (7) – защищать, *struggle* (1) – сражаться; существительными *counterintelligence* (1) – контрразведка, *defense* (14) – оборона, *deployment* (1) – развертывание, *detection* (4) – обнаружение, *guard* (2) – охрана, караул, *intelligence* (8) – разведка, *protection* (4) – защита.

Как показывает наше исследование, самой частотной номинативной метафорой является *attack* – нападение, атака, используемая как наиболее общий термин для обозначения «целенаправленного воздействия программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации» (Безопасность пользователей в сети Интернет. Глоссарий).

Лексема *attack* является частью таких словосочетаний, как *state-sponsored attack* – атака, финансируемая государством, *ransomware attack* – атака вымогателей, *web application attack* – взлом веб-приложения, *credentials stuffing attack* – атака с использованием учетных данных, *poison attack* – заражение, *software attack* – программная атака, *swatting attack* – сваттинг, *credential stuffing attack* – вброс учетных данных, *network-based attack* – сетевая атака и др.

Самыми частотными метафорами «обороны» являются существительное *defense* – оборона, а также глаголы *detect* – обнаруживать, например *detect attacks* – обнаруживать атаки, *detect bots* – обнаруживать ботов, *detect fraudulent calls* – отслеживать звонки мошенников, и *combat* – бороться, который описывает меры противодействия различным видам киберугроз и встречается в таких сочетаниях, как *combat doxing* – бороться с утечкой данных, *combat cybersecurity threats* – бороться с киберугрозами, *combat computational propaganda* –

бороться с компьютерной пропагандой, *combat online trolling* – бороться с интернет-троллингом, *combat piracy* – бороться с пиратством. Отметим, что многие из приведенных выше лексических единиц стали штампами и утратили свою образность. В связи с этим особый интерес для нас представляют оригинальные метафоры.

Говоря о военных метафорах «нападения», нельзя не отметить один из самых значимых образов, Перл Харбор. Ранее в наших работах мы уже упоминали о том, что нападение на военно-морскую базу США в 1941 году стало символом вероломной внезапной атаки (Савченко, 2018, с. 154), который широко используется в медийном и политическом англоязычном дискурсе, а также в научных и научно-популярных статьях о кибербезопасности, не только с целью привлечь внимание к данной проблеме, но и добиться определенного эмоционального отклика у читателя в связи с возможным кибер-апокалипсисом. Подобный эффект достигается за счет апроприации страха и тревоги, вызванных данным историческим событием. Особенно часто этот образ используется в заголовках публикуемых материалов: “How to Survive a *Cyber Pearl Harbor*” (IEEE IT Computer Society). / «Как пережить *кибер Перл Харбор*» (здесь и далее – перевод автора статьи. – А. С.); “Never Mind *Pearl Harbor* – What about a Cyber Love Canal?” (Semantic Scholar). / «Забудьте о *Перл Харборе* – как насчет кибер Лав Канала?»; “*Cyber Pearl Harbor*: A date that will live in infamy, and the marketing machine that hijacked it” (CSO Online). / «*Кибер Перл Харбор*: позорная дата, эксплуатируемая маркетинговой машиной».

Еще одним примером метафоры, связанной с Перл Харбор, является *island hopping* – прыжки по островам, что в контексте компьютерных угроз означает «хакерскую атаку, в ходе которой злоумышленник взламывает компьютер жертвы через более уязвимые системы и ПО, взаимодействующие с ним, с целью получения доступа к сети» (TechTarget Network). В основе данной метафоры лежит стратегия, которую США применили в войне против Японии, отвоевывая территории путем захвата острова за островом. Данное значение актуализируется в следующем примере: “Cybercrime cartels and rogue nation intelligence services appreciate that the future is *island hopping*, which lies in *colonizing* the cloud,” he said (The Register). / «Картели киберпреступников и разведслужбы стран изгоев понимают, что будущее за тактикой *island hopping* (прыжки по островам) с целью захвата облачных систем, – сказал он».

Как известно, хакерские атаки отличаются скоростью и внезапностью, что находит отражение в следующем контексте: “A denial-of-service attack cannot be projected across many hops without eventual diminution; it is a *storm*, not a *siege*” (IEEE IT Computer Society). / «Атака на систему с целью довести ее до отказа не может проводиться через большое число узлов без потери деструктивной мощности: это *шторм*, а не *осада*».

В некоторых случаях те или иные номинации данного фрейма являются частью развернутой метафоры, например: “In this age where every company is falling prey to hackers, encryption is *the first line of defense you need to put up against cyberattacks*” (StealthLabs). / «В эпоху, когда любая компания может подвергнуться хакерской атаке, шифрование является *первой линией обороны, которую необходимо воздвигнуть* с целью защиты от кибератак»; “Zatko’s most damning accusations center around Twitter’s alleged failure to have a solid cybersecurity plan to *protect user data, deploy* internal controls *to guard against* insider threats and ensure the company’s systems were current and properly updated” (CNBC). / «Самые серьезные обвинения Затко были связаны с неспособностью Твиттер надежно *защитить* пользовательские данные, *развернуть* систему внутреннего контроля *для устранения* инсайдерских угроз и обеспечить своевременное обновление систем компании».

Таким образом, фрейм «Военные действия» представлен именными и глагольными метафорами со значением «нападения» и «обороны». В количественном отношении преобладают метафоры нападения (201 и 86 контекстов употребления соответственно).

Интересно отметить, что метафоры «нападения» в большей степени представлены именными номинациями (ср.: 13 именных номинаций по сравнению с 7 глагольными), тогда как среди метафор «обороны» чаще встречаются глагольные (10 глагольных номинаций по сравнению с 7 именными). Наиболее частотными являются *attack* – атака, *campaign* – кампания, *defense* – оборона, *detect* – обнаруживать, *combat* – бороться.

В целом достаточно большое разнообразие метафор этого фрейма, на наш взгляд, объясняется тем, что данные номинации точно описывают основные характеристики кибератак: внезапность, скорость, масштабность и др., что вызывает определенную эмоциональную реакцию у аудитории и может мотивировать к действию.

#### **Фрейм «Оружие и военный арсенал»**

К данному фрейму относятся номинации, обозначающие различные виды вооружения, среди которых существительные *ammunition* (1) – боеприпасы, *arms* (4) – оружие, *bomb* (1) – бомба, *gun* (2) – пистолет, оружие, *scattergun* (1) – дробовик, *sword* (1) – меч, *weaponry* (1) – оружие, *weapon* (2) – оружие; глаголы *arm* (1) – вооружать, *weaponize* (1) – вооружать. Приведем некоторые примеры.

Pundits and journalists have fueled this: There have been extremely provocative stories about the rise of a “*weaponized* AI propaganda machine”, and stories claiming that “artificial intelligence *conquered* democracy” (MIT Technology Review). / «Эти настроения подогревались экспертами и журналистами: было множество провокационных материалов о том, что “пропагандистская машина, *вооруженная* искусственным интеллектом”, набирает обороты, и о том, что “искусственный интеллект *подчинил себе* демократию»; “*Campaigns* of this type are sometimes referred to as astroturf or *Twitter bombs*” (Communications of the ACM). / «Подобные *кампании* иногда называются астротурфингом или *твиттер-бомбами*».

Отметим, что метафоры данного фрейма могут быть использованы в контексте военных действий в буквальном смысле, например: “These are the so-called ‘*cyber weapons*’ that might be used to shut off electricity in enemy territory during a war” (Prey Project). / «Это так называемое “*кибероружие*”, которое во время войны может быть использовано с целью отключения электричества на территории врага».

Интересным примером представляется атрибутивная группа *cyber power*, образованная по аналогии с *nuclear power* – ядерная держава. Поскольку ядерная держава – это страна, обладающая ядерным оружием, очевидно, что *cyber power* – это государство, имеющее в своем арсенале кибероружие, использование которого может привести к катастрофическим последствиям. Данный образ реализуется в следующем контексте: For example, Chris Painter of the U.S. Department of State commented in a Brookings Institution article that China and North Korea “have frequently exercised their *cyber power* to achieve their strategic goals around the globe” (Prey Project). / «Например, в статье, опубликованной Брукинским институтом, со ссылкой на представителя госдепартамента США Криса Пейнтера говорится, что Китай и Северная Корея “неоднократно применяли *кибероружие* для достижения своих стратегических целей по всему миру»».

Еще одним оригинальным примером рассматриваемого фрейма является *arms race* – гонка вооружений. Данное выражение представляет собой политическую метафору и означает «процесс ускоренной разработки, производства и накопления оружия и военной техники, их качественного совершенствования на базе милитаризации экономики, науки и других сфер жизни общества» (Большая Российская энциклопедия, 2004-2017). В контексте кибербезопасности конфликтующие стороны – это разработчики вредоносных программ и те, против кого они направлены. Поскольку данное словосочетание имеет отрицательную коннотацию, оно используется исключительно в отношении злоумышленников, например: “As we build better detection systems, we expect *an arms race* similar to that observed for spam in the past” (Communications of the ACM). / «По мере того, как создаются все более совершенные системы обнаружения, есть все основания полагать, что начнется *гонка вооружений*, похожая на ту, что была во времена борьбы со спамом».

К данному фрейму также относятся идиомы *double-edged sword* – палка о двух концах (Merriam-Webster Dictionary) и *smoking gun* – дымящееся ружье, т. е. неопровержимое доказательство того, что было совершено противоправное действие. На основе этого устойчивого сочетания строится развернутая метафора: “People are always looking for the *smoking gun* in these technologies,” Joyce said. “I characterize it much more as a *loaded gun*” (CNN). / «Люди часто ищут *неопровержимое доказательство* того, что эти технологии были использованы со злым умыслом, – сказал Джойс. – Я же считаю, что нужно искать *потенциальные угрозы*».

Итак, данный фрейм представлен преимущественно именными метафорическими номинациями (9 именных номинаций и 2 глагольные номинации), в числе которых политические метафоры и идиомы. Милитарные метафоры данного фрейма описывают тактики, применяемые атакующими, и имеют отрицательную коннотацию.

#### **Фрейм «Участники военных действий и воинские подразделения»**

Лежащее в основе военной метафоры противопоставление «свой – чужой» наиболее ярко проявляется в метафорах данного фрейма, к которым относятся существительные *ally* (3) – союзник, *army* (7) – армия, *attacker* (9) – атакующий, *defender* (2) – защитник, *enemy* (3) – враг, *fleet* (1) – флот. В данный фрейм также включаем слово *target* (18) – цель, мишень, используемое в отношении отдельных лиц, организаций или групп. Рассмотрим два примера:

“Again, it is a mindset well suited to cybersecurity, where there is continuous evolution in technologies used and techniques employed by *cyber attackers*” (Infosecurity Magazine). / «И опять же такая установка соответствует сфере кибербезопасности, в которой наблюдается постоянное усовершенствование как защитных технологий, так и способов осуществления *кибератак*».

“*Defenders* don’t have to learn something new,” he said. “The cloud is a new paradigm, but the way cloud resources are successfully attacked the most isn’t” (The Register). / «Здесь нет ничего нового для специалистов в сфере безопасности, – сказал он. – Облако – это новая модель, но способы взлома облачных хранилищ – нет».

Наши наблюдения показали, что лексема *army* со значением «множество» метафорически используется как в положительном (3 контекста употребления), так и в отрицательном смысле (4 контекста употребления), в зависимости от существительного, к которому оно относится, ср.: *armies of smart AI bots working to manipulate public opinion* (MIT Technology Review) – армии смарт-ботов, используемые с целью повлиять на общественное мнение, *troll armies* (BBC) – армии троллей, *a vast army of fake social media profiles* (The Guardian) – огромная армия фейковых интернет-аккаунтов, а также *under-praised army that keeps the internet as we know it going* (The Guardian) – недооцененная армия, которая обеспечивает бесперебойную работу интернета, *army of web crawlers* (New Scientist) – армия веб-сканеров, *spider armies* (New Scientist) – армии спайдерботов. Иногда данное существительное становится частью развернутых метафор, например: “But an AI like ChatGTP would make it much easier for so-called *troll armies to scale up their operations*” (BBC). / «Но благодаря искусственному интеллекту, такому как ChatGTP, *армиям так называемых троллей* будет гораздо проще *расширить масштаб операций*».

Таким образом, фрейм «Участники военных действий и воинские подразделения» представлен именными метафорами, описывающими противоборствующие стороны, причем метафорическая номинация *army* употребляется как в отношении злоумышленников, так и в отношении технологий, используемых службами кибербезопасности.

#### **Фрейм «Начало войны и ее итоги»**

В исследуемом материале данный фрейм представлен только слотом «Исход войны», к которому относятся существительные *victim* (19) – жертва, используемое в отношении пострадавшей от кибератаки стороны,

*surrender* (1) – поражение, *slaughter* (1) – кровопролитие, *victory* (1) – победа, а также глаголы *colonize* (1) – колонизировать, *conquer* (1) – завоевать, *kill* (1) – убивать. Проанализируем некоторые контексты употребления.

Несмотря на то, что использование искусственного интеллекта, в частности чат-ботов, во взаимодействии с клиентами становится все более распространенным явлением, не все проблемы могут быть решены без участия человека. Для подобных ситуаций предусмотрена опция *human fallback* – переключение на оператора, в случае если автоматизированная система не способна справиться с запросом. Подобная ситуация метафорически отражена в примере из статьи о чат-боте по имени Бренда: “HUMAN\_FALLBACK was Brenda’s *white flag of surrender*” (The Guardian). / «Для Бренды переключение на оператора было равноценно *белому флагу поражения*» и означало, что она не может справиться с поставленной задачей. Экспрессивность данного предложения усиливается за счет использования двух метафор одновременно: *white flag* – белый флаг, традиционный символ поражения, и *surrender* – капитуляция.

Отдельно отметим глагол деструктивной семантики *kill* – убивать, а также существительное *slaughter* – резня, кровопролитие, которые метафорически описывают последствия кибератак: “After all, Musk’s volte face happened in response to pleas from that account’s owner that Musk’s policy change would ‘*kill*’ his profile” (The Guardian). / «В конце концов, мнение Маска кардинально изменилось после заявления владельца аккаунта о том, что подобная политика компании “*убьет*” его профиль»; “Hardware *slaughter* is not strategic *victory*” (IEEE UIT Computer Society). / «Уничтожение аппаратного обеспечения не является стратегической *победой*».

Итак, в иллюстративном корпусе фрейм «Начало войны и ее итоги» представлен только слотом «Исход войны», в который входят 3 именные и 2 глагольные номинации, а также 1 существительное и 1 глагол деструктивной семантики. Самой частотной метафорой данного фрейма является *victim* – жертва.

#### **Фрейм «Воинские символы и атрибуты»**

Данный фрейм представлен существительным *flag* (5) – флаг, знамя, которое встречается в словосочетаниях *white flag* (1) – белый флаг (символ капитуляции) и *red flag* (4) – красный флажок, который в социальных сетях используется как предупреждающий об опасности сигнал, например: “Still, in recognition of the problem, Match Group rolled out a public awareness campaign earlier this month alerting users of *red flags*” (The New York Times). / «Тем не менее, признав проблему, ранее в этом месяце Match Group, которой принадлежат несколько сайтов знакомств, развернула кампанию в целях информирования широких масс населения и предупреждения пользователей *об опасностях*». Зачастую экспрессивность усиливается за счет использования определения или развернутых метафор, как в следующих примерах: “If someone claims to be overseas, or otherwise says they can’t meet in person, consider it *a big red flag*” (CNET). / «Если ваш новый знакомый утверждает, что находится за границей или по каким-либо другим причинам не может встретиться лично, воспринимайте это как *серьезный сигнал об опасности*»; “Lensa has been climbing the app store hit lists with its avatar-generating AI that is making artists *wave the red flag*. Now there’s another reason *to fly the flag*: As it turns out, it’s possible – and way too easy – to use the platform to generate non-consensual soft porn” (Yahoo!). / «Нейросеть Lensa набирает популярность среди приложений, а ее способность генерировать аватары *вызывает беспокойство* у художников. Теперь есть еще одна причина *бить тревогу*: как оказалось, при помощи этой платформы можно создавать легкое порно без согласия пользователей».

Таким образом, в анализируемом материале единственной метафорической номинацией фрейма «Воинские символы и атрибуты» является существительное *flag* (5) – флаг, знамя, которое главным образом используется как символ опасности в интернет-пространстве.

#### **Заключение**

Проведенное исследование позволяет сделать следующие выводы:

1. Милитарные метафоры представляют собой номинации из сферы-источника «Война», обозначающие военные действия и отражающие противостояние «свой» – «чужой», т. е. враг.

2. В англоязычном научно-популярном дискурсе метафорическая модель войны обладает значительным потенциалом в интерпретации киберугроз и мер, направленных на их предотвращение. В анализируемых текстах она представлена фреймами «Военные действия» (287 контекстов употребления, 77% от общего количества), «Участники военных действий и воинские подразделения» (42 контекста употребления, 11%), «Начало войны и ее итоги» (23 контекста употребления, 6%), «Оружие и военный арсенал» (17 контекстов употребления, 5%), «Воинские символы и атрибуты» (5 контекстов употребления, 1%). Наиболее частотными номинациями рассматриваемой метафорической модели являются существительные: *attack* (133) – атака, *campaign* (26) – кампания, *victim* (19) – жертва, *defense* (14) – оборона – и глаголы: *target* (26) – направлять удар, *detect* (16) – обнаруживать.

3. Несмотря на то, что многие милитарные метафоры стали штампами, в анализируемой метафорической модели представлены оригинальные способы концептуализации киберугроз и мер противодействия. Основанием для метафоризации является то, что данные номинации точно описывают основные характеристики кибератак, внезапность, скорость, масштабность и др., что делает их мощным инструментом коммуникативного воздействия. Подавляющее большинство милитарных метафор иллюстративного корпуса обладают отрицательным коннотативным значением (ср.: 279 против 95) и используются в отношении злоумышленников, их действий или последствий их действий.

Перспективы дальнейшего исследования видятся в продолжении сбора репрезентативного материала по метафорике англоязычных и русскоязычных научно-популярных текстов данной тематической направленности с целью выявления наиболее частотных метафорических моделей и последующего сопоставительного анализа.

### Источники | References

1. Баранов А. Н. Дескрипторная теория метафоры. М.: Языки славянской культуры, 2014.
2. Баранов А. Н. Метафорические модели как дискурсивные практики // Известия Российской академии наук. Серия литературы и языка. 2004. Т. 63. № 1.
3. Баранов А. Н., Михайлова О. В., Шипова Е. А. Некоторые константы русского политического дискурса сквозь призму политической метафорики ('взаимоотношения бизнеса и власти', 'коррупция'). М.: Фонд ИНДЕМ, 2006.
4. Будаев Э. В., Чудинов А. П. Метафоры, которыми мы живем: преобразования прецедентного названия // Политическая лингвистика. 2007. Вып. 2 (22).
5. Крышталева В. Е. Милитарные метафоры в дискурсе президентов России и Франции в начале XXI века // Вестник Новосибирского государственного университета. Серия «Лингвистика и межкультурная коммуникация». 2019. № 17 (2). <https://doi.org/10.25205/1818-7935-2019-17-2-77-90>
6. Кудрин С. А. Базовые метафоры спортивного дискурса как текстопорождающие модели: автореф. дисс. ... к. филол. н. М., 2011.
7. Лакофф Дж., Джонсон М. Метафоры, которыми мы живем / пер. с англ.; под ред. и с предисл. А. Н. Баранова. М.: Едиториал УРСС, 2004.
8. Малышева Е. Г. Метафорическая модель «Спорт – это война» в журналистском спортивном дискурсе (на материале текстов современных печатных и электронных СМИ) // Вестник Томского государственного университета. 2009. № 328.
9. Савченко А. А. Экспрессивность англоязычного научного и научно-популярного текста и способы ее передачи на русский язык // Актуальные аспекты лингвистики, лингводидактики и межкультурной коммуникации: мат. всерос. науч.-практ. конф. (г. Краснодар, 31 марта 2018 г.) / под ред З. И. Гурьевой. Краснодар: Кубанский государственный университет, 2018.
10. Чудинов А. П. Россия в метафорическом зеркале: когнитивное исследование политической метафоры (1991-2000): монография / Уральский государственный педагогический университет. Екатеринбург, 2001.

### Информация об авторах | Author information



**Савченко Анна Александровна**<sup>1</sup>, к. филол. н.  
<sup>1</sup> Кубанский государственный университет, г. Краснодар



**Savchenko Anna Aleksandrovna**<sup>1</sup>, PhD  
<sup>1</sup> Kuban State University, Krasnodar

<sup>1</sup> [bugaeva\\_anna@inbox.ru](mailto:bugaeva_anna@inbox.ru)

### Информация о статье | About this article

Дата поступления рукописи (received): 01.08.2023; опубликовано online (published online): 08.09.2023.

**Ключевые слова (keywords):** милитарная метафора; военная метафора; научно-популярный текст; фрейм; military metaphor; war metaphor; popular science text; frame.