[Научный диалог = Nauchnyi dialog = Nauchnyy dialog, 12(3), 2023]
[ISSN 2225-756X, eISSN 2227-1295]

Кочетова Л. А. Лингвокультурная специфика дискурсивных практик репрезентации кибербезопасности в русскоязычном медийном пространстве : корпусный подход / Л. А. Кочетова, Е. Ю. Ильинова // Научный диалог. — 2023. — Т. 12. — № 3. — С. 134—152. — DOI: 10.24224/2227-1295-2023-12-3-134-152.

Kochetova, L. A. Ilyinova, E. Yu. (2023). Linguocultural Specifics of Cybersecurity Discursive Practices Representation in Russian Media Communication: Corpus-Assisted Approach. *Nauchnyi dialog, 12* (3): 134-152. DOI: 10.24224/2227-1295-2023-12-3-134-152. (In Russ.).

Журнал включен в Перечень ВАК

DOI: 10.24224/2227-1295-2023-12-3-134-152

Лингвокультурная специфика дискурсивных практик репрезентации кибербезопасности в русскоязычном медийном пространстве: корпусный подход

Кочетова Лариса Анатольевна *
orcid.org/0000-0002-5278-7373
доктор филологических наук,
профессор, профессор кафедры теории
и практики перевода и лингвистики
**** корреспондирующий автор***
kochetova@volsu.ru

Ильинова Елена Юрьевна
orcid.org/0000-0002-3310-4020
доктор филологических наук, профессор,
профессор кафедры теории и практики
перевода и лингвистики
ilynov@volsu.ru

Волгоградский
государственный университет
(Волгоград, Россия)

Благодарности:
Исследование выполнено за счет гранта
Российского научного фонда
№ 23-28-00509,
https://rscf.ru/project/23-28-00509/

Linguocultural Specifics of Cybersecurity Discursive Practices Representation in Russian Media Communication: Corpus-Assisted Approach

Larisa A. Kochetova *
orcid.org/0000-0002-5278-7373
Doctor of Philology, Professor,
Professor of the Department
of Theory and Practice
of Translation and Linguistics
**** Corresponding author***
kochetova@volsu.ru

Elena Yu. Ilyinova
orcid.org/0000-0002-3310-4020
Doctor of Philology, Professor,
Professor of the Department
of Theory and Practice
of Translation and Linguistics
ilynov@volsu.ru

Volgograd State University
(Volgograd, Russia)

Acknowledgments:
The study is supported
by Russian Science Foundation,
project number 23-28-00509,
https://rscf.ru/project/23-28-00509/

ОРИГИНАЛЬНЫЕ СТАТЬИ

Аннотация:

Рассматривается вопрос о семантической, прагматической и ценностной специфике дискурсивных практик кибербезопасности. Новизна работы состоит в применении методологии корпусной лингвистики к исследованию дискурса, понимаемого как опосредованная языком социальная практика. Актуальность работы обусловлена интересом лингвистики к изучению русскоязычных дискурсивных практик, формирующих новую социальную реальность в цифровом обществе. Методами корпусной лингвистики реконструирована когнитивно-семантическая структура дискурсивного тезауруса, включающая новый пласт лексических единиц русского языка, выявлены тематические группы слов и проанализирована их дистрибуция в различных жанрах дискурса кибербезопасности. Установлено, что наряду с терминологией, ориентированной на трансфер операционального, практического знания о безопасных онлайн-практиках, в корпусе регулярно используются лексические единицы милитарной и агрессивной семантики, что указывает на противоречие между целями дискурса, направленными на формирование позитивного ценностного отношения к цифровым технологиям, и языковыми средствами их достижения. Показано, что нейтральные лексемы в результате регулярного употребления в негативно окрашенных контекстах приобретают отрицательные оценочные коннотации, что также может способствовать формированию недоверия пользователей к новым технологиям, усиливая ощущения риска, порождая тревогу и обеспокоенность.

Ключевые слова:
дискурс; корпус; дискурсивная практика; корпусная методология; дискурс кибербезопасности; русский язык.

ORIGINAL ARTICLES

Abstract:

The issue of the semantic, pragmatic and axiological specifics of cybersecurity discursive practices as it is displayed in the genres of media and online communication is considered. The novelty of the work lies in the application of the corpus linguistics methodology to the study of discourse, understood as a language-mediated social practice. The relevance of the work is due to the interest of linguistics in the study of discursive practices that shape a new social reality formed as a result of the Russian language functioning. By using the methods of corpus linguistics, the cognitive-semantic structure of discursive thesaurus, which comprise a new layer of lexical units, has been reconstructed, thematic groups of lexical units have been identified and their distribution in various genres of cybersecurity discourse has been established. It has been found that along with the terminology focused on the transfer of operational, practical knowledge about safe online practices, the texts in the corpus regularly employ lexical units with military and aggressive semantics, which indicates the contradiction between the goals of the discourse aimed at forming a positive attitude towards digital technologies, and language means employed to achieve them. It is shown that due to regular occurrence of neutral lexical units in negatively colored contexts, they develop negative evaluative connotations, which also contributes to the formation of users' distrust of new technologies, enhances the feeling of risk, and generates anxiety and concern.

Key words:
discourse; corpus; discursive practice; corpus methodology; cybersecurity discourse; Russian.

OPEN ACCESS
[Научный диалог = Nauchnyi dialog = Nauchnyy dialog, 12(3), 2023]
[ISSN 2225-756X, eISSN 2227-1295]

УДК 811.161.1’42:004.738.5

Научная специальность ВАК
5.9.8. Теоретическая, прикладная и сравнительно-сопоставительная лингвистика

Лингвокультурная специфика репрезентации дискурсивных практик кибербезопасности в русскоязычном медийном пространстве: корпусный подход

© Кочетова Л. А., Ильинова Е. Ю., 2023

1. Введение = Introduction

Безопасность как состояние защищенности от угроз жизни, имуществу и здоровью личности, общим интересам социума всегда воспринимается как одна из базовых потребностей, что определяет значимость этого концепта в системе коллективных и индивидуальных ценностей человека. Вместе с тем общее представление о безопасности демонстрирует определенную динамику, приобретая на каждом этапе развития социума новые концептуальные признаки. Проблематика безопасности в современном мире имеет множество измерений, одним из которых становится безопасность в сфере использования информационно-коммуникационных технологий, так называемая информационная, или кибербезопасность. Масштабное использование информационно-коммуникационных технологий вывело на повестку дня вопрос о безопасности в компьютерно-цифровом пространстве, которое на сегодняшний день предоставляет особые инструменты сбора, хранения, распространения информации, цифровые средства и каналы институциональной и межличностной коммуникации. Указанный феномен неизбежно вызывает интерес современных философов и культурологов, социологов, политологов, психологов, специалистов финансово-экономических и иных сфер. Лингвистический аспект изучения особенностей репрезентации стратегий кибербезопасности в современном дискурсивном пространстве также актуален и требует научного осмысления.

Активное внедрение компьютерных технологий в повседневную жизнь широких слоев общества предполагает трансфер знаний о принципах и сферах их безопасного применения, что находит отражение в дискурсивных практиках кибербезопасности. Можно утверждать, что в идеале целью данных дискурсивных практик является трансфер знаний о безопасных моделях онлайн-поведения пользователей, стимулирование онлайн-практик, защищающих личное пространство и информацию от посягательств

со стороны внешних акторов, что неизбежно объективируется в семантике и прагматике языковых знаков, которые концептуализируют представления об этом социально-значимом феномене, задают поведенческие паттерны, определяют ценностное отношение членов дискурсивного сообщества к компьютерно-информационным технологиям.

Цель данной статьи — на основе корпусной методологии реконструировать когнитивно-семантическую структуру дискурсивного тезауруса кибербезопасности, определяющего ценностно окрашенное восприятие изучаемого явления членами дискурсивного сообщества. Признавая, что трансфер знаний о кибербезопасности является неотъемлемой частью образа жизни в XXI веке, наше исследование отвечает на вопросы о том, как организована когнитивно-семантическая структура дискурсивного тезауруса кибербезопасности и какие тематические группы образуют единицы языка, транслирующие знания об этом феномене; как распределяются выделенные тематические группы лексики в текстах различных жанров и какие дополнительные оценочные смыслы возникают в результате регулярного использования нейтральных и терминологических единиц в негативно окрашенных контекстах; как когнитивно-семантическая структура дискурсивного тезауруса влияет на поведение, ожидания, установки и реакции адресата в области кибербезопасности.

2. Материал, методы, обзор = Material, Methods, Review

Теоретическую базу исследования составили: конструктивистская теория дискурса, рассматривающая его как набор текстов и речевых конструкций, определяющих социальный и политический контекст того или иного явления, формирующих идеологию или образ мышления [Laclau 1995]; понимание дискурса как «содержательно-тематической общности текстов» [Чернявская, 2017, с. 142] и как опосредованной языком формы социальной практики; корпусный анализ дискурса [Baker, 2006; Teubert et al., 2007; Анашкина и др., 2021]; методика корпусного анализа, основанная на методе извлечения ключевых слов [Gabrielatos, 2018; Кочетова и др., 2019]; работы по семантическому дискурсивному анализу [Орлова, 2021]; метод категориально-семантической реконструкции дискурсивного тезауруса [Ильинова, 2016]; труды, посвященные анализу современных российских практик социализации и влияния на различные целевые аудитории в медиакоммуникации [Бродовская и др., 2019; Змазнева, 2018]; общей аксиологической проблематике и прагматике медиатекста [Карасик, 2013; Общая и русская лингвоаксиология, 2022]; труды, рассматривающие отдельные социально-значимые феномены [Ефремова, 2021; Леонтьева и др., 2020; Ребрина, 2021; Parvaresh, 2023].

Дискурс кибербезопасности объединяет русскоязычные медийные тексты различной целевой и адресной направленности. Он включает регулятивные тексты, в частности, документы российского законодательства и политико-правовые акты (Указ Президента РФ от 05.12.2016 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022)), регламентирующие документы (стандарт ISO/IEC 27032:2012 «Информационные технологии. — Методы обеспечения безопасности — Наставления по кибербезопасности»), профессионально-ориентированные и рекламно-маркетинговые тексты, размещенные на сайтах технологических компаний (например, сайт компании «Лаборатория Касперского»), информационно-просветительский контент, размещенный на специализированных сайтах бизнес-структур (ярким примером которого является сайт «Кибрарий», разработанный «Сбером»), а также авторскую публицистику в жанрах сетевой коммуникации (форумы, блоги, чаты и др.).

Методика корпусного анализа включала когнитивно-семантическое моделирование дискурсивного тезауруса собранной коллекции медиатекстов о кибербезопасности, контекстуальный анализ прямых номинаций и имплицитных оценочных семантических знаков, интерпретативный анализ ценностной прагматики медийного контента, уточнение специфики способов концептуализации представлений о кибербезопасности в дискурсивных практиках профессионально-ориентированного, новостного, информационно-просветительского форматов, ориентированных на трансфер операционального, практического знания, а также практиках рекламно-маркетингового воздействия, направленного на продвижение продуктов и услуг, обеспечивающих безопасность использования компьютерных технологий.

Для создания тематического корпуса, репрезентирующего дискурсивные практики кибербезопасности, использовался список ключевых слов и словосочетаний, который формировался вокруг таких стержневых единиц, как *информационная безопасность, кибербезопасность*, а также включал тематически связанные с проблемой цифровой безопасности специальные словосочетания: *риск для информационной безопасности, киберриск, риск для кибербезопасности, кибератака, риск кибератаки, риск атаки на кибербезопасность*.

Тексты для специализированного корпуса отбирались из медийного контента, включающего профессионально ориентированные тексты https://securitylab.ru, cyberrus.com, https://bit.spels.ru/index.php/bit и др.); новостные тексты (tass.ru, ura-news.ru, ria.ru, irkutskmedia.ru, newsclick.ru, kommersant.ru, vedomosti.ru и др.); информационно-просветительский контент, размещенный на специализированных сайтах (https://promo.sber.

ru/kibrary, psblog.ru, https://www.anti-malware.ru, securitylab.ru, itworld.ru, osp.ru, withsecurity.ru, vsluh.net, csaa.ru), рекламно-маркетинговые тексты, предлагающие решения для обеспечения кибербезопасности (securityvision.ru, rt-solar.ru, staffcop.ru и др.), а также тексты, размещенные в сетевых медиа (https://netology.ru/blog, https://vk.com/cybersi).

Структура корпуса «Дискурсивные практики кибербезопасности» (КДПК), отражающая его количественные характеристики и жанровое разнообразие, представлена далее (табл. 1). Корпус включает 531 документ объемом 298 157 слов.

Таблица 1

Структура корпуса
«Дискурсивные практики кибербезопасности (КДПК)»

Жанры медиаконтента	**Пропорция (%)**	**Количество слов**	**Количество текстов**
Профессионально-ориентированные: в т.ч.			
экспертные	41,40	123 544	220
доклады и отчеты	2,52	540	14
Информационно-просветительские	18,21	54 314	97
Новостные	18,10	54 241	96
Рекламно-маркетинговые	18,08	53 929	96
Сетевые	1,53	4 589	8
Всего	100	298 157	531

Собранный корпус подвергался компьютерной обработке при помощи встроенного функционала сервера «CQPweb» («Corpus Query Processor») [https://cqpweb.lancs.ac.uk/], предлагающего функцию загрузки собственного корпуса. Анализ лексического материала КДПК проводился с помощью методов корпусной лингвистики, включающих построение списков слов, конкордансов и их контекстуальный анализ, выделение ключевых слов, лингвостатистику, приемы интерпретации дискурсивной семантики. Применялись методы систематизации, типологизации средств лексической репрезентации кибербезопасности, моделирования тематических групп лексики, регулярно присутствующих в дискурсивных практиках.

3. Результаты и обсуждение = Results and Discussion

3.1. Языковые характеристики корпуса дискурсивных практик кибербезопасности

Специфика семантической организации дискурсивных практик кибербезопасности определялась при помощи функции построения списка слов

корпуса, а также метода выделения ключевых слов, что позволило выявить наиболее частотные и уникальные лексические единицы, определить их частеречную принадлежность, проанализировать семантическое наполнение текстов и на этой основе провести когнитивно-семантическую реконструкцию дискурсивного тезауруса, уточнить прагматическую специфику и определить ценностное наполнение дискурсивных практик кибербезопасности.

Далее представлено «облако» ключевых слов (рис. 1), полученное в результате сопоставления частотности слов исследуемого корпуса «КДПК» с референциальным корпусом, в качестве которого использовался корпус русскоязычных текстов средств массовой информации «Uppsala Russian Corpus», доступный на платформе «CQPweb».

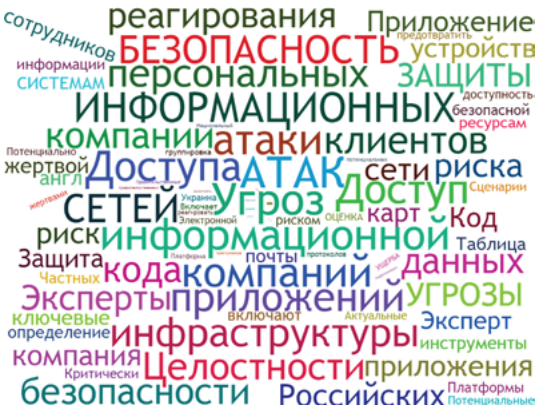

Рис. 1. Облако «ключевых слов» русскоязычного корпуса дискурсивных практик кибербезопасности в сопоставлении с корпусом «Uppsala Russian Corpus», построенного с использованием статистической меры Log Ratio (0.01 % фильтр значимости, адаптированной к пороговому уровню LL = 36.49); лексические единицы имеют минимальную частоту 3 в списке слов обоих корпусов.

Как показывает анализ ключевых слов (рис. 1), исследуемый корпус характеризуется высокой плотностью семантических единиц, относящихся к тематическому полю «Информационно-технологический дискурс» (*приложение, сеть, код, платформа* и др.), отсутствием эмоционально-оценочной лексики, выражающей отношение и мнение, наличием нейтральных дескриптивных прилагательных (*информационный*, *электронный, компьютерный, персональный* и др.). Результаты семантического анализа уникальных ключевых слов корпуса (то есть лексем, отсутствующих русскоязычном корпусе, с которым проводится сопоставление) показали, что тезаурус дискурса кибербезопасности отличается терминологической си-

стемностью и включает сложносоставные единицы с компонентом *кибер-*, означающим ‘связанный с компьютерами, существующий в интернете’ (*кибербезопасность, кибератака, киберугроза* и др.) и специализированные словосочетания: *стратегия кибербезопасности, сфера кибербезопасности, основа кибербезопасности, область кибербезопасности, обеспечение кибербезопасности* и др. Следует отметить, что приставка *кибер-* присоединяется к самым обычным словам, образуя их аналоги в виртуальном пространстве (о формировании двойственной реальности в цифровом пространстве см. [Маринова, 2023]).

Изучение системных характеристик корпуса проводилось с учетом дистрибуции некоторых категориально-семантических классов слов в аспекте жанровой вариативности, отражающей способы концептуализации смыслов в дискурсе. Результаты анализа представлены далее (табл. 2). В соответствии с полученными данными основу тезауруса дискурса кибербезопасности составляют классы существительных, глаголов и прилагательных (в среднем 33,25 % от общего числа, 8,15 % и 9,76 %, соответственно).

Таблица 2

Жанровая вариативность частеречных характеристик
корпуса дискурсивных практик кибербезопасности (КДПК)

Жанры / **Частеречная принадлежность**	**профессионально-ориентированные**	**информационно-просветительские**	**новостные**	**рекламно-маркетинговые**	**сетевые, блоги**
существительные	40 378 (32,6 %)	17 809 (32,7 %)	17 454 (32,1 %)	18 976 (35,1 %)	1 480 (32,3 %)
прилагательные	11 630 (9,4 %)	5 516 (10,1 %)	4 985 (9,1 %)	5 399 (10,0 %)	420 (9,2 %)
глаголы	5 023 (4,0 %)	3 824 (7,0 %)	5 687 (10,4 %)	5 023 (9,3 %)	488 (10,6 %)
наречия	2 849 (2,3 %)	835 (1,5 %)	1 412 (2,6 %)	1 129 (2,1 %)	140 (3,0 %)
местоимения	792 (0,6 %)	83 (0,1 %)	285 (0,5 %)	298 (0,6 %)	46 (1,1 %)
союзы	6 648 (5,3 %)	2 176 (4,0 %)	2 851 (5,2 %)	2 864 (5,4 %)	324 (7,0 %)
прочие	56 224 (45,8 %)	24 071 (44,6 %)	21 567 (40,1 %)	20 240 (37,5 %)	1 691 (36,8 %)
Кол-во слов	123 544	54 314	54 241	53 929	4 589

Анализ дистрибуции количественных характеристик категориально-семантических классов слов в текстах различных жанров не выявил их ярко выраженной специфики. Существенное преобладание существительных, номинирующих ключевые понятия дискурса кибербезопасности, низкая частота глагольной лексики и прилагательных, личных местоимений, служебных и дискурсивных единиц, формирующих смысловую связность текстов, свидетельствуют о доминировании информативной тональности в различных жанрах.

Анализ сочетаемости ядерных единиц, номинирующих рассматриваемую концептуальную сферу (*безопасность, кибербезопасность*), показывает, что они образуют характерные терминологические сочетания с дескриптивными прилагательными, формируя «семантическое ядро» дискурсивного тезауруса (например, *индивидуальная кибербезопасность, оперативная кибербезопасность, глобальная кибербезопасность, национальная безопасность, национальная стратегия кибербезопасности*). Нейтральные дескриптивные прилагательные дискурса кибербезопасности образуют множественные коллокации с ядерными существительными информационно-технологической тематики: *информационн- (-ая / -ый / -ое)* (*безопасность, система, инфраструктура, среда, ресурс, пространство, актив, поток*); *цифров- (-ая / -ой)* (*трансформация, информация, идентификация, эпоха, среда, грамотность, формат, мир, след*); *компьютерн- (-ый / -ая / -ое)* (*сеть, система, информация, программа, техника, безопасность*); *программн- (-ый / -ое / -ый)* (*обеспечение, продукт, код, закладка, инструмент, модуль, среда, компонент, средство, комплекс*).

Однако сочетания нейтральных в оценочном отношении прилагательных и негативных оценочно окрашенных существительных (*информационная война, компьютерное мошенничество*, *компьютерный вирус*), регулярно используемых в дискурсивной практике кибербезопасности, приобретают негативные оценочные импликации, формирующие осторожно-критичный взгляд на компьютерные технологии, который может выражаться в их неприятии вследствие нежелания подвергаться рискам. Следует отметить, что формирование негативной семантической просодии (о семантической просодии см. [Louw, 1993; Stubbs, 1995]) наблюдается и в использовании регулярной словообразовательной модели, в которой морфема «кибер-» объединяется с единицей, обозначающей отрицательно оцениваемые явления реальности, что приводит к появлению негативно-оценочной семы в значении ключевого термина *кибернетика*, определяющего терминологическую специализацию общего дискурсивного тезауруса кибербезопасности.

Изменением оценочного знака могут отличаться и другие общеупотребительные лексические единицы. Так, прилагательное *новый* регулярно

используется в качестве атрибута в терминологических сочетаниях, актуализирующих в своей семантике негативные явления и действия в цифровом пространстве (например: *новые методы взлома, новые риски, новые и новые угрозы, новые векторы атаки, новые опасности, новые преступные IT-профессии*), и, как следствие, приобретает отрицательно окрашенное значение.

Как показывает таблица 2, глагольная лексика в изучаемых текстах отмечена существенно меньшей частотой употребления по сравнению с существительными. Тем не менее глаголы чаще используются в новостных, сетевых и рекламно-маркетинговых текстах, что указывает на присутствие в них нарратива, выступающего как средство информирования и убеждения; в профессионально-ориентированных и информационно-просветительских текстах доля глаголов существенно меньше. Насыщенность информационно-просветительских текстов номинативными лексическими единицами, образующими дистанцию между адресантом текста и его получателями, отсутствие эмоциональной привязки свидетельствуют о расхождении между целями дискурса кибербезопасности (донесение до широкого круга пользователей компьютерными технологиями стратегий безопасного поведения) и средствами их реализации.

Анализ семантики глаголов дискурса кибербезопасности позволил выделить разноплановые в тематическом и оценочном отношении группы лексики. В дискурсе кибербезопасности используются глагольная лексика, актуализирующая стратегии безопасного поведения в виртуальном пространстве: *избегать, распознавать, минимизировать, устранять, ограничивать, контролировать, обновлять, удалять* и др., например: (1) *Регулярно* ***обновляйте*** *свой сайт и* ***устраняйте*** *известные уязвимости. Любое ПО, как-либо связанное с работой ваших сервера и сайта, всегда должно быть обновлено* (https://www.securitylab.ru/analytics).

В семантической организации текстов корпуса идентифицируются глагольные единицы, обозначающие различные виды преступных действий. Отметим, что в дискурсе кибербезопасности семантика слов данной группы расширяется, поскольку они, образуя коллокации с существительными, обозначающими понятия виртуальной среды, семантизируют противозаконные действия в цифровом пространстве, направленные на нарушение целостности и неприкосновенности нематериальных объектов: *взломать / взламывать* (*приложение, систему защиты, сеть, сервис, аккаунт, учетную запись, веб-камеру, программное обеспечение), проникать* (*сеть, защищенные системы, системы компании, компьютер, виртуальное пространство*)*, подвергнуться* (*кибератакам, хакерским атакам, кибернападениям, риску, опасности сбоев, взлому*)*, нарушать* (*аутентификацию,*

информационную безопасность, конфиденциальность), украсть (данные, ценную информацию, персональные данные).

Заметное место в дискурсивных практиках кибербезопасности занимают глаголы и глагольные сочетания милитарной семантики: *проводить кампанию, бороться (с угрозами, атаками, вредоносным ПО, вирусами, киберпреступниками), противостоять (кибератакам, угрозам, ударам), атаковать, наносить удары*. Высокую частотность в корпусе имеют глаголы *защищать, защищаться*, образующие коллокации с лексическими единицами, обозначающими как реальные, так и виртуальные объекты атак: *данные, целостность, информацию, сеть, организацию, систему, приложение, инфраструктуру, актив, запись, человека, пользователя, компании, госучреждения, мобильные устройства, компьютеры, IT-инфраструктура, сети, программное обеспечение, сайты, стратегические объекты, системы водоснабжения, персональные данные, отрасль здравоохранения, информационные ресурсы*, что придает угрозам глобальный характер. Таким образом, формируется новый пласт лексики и терминологических сочетаний, которые образуют основу тезауруса дискурса и определяют его ценностное наполнение, задающее поведенческие стратегии и формирующее восприятие кибербезопасности как социально-значимого феномена членами русского дискурсивного сообщества.

Прагматика дискурсивных практик кибербезопасности, в значительной мере обусловленная специфической дистрибуцией тематических групп лексики, моделирующих концептуальное пространство различных жанров, будет рассмотрена в следующем разделе.

3.2. Жанровая специфика дистрибуции тематических групп тезауруса корпуса дискурсивных практик кибербезопасности

В исследуемом материале дискурсивный тезаурус кибербезопасности репрезентирован следующими группами лексики, определяющими специфику различных жанров в репрезентации смыслов: «Информационные и компьютерные технологии», «Знания», «Закон» и «Преступление», а также «Опасность», «Война», «Агрессия».

Тематическая группа лексики «Информационные и компьютерные технологии» включает терминологические единицы сферы компьютерных технологий (например, *кибер, интернет, программное обеспечение, приложение, система аутентификации, облачные технологии, IT-инфраструктура, ботнет, маршрутизатор, фильтрация, приложение, сервер, брандмауэр* и др.). Тематическая группа «Знание» объединяет лексические единицы с антонимичными семантическими признаками наличия / отсутствия знания (например, *информация, осведомленность, иден-*

тификация, знание, учение, киберкомпетентность, киберграмотность, кибersознание, сомнение, пробел, формула, опыт, навык, компетенция).

Отдельные лексические единицы входят в пласт общей и специальной лексики, которая соотносится с административно-правовым регулированием информационной деятельности, например, тематическая группа «Закон» ассоциируется с законодательными и нормативно-правовыми актами (*закон, юридический, киберстрахование, кибернетическая ответственность, киберзаконодательство*, *конвенция, согласование, юрист, доктрина, указ, кодекс, документ, статья, право, закон*); логически связанная с ней группа «Преступление» включает слова, обозначающие типы угроз, виды преступлений, номинации субъектов преступлений и пострадавших, способы расследования (например, *киберпреступность, киберпреступление, киберпреступный, киберзахват, кибервзлом, кибермошенничество, кибершпионаж, киберограбление, киберзапугивание, киберпроникновение, кибершпионский, кибердетектив, киберполиция, киберрасследование, кибертерроризм, киберфорензика, киберкриминалистика, кибер-разоблачение, кибер-буллинг; киберпреступник, киберзлоумышленник, кибер-бандит, киберхулиган, кибер-шантажист, кибербанда; кибервзломщик, кибервымогатель, кибершантаж, жертва*).

Регулярное использование в дискурсивном тезаурусе лексических единиц, номинирующих социально неодобряемые явления и действия, указывает на негативное оценочное информирование об отдельных формах деятельности в информационно-коммуникативном пространстве. Тональность негативной оценки поддерживается словами с семантикой опасности (семантизация вреда, угрозы: *риск, беспокойство, страх, опасение, брешь, уязвимость, вредоносный, утеря, срыв, перебой, сокрытие*), милитарной лексикой, включающей лексические единицы, концептуализирующие незаконные действия акторов в сфере кибердеятельности в терминах военных действий: *кибервойна, киберфронт, кибервойско, киберучения, кибер-армия, киберпротивник, кибератака, кибервоздействие, кибероружие, кибернападение, киберзахват, кибернаступление, кибернаступательный, кибервторжение, киберсдерживание, кибервмешательство, кибер-рейд, кибер-агрессия, киберполигон, кибероперация, кибероборона, киберразведка.* Сопряженная с данной тематической группой лексика, передающая семантику агрессии, усиливает общую прагматику опасности и угрозы безопасности пользователей виртуального интернет пространства: *киберугроза, насилие, давление, эскалация, блокирование, противостояние, жертва, вред, борьба, вторжение*.

Установив общую семантическую организацию дискурсивного тезауруса, мы провели анализ дистрибуции тематических групп лексики в раз-

OPEN ACCESS [Научный диалог = Nauchnyi dialog = Nauchnyy dialog, 12(3), 2023]
[ISSN 2225-756X, eISSN 2227-1295]

личных жанрах кибербезопасности с целью определения жанровой специфики семантических доминант, репрезентирующих смыслы.

Таблица 3

Дистрибуция тематических групп лексики
в жанрах дискурсивных практик кибербезопасности

Жанры контента / **Тематическая группа**	**новостной**	**информационно-просветительский**	**профессионально-ориентированный**	**рекламно-маркетинговый**	**сетевой**
«Знание»	4 959.35	5 228.85	5 188.43	9 178.74	3 704.51
«Закон»	2 046.62	3 627.07	2 452.57	3 727.12	2 179.12
«Преступление»	2 249.22	349.82	1586.48	1 186.75	871.75
«Опасность»	4 664.37	10 807.53	11 348.18	11 088.65	3 268.69
«Агрессия»	1 696.13	1 159.92	1 068.45	1 019.86	1 089.56
«Война»	4 664.36	3 961.00	3 083.92	2 299.32	1 525.39

Как показывает таблица 3, в количественном выражении в каждом из рассматриваемых жанров семантическая доминанта дискурсивных практик кибербезопасности образована лексическими единицами с семантикой опасности, которая поддерживается темой «Агрессия». Так, в информационно-просветительском, профессионально-ориентированном, рекламно-маркетинговым контенте объектом описания становятся проблемы, нарушения, негативные последствия использования интернет-технологий, вызывающие ощущения риска и беззащитности: (2) *Эпоха цифровизации и процессы цифровой трансформации* ***грозят*** *снова изменить парадигму защиты — все становится цифровым и вместе с возможностями* ***порождает и новые риски*** (https://www.it-world.ru/cionews/security); (3) *Сегодня один из векторов — это* ***подача фейковой информации*** *от имени* ***взломанных источников*** (kommersant.ru); (4) *Такие* ***типы атак*** *фактически* ***превращают сервисы и информацию в оружие*** (myseldon.com).

В исследуемых жанрах важное место занимает тематика экспертного знания и просвещения, что связано с необходимостью внедрения в общественное сознание терминологических и юридических понятий, передающих знание о новых технологиях, способах преодоления угроз и рисков. Примечательно, что тема знания в текстах информационно-просветительских и профессионально-ориентированных жанров сопряжена с доминирующей стратегией медиатизации опасности и рисков, например: (5) *Раньше хакерам необходимо было обладать огромными знаниями, чтобы на-*

писать зловред, внедрить его и украсть данные. Теперь человек без специальных навыков может воспользоваться услугами посредников (https://www.forbes.ru/tehnologii). В новостных и рекламно-маркетинговых текстах доминируют лексические единицы с семантикой преступления и используется метафорическая семиотика войны: (6) *В США идет* ***расследование*** *самой крупной* ***кибератаки*** *современности,* ***целью*** *которой стали многие жизненно важные правительственные учреждения страны. Хакеры чаще всего предпочитают* ***атаковать*** *не конкретную цель, а стремятся охватить максимально возможное количество* ***жертв*** (https://www.rbc.ru/technology_and_media).

Состав лексики рекламно-маркетинговой сферы указывает на жанровую специфику семантической организации текстов. Доминантой в них становится лексика с семантикой «Знание» (9178.74) и «Опасность» (11088.75), что позволяет предположить, что в целях маркетингового воздействия на адресата (возможного потребителя услуги) составители текстов позиционируют себя как носителей экспертного знания, например: (7) *Компания «Интеллектуальная безопасность» является* ***резидентом ИТ-кластера*** *Сколково по направлению «Кибербезопасность» и* ***разрабатывает передовые решения*** *в области управления и автоматизации процессов* ***информационной безопасности*** *для практического применения в государственном и корпоративном сегментах* (https://www.securityvision.ru); эксплуатируют страх перед технологиями, намеренно усиливая семантику опасности: (8) *«ДиалогНаука» поставляет широкий спектр программных и аппаратных* ***средств защиты информации*** *производства ведущих отечественных компаний для* ***защиты от вирусов, спама, сетевых атак, утечки конфиденциальной информации и других угроз информационной безопасности*** (https://www.dialognauka.ru)*;* (9) *Это* ***недостаток*** *программно-технического средства или информационной системы в целом, который может быть использован для* ***реализации угроз безопасности информации,*** *то есть уязвимость — это* ***слабое место*** *актива или средства контроля и управления, которое может быть* ***использовано злоумышленниками*** (https://www.securityvision.ru/blog).

Публикации в сетевом дискурсе часто преследуют цели, сходные с рекламно-маркетинговым контентом. Авторы блогов, претендуя на роль «лидера мнения», пытаются совместить реализацию информативно-просветительской цели с интенцией саморекламы: (9) *Обычные люди тоже становятся* ***целью для киберпреступников****.* ***Злоумышленники*** *используют для* ***кибермошенничества*** *актуальные проблемы. Например, в активно эксплуатируется тема вакцинации и QR-кодов* (https://vk.com/cybersi). Для этой разновидности медийного контента характерно минимальное ис-

пользование специальной лексики, стремление к упрощенному разъяснению причин и последствий кибератак с целью предупреждения пользователей о возможных угрозах.

4. Заключение = Conclusions

Использование методологии корпусной лингвистики в анализе текстовых массивов дискурсивных практик кибербезопасности на материале русскоязычного медийно-сетевого контента позволило провести когнитивно-семантическую реконструкцию дискурсивного тезауруса и верифицировать основные черты его системной организации. Семантически тезаурус организован вокруг стержневого понятия «кибербезопасность», которое вербализовано терминологическими единицами и словосочетаниями, представляющими собой специализированные именные и глагольные коллокации, характеризующимися информативной, описательно-дескриптивной семантикой научно-технического содержания, номинирующими виды информационной безопасности, ее субъектов и типы действий, определяющих безопасное онлайн-поведение и направленных на предотвращение угрозы. С другой стороны, тезаурус включает значительный пласт негативно окрашенных лексических единиц и коллокаций, формирующий отрицательное оценочное поле дискурса.

Проведенное исследование позволило провести категоризацию лексических единиц дискурсивной практики «кибербезопасность» и изучить их дистрибуцию и контекстуально-семантические особенности в различных форматах русскоязычного медийного и сетевого контента. Анализ показал, что, наряду с терминами и единицами общего характера, относящимися к сферам «Информационные и компьютерные технологии», «Знание», «Закон», в дискурсе кибербезопасности регулярно присутствует милитарно-агрессивная лексика, образующая тематические группы «Опасность», «Преступление», «Война», «Агрессия» и формирующая негативную рецепцию компьютерных технологий в сознании представителей русскоязычного дискурсивного сообщества. Выявленная специфика организации тезауруса дискурса объективирует научную гипотезу данного исследования о биполярности ценностных представлений о кибербезопасности как новой социальной реальности в современных дискурсивных практиках, где наряду с реализацией информативной, информационно-просветительской функций и интенцией позитивной маркетизации компьютерных технологий формируется дискурсивная негативная оценка у нейтральных в оценочном плане языковых единиц, что усиливает семантику риска и опасности, формирует критичное отношение и недоверие к ним пользователей.

Предложенная методика изучения семантической, прагматической и аксиологической дискурсивных составляющих с помощью методов корпусного анализа представляется перспективной для решения важной методологической задачи — фиксации и анализа актуальных дискурсивных практик, ориентированных на ценностное освоение феноменов новой социальной реальности.

Заявленный вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. **Авторы заявляют об отсутствии конфликта интересов.**	**Contribution of the authors:** the authors contributed equally to this article. **The authors declare no conflicts of interests.**

Источники и принятые сокращения

1. КДПК — *Корпус* дискурсивных практик кибербезопасности. — CQPweb [Электронный ресурс]. — Режим доступа : https://cqpweb.lancs.ac.uk/usr/6c/lakvolgu/ (дата обращения 14.01.2023).

2. Uppsala Russian Corpus — *CQPweb* [Electronic resource]. — Access mode : https://cqpweb.lancs.ac.uk/ (accessed 16.01.2023).

Литература

1. *Анашкина И. А.* Корпусно-ориентированный метод дискурс-анализа (на материале английского языка) / И. А. Анашкина, И. И. Конькова // Вестник Пермского национального исследовательского политехнического университета. Проблемы языкознания и педагогики. — 2021. — № 2. — С. 30—42. — DOI: 10.15593/2224-9389/2021.2.3.

2. *Бродовская Е. В.* Влияние цифровых коммуникаций на формирование профессиональной культуры российской молодежи : результаты комплексного прикладного исследования / Е. В. Бродовская, А. Ю. Домбровская, Р. В. Пырма, А. В. Синяков, А. А. Азаров // Мониторинг общественного мнения : Экономические и социальные перемены. — 2019. — № 1. — С. 228—251. — DOI: 10.14515/monitoring.2019.1.11.

3. *Ефремова М. П.* Концепт «SAFETY/SECURITY» в английской языковой картине мира : автореферат диссертации … кандидата филологических наук : 10.02.04 / М. П. Ефремова. — Санкт-Петербург, 2021. — 25 с.

4. *Змазнева О. А.* Коммуникативное пространство соцсетей начала XXI в. : файлы образов и потоки сознания / О. А. Змазнева // Вестник Московского городского педагогического университета. Серия : Философские науки. — 2018. — № 3 (27). — С. 16—22.

5. *Ильинова Е. Ю.* Семантическая категоризация при реконструкции тематического содержания текста новостного сообщения / Е. Ю. Ильинова // Когнитивные исследования языка. — 2016. — № 26. — С. 537—539.

6. *Карасик В. И.* Языковая матрица культуры / В. И. Карасик. — Москва : Гнозис, 2013. — 320 с. — ISBN 978-5-94244-043-5.

7. *Кочетова Л. А.* Когнитивно-корпусный подход к анализу конструирования ценностных смыслов в рекламном дискурсе / Л. А. Кочетова, И. В. Кононова // Вопросы когнитивной лингвистики. — 2019. — № 2. — С. 65—74.

8. *Леонтьева Т. В.* Репрезентация противоположностей в слове друг-враг : контекстный анализ / Т. В. Леонтьева, А. В. Щетинина // Мир русского слова. — 2020. — № 2. — С. 35—39. — DOI: 10.24411/1811-1629-2020-12035.

9. *Маринова Е. В.* Эволюция понятия «виртуальная личность» в цифровую эпоху (социо-лингвистическое исследование на материале русских текстов) / Е. В. Маринова // Научный диалог. — 2023. — Т. 12. — № 1. — С. 151—169. — DOI: 10.24224/2227-1295-2023-12-1-151-169.

10. *Общая* и русская лингвоаксиология : коллективная монография / М. С. Милованова (отв. ред.), К. Я. Сигал, В. И. Карасик, Г. Г. Слышкин, Б. И. Фоминых, Н. А. Боженкова, Л. М. Гончарова, А. Н. Матрусова, Р. Р. Шамсутдинова ; ИЯз РАН, Гос. ИРЯ им. А. С. Пушкина. — Москва — Ярославль : Издательство «Канцлер», 2022. — 390 с. — ISBN 978-5-98269-258-0.

11. *Орлова Н. В.* Семантические ряды как инструмент анализа дискурса (на материале дискурса о поколениях) / Н. В. Орлова // Научный диалог. — 2021. — № 1 (7). — С. 108—122. — DOI: 10.24224/2227-1295-2021-7-108-122.

12. *Ребрина Л. Н.* Семантика вражды : обозначения агрессивного субъекта в Интернет-коммуникации / Л. Н. Ребрина // Вестник Волгоградского государственного университета. Серия 2, Языкознание. — 2021. — Т. 20. — № 4. — С. 74—90. — DOI: https://doi.org/10.15688/jvolsu2.2021.4.6.

13. *Чернявская В. Е.* Методологические возможности дискурсивного анализа в корпусной лингвистике / В. Е. Чернявская // Вестник Томского государственного университета. Филология. — 2017. — № 50. — DOI: 10.17223/19986645/50/9.

14. *Baker P.* Using Corpora in Discourse Analysis / P. Baker. — London : Continuum, 2006. — 208 p.

15. *Gabrielatos C.* Keyness Analysis: nature, metrics and techniques / C. Gabrielatos // Taylor, C. & Marchi, A. (eds.) Corpus Approaches to Discourse : A critical review. — Oxford : Routledge, 2018. — Pp. 225—258.

16. *Laclau E.* The Time is out of Joint / E. Laclau // Diacritics. — 1995. — Vol. 25. — № 2. — Pp. 85—96.

17. *Louw B.* Irony in the text or insincerity in the writer? The diagnostic potential of semantic prosodies / B. Louw // M. Baker, G. Francis and E. Tognini-Bonelli (eds), Text and Technology : In Honour of John Sinclair. — Amsterdam : John Benjamins, 1993. — Pp. 157—175.

18. *Parvaresh V.* Covertly communicated hate speech : A corpus-assisted pragmatic study / V. Parvaresh // Journal of Pragmatics. — 2023. — Vol. 205. — Pp. 63—77. — DOI: 10.1016/j.pragma.2022.12.009.

19. *Stubbs M.* Collocations and semantic profiles. On the cause of the trouble with quantitative studies / M. Stubbs // Functions of Language. — 1995. — № 2/1. — Pp. 23—55.

20. *Teubert W.* Corpus Linguistics. A short introduction / W. Teubert, A. Cermakova. — London et al. : Continuum, 2007. — 176 p. — ISBN 9780826494801.

Статья поступила в редакцию 16.03.2023,
одобрена после рецензирования 18.04.2023,
подготовлена к публикации 24.04.2023.

Material resources

KDPC is a corpus of discursive cybersecurity practices — *CQPweb.* Available at: https://cqpweb.lancs.ac.uk/usr/6c/lakvolgu / (accessed 14.01.2023). (In Russ.).

Uppsala Russian Corpus — *CQPweb.* Available at: https://cqpweb.lancs.ac.uk/ (accessed 16.01.2023).

References

Anashkina, I. A., Konkova, I. I. (2021). Corpus-oriented method of discourse analysis (based on the material of the English language). *Bulletin of Perm National Research Polytechnic University. Problems of linguistics and pedagogy, 2:* 30—42. DOI: 10.15593/2224-9389/2021.2.3. (In Russ.).

Baker, P. (2006). *Using Corpora in Discourse Analysis.* London: Continuum. 208 p.

Brodovskaya, E. V., Dombrovskaya, A. Yu., Pyrma, R. V., Sinyakov, A. V., Azarov, A. A. (2019). The influence of digital communications on the formation of professional culture of Russian youth: the results of a comprehensive applied research. *Monitoring of public opinion: Economic and social changes, 1:* 228—251. DOI: 10.14515/monitoring.2019.1.11. (In Russ.).

Chernyavskaya, V. E. (2017). Methodological possibilities of discursive analysis in corpus linguistics. *Bulletin of Tomsk State University. Philology, 50.* DOI: 10.17223/19986645/50/9. (In Russ.).

Efremova, M. P. (2021). *The concept of "SAFETY/SECURITY" in the English language picture of the world.* Author's abstract of PhD Diss. St. Petersburg. 25 p. (In Russ.).

Gabrielatos, C. (2018). *Keyness Analysis: nature, metrics and techniques.* Oxford: Routledge. 225—258.

General and Russian linguoaxiology: A collective monograph. (2022). Moscow—Yaroslavl: Publishing house "Chancellor". 390 p. ISBN 978-5-98269-258-0. (In Russ.).

Ilinova, E. Yu. (2016). Semantic categorization in the reconstruction of the thematic content of the text of a news message. *Cognitive studies of language, 26:* 537—539. (In Russ.).

Karasik, V. I. (2013). *Language matrix of culture.* Moscow: Gnosis. 320 p. ISBN 978-5-94244-043-5. (In Russ.).

Kochetova, L. A., Kononova, I. V. (2019). Cognitive-corpus approach to the analysis of the construction of value meanings in advertising discourse. *Questions of cognitive linguistics, 2:* 65—74. (In Russ.).

Laclau, E. (1995). The Time is out of Joint. *Diacritics, 25 (2):* 85—96.

Leontieva, T. V., Shchetinina, A. V. (2020). Representation of opposites in the word friend-enemy: contextual analysis. *The world of the Russian word, 2:* 35—39. DOI: 10.24411/1811-1629-2020-12035. (In Russ.).

Louw, B. (1993). Irony in the text or insincerity in the writer? The diagnostic potential of semantic prosodies. In: *Text and Technology: In Honour of John Sinclair.* Amsterdam: John Benjamins. 157—175.

Marinova, E. V. (2023). Evolution of the concept of "virtual personality" in the digital age (socio-linguistic research based on Russian texts). *Nauchnyj dialog, 12 (1):* 151—169. DOI: 10.24224/2227-1295-2023-12-1-151-169. (In Russ.).

Orlova, N. V. (2021). Semantic series as a discourse analysis tool (based on the discourse on generations). *Nauchnyj dialog, 1 (7):* 108—122. DOI: 10.24224/2227-1295-2021-7-108-122. (In Russ.).

Parvaresh, V. (2023). Covertly communicated hate speech: A corpus-assisted pragmatic study. *Journal of Pragmatics, 205:* 63—77. DOI: 10.1016/j.pragma.2022.12.009.

Rebrina, L. N. (2021). Semantics of enmity: designations of an aggressive subject in Internet communication. *Bulletin of the Volgograd State University. Series 2, Linguistics, 20 (4):* 74—90. DOI: https://doi.org/10.15688/jvolsu2.2021.4.6. (In Russ.).

Stubbs, M. (1995). Collocations and semantic profiles. On the cause of the trouble with quantitative studies. *Functions of Language, 2/1:* 23—55.

Teubert, W., Cermakova, A. (2007). *Corpus Linguistics. A short introduction.* London et al.: Continuum. 176 p. ISBN 9780826494801.

Zmazneva, O. A. (2018). The communicative space of social networks of the beginning of the XXI century: image files and streams of consciousness. *Bulletin of the Moscow City Pedagogical University. Series: Philosophical Sciences, 3 (27):* 16—22. (In Russ.).

The article was submitted 16.03.2023;
approved after reviewing 18.04.2023;
accepted for publication 24.04.2023.