ИЗДАТЕЛЬСТВО грамота

Филологические науки. Вопросы теории и практики
Philology. Theory & Practice

ISSN 2782-4543 (online)
ISSN 1997-2911 (print)

2025. Том 18. Выпуск 6 | 2025. Volume 18. Issue 6
Материалы журнала доступны на сайте (articles and issues available at): philology-journal.ru

RU

«Цифровая преступность» в финансово-экономическом дискурсе (на материале английских неологизмов)

Катермина В. В., Плаксин В. А.

Аннотация. Цель исследования – путем комплексного анализа выявить семантико-аксиологические особенности выделенного комплекса неологизмов финансово-экономического дискурса (на материале англоязычных неографических электронных источников за период с 2017 по 2025 г.). В статье определены основные компоненты неологических единиц анализируемого дискурса (сферы влияния, объекты, инструменты, особенности цифровых преступлений), а также указана роль отрицательной коннотации неологизмов, обозначающих киберпреступления. Научная новизна исследования заключается в комплексном изучении цифровых преступлений, выраженных при помощи английских неологизмов, относящихся к финансово-экономическому дискурсу: проведена классификация конкретного пласта новой англоязычной лексики финансово-экономического дискурса; через лингвистический анализ неологизмов финансово-экономического дискурса определены некоторые ценностные ориентиры носителей языка. С развитием современных технологий сформировались условия для появления нового вида преступлений – преступлений, совершаемых в цифровом пространстве (цифровых преступлений). В результате исследования выявлено влияние анализируемых неологизмов на мировосприятие англоязычного общества посредством экспликации определенных заданных ценностей в дискурсе, обслуживающем данный институт, а также рассмотрены способы включения тех или иных явлений в ценностное поле языка путем их номинации и категоризации.

EN

“Digital crime” in financial and economic discourse (based on English neologisms)

V. V. Katermina, V. A. Plaxin

Abstract. The aim of the study is to conduct a comprehensive analysis of the semantic and axiological features of the selected set of neologisms of the financial and economic discourse (based on English neographic electronic sources from 2017 to 2025). The article highlights the main components of the neological units of the analyzed discourse (spheres of influence, objects, tools, features of digital crimes), and also indicates the role of the negative connotation of neologisms denoting cybercrimes. The scientific novelty of the work lies in a comprehensive study of digital crimes expressed by English neologisms related to the financial and economic discourse: a classification of a certain layer of new English vocabulary of the financial and economic discourse is carried out; using a linguistic analysis of neologisms of the financial and economic discourse, some axiological orientations of native speakers are determined. With the development of modern technologies, conditions have been formed for the emergence of a new type of crime – crimes committed in the digital space (digital crimes). As a result of the study, the influence of the analyzed neologisms on the worldview of the English-speaking society was revealed through the explication of certain given values in the discourse serving this institution, and the ways of including certain phenomena in the axiological field of the language by means of their nomination and categorization were considered.

Введение

В наше время «человек проживает в двух плоскостях: реальной жизни и киберпространстве. Практически все явления его бытийности дублируются в двух мирах, как положительные, так и отрицательные. Интернет дарит индивиду сотни возможностей: обладание и управление безграничной информацией, совершение мелких и крупных покупок, поиск желаемого в считанные секунды. Но, цитируя произведения массовой культуры, “с большой силой приходит большая ответственность”. Особенно остро это ощущается с появлением искусственного интеллекта» (Бобр, 2024, с. 41).

Научная статья (original research article) | https://doi.org/10.30853/phil20250328

© 2025 Авторы. © 2025 ООО Издательство «Грамота» (© 2025 The Authors. © 2025 Gramota Publishing, LLC). Открытый доступ предоставляется на условиях лицензии CC BY 4.0 (open access article under the CC BY 4.0 license): https://creativecommons.org/licenses/by/4.0/

Актуальность исследования обусловлена теоретическими и практическими аспектами развития лингвистики, ее полидисциплинарным и интегративным характером. Экономика – «область знаний современника о мире, где особенно отчетливо проявляются базовые интересы социума и этноса, где заметны изменения в общественном сознании, ментальное носителя языка, где имеет место активная языковая динамика» (Петушинская, 2008, с. 6). Изучение англоязычных неологизмов финансово-экономического дискурса, семантических основ неономинаций позволяет выявить тесную связь между культурой и языком носителя, определить его ценностные ориентации. Следует указать, что аксиологическая трансформация ряда понятий, вызванная развитием информационных технологий и, как следствие, информационной безопасности, также определяет трактовку ценностной картины мира носителя языка.

В статье необходимо решить следующие задачи:

1) выявить английские неологизмы, называющие киберпреступления, функционирующие в финансово-экономическом дискурсе;

2) выделить основные компоненты анализируемых единиц, а также раскрыть роль отрицательной коннотации английских неологизмов, обозначающих киберпреступления в финансово-экономическом дискурсе;

3) рассмотреть влияние «цифровых преступлений», выраженных неологизмами, на возникновение новых аксиологических установок в англоязычном обществе.

Для поиска новых слов и их дефиниций, помимо данных неографических электронных словарей (Word Spy. https://wordspy.com/; Urban Dictionary. http://www.urbandictionary.com; Cambridge Dictionary. https://dictionary.cambridge.org/ru/; Collins Dictionary. https://www.collinsdictionary.com), использовались контексты из медиатекстов (Nihad A. Hassan, Quishing attacks 101: how QR codes are exploited for phishing // Authentic8. 2024. https://www.authentic8.com/blog/quishing-qr-code-phishing; Katie Rees. What is an Infostealer? Is It dangerous? // Make Use Of. 2022. https://www.makeuseof.com/what-is-an-infostealer/; Pathak P. What is Quishing and how to protect yourself against it // All Things How. 2024. https://allthings.how/what-is-quishing-and-how-to-protect-yourself-against-it).

При решении задач, определенных в работе, использовались следующие методы исследования: метод сплошной выборки неологических единиц из электронных неографических источников; метод дефиниционного анализа, нацеленный на выявление компонентов значений исследуемых неологических единиц; лексикологический анализ, позволяющий увидеть неологические единицы англоязычного финансово-экономического дискурса с позиции как их семантики, так и прагматики, а также описательный метод.

Теоретической базой исследования послужили труды С. И. Алаторцевой (1998), И. С. Криворучко (2022), О. П. Матиенко (2022), Е. Г. Петушинской (2008), Е. В. Розен (2000), Е. В. Сенько (2007), Т. Л. Тропиной (2005), которые отражают современные тенденции неологии и неографии, а также развитие финансово-экономического дискурса. Вопросам лингвистической аксиологии посвящены работы Н. Д. Арутюновой (1988), В. И. Карасика, И. А. Долговой (2023), Е. Ф. Серебренниковой (2011).

Практическая значимость исследования состоит в возможности применения полученных данных при подготовке специалистов в области финансов, экономики, права и информационных технологий; для улучшения коммуникации между экспертами; для интеграции языка и цифровых знаний в финансово-экономическую практику. Результаты работы могут быть использованы в курсах по неологии английского языка, курсах по аксиологии и дискурсу.

Обсуждение и результаты

Cyberspace – “all of the data stored in a large computer or network represented as a three-dimensional model through which a virtual-reality user can move” (Collins Dictionary). / «Киберпространство – все данные, хранящиеся в большом компьютере или сети, представленные в виде трехмерной модели, по которой может перемещаться пользователь виртуальной реальности» (здесь и далее перевод выполнен авторами статьи. – *В. К., В. П.*). Это глобально сетевая, поддерживаемая компьютером, доступная для компьютера и генерируемая компьютером, многомерная, искусственная или виртуальная реальность. В этой реальности, окном к которой является каждый компьютер, видимые или слышимые объекты не являются ни физическими, ни, обязательно, представлениями физических объектов, а скорее по форме, характеру и действию состоят из данных, чистой информации (Benedikt, 1992).

Киберпреступные действия – это «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных» (Тропина, 2005, с. 36).

Агрессию и конфликт в языке как отражении киберпространства можно считать сложным многокомпонентным феноменом действительности и рассматривать с точки зрения поведения, образа мировосприятия, набора эмоциональных и эмоционально-модальных состояний (Бобр, Ахренова, 2024; Бобр, Мигдаль, 2023; Комалова, 2020; Bisno, 1988; Eden, Roberto, 2021; Theocharis, Bekiari, 2018).

Возникновение неологизмов в обществе рассматривается как «обязательный спутник нового в области культуры общества, будь то материальное производство, духовная или общественная жизнь, экономическая сфера, взаимоотношения между людьми разных социальных групп и профессий и между государствами» (Катермина, 2019, с. 4-5). Следует подчеркнуть необходимость изучения неологизмов в финансово-экономической сфере, обусловленную ролью, которую «экономическая часть культуры занимает в жизни социума и ее особой значимостью в современных мировых процессах» (Матиенко, 2022, с. 5-6).

Неология как наука может быть признана важным лингвистическим направлением будущего, поскольку рост неологических единиц связан с развитием языковых процессов; неологизмы отражают культурные нормы, социальные взаимоотношения, указывают на аксиологические доминанты.

«Новая лексика должна соответствовать прагматике ее употребления – быть краткой, выразительной, соответствующей нормам языка, адекватно передающей специфику окружающего континуума» (Катермина, Липириди, 2021, с. 55).

К основным типам киберпреступлений в современное время можно отнести хакинг (*hacking*) и фишинг-атаки (*phishing*).

Хакинг – «внесение изменений (взлом защиты компьютерной сети, отключение сайтов и пр.) в программном обеспечении для достижения определенных целей, отличающихся от целей создателей программ, изменения очень часто являются вредоносными» (Тугай, 2021, с. 7).

В финансово-экономическом дискурсе частотным становится хакерство, что подтверждается большим количеством новых слов (например, *phone hacking* (*взлом телефона*) – возможность для злонамеренных лиц, включая киберпреступников, хакеров или даже нечестных друзей, получить несанкционированный доступ к чужому смартфону или его данным.

Статистика взлома мобильных телефонов показывает, что более 60% случаев мошенничества происходят с мобильных устройств. Хакеры знают, что смартфон содержит конфиденциальную информацию и обеспечивает доступ к самым личным аккаунтам. Мошенники получают доступ к смартфону и всем его данным через вредоносные URL-адреса, смишинг (фишинг текстовых сообщений) и даже мошеннические сайты знакомств.

Фишинг-атаки – «это вид интернет-мошенничества, построенный на принципах социальной инженерии (хищение с использованием электронных средств доступа персональных данных, номеров кредитных карт, паролей и персональных данных с целью дальнейшего их использования для хищения денежных средств, которые в дальнейшем невозможно оспорить)» (Тугай, 2021, с. 7).

Quishing works similarly to traditional phishing attacks, where the URL to the malicious website is delivered via email or SMS messages. However, in quishing, the QR code is decoded into a URL that points to the malicious website. The malicious QR code can be printed on paper or simply created digitally on digital posters and delivered via social media posts or emails (https://www.authentic8.com/blog/quishing-qr-code-phishing). / *«Подавление» работает аналогично традиционным фишинговым атакам, когда URL вредоносного веб-сайта доставляется по электронной почте или SMS-сообщениям. Однако при «подавлении» QR-код декодируется в URL, который указывает на вредоносный веб-сайт. Вредоносный QR-код может быть напечатан на бумаге или просто создан в цифровом виде на цифровых плакатах и доставлен через сообщения в социальных сетях или электронные письма*.

Выше указывалось, что большинство киберпреступлений совершается в экономической сфере. Примерами, подтверждающими сферы влияния, могут выступать *банкоматы, наименование компаний, номинации нового типа валюты, система платежей, банковские счета, деньги,* встречающиеся в многочисленных неологических единицах: *jackpotting* (*джекпотминг*) – *the act of hacking an* ***ATM machine*** *to make it dispense all of its* ***cash*** (https://dictionaryblog.cambridge.org/category/new-words) (взлом банкомата с целью выдачи всех наличных); *transaction laundering* (*отмывание денег при помощи транзакций*) – *a form of* ***money laundering*** (https://dictionaryblog.cambridge.org/category/new-words) (форма отмывания денег); *cryptojacking* (*криптоджекинг*) – вид киберпреступности, включающий несанкционированное использование чужих устройств (компьютеров, смартфонов, планшетов или даже серверов) киберпреступниками для добычи криптовалюты); *crypto mugging* (*крипто-грабеж*) – *a crime involving the theft of* ***digital currencies*** (https://dictionaryblog.cambridge.org/category/new-words) (преступление, связанное с кражей цифровых валют); *infostealer* (*«инфокрад»*)–– *a type of* ***malware*** *with the capability of scanning for and exfiltrating* ***data*** *and credentials from your device* (http://www.urbandictionary.com) (вид вредоносного ПО, способного сканировать и извлекать данные и учетные данные с чужого устройства).

Как показывает анализ английских неологических единиц, обозначающих кибермошенничество, к основным объектам цифровых нарушений можно отнести следующие компоненты: *мобильные устройства, компьютеры, смартфоны, кредитные карты*: *digital pickpocketing* (*цифровая карманная кража*) – форма взлома, похожая на карманную кражу, но включающая использование технологий для получения доступа к секретной информации, например, к данным кредитных карт; *juice jacking* (*джус-джекинг*) – *an attack method in which attackers infect users'* ***phones*** *and* ***tablets*** *through publicly available power banks or USB ports* (http://www.urbandictionary.com) (метод атаки, при котором злоумышленники заражают телефоны и планшеты пользователей через общедоступные пауэрбанки или порты USB); *illware* (*вредоносное ПО*) – *any program or file that is intentionally harmful to a* ***computer, network*** *or* ***server*** (https://wordspy.com) (любая программа или файл, которые намеренно наносят вред компьютеру, сети или серверу).

Инструменты киберпреступлений: *a charging port* (*порт для зарядки*), *a type of computer program* (*тип компьютерной программы*), *using a company's payment system* (*использование платежной системы компании*), *a type of computer software* (*тип компьютерного программного обеспечения*), *QR codes* (*QR-коды*).

Так, например, в следующем примере, при описании «работы» квишинга, выделяется особенность данного преступления: QR-код декодируется в URL-адрес, указывающий на вредоносный веб-сайт.

Quishing, also known as QR phishing, is a cybersecurity threat that uses malicious QR codes to redirect users to harmful websites and trick them into downloading dangerous content on their devices. As with other phishing attacks, the main

goal of quishing attacks is to steal sensitive information like credentials or financial information or to install malicious software on users' devices (https://allthings.how/what-is-quishing-and-how-to-protect-yourself-against-it). / *Квишинг, также известный как QR-фишинг, представляет собой угрозу кибербезопасности, которая использует вредоносные QR-коды для перенаправления пользователей на вредоносные веб-сайты и обмана, заставляя их загружать опасный контент на свои устройства. Как и в случае с другими фишинговыми атаками, основная цель атак квишинг – украсть конфиденциальную информацию, такую как учетные данные или финансовая информация, или установить вредоносное программное обеспечение на устройства пользователей.*

Или, например, создание программного обеспечения, которое специально разрабатывается для кражи паролей, данных банковских счетов:

There's a wide range of data that cybercriminals aim to access through the use of infostealers. Most notably, payment card details and login credentials are highly valuable. A criminal could either directly use this data to their advantage or sell it on a dark web marketplace to other malicious actors (https://www.makeuseof.com/what-is-an-infostealer). / *Существует широкий спектр данных, к которым киберпреступники стремятся получить доступ с помощью «инфокрадов». В частности, данные платежных карт и учетные данные для входа в систему имеют большую ценность. Преступник может либо напрямую использовать эти данные в своих интересах, либо продать их на рынке даркнета другим злоумышленникам*.

Массовое распространение киберпреступлений привело к тому, что возникло «мошенничество как услуга» (*FaaS*). *Fraud as a service is a model used in cybercrime that involves providing fraudulent services or tools over the Internet* (https://dictionaryblog.cambridge.org/category/new-words). / *Мошенничество как услуга – модель, используемая в киберпреступлениях, которая предполагает предоставление мошеннических услуг или инструментов через Интернет*.

«Мошенничество как услуга» – это бизнес-модель киберпреступности, в которой злоумышленники продают инструменты, инфраструктуру и экспертные знания, которые позволяют другим совершать мошенничество более легко и эффективно. Предложения FaaS (Мошенничество как услуга), часто встречающиеся на торговых площадках даркнета или подпольных форумах, часто автоматизируют и совершенствуют процессы, такие как попытки массового фишинга. Это позволяет пользователям создавать убедительные поддельные веб-сайты и отправлять массовые электронные письма потенциальным жертвам, собирая учетные данные и личную информацию в больших масштабах.

Безусловным является тот факт, что во всех неологизмах, номинирующих киберпреступления, содержатся семы с отрицательной коннотацией: *illegal* (*contrary to, forbidden, or not authorized by law, especially criminal law*) – *нелегальный* (*противоречащий, запрещенный или не разрешенный законом, особенно уголовным законодательством*), *theft* (*the act of stealing property*) – *кража* (*акт кражи имущества*), *harm* (*to damage, hurt, or injure something, usually an inanimate object*) – *вредить* (*повреждать, ранить или травмировать что-либо, обычно неодушевленный предмет*), *attack* (*to apply violent force to someone or something*) – *нападать* (*применять грубую силу к кому-либо или чему-либо*), *steal* (*to take illegally, or without the owner's permission, something owned by someone else without intending to return it*) – *красть* (*незаконно или без разрешения владельца забрать что-либо, принадлежащее другому лицу, без намерения вернуть это*), *trick* (*to fool*; *to cause to believe something untrue*) – *обманывать* (*заставлять верить чему-либо ложному*), *to deceive* (*to trick or mislead*) – *обманывать* (*вводить в заблуждение*), *fraudulent* (*dishonest*; *based on fraud or deception*) – *мошеннический* (*нечестный*; *основанный на мошенничестве или обмане*).

Как видно из вышеперечисленных единиц, дерогативный компонент указывает на нелегальный, мошеннический характер совершения действия, часто связанный с нанесением морального или физического ущерба.

Атака с использованием телефонной связи (*TOAD attack* (*телефонно-ориентированная атака*)) – это форма многоуровневой фишинговой атаки. Из-за звуковой оболочки данного акронима (*toad – жаба*) в сознании говорящего сразу же возникает негативный образ. В нашей жизни нападение «жаб» – это реальное явление, демонстрирующее удивительную агрессию и силу этих существ: **T**elephone-**O**riented **A**ttack **D**elivery – кибератака, в которой злоумышленники используют телефонные звонки для обмана жертв. Данный неологизм обозначает телефонно-ориентированную атаку, форму многоуровневой фишинговой атаки, которая сочетает в себе такие элементы, как текстовые или мгновенные сообщения (смишинг), голосовые сообщения (вишинг) или электронную почту с социальной инженерией, чтобы обманом заставить пользователей раскрыть конфиденциальные, личные или финансовые данные.

Разновидностью атаки с использованием телефонной связи служит «атака посредника» (*MITM attack*), источником которой являются публичные точки доступа Wi-Fi. Публичные маршрутизаторы Wi-Fi имеют меньше протоколов безопасности, чем домашние или рабочие маршрутизаторы Wi-Fi. Это упрощает подключение к сети для пользователей, находящихся поблизости. Но это также облегчает хакерам задачу взлома маршрутизатора, чтобы они могли прослушивать интернет-трафик и собирать данные пользователей. Оба английских неологизма являются примером единиц-аббревиатур, функционирующих в финансово-экономическом дискурсе в большом количестве.

В заключении отметим новую тенденцию в работе организаций быстро и эффективно адаптироваться к ситуации и использовать методы для шифровки своих данных при защите от кибератак (*Crypto agility – the ability of an organization to quickly adapt and change the methods it uses to encrypt its data to protect it from cyberattacks* (https://dictionaryblog.cambridge.org/category/new-words). / *Криптогибкость – способность организации быстро адаптироваться и изменять методы, используемые для шифрования данных, чтобы защитить их от кибератак*). Считается, что криптогибкость (*crypto agility*) как проблема для ИТ-специалистов ушла в прошлое. Сейчас же она представляет из себя критическую проблему, затрагивающую все организации

и сотрудников, от руководителей до стажеров. По мере развития киберугроз, особенно в сфере квантовых вычислений, криптогибкость помогает обеспечить безопасность систем.

Таким образом, постижение людьми окружающего их континуума –фактор постоянного пополнения словарного состава языка новыми словами, отражающими когнитивную активность человеческого мышления с помощью ее отображения в языке. Анализ когнитивных причин генезиса неологизмов порождает необходимость в рассмотрении прагматических особенностей введения новых слов в речь.

Появление неологизмов связано с ценностными и антиценностными ориентирами англоязычного общества. Оказывая влияние на возникновение новых аксиологических установок в обществе, неологизмы непосредственно связаны с формированием оригинальных принципов и концепций.

Заключение

Стремительное увеличение количества англоязычных неологизмов финансово-экономического дискурса является результатом активного развития новых каналов передачи информации, повышения уровня финансовой безопасности людей.

Разнообразие английских неологизмов (возможная классификация и выделение основных компонентов – сферы влияния, объекты, инструменты, особенности цифровых преступлений), обозначающих киберпреступления в финансово-экономическом дискурсе, свидетельствует о важности данной проблемы для современного общества.

Лексико-семантические номинации хакерства, разнообразных видов кибератак отражают современные угрозы и методы борьбы с ними. Особое внимание при изучении анализируемых неологизмов уделяется их роли в формировании общественного восприятия цифровых экономических преступлений.

Выделением отрицательной коннотации при анализе англоязычных неологизмов финансово-экономического дискурса формируется представление о ценностной картине мира носителя языка, о культурном коде этноса, об интенции носителя и его когнитивной сфере. Информационная безопасность становится одной из ведущих аксиологических установок, превалирующих в современном обществе.

Перспективами дальнейшего исследования может служить последующее изучение англоязычных неологизмов финансово-экономического дискурса, их систематизации, определение аксиологического потенциала новых лексических единиц, что будет способствовать лучшему пониманию лингвистических процессов, сопровождающих трансформацию финансово-экономической сферы в эпоху цифровизации.

Источники | References

1. Алаторцева С. И. Русская неология и неография (современное состояние и перспективы). СПб.: ЛГОУ, 1998.
2. Арутюнова Н. Д. Типы языковых значений. Оценка. Событие. Факт. М.: Наука, 1988.
3. Бобр А. Д. Маркеры вербальной агрессии в комментариях пользователей социальных сетей: дисс. … к. филол. н. Мытищи, 2024.
4. Бобр А. Д., Ахренова Н. А. Гендерные особенности проявления вербальной агрессии в киберпространстве // Военно-филологический журнал. 2024. № 1.
5. Бобр А. Д., Мигдаль И. Ю. Маркеры вербальной агрессии в комментариях социальной сети «ВКонтакте» // Вопросы прикладной лингвистики. 2023. № 4 (52). https://doi.org/10.25076/vpl.52.02
6. Карасик В. И., Долгова И. А. Лингвоаксиология мировосприятия // Современная лингвоаксиология: коллективная монография. М.: Государственный институт русского языка им. А. С. Пушкина, 2023.
7. Катермина В. В. Словообразовательный потенциал неологизмов в англоязычном массмедийном дискурсе: монография. Краснодар: КубГУ, 2019.
8. Катермина В. В., Липириди С. Х. Прагматико-аксиологический потенциал сетевых английских неологизмов туристического дискурса: монография. Краснодар: Кубанский гос. ун-т, 2021.
9. Комалова Л. Р. Агрессогенный дискурс: типология мультилингвальной вербализации агрессии = Aggressogen discourse: the multilingual aggression verbalization typology: монография. Изд-е 2-е, стер. М.: Спутник+, 2020.
10. Криворучко И. С. Неологическая метафора как изобразительное средство современной деловой коммуникации // Вестник Костромского государственного университета. 2022. Т. 28. № 2. https://doi.org/10.34216/1998-0817-2022-28-2-224-227
11. Матиенко О. П. Ключевые метафоры экономики в текстах российских СМИ: дисс. … к. филол. н. Омск, 2022.
12. Петушинская Е. Г. Язык популярного экономического дискурса (на материале англоязычной публицистики): автореф. дисс. … к. филол. н. М., 2008.
13. Розен Е. В. На пороге XXI века: новые слова и словосочетания в немецком языке. М.: Менеджер, 2000.
14. Сенько Е. В. Неологизация в современном русском языке: межуровневый аспект. СПб.: Наука, 2007.
15. Серебренникова Е. Ф. Лингвистика и аксиология: этносемиометрия ценностных смыслов: коллективная монография. М.: ТЕЗАУРУС, 2011.
16. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дисс. … к. юрид. н. Владивосток, 2005.

17. Тугай Л. А. Лингвистические аспекты расследования киберпреступлений // Вестник магистратуры. 2021. № 11-3 (122).
18. Benedikt M. Cyberspace: First Steps. Cambridge: The MIT Press, 1992.
19. Bisno H. Managing Conflict. Newbury Park: Sage Publications, 1988.
20. Eden J., Roberto A. J. The Role of Verbal Aggression in Cyberbullying Perpetration and Victimization by Middle School Students // Future Internet. 2021. № 13. https://doi.org/10.3390/fi13090223
21. Theocharis D., Bekiari A. Dynamic analysis of verbal aggressiveness networks in school // Open Journal of Social Sciences. 2018. № 06 (01). https://doi.org/10.4236/jss.2018.61002

Информация об авторах | Author information

RU

Катермина Вероника Викторовна[1], д. филол. н., проф.
Плаксин Владимир Аркадьевич[2], к. филол. н., доц.
[1] Кубанский государственный университет, г. Краснодар
[2] Финансовый университет при Правительстве Российской Федерации, г. Краснодар

EN

Veronika Viktorovna Katermina[1], Dr
Vladimir Arkadievich Plaxin[2], PhD
[1] Kuban State University, Krasnodar
[2] Financial University under the Government of the Russian Federation, Krasnodar

[1] *veronika.katermina@yandex.ru,* [2] *vladimirplaxin@rambler.ru*

Информация о статье | About this article

Дата поступления рукописи (received): 12.05.2025; опубликовано online (published online): 22.06.2025.

Ключевые слова (keywords): англоязычные неологизмы; онлайн-мошенничество; семантика; аксиология; отрицательная коннотация; финансово-экономический дискурс; English neologisms; online fraud; semantics; axiology; negative connotation; financial and economic discourse.