ИЗДАТЕЛЬСТВО грамота

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

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

2026. Том 19. Выпуск 4 | 2026. Volume 19. Issue 4
Материалы журнала доступны на сайте (articles and issues available at): philology-journal.ru

RU

Фреймирование ситуации AI-ENABLED FRAUD в англоязычном медиадискурсе

Филошина И. О.

Аннотация. Цель исследования – построить фреймовую модель ситуации AI-ENABLED FRAUD / МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ИИ в англоязычном медиадискурсе США, Великобритании, Канады, Австралии, Сингапура и Китая и выявить особенности фреймирования данной ситуации в образцах медиадискурса указанных стран. Научная новизна исследования состоит в том, что в нем впервые описаны и систематизированы вариации во фреймировании ситуации AI-ENABLED FRAUD в медиадискурсе шести стран с учетом принятых в нем коммуникативных интенций и стратегий. В результате исследования разработана фреймовая модель ситуации AI-ENABLED FRAUD на основе фреймов ПРЕСТУПЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИИ и ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ДЛЯ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ; ее иерархическая структура содержит субфреймы, слоты и подслоты. Установлено, что образцы медиадискурса шести указанных стран, посвященного проблеме использования технологии ИИ в мошеннических целях, демонстрируют как сходства, так и различия в выборе направления фреймирования при моделировании данной ситуации. Сходства в направлении фреймирования определяются реализацией коммуникативной интенции информирования в целях предупреждения преступности; при этом наблюдается ряд особенностей моделирования ситуации: в медиадискурсе США и Великобритании они обусловлены дискурсивной практикой конструирования достоверности; а в медиадискурсе Сингапура – дискурс-периферией с образовательной функцией. Также в ходе исследования выявлена вариативность в выборе лексических средств объективации слотов инвариантных субфреймов.

EN

Framing the AI-ENABLED FRAUD situation in English-language media discourse

I. O. Filoshina

Abstract. The research aims to construct a frame model of the AI-ENABLED FRAUD situation in the English-language media discourse of the USA, the UK, Canada, Australia, Singapore, and China and to identify the specific features of framing this situation in the media samples of these countries. The scientific novelty of the study lies in the first systematic description and classification of variations in framing the AI-ENABLED FRAUD situation across the media discourses of six countries, taking into account the communicative intentions and strategies adopted within them. As a result of the study, a frame model of the AI-ENABLED FRAUD situation was developed based on the frames CRIME USING AI TECHNOLOGY and TECHNOLOGIES USED FOR FRAUDULENT OPERATIONS; its hierarchical structure comprises subframes, slots, and subslots. It was established that the media discourse samples from the six countries dedicated to the problem of using AI technology for fraudulent purposes demonstrate both similarities and differences in the direction of framing when modeling this situation. Similarities in the framing direction are determined by the implementation of the communicative intention to inform for the purpose of crime prevention. At the same time, several modeling features were observed: in the US and UK media discourse, they are conditioned by the discourse practice of constructing credibility, while in the Singaporean media discourse, they stem from the discourse periphery with an educational function. The study also revealed variability in the choice of lexical means for the objectification of slots within invariant subframes.

Введение

Актуальность данного исследования обусловлена интересом лингвистов к сопоставительным когнитивным исследованиям, проявляющимся в сосредоточении научного интереса на проблеме сопоставительного

Научная статья (original research article) | https://doi.org/10.30853/phil20260170

анализа моделей воспроизведения знаний в тексте, обусловливающих характер репрезентации политических и социальных феноменов как в различных видах медиадискурса, так и в медиадискурсе разных стран. Такого рода исследования позволяют установить различия между содержанием когнитивной и когнитивно-дискурсивной моделей ситуации при анализе формирования репрезентативных структур в медиадискурсе. Кроме того, они выявляют и систематизируют экстралингвистические и жанрово обусловленные факторы, коммуникативные стратегии, тактики и дискурсивные практики СМИ, непосредственно соотносимые с особенностями репрезентации ментально-языковых феноменов; а также способствуют установлению как универсальных, так и лингвокультурных особенностей процесса миромоделирования в медиадискурсе разных стран.

Для достижения вышеуказанной цели исследования необходимо решить следующие задачи:

1) определить ключевые элементы категориально-понятийного аппарата англоязычных юридических текстов, посвященных проблеме ИИ-мошенничества;

2) разработать фреймовую модель ситуации AI-ENABLED FRAUD, релевантную для образцов медиадискурса США, Великобритании, Канады, Австралии, Сингапура и Китая;

3) выделить инвариантные и вариативные субфреймы ситуационного фрейма AI-ENABLED FRAUD, представленные в образцах медиадискурса указанных стран;

4) определить максимальные и минимальные количественные показатели употребления в отдельно взятом тексте лексических единиц, объективирующих субфреймы и слоты ситуационного фрейма AI-ENABLED FRAUD;

5) определить факторы, влияющие на направление фреймирования ситуации AI-ENABLED FRAUD в образцах медиадискурса указанных стран; установить роль жанрово обусловленных, интенциональных и лингвокультурных факторов, влияющих на особенности моделирования ситуации AI-ENABLED FRAUD в медиадискурсе указанных стран;

6) сопоставить репертуар лексических единиц, объективизирующих слоты инвариантных (облигаторных) субфреймов в образцах медиадискурса указанных стран.

Материалом для исследования послужили публикации электронных версий англоязычных изданий NBC, CNN, Bloomberg (США), Financial Times, The Mirror, The Guardian, The Independent, Reuters (Великобритания), CBC, The National Post (Канада), The Straits Times (Сингапур), Sixth Tone, China Daily, Yicai Global (Китай), ABC (Australian Broadcasting Corporation), The Sydney Morning Herald (Австралия) за 2023-2025 гг.

Теоретическую базу исследования составляют работы, посвященные теории когнитивно-дискурсивного миромоделирования (Кушнерук, 2018), фреймированию ситуации в СМИ (Резанова, Степаненко, 2023); лонгитюдные когнитивно-сопоставительные исследования медиафреймов и сетевых фреймов (Имамгаязова, 2023a; 2023b; Девятияров, 2024); когнитивные и сопоставительно-когнитивные исследования профессионального дискурса и медиадискурса с применением количественных методов анализа (Ампикян, 2023, Вдовиченко, Каменева, 2025); сопоставительно-когнитивные исследования дискурса криминальных сводок с применением количественных методов анализа (Мельникова, 2016; 2017; Ильинова, Волкова, 2016; Бокова, 2011).

Выбор методов исследования обусловлен целью и совокупностью поставленных задач. Описательно-аналитический метод использовался для создания классификации инвариантных и вариативных элементов фреймовой структуры; метод фреймового анализа – для создания фреймовой модели ментального пространства медиадискурса, посвященного проблеме ИИ-мошенничества; дискурс-анализ – для определения роли экстралингвистического контекста в выборе актуализируемых элементов фреймовой структуры; сравнительно-сопоставительный метод – для выявления сходств и различий, демонстрируемых дискурсивными вариантами медиафрейма; интент-анализ – для определения факторов, обусловливающих направление фреймирования, включая коммуникативные стратегии и тактики; количественный метод – для определения минимального и максимального показателей актуализации субфреймов/слотов в тексте; а также при исследовании вариативности в использовании лексических средств объективации последних. Отбор материала осуществлялся методом сплошной выборки из публикаций англоязычных изданий вышеуказанных шести стран за 2023-2025 гг.

Практическая значимость исследования состоит в возможности использования его материалов в практике преподавания дискурсологии, медиалингвистики, медиадискурсологии, юрлингвистики, при разработке и чтении теоретических и практических курсов, посвященных вопросам межкультурной коммуникации, лингвокультурологии. Представленный в статье лексический материал может использоваться при составлении словарей.

Обсуждение и результаты

Одним из основных понятий, используемых при описании способов представления знаний, является фрейм, или структура данных для репрезентации стереотипной ситуации. «Верхние уровни» фрейма образованы понятиями, которые всегда справедливы по отношению к предполагаемой ситуации. Нижние уровни фрейма содержат вершины-терминалы, заполняемые характерными данными; терминалы могут входить в состав нескольких фреймов системы. В данном исследовании мы используем структуру фрейма, иерархические уровни которой заполнены субфреймами, или фреймами следующего по рангу уровня, и слотами – категориями более низкого порядка (Минский, 1979, с. 7; Салькова, 2025, с. 1640). Слоты «членят субфреймы по тематическому признаку и несут основную концептуальную и содержательную нагрузку фрейма» (Девятияров, 2024, с. 53). Фреймовое моделирование, или моделирование фреймовой структуры, состоит в поэтапном выделении терминальных узлов на разных уровнях иерархической структуры фрейма и рассмотрении

вариантов их заполнения (Имамгаязова, 2023a, с. 5; Кононова, Кульчицкая, 2022, с. 178-179). Фреймирование понимается как «принцип отбора, выделения и представления информации либо как способ написания или создания сообщения, а также как инструмент, используя который СМИ «“упаковывают” информацию для аудитории» (Асмус, Журкова, Ковальчук, 2021, с. 60).

Согласно теории когнитивно-дискурсивного миромоделирования, развиваемой С. Л. Кушнерук (2018) на основе положений трудов Т. А. ван Дейка, Дж. Лакоффа, Ч. Дж. Филлмора, Н. Н. Болдырева, В. З. Демьянкова и описывающей влияние когнитивных и коммуникативных факторов на дискурсивную картину мира, структурирование информации в дискурсе соответствует социально-конструкционистским трактовкам дискурса и представлениям о проективности дискурса как носителя преобразованных агентом ментальных представлений, порождающих прагматически-релевантные «версии» фрагмента действительности. Модели действительности, зависящие от способа структурирования и представления информации, порождают ментальные репрезентации или репрезентационные структуры, чьи макроструктуры основаны на упорядочивающих знания о некотором фрагменте действительности макрофреймах, состоящих из фреймов и слотов. Репрезентационные структуры влияют на восприятие, оценки и убеждения адресата в соответствии с интересами политических субъектов и элит, которые тем самым актуализируют идеологически востребованные интенционально-детерминированные смыслы и ценностные установки (Кушнерук, 2018, с. 117-120).

Объектом исследований, сопоставляющих различные способы фреймирования некоторой ситуации в СМИ, являются дискурсивно обусловленные варианты интерпретации ситуации, или ситуационные фреймы – более детализированные дискурсивные варианты ее инвариантного фрейма. Методика, примененная З. И. Резановой и А. А. Степаненко (2023) для выявления дискурсивно обусловленной вариативности фреймирования одной и той же ситуации в разных видах СМИ (на примере фреймового моделирования ситуации пандемии COVID-19), основана на анализе пропозитивных струкур. На первом этапе моделируется обобщенная фреймовая модель посредством семантического анализа репрезентирующих его лексем; на последующих этапах – на основе ядерной пропозиции выстраивается ряд пропозитивных струкур, отражающих разные аспекты явления. При этом приспособление фрейма к конкретной ситуации осуществляется через несколько уровней конкретизации основных предикатов с введением новых субфреймов – субфреймы каждого уровня конкретизации отражают новые аспекты данного явления. Затем сопоставляются направления конкретизации узлов базового фрейма в ситуативных моделях медиатекстов разных видов СМИ, в результате чего между разными способами фреймирования ситуации устанавливаются различия в тематических фокусировках, связанных с узлами разных уровней фреймовой структуры, а также в частотности актуализации субфреймов, спектре конкретизаций и лексической репрезентации субфреймов (Резанова, Степаненко, 2023, с. 7-11).

Основные положения методики, примененной Д. В. Девятияровым в лонгитюдном когнитивно-сопоставительном исследовании сетевых вариантов фреймов в разноязычных СМИ, включают моделирование фрейма на основе инвариантных моделей фреймов, представленных в электронной библиотеке FrameNet университета Беркли (https://framenet.icsi.berkeley.edu/), и сопоставление текстов по следующим параметрам: 1) состав тематических групп наиболее распространенных сетевых фреймов и факторы актуализации фреймов; 2) состав субфреймов и слотов ближней, средней и дальней зоны периферии фрейма; 3) характер изменений во фреймовой структуре (появление или исчезновение субфреймов, перемещение субфреймов между зонами периферии фрейма); 4) диапазон, концентрация и частотность ключевых лексических единиц, объективирующих фреймы; 5) содержательная динамика (изменение содержательного наполнения слотов). Результаты исследования показали, что сопоставляемые тексты могут отличаться набором актуализированных в них фреймов и слотов, изменением количества фреймов периферии, содержанием слотов и как следствие – «смещением акцентов», концентрацией лексических единиц в определенных фреймах и субфреймах (Девятияров, 2024, с. 65-66, 68, 70, 72,74, 76-77, 81-83, 88).

Применение количественного метода в когнитивно-сопоставительных исследованиях медиафреймов Д. В. Девятиярова и Д. И. Имамгаязовой позволило путем анализа концентрации объективирующих фреймы и субфреймы лексических единиц определить наиболее частотные фреймы, инвариантные и вариативные субфреймы; также фиксировать количество актуализуемых слотов (Девятияров, 2024, с. 66, 68, 70, 127). Показатель частотности актуализации слотов важен для выявления лингвокультурных особенностей дискурса (Имамгаязова, 2023b, с. 7, 95).

Применение количественного метода при проведении сопоставительного лингвокультуроведческого исследования способов фреймирования информации в профессиональном педагогическом дискурсе, выполненного А. Г. Ампикян (2023, с. 5, 7) на материале русского и французского языков, помогло установить различия в числе актуализируемых макрофреймов, микрофреймов и слотов, отражающие специфику репрезентации ситуации в данных лингвокультурах.

Медиамоделирование криминального события зависит от когнитивно-дискурсивных факторов и демонстрирует вариабельность, необходимую для осуществления воздействия на адресата через информирование и интерпретацию события; когнитивная структура новостных сообщений и криминальных сводок реализуется в форме различных ее вариантов (Мельникова, 2017, с. 128; Ильинова, Волкова, 2016, с. 88-89, 94).

Согласно результатам исследования Е. А. Мельниковой (2017, с. 127-128), когнитивно-семантическая модель медиарепрезентации преступления (Robbery) включает каузатора-деструктора (criminal), каузата (victim), посредника-протектора (police), хронотоп; а также процессуальные конституенты (to injure a victim, to plead (smb) guilty). Е. Ю. Ильинова и О. С. Волкова (2016, с. 89) отмечают, что когнитивно-дискурсивное

моделирование правонарушения в новостном дискурсе СМИ требует не только указания действия, деятеля, пространственно-временной локализации события и его участников, но и внешнего наблюдателя, результата и причины произошедшего.

О. В. Бокова (2011, с. 13-15) в сопоставительном исследовании «Малоформатный текст “сообщение о преступлении”: особенности его семантической и структурной организации», выполненном на немецкоязычном материале, использует термин «макрокомпоненты текста» и выделяет в криминальных сводках следующее: «описание преступления», «последствия преступления», «расследование», «показания потерпевших», «преступники», «похищенное имущество», «мнение экспертов», «рекомендации полиции», «призыв помочь следствию». В исследовании установлено минимальное и максимальное количество актуализируемых в образцах этого жанра макрокомпонентов и объективные факторы, влияющие на этот показатель (например, характер преступления и хода следствия).

Особенности когнитивно-дискурсивного конструирования и медиарепрезентации криминальных происшествий в англоязычных электронных СМИ определяются социальной значимостью событий и связаны с применением лингвостратегических приемов, особых стратегий, соответствующих прагматическим задачам новостной журналистики, которые определяют дискурсивные тактики представления криминальных происшествий, включая точность, достоверность, аттрактивность и фокусность; кроме того, они зависят от композиционной практики, применяемой при создании текстов этого жанра (Мельникова, 2016, с. 3; 2017, с. 126-127).

Лингвокультурные и социокультурные факторы влияют на содержательные и структурные параметры текстов «сообщение о преступлении» в СМИ Австрии, Германии или Швейцарии, что проявляется в характере дополнительной информации и в частотности примеров с добавлением в структуру текста сообщения тех или иных информационных блоков (Бокова, 2011, с. 12-13).

Структура медиафрейма AI-ENABLED FRAUD

В настоящем исследовании мы исходим из трактовки медиадискурса как сферы, где происходит «когнитивно-синергетическая обработка событийной, социокультурной, коммуникативно-прагматической и языковой информации» (Alefirenko, 2016).

Анализ англоязычных юридических текстов, посвященных проблеме использования технологии AI в противоправных целях, позволил выделить следующие ключевые элементы их категориально-понятийного аппарата: *generative AI technology / технология генеративного ИИ, developer / разработчик, user / пользователь, Dark AI, illicit markets / подпольные рынки, deepfakes / дипфейки, AI crime / преступление, совершенное посредством использования ИИ, rise in these attacks / рост числа кибератак, criminals / преступники, victims / потерпевшие, methods / методы, sensitive information / конфиденциальная информация, detection / распознавание фейков, criminal justice system / система уголовного правосудия* (см. *AI crime…*; *Criminals Use Generative…*) (здесь и далее перевод автора статьи. – *И. Ф.*). Данные элементы и анализ пропозитивных структур послужили основой для разработки фреймовой модели ситуации.

Затем на основе материалов выборки объемом 468 лексических единиц из образцов медиадискурса США, Великобритании, Канады, Австралии, Сингапура и Китая за период с 2023 по 2025 г. построена ситуационная модель AI-ENABLED FRAUD. Ее иерархическая структура содержит фреймы, субфреймы, слоты и подслоты. Большинство инвариантных и вариативных субфреймов и слотов – помимо входящих во фрейм глаголов, которые не рассматриваются в данном исследовании, – относятся к основным фреймам, а именно: ПРЕСТУПЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИИ и ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ДЛЯ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ; концепты «преступление» и «технологии» являются опорными концептами, вокруг которых развертывается содержание дискурса (Демьянков, 2002, с. 31).

Фрейм ПРЕСТУПЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИИ

На первом этапе моделирования фрейма ПРЕСТУПЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИИ (ИИ-МОШЕННИЧЕСТВО) выделены его инвариантные субфреймы: **Правонарушители**, **Потерпевшие**, **Предмет преступления** (центральная цель, предварительная цель и пост-цель по терминологии И. В. Смирновой (2025), напр., *collecting **money** in high-tech deception*), **Материальный ущерб, Виды преступлений**, **Противодействие со стороны экспертного сообщества, Масштаб использования мошеннических схем с применением ИИ**.

К вариативным субфреймам относятся **Причина распространения ИИ-мошенничества** и **Возможность распознания ИИ-мошенничества** (*the majority of Canadians still believe themselves **capable of detecting** illicit AI-powered schemes / большинство канадцев по-прежнему уверены, что **способны распознать** преступные схемы на основе технологии ИИ*).

На втором этапе моделирования данного фрейма выделены слоты, входящие в состав вышеуказанных субфреймов:

– слоты, реализующие субфрейм **Виды преступлений**, приведены в Таблице 2;

– слоты, реализующие субфрейм **Правонарушители**, включают: Bad actors / Злоумышленник, Call-centre / Кол-центр, Criminals / Преступники, Cyber-attackers / Киберпреступники, Fraudsters / Мошенники, Offenders / Правонарушители, Perpetrators / Преступники, Scam centres / Мошеннические кол-центры;

– слоты, реализующие субфрейм **Потерпевшие**, включают: Customers / Клиенты, the Elderly, Older people, Senior citizens / Пожилые люди, Grandparents / Бабушки и дедушки, Fraud victim, Scam victim, Scam target /

Жертва мошенников, Recipients / Получатели, Target, Victim / жертва, Victim companies / Компании, ставшие жертвами мошенников, Trafficked victims / Жертвы торговли людьми;

– слоты, реализующие субфрейм **Предмет преступления**, включают: Consumer details / Персональные данные клиента, Personal details / Персональные данные, Money / Деньги, Personally identifiable information / Персональные данные, Savings / Сбережения, Sensitive information / Конфиденциальная информация;

– слоты, реализующие субфрейм **Материальный ущерб**, включают: Losses / Ущерб, Average loss / Средний показатель ущерба, Globe and total losses / Ущерб в общемировом масштабе, Overall losses / Общий ущерб;

– слоты, реализующие субфрейм **Противодействие со стороны экспертного сообщества**, включают: Fraud detection and prevention / Выявление и предотвращение мошенничества и Efforts to clamp down on Cracked / Попытки "взяться" за взломанные чат-боты.

Вариативные субфреймы

Выделены слоты, реализующие вариативные субфреймы:

– субфрейм **Преследование** реализуется слотами Заявление; Дело; Предполагаемые преступники *(suspects)*; Обвиняемый *(accused, defendants)*; Обвинение *(charged with scamming 400 Grandparents / обвинен в мошенничестве в отношении 400 бабушек и дедушек)*; Наказание *(punishable by up to 20 years in prison / наказывается лишением свободы на срок до 20 лет)*;

– субфрейм **Причина распространения ИИ-мошенничества** представлен слотами Массовый характер кибератак с использованием ИИ (*AI lowers the barrier to entry for sophisticated cybercrime operations / ИИ упрощает осуществление изощренных кибер-операций*) и Продажа оборудования для ИИ;

– субфрейм **Последствия использования ИИ криминальными кругами** реализуется словосочетанием *Cyber-security concerns / Проблемы кибербезопасности*;

– субфрейм **Состав преступления** представлен слотами, конкретизирующими: 1) подготовку преступления (*collected information about … the grandchildren, manufactured scenarios like needing bail money / собирали информацию о… внуках, придумывали сценарии с необходимостью дать деньги для уплаты залога*); 2) цели использования ИИ правонарушителями (помимо предмета преступления, напр., *to automate an 'unprecedented' cybercrime spree / поставить киберпреступления на поток*); 3) Источник образцов видео/голоса (напр. *publicly available footage / имеющийся в открытом доступе видеоматериал*); 4) Манипуляции (Угрозы); 5) Счет; 6) Транзакции; 7) Период совершения преступления;

– вариативный субфрейм **Нематериальный ущерб** реализуется слотами Косвенный ущерб *(Our business operations were not affected / Это не отразилось на наших бизнес-процессах)* и Эмоциональный ущерб *(lost their sense of safety, judgment and trust / потеряли чувство защищенности, доверие [к людям] и усомнились в своем здравомыслии)*;

– вариативный субфрейм **Оценка** реализуется слотами Моральная оценка *(the nefarious uses it can be put to / гнусные цели, в которых она [deepfake technology] может быть использована)* и Отличие преступлений с использованием ИИ от традиционных преступлений *(intelligent decision-making agents may violate some basic principles preset by humans / ИИ-агенты могут нарушать основные морально-этические нормы, присущие всем людям)*.

На третьем этапе выделяем подслоты:

– подслот **Эффективность мошеннических схем** (social engineering scams with alarming success rates / опасные мошеннические схемы с использованием методов социальной инженерии; the success rate of phishing messages / доля успешных фишинговых атак) конкретизирует слоты Scams / Мошенничество и Phishing messages / Фишинговые письма (субфрейм Виды преступлений);

– подслоты, конкретизирующие слоты субфрейма **Правонарушители**, включают следующее:

1) организованное преступное сообщество*:* Criminal syndicates / Преступные синдикаты; Criminal group / Преступные группы, Fraud gangs / Банды мошенников, Gangs / Банды, Global empire / Глобальная империя, International criminal enterprise / Транснациональная организованная преступная группа, Organized call centers / Кол-центры, Organised criminal gangs / Организованные преступные группы, Organised crime network / Организованная преступная группа;

2) взаимодействие в преступном сообществе (*scammers operate **as a business model** / мошенники используют **бизнес-модель***);

3) роли членов преступного сообщества: Bosses / Боссы, Compound managers / Менеджеры кол-центров, Computer engineer / Инженер по вычислительной технике, Hacker / Хакер, Identity thief / Преступники, похищающие персональные данные, Face-swapping scammer / Мошенники, использующие метод замены лица на фото и видео, Fake vendors / Фейковые поставщики, Identity fraudsters / Мошенники, использующие чужие персональные данные, "Keyboarders" / «Клавишники», Models / Модели, Pig butchering keyboarders, Pig butchering scammers / Мошенники, использующие схему «Забой свиней», Trafficked workers / Работники, ставшие жертвой торговли людьми.

4) доходы преступного сообщества (*a **$100 million** dollar industry / индустрия с оборотом в **100 млн** долларов*);

5) условия работы в кол-центрах (*slave-like conditions/рабские условия труда*);

6) наказания сотрудников кол-центров (*tasered or beaten / к ним применяют воздействие электрошокером или побои*);

7) криминогенные факторы (*economic uncertainty and cost-of-living pressures / экономическая нестабильность и высокая стоимость жизни*).

Слот Персональные данные в составе субфрейма **Предмет преступления** конкретизируется подслотами Accounts / Счета, Bank details / Банковские реквизиты, Personal bank accounts / Личные банковские счета, Social Security numbers / Номера социального страхования; а слот Конфиденциальная информация – подслотами Sensitive defense information / Военные тайны, Sensitive medical information / Конфиденциальная медицинская информация и Trade secrets / Коммерческая тайна.

В субфрейме **Масштаб использования мошеннических схем с применением ИИ** выделены подслоты Количество преступлений; Наиболее распространенные преступления с использованием ИИ (*Identity theft remained the most prevalent type of fraud / Кража персональных данных оставалась наиболее распространенным видом мошенничества*); Доля преступлений с использованием ИИ в общем количестве преступлений; Доля случаев мошенничества с использованием ИИ в общем количестве случаев мошенничества; Причины роста числа преступлений с использованием ИИ (*The cost and availability of the technology / Стоимость и доступность технологии*); Количество зарегистрированных в базе случаев; Количество случаев в год.

В субфрейме **Противодействие со стороны экспертного сообщества** подслоты конкретизируют Технические средства предотвращения ИИ-мошенничества (Guardrails / Механизмы контроля, AI detection systems / Системы обнаружения контента, сгенерированного ИИ, AI-powered tools to detect anomalies / Детекторы аномалий ИИ, Multiple layers of defense / Многоуровневая защита, Safeguards against the potential misuse of AI / Средства блокировки создания противоправного контента, Security systems / Системы безопасности, Systems for detecting AI crimes / Системы обнаружения преступлений, совершаемых с использованием ИИ, Training and tools to combat cyber crime / Обучение и инструменты для борьбы с киберпреступностью); Ресурсы, необходимые для предотвращения преступлений с использованием ИИ (*a huge multi-sector, collaborative effort / многосекторальное взаимодействие*); Компании, противодействующие *ИИ*-мошенничеству (Cybersecurity company / ИБ-компания, Cyber-security sector / Сектор кибербезопасности, Identity verification firms / Компании, проводящие верификацию персональных данных); Эффективность организации, противодействующей совершению преступлений с использованием ИИ (*its members managed to prevent £1.8billion worth of fraud losses / ее сотрудники смогли предотвратить потери на сумму в 1,8 млрд фунтов*); Использование ИИ в сфере кибербезопасности (*using AI for cyber security / использование ИИ в сфере кибербезопасности*); Предостережение экспертов (*an ACCC spokesperson warned of the emergence of new technologies / представитель ACCC предупредил о появлении новых технологий*); Рекомендации по защите от ИИ-мошенничества (*multi-factor authentication / многофакторная аутентификация*); Регулирование ИИ (*adapting laws and regulations to the development and application of AI technologies / принятие законов и нормативных актов, регулирующих разработку и применение технологий ИИ)*; Последствия регулирования ИИ (*it's important not to bring in regulation that makes it so heavy-handed that all AI development moves overseas / важно, чтобы внедряемое регулирование не было слишком жестким и не заставило всех ИИ-разработчиков покинуть страну*).

Фрейм ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ В МОШЕННИЧЕСКИХ ОПЕРАЦИЯХ

На первом этапе был выделен инвариантный субфрейм данного фрейма – ***Технологии*, каналы связи, методы и тактики**, что соответствует особенностям преступлений, осуществляемых с помощью технологии ИИ (ср. с описанием факультативных слотов структуры субфрейма «Киберпреступность», представленным в диссертационном исследовании Д. И. Имамгаязовой (2023b, с. 131)). Лексические единицы, объективирующие указанный субфрейм, включая модели ИИ, технологии, продукты и процессы на основе ИИ, каналы связи, инструменты поиска информации, методы социальной инженерии и др., приведены в Таблице 1.

На втором этапе выделены слоты, конкретизирующие указанный субфрейм: 1. **Возможности ИИ** (напр., *to evade and fool AI detection systems / обходить и обманывать системы обнаружения ИИ*). 2. **Усовершенствование технологий на основе ИИ, используемых для совершения преступления** (напр., *Live face-swapping technology and its online transmission have improved dramatically / Технология замены лица в режиме реального времени и качество передачи его изображения значительно улучшились*). 3. **Роль ИИ в повышении эффективности мошеннических схем** (*AI will make it harder to detect / ИИ затруднит распознавание [мошеннических схем]*). 4) **Подпольный рынок ИИ** (*underground market for rogue AI / подпольный рынок мошеннического ИИ*) и **Сфера распространения вредоносного ИИ** (*Underground forums / Подпольные форумы, the Dark Web / Даркнет*); **Субъекты** (*Users / Пользователи*; *Developers / Разработчики*; *Providers / Провайдеры*).

Регулярную актуализацию в образцах медиадискурса указанных стран субфреймов и слотов **Виды преступлений**, **Предмет преступления, Возможности ИИ, Усовершенствование технологий на основе ИИ, используемых для совершения преступления,** мы объясняем реализацией коммуникативных стратегий информирования и предупреждения (Дзялошинский, 2013, с. 230).

Кроме того, наблюдается регулярная конкретизация на уровне субфрейма **Противодействие со стороны экспертного сообщества**, она проявляется в актуализации слотов «Организация, противодействующая совершению преступлений с использованием ИИ» (*Canadian Anti-Fraud Centre / Канадский центр по борьбе с мошенничеством*), «Эксперт» (*Jonathan Anderson, associate professor and cybersecurity expert at Memorial University / Джонатан Андерсон, доцент и эксперт по кибербезопасности в Мемориальном университете*), «Доклад» (*Microsoft's latest Cyber Signals report / новый отчет Cyber Signals Компании Майкрософт*), «Исследование» (*A 2024 survey by Regula Forensics / Отчет за 2024 г. компании Regula Forensics*), «Полиция» (*Sgt. Kevin Talbot of the Lethbridge Police Service in southern Alberta / Кевин Талбот, сержант полиции из Летбриджа, Южная*

Альберта). Данную особенность фреймирования ситуации можно считать признаком реализации дискурсивных практик конструирования достоверности (Никонова, 2022, с. 71) и одной из составляющих формализованной, институционально маркированной дискурсивной практики (Ермоленкина, 2022, с. 21).

Сопоставление образцов медиадискурса показывает вариативность в количестве актуализированных в отдельно взятом тексте субфреймов и слотов. Так, анализ 21 публикации объемом от 315 до 4298 слов продемонстрировал, что минимальный показатель равен 12, максимальный – 24. Самые высокие показатели составляют 23 и 24 единицы; они представлены в публикации китайского издания China Daily за 2025 г. *Vietnamese authorities warn of rising AI-driven deepfake extortion rackets* объемом 744 слова (https://www.chinadaily.com.cn/a/202504/10/WS67f73651a3104d9fd381e8ed.html) и в публикации австралийской корпорации ABC за 2024 г. *How South-East Asia's pig butchering scammers are using artificial intelligence technology* объемом 2436 слов (https://www.abc.net.au/news/2024-05-16/pig-butchering-scams-artificial-intelligence-ai-face-swapping-/103804830).

Актуализация широкого спектра вариативных субфреймов и слотов в образцах медиадискурса сингапурских изданий позволяет более подробно охарактеризовать данное явление действительности и не связано с параметрами индивидуальных ситуаций. Например, в публикации газеты *The Straits Times* за 2024 г. *Growing underground market for rogue AI sparks cyber-security concerns* (https://www.straitstimes.com/singapore/growing-underground-market-for-rogue-ai-sparks-cyber-security-concerns?ref=more-on-this-topic) актуализируются вариативные субфреймы и слоты **Пользователи ИИ, Разработчики, Подпольный рынок ИИ**, **Сфера распространения ИИ, генерирующего scam-контент** (*Underground forums, the Dark Web, The Telegram channel promoting WormGPT*), **Риски и последствия преступного использования ИИ**, **Доля мошенничеств с использованием ИИ в общем количестве случаев мошенничества, ИИ в противодействии ИИ** *(challenges in using AI for cyber security / сложности в использовании ИИ в целях кибербезопасности)*. Кроме того, конкретизация на уровне субфрейма **Цели использования ИИ правонарушителями** осуществляется посредством 18 слотов; приведем лишь несколько примеров: *to gather critical information about software to find vulnerabilities in companies' systems / собирать критически важную информацию о программном обеспечении для поиска уязвимостей в системах компаний*; *to study technical protocols for military-related equipment such as radars and satellites / изучать технические протоколы для военного оборудования, например радаров и спутников*; *to bypass biometric authentication / обходить биометрическую аутентификацию* и др. Подобная детализация избыточна в контексте реализации коммуникативной интенции информирования аудитории в целях предупреждения преступности. В сочетании с фактом наличия в примерах терминов и терминологических словосочетаний все это позволяет сделать вывод о гибридизации данного дискурса, заключающейся в добавлении образовательной составляющей – дискурс-периферии, связанной с научно-техническим дискурсом (Шермазанова, 2025, с. 126).

В публикации британского таблоида *The Mirror* за 2024 год *Criminals are using AI and deepfake technology to steal consumer details* (https://www.mirror.co.uk/money/criminals-using-ai-deepfake-technology-32595761) объемом 423 слова актуализировано 22 субфрейма и слота. Они включают следующее: **Правонарушитель, Потерпевший, Виды преступлений**, **Технологии, используемые в мошеннических схемах, Предмет преступления**, **Эффективность мошеннических схем**. Кроме того, конкретизация на уровне субфрейма **Масштаб использования мошеннических схем с применением ИИ** достигается актуализацией четырех слотов, включая Количество зарегистрированных в базе случаев, Количество случаев в году, Наиболее распространенные преступления с использованием ИИ, Криминогенные факторы. Конкретизация на уровне субфрейма **Противодействие ИИ-мошенничеству** выражена через актуализацию 9 слотов: Способы предотвращения ИИ-мошенничества, Ресурсы, необходимые для предотвращения преступлений с использованием ИИ, Предостережение экспертов, Организация, противодействующая совершению преступлений с использованием ИИ, Руководитель организации, Количество сотрудников в указанной организации, Эффективность данной организации, Доклад, Профилактика преступлений среди молодежи. Подобную детализацию на уровне инвариантных и вариативных субфреймов мы связываем с особенностями медиарепрезентации правонарушений в британских СМИ, которые отвечают достоверному и точному представлению события, в чем проявляется реализация фактологической стратегии информирования и документирования (Мельникова, 2017, с. 126-127, 129).

Аналогичный пример мы наблюдаем в публикации NBC за 2025 г. *'Cold-hearted' scammers targeted hundreds by posing as grandkids in distress, prosecutors say* (https://www.nbcnews.com/news/us-news/cold-hearted-scammers-targeted-hundreds-posing-grandkids-distress-pros-rcna224561), где конкретизация проявляется в добавлении количественной, локальной, темпоральной и демографической информации на уровне субфреймов и слотов, преимущественно относящихся к фрейму ПРЕСТУПЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИИ: **Правонарушители** *(13 defendants / 13 обвиняемых);* **Потерпевшие** (*400 grandparents in five states / 400 бабушек и дедушек в пяти штатах*; *the average age of the victims was 84 / средний возраст жертв составил 84 года*); Полиция *(federal prosecutors in Boston / федеральные обвинители в Бостоне*); Дело (***the first*** *publicly documented instance in which a hacker used a leading AI company's chatbot / первый официально задокументированный случай использования хакером чат-бота ведущей AI-компании*); Период совершения преступления (*the campaign appeared to happen over the span of* ***three months*** */ кампания… осуществлялась в течение трех месяцев*).

Лексическое заполнение слотов инвариантных субфреймов

В сопоставляемых образцах медиадискурса шести стран наблюдается заметная концентрация лексических единиц, вербализирующих слоты субфрейма **Технологии, каналы связи, методы и тактики** (Таблица 1);

эти слоты объективируют виды технологий, систем, каналов связи, методов и тактик и пр., используемых в мошеннических операциях. Из 77 зафиксированных нами лексических единиц в образцах медиадискурса Великобритании представлено 23; Австралии – 22; Сингапура – 22; Китая – 20; Канады – 18; США – 8.

Таблица 1. *Лексическое заполнение субфрейма* ***Технологии, каналы связи, методы и тактики***

	Велико-британия	США	Австралия	Канада	Сингапур	Китай
1. AI chatbots / чат-боты с искусственным интеллектом	+	+				
2. AI deepfakes / дипфейки, созданные с помощью ИИ				+		+
3. AI-generated spam content / спам-контент, сгенерированный ИИ					+	
4. AI-mimicked voices / голоса, имитированные ИИ				+		+
5. AI technology / технология ИИ			+			+
6. AI models / модели ИИ			+			
7. AI systems / системы ИИ					+	
8. AI platform / платформа ИИ				+		+
9. AI tools / инструменты ИИ		+	+		+	
10. AI-assisted translation integrated with messaging services / перевод с помощью ИИ, интегрированный со службами обмена сообщениями			+			
11. AI-powered password generators / генераторы паролей на основе ИИ					+	
12. Anthropic's Claude / Claude chatbot / Нейросеть Claude AI	+	+				
13. Automation / автоматизация			+			
14. Bots / боты	+		+			
15. Chatbots / чат-боты	+	+	+		+	
16. Chatbots on social media sites / чат-боты на сайтах социальных сетей			+			
17. Computer-generated images and voices / сгенерированные компьютером изображения и голоса			+			
18. Dark web / Даркнет				+		+
19. Data harvesting techniques / методы сбора данных	+					
20. Dating app / приложение для знакомств	+					
21. Deepfake images, videos, photos, and audio, deep fakes, deepfaked images of celebrities / изображения, видео, фото и звуки, изображения знаменитостей, сгенерированные ИИ	+			+	+	+
22. Deepfake technology / технология deepfake	+		+			
23. Deepfake voice call / голосовой вызов с использованием генератора голоса	+					
24. Deepseek / нейросеть deepseek	+					
25. Email (charity), phishing e-mails /некоммерческие письма, фишинговые письма	+	+			+	+
26. Encrypted messaging platform Telegram / платформа шифрованных сообщений Telegram			+			
27. Face-swapping software / ПО для замены лица на видео и фото			+			
28. Face-swopping apps / приложения для замены лица на видео и фото					+	
29. Facial replica / копия лица	+					
30. Fake social media accounts / поддельные аккаунты в социальных сетях					+	
31. Generative AI / generative artificial intelligence (AI) tools / генеративный ИИ / инструменты генеративного искусственного интеллекта	+				+	
32. Generative AI chatbots / чат-бот с генеративным ИИ			+			
33. Google's Gemini / инновационные языковые модели Gemini от компании Google	+					
34. Google searches / поисковые запросы Google				+		+
35. GPT, FraudGPT				+	+	+
36. Grok	+					
37. Job advertisements / объявления о вакансиях					+	
38. Impersonation services / олицетворение					+	
39. Internet				+		+
40. Large language model-based chatbots / чат-боты на основе больших языковых моделей			+			
41. Links / ссылки	+					
42. Live deepfakes / дипфейки в реальном времени	+					
43. live face-swapping technology / технология замены лиц в реальном времени	+					
44. LLM / большая языковая модель			+			
45. Malware / вредоносный код	+					
46. Messages /сообщения	+					
47. Messaging platforms / платформа для обмена сообщениями	+					
48. Meta's Meta AI / ИИ –помощник от компании Meta	+					
49. Modified versions of chatgpt / модифицированные версии chatgpt					+	
50. Modified versions of openai's chatbot / модифицированные версии чат-бота openai					+	
51. Online ad / Онлайн-реклама					+	
52. Online investment opportunities/мошеннические инвестиционные сайты				+		
53. PassGAN					+	
54. OpenAI's ChatGPT	+					
55. Phone calls / телефонные звонки		+		+	+	+
56. Real-time AI-generated videoconference / видеоконференция, созданная с помощью ИИ в реальном времени					+	
57. Real-time deepfake face-swapping system / система замены лиц с помощью дипфейков в реальном времени			+			
58. Real-time face-swap technology / технология замены лиц в реальном времени			+			
59. Scam content / мошеннический контент					+	

	Велико-британия	США	Австралия	Канада	Сингапур	Китай
60. Social engineering tactics / тактики социальной инженерии	+					
61. Social media / социальные сети			+			+
62. Social media ad / реклама в социальных сетях				+		+
63. Software (malicious~) / ПО вредоносное~)	+	+		+		+
64. Spoof voice / имитация голоса	+					
65. Text messages / текстовые сообщения		+	+			
66. *Video call*, video conference / видеозвонок, видеоконференция	+			+		+
67. Virtual assistant / виртуальный помощник					+	
68. Virtual reality / виртуальная реальность				+		+
69. Voice changing devices, voice changing technology, AI voice-changing software, Voice changing AI / Устройства для изменения голоса / технологии для изменения голоса / ПО на основе ИИ для изменения голоса	+			+		+
70. Voice cloning / клонирование голоса	+		+	+		+
71. Voice deepfake technology / технологии клонирования голоса	+					
72. Voicemails / голосовая почта				+		+
73. Website (fraudulent ~) / мошеннический веб-сайт				+		+
74. Whatsapp			+			
75. Whatsapp voice spoofing / имитация голоса в сообщениях whatsapp	+					
76. Wormgpt					+	
77. xAI	+		+			

Слоты субфрейма **Виды преступлений** (Таблица 2) вербализуются 70 лексическими единицами, из них в образцах медиадискурса Великобритании представлено 26; Канады – 20; Сингапура – 17; Китая – 17; США – 12; Австралии –10.

Таблица 2. *Лексические средства объективации слотов субфрейма* ***Виды преступлений***

	Велико-британия	США	Австралия	Канада	Сингапур	Китай
1. AI cybercriminal operation / кибероперация с использованием ИИ		+				
2. AI deepfake frauds / мошенничество с использованием дипфейков, созданных с помощью ИИ						+
3. AI-driven deepfake extortion rackets / рэкет с использованием дипфейков, созданных ИИ						+
4. AI-driven fraud / мошенничество с использованием ИИ						+
5. AI-enabled identity fraud / хищение личных данных с использованием ИИ	+					
6. AI Fraud / ИИ-мошенничество						+
7. AI-generated fraud / ИИ-мошенничество	+					
8. AI-powered fraud / ИИ-мошенничество						+
9. AI-related crimes / преступления, совершаемые с помощью ИИ						+
10. Catfishing /создание фальшивых аккаунтов			+			
11. CRA-related scams / аферы, связанные с уплатой налогов				+		
12. Cryptocurrency fraud / мошенничество с криптовалютой				+		
13. Cryptocurrency pig butchering / мошенничество с инвестициями в криптовалюте			+			
14. Cyber attacks / кибератаки					+	+
15. Cybercrime / киберпреступность	+	+				+
16. Cybercrime operations / киберпреступные операции		+				
17. Cyber-enabled fraud / мошенничество с использованием кибер-технологий					+	
18. Cyber extortion / вымогательство в сети Интернет		+				
19. Cyber fraud / кибермошенничество			+			
20. Cyberscams / кибермошенничество			+			
21. Deepfake fraud / мошенничество с применением технологии дипфейк	+				+	
22. Deepfake scams / мошенничество с применением технологии дипфейк	+			+	+	+
23. Extortion scams / мошенничество с вымогательством	+					
24. “Face-swapping” scams / мошенничество с заменой лица						+
25. Fake investment schemes / мошеннические инвестиционные схемы			+			
26. Fraud / мошенничество	+					+
27. Fraud (AI-generated~) / ИИ-мошенничество	+					
28. Fraud schemes / мошеннические схемы		+		+	+	
29. Frauds (AI-augmented~) / ИИ-мошенничество				+		
30. Fraudulent activities / мошеннические действия	+					+
31. Fraudulent schemes / мошеннические схемы	+			+		
32. Grandparent scam / мошенничество с пожилыми родственниками		+				
33. High-tech crime / высокотехнологичное преступление						+
34. High-tech scam / высокотехнологичное преступление	+					
35. Job scams / мошенничество при трудоустройстве			+			

	Великобритания	США	Австралия	Канада	Сингапур	Китай
36. Identity fraud (AI-enabled~) / мошенничество с персональными данными с использованием ИИ	+					
37. Identity theft / кража личных данных	+					
38. Illicit activity / незаконная деятельность	+					
39. Illicit AI-powered schemes / преступные схемы с использованием ИИ				+		
40. Impersonating celebrities (scams) / имперсонация знаменитости			+			
41. Investment fraud / мошенничество в сфере инвестиций	+			+		
42. Investment scams / мошенничество в сфере инвестиций			+			
43. Invoice fraud / мошенничество со счет-фактурой	+					
44. Love scams / мошенничество в сфере онлайн-знакомств					+	
45. Mail fraud / мошенничество с электронными письмами		+				
46. Mass-dialling telco fraud operations / мошеннические операции с массовым обзвоном абонентов					+	
47. Misuse / противоправное использование		+				
48. Online fraud / Интернет-мошенничество	+					+
49. Online scams / Интернет-мошенничество	+				+	
50. Phishing / фишинг	+			+	+	+
51. Phishing scams / фишинг	+				+	
52. Phishing schemes / фишинговые схемы	+					
53. Pig butchering / мошенническая схема «Забой свиней»					+	
54. Pig butchering cyberscam / кибермошенничество, использующее схему «Забой свиней»			+			
55. Pig-butchering scams / мошенничество , использующее схему «Забой свиней»		+				
56. Rental scams / аферы с арендой жилья				+		
57. Romance fraud / мошенничество в сфере онлайн-знакомств	+					
58. Romance scams / мошенничество в сфере онлайн-знакомств	+			+		
59. Scam(s) (AI-augmented~) / мошенничество с использованием ИИ	+	+		+	+	+
60. Scam campaign / мошенническая кампания	+				+	
61. Scam operation / мошенническая операция	+	+			+	
62. Scheme / махинация				+		
63. Social engineering scams / мошенничество с использованием социальной инженерии			+	+		
64. Spear phishing / целевой фишинг				+		
65. Targeted phishing / целевой фишинг				+		
66. Transnational fraud / транснациональное мошенничество					+	
67. Untargeted schemes / масштабные махинации				+		
68. Vishing/вишинг				+		
69. Voice cloning scams / мошенничество с клонированием голоса				+		
70. Wire fraud / мошенничество с использованием электронных средств коммуникации		+				

Данные Таблицы 1 указывают на то, что в выборе лексических средств объективации слотов субфрейма **Технологии, каналы связи, методы и тактики** наблюдаются параллели в медиадискурсе Канады и Китая, а также Великобритании и Австралии; в случаях употребления терминологии сходство демонстрируют образцы медиадискурса Канады и Китая; а также Великобритании, Канады и Китая. В выборе лексических средств объективации слотов субфрейма **Виды преступлений** (Таблица 2) обнаруживаются параллели в медиадискурсе Великобритании и Сингапура; Великобритании и Канады; Великобритании и Китая. Составные терминологические сочетания (напр., *AI-driven deepfake extortion rackets*) преимущественно присутствуют в медиадискурсе Великобритании, Канады и Китая.

Заключение

Таким образом, проведенное исследование позволило прийти к следующим выводам:

1. Ключевые элементы категориально-понятийного аппарата англоязычных юридических текстов, посвященных проблеме использования технологии AI в противоправных целях, включают *generative AI technology / технология генеративного ИИ, developer / разработчик, user / пользователь, Dark AI, illicit markets / подпольные рынки, deepfakes / дипфейки, AI crime / преступление, совершенное посредством использования ИИ, rise in these attacks / рост числа кибератак, criminals / преступники, victims / потерпевшие, methods / методы, sensitive information / конфиденциальная информация, detection / распознавание фейков, criminal justice system / система уголовного правосудия*. Данные элементы и анализ пропозитивных структур послужили основой для разработки фреймовой модели ситуации AI-ENABLED FRAUD.

2. В результате отбора методом сплошной выборки из образцов медиадискурса США, Великобритании, Канады, Австралии, Сингапура и Китая за 2023-2025 гг. 468 лексических единиц, обозначающих различные аспекты проблемы ИИ-мошенничества, разработана фреймовая модель ситуации AI-ENABLED FRAUD. Вышеуказанная модель основана на субфреймах, слотах и подслотах фрейма ПРЕСТУПЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИИ и фрейма ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ В МОШЕННИЧЕСКИХ ОПЕРАЦИЯХ.

3. Субфреймы **Правонарушители, Потерпевшие, Предмет преступления, Материальный ущерб, Масштаб использования мошеннических схем с применением ИИ, Виды преступлений, Противодействие**

со стороны экспертного сообщества являются инвариантными субфреймами фрейма ПРЕСТУПЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИИ. Регулярно актуализируются слоты Возможности ИИ и Усовершенствование технологий на основе ИИ, используемых для совершения преступления, входящие в состав субфрейма **Технологии, каналы связи, методы и тактики** (фрейм ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ В МОШЕННИЧЕСКИХ ОПЕРАЦИЯХ). Отмечены различные паттерны в актуализации вариативных субфреймов.

4. Наблюдается вариативность в количестве субфреймов и слотов, актуализируемых в отдельно взятом тексте; минимальный показатель составляет 12, максимальный – 24. Высокие показатели, 23 и 24 единицы, представлены в публикациях китайского и австралийского изданий.

5. Состав кластера регулярно актуализируемых субфреймов, относящихся к фреймам ПРЕСТУПЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИИ и ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ДЛЯ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ, обусловлен реализацией коммуникативной стратегии информирования и функции предупреждения об опасности. В отдельных примерах медиадискурса США и Великобритании основными факторами, обусловливающими направление фреймирования при высоких показателях, отражающих количество актуализированных в тексте субфреймов и слотов, является дискурсивная практика конструирования достоверности; в медиадискурсе Сингапура – наличие дискурс-периферии с образовательной функцией.

6. На примере лексических единиц, вербализирующих слоты субфрейма **Технологии, каналы связи, методы и тактики** и субфрейма **Виды преступлений,** показано, что образцы медиадискурса указанных стран демонстрируют значительную вариативность в выборе лексических средств объективации слотов инвариантных субфреймов фреймовой структуры.

Перспективы дальнейшего исследования связаны с проведением лонгитюдного когнитивно-сопоставительного исследования данного медиафрейма в дискурсе СМИ США, Великобритании, Канады, Австралии, Сингапура и Китая.

Материалы исследования | Research materials

1. AI crime: what we know, what we don’t know, and what we need to know. https://unicri.org/sites/default/files/2026-01/F3-Jan-2026-AI-crime-what-we-know-what-we-dont-know-and-what-we-need-to-know-by-Marie-Helen-Maria-Maras.pdf
2. ‘Cold-hearted’ scammers targeted hundreds by posing as grandkids in distress, prosecutors say. https://www.nbcnews.com/news/us-news/cold-hearted-scammers-targeted-hundreds-posing-grandkids-distress-pros-rcna224561
3. Criminals are using AI and deepfake technology to steal consumer details. https://www.mirror.co.uk/money/criminals-using-ai-deepfake-technology-32595761
4. Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud. https://www.ic3.gov/PSA/2024/PSA241203
5. Growing underground market for rogue AI sparks cyber-security concerns. https://www.straitstimes.com/singapore/growing-underground-market-for-rogue-ai-sparks-cyber-security-concerns?ref=more-on-this-topic
6. How South-East Asia's pig butchering scammers are using artificial intelligence technology. https://www.abc.net.au/news/2024-05-16/pig-butchering-scams-artificial-intelligence-ai-face-swapping-/103804830
7. Vietnamese authorities warn of rising AI-driven deepfake extortion rackets. https://www.chinadaily.com.cn/a/202504/10/WS67f73651a3104d9fd381e8ed.html

Источники | References

1. Ампикян А. Г. Дискурсивно-фреймовая характеристика концепта «одарённость» в русском и французском педагогическом дискурсах (на материале контекстов коммуникативного пространства «Работа с одарёнными детьми»: автореф. дисс. … к. филол. н. Краснодар, 2023.
2. Асмус Н. Г., Журкова М. С., Ковальчук Л. П. Медийная репрезентация социальных проблем городов-побратимов: монография. Челябинск: Челябинский государственный университет, 2021.
3. Бокова О. В. Малоформатный текст «сообщение о преступлении»: особенности его семантической и структурной организации: на материале актуальных немецкоязычных медиатекстов: автореф. дисс. … к. филол. н. Воронеж, 2011.
4. Вдовиченко Е. А., Каменева В. А. Параметры оценки сложности политических новостных текстов со структурой “inverted pyramid” («перевернутая пирамида») для детской аудитории // Политическая лингвистика. 2025. № 3 (111).
5. Девятияров Д. В. Динамика сетевых фреймов в русско- и англоязычном непрофессиональном политическом дискурсе кризисов легитимности власти: детерминационный аспект: автореф. дисс. … к. филол. н. Кемерово, 2024.
6. Демьянков В. З. Политический дискурс как предмет политологической филологии // Политическая наука. 2002. № 3.
7. Дзялошинский И. М. Медиапространство России: коммуникационные стратегии социальных институтов: монография. М.: Изд-во Академии повышения квалификации и профессиональной переподготовки работников образования, 2013.

8. Ермоленкина Л. И. Дискурсивная картина мира современного радио: автореф. дисс. … д. филол. н. Томск, 2022.
9. Ильинова Е. Ю., Волкова О. С. Когнитивно-дискурсивный аспект медиарепрезентации события // Вестник Московского государственного лингвистического университета. Гуманитарные науки. 2016. № 7 (746).
10. Имамгаязова Д. И. Фрейм «киберпространство» в медиадискурсе (на материале русскоязычных СМИ): автореф. дисс. …к. филол. н. Уфа, 2023a.
11. Имамгаязова Д. И. Фрейм «киберпространство» в медиадискурсе (на материале русскоязычных СМИ): дисс. … к. филол. н. Уфа, 2023b.
12. Кононова И. В., Кульчицкая Е. Р. Моделирование фрейма HEALTHY LIFESTYLE: корпусный подход // ДИСКУРС. 2022. Т. 8. № 4. https://doi.org/10.32603/2412-8562-2022-8-4-172-186
13. Кушнерук С. Л. Развитие теории когнитивно-дискурсивного миромоделирования за рубежом и в России // Вопросы когнитивной лингвистики. 2018. № 4. https://doi.org/10.20916/1812-3228-2018-4-115-125
14. Мельникова Е. А. Когнитивно-дискурсивные особенности медиарепрезентации события в англоязычном тексте новостного сообщения: автореф. дисс. … к. филол. н. Волгоград, 2016.
15. Мельникова Е. А. Особенности реализации стратегии информирования о криминальном происшествии в англоязычном новостном дискурсе // Филологические науки. Вопросы теории и практики. 2017. № 12-2 (78).
16. Минский М. Фреймы для представления знаний. М.: Энергия, 1979.
17. Никонова Е. А. Дискурсивные практики конструирования достоверности повествования в аналитической статье (на примере англоязычного масс-медиа дискурса) // Филологические науки. Вопросы теории и практики. 2022. Т. 15. Вып. 1. https://doi.org/10.30853/phil20220013
18. Резанова З. И., Степаненко А. А. Фреймирование кризисной ситуации в институциональных и персональных медиа (на материале текстов о COVID-19) // Вестник Томского государственного университета. 2023. № 495.
19. Салькова Н. В. Когнитивно-фреймовое моделирование терминосистемы корпоративного права США // Филологические науки. Вопросы теории и практики. 2025. Т. 18. № 4. https://doi.org/10.30853/phil20250232
20. Смирнова И. В. Функционально-прагматическая специфика мошеннического дискурса: автореф. дисс. … к. филол. н. Ставрополь, 2025.
21. Шермазанова С. В. Гибридизация и дискурсивная «экспансия» институционального военного дискурса // Политическая лингвистика. 2025. № 4 (112).
22. Alefirenko N. F. Media discourse and it's communicative and pragmatic entity // Media Linguistics. 2016. № 1 (11). https://medialing.ru/mediadiskurs-i-ego-kommunikativno-pragmaticheskaya-sushchnost/

Информация об авторах | Author information

RU

Филошина Ирина Олеговна[1], к. филол. н.
[1] Санкт-Петербургский гуманитарный университет профсоюзов

EN

Irina Olegovna Filoshina[1], PhD
[1] Saint Petersburg University of the Humanities and Social Sciences

[1] *filir1@mail.ru*

Информация о статье | About this article

Дата поступления рукописи (received): 16.02.2026; опубликовано online (published online): 02.04.2026.

Ключевые слова (keywords): сопоставительно-когнитивные исследования медиадискурса; варианты ситуационного фрейма; фреймовое наполнение медиадискурса; объективация слотов; дискурсивная практика конструирования достоверности; comparative-cognitive studies of media discourse; situational frame variants; frame filling of media discourse; slot objectification; discourse practice of constructing credibility.