ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ СПЕЦИАЛИСТОВ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ТЕХНОЛОГИЯМ ДИПФЕЙКОВ

***Шевцова Г.А.*[1], *Лось В.П.*[2], *Тышук Е.Д.*[3]**

Ключевые слова: *правовые основы противодействия, искусственный интеллект, методы обнаружения, план траектории, специальности и направления подготовки, технолого-аналитический интеллект, гуманитарно-психологическая экспертиза, процедурно-операционный менеджмент, стратегическое прогнозирование и образование, образовательный стандарт.*

Аннотация

Цель: *состоит в анализе и разработке компетенций специалистов в области противодействия технологиям дипфейков.*

Метод: *исследование основано на анализе существующей нормативно-правовой базы борьбы с дипфейками, оценке из опасности и степени разработанности технологий их обнаружения.*

Результаты: *в статье проведен анализ публикаций, в которых освещаются вопросы правовой основы борьбы с дипфейками и их опасности для общества. Проведен обзор публикаций, раскрывающих возможные подходы к обнаружению дипфейков. Сделаны выводы о выявленных пробелах в правовом регулировании. Проведена оценка перспективности рассмотренных методов обнаружения. Обоснована новизна и теоретическая значимость предложенной модели компетенций для развития соответствующей научной области. Приведен пример плана траектории формирования компетенций специалистов в области противодействия технологиям дипфейков, который включает в себя четыре фундаментальных блока компетенций: Блок А. Технолого-аналитический интеллект; Блок Б. Гуманитарно-психологическая экспертиза; Блок В. Процедурно-операционный менеджмент и Блок Д. Стратегическое прогнозирование и образование. Внедрение данных компетенций в практику позволит повысить уровень готовности выпускников к противодействию широкому спектру угроз, в том числе технологиям дипфейков.*

DOI: 10.24412/1994-1404-2026-2-370-379

Введение

Вместе с цифровизацией всех отраслей экономики развиваются не только методы защиты критической информационной инфраструктуры, но и совершенствуются методы негативного противоправного воздействия на различные системы, в которых хранится и обрабатывается важная информация. По данным МВД России за январь — сентябрь 2025 года зарегистрировано преступлений, совершенных с использованием информационно-телекоммуникационных технологий на 7,4 % меньше, чем в январе — сентябре 2024 года[4]. В январе — июле 2025 года зарегистрировано 424,9 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Ущерб от IT-преступлений в России за семь

[4] URL: https://мвд.рф/. Дата обращения 25.04.2026.

[1] ***Шевцова Галина Александровна****, кандидат исторических наук, доцент, директор Института информационных наук и технологий безопасности, Российский государственный гуманитарный университет, Москва, Россия.*

E-mail: shevtsova-g@mail.ru

[2] ***Лось Владимир Павлович****, доктор военных наук, профессор, главный научный сотрудник, Российский государственный гуманитарный университет, Москва, Россия.*

E-mail: los-vladimir@yandex.ru

[3] ***Тышук Екатерина Дмитриевна****, старший научный сотрудник, Российский государственный гуманитарный университет, Москва, Россия.*

E-mail: umo.azi@mail.ru

месяцев текущего года увеличился на 16% — с 100,5 млрд рублей до 119,6 млрд рублей[5].

Особое место среди преступлений занимают преступления с использованием технологии дипфейк[6].

В последние годы дипфейки стали не только технологической новинкой, но и серьёзной угрозой для общества, бизнеса и государства. В ответ на это в России и мире формируются новые организационные и правовые механизмы противодействия.

Среди организационных мер следует отметить следующие:

– создание межведомственных рабочих групп. В России, например, по приказу[7] Минцифры России создана специальная рабочая группа с участием представителей различных ведомств, включая МВД России, ФСБ России, Минюст России, Роскомнадзор и другие. Задачи этой группы — выработка предложений по противодействию противоправному использованию дипфейков, разработка технологической защиты, формирование нормативной базы и образовательных программ;
– внедрение технологических стандартов. На международном уровне внедряются стандарты происхождения контента (например, C2PA[8]), которые позволяют маркировать и верифицировать ИИ-контент. Это помогает отличать подлинные материалы от подделок.

Правовые меры противодействия дипфейкам направлены на установление норм и санкций за их неправомерное использование.

Во-первых, происходит ужесточение законодательства. В России в 2025—2026 годах внесены изменения в Уголовный кодекс Российской Федерации (УК РФ)[9], чтобы привлекать к ответственности не только за распространение, но и за сам факт автоматизированной обработки персональных данных для создания дипфейков. Теперь преступлением считается сам запуск программы для создания дипфейка на основе незаконно полученных данных.

Во-вторых, вводится обязательная маркировка ИИ-контента. Внесён законопроект о введении обязательной маркировки видеоматериалов, созданных или изменённых с помощью ИИ. За отсутствие или некорректность маркировки предусмотрена административная ответственность.

В-третьих, развивается международное сотрудничество. Ведётся диалог на площадках Международного союза электросвязи и других организаций для выработки единых стандартов и норм регулирования, чтобы избежать цифровой фрагментации и использовать регулирование не как инструмент давления, а как средство защиты.

Осуществляются образовательные инициативы. Ведётся работа по повышению цифровой грамотности населения, чтобы люди могли распознавать дипфейки и защищаться от мошенничества. Таким образом, определенные меры, связанные с противодействием технологиям дипфейка в настоящее время реализуются. Однако отсутствие в законодательстве понятия «дипфейк» усложняет правоприменительную практику. Отсутствие предмета регулирования приводит к ситуации, когда противоправное деяние, связанное с использованием дипфейка, квалифицируется в рамках других статей УК РФ: незаконное использование персональных данных, незаконное использование компьютерной информации, содержащей персональные данные, нарушение неприкосновенности частной жизни, клевета и так далее.

Правовое определение дипфейка позволит более четко определить границы необходимых мер противодействия этому явлению и конкретизировать формулировки необходимых навыков специалистов по борьбе с дипфейками.

Постановка задачи

Научная задача, решаемая в данной статье, заключается в определении содержания дополнительных (новых) компетенций специалистов по информационной безопасности, определяющих их способность противодействовать технологиям дипфейка.

Такие компетенции, которые отсутствуют в настоящее время в образовательных стандартах, должны быть основаны на знаниях, с одной стороны, соответствующих правовых основ борьбы с дипфейками и, с другой стороны, на умении разрабатывать и применять технологии обнаружения и противодействия дипфейкам.

В условиях отсутствия нормативного определения понятия «дипфейк» в качестве правовых основ борьбы с дипфейками следует использовать соответствующие положения Кодекса РФ об административных правонарушениях[10] (КоАП РФ) и Уголовного кодекса РФ.

---

[5] В России за январь — июль 2025 года ущерб от IT-преступлений вырос на 16% // Официальный сайт. «Ассоциация юристов России». URL: https://alrf.ru/news/v-rossii-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd/

[6] В Законопроекте № 718538-8 (внесён в Госдуму в 2024 году) дипфейк описывается как технологии, позволяющие создавать видео и аудиоматериалы на основе образцов изображений и голоса гражданина, искусственно воссоздающие несуществующие события.

[7] Приказ Минцифры России от 19.01.2026 № 16 «О межведомственной рабочей группе при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации по вопросу противодействия противоправному использованию технологий типа "Дипфейк"» // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения 26.05.2026).

[8] C2PA (Coalition for Content Provenance and Authenticity) // Официальный сайт. URL: https://c2pa.org/ (дата обращения 06.05.2026).

[9] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026).

[10] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 02.05.2026).

КоАП РФ предусматривает административную ответственность в виде штрафа за распространение в СМИ и Интернете заведомо недостоверной общественно значимой информации (ст. 13.15).

УК РФ предусматривает уголовную ответственность в виде штрафа или лишение свободы: за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207.1); за публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия (ст. 207.2); за публичное распространение заведомо ложной информации об использовании Вооружённых Сил РФ, исполнении государственными органами своих полномочий (ст. 207.3).

Существующие по заявленной тематике публикации можно разделить на две большие группы. В первой группе публикаций анализируется практика неправомерного использования технологий дипфейка. Во второй группе публикаций описываются методы обнаружения дипфейков.

Среди работ первой группы отметим следующие. В статье 2023 года Клевенский М.С. рассматривает технологии дипфейка как инструмент ведения информационного противоборства, поскольку дипфейк может быть применен в интересах «черного пиара» для дискредитации того или иного политика, или для явной дезинформации [1].

В работе 2023 года Семененко В.А. анализирует проблему неправомерного применения технологий искусственного интеллекта, в частности, для подмены изображения на цифровых фотографиях и видеозаписях [2].

В статье 2024 года Шатохина С.П. рассматривает негативные последствия применения технологии дипфейка для социальной и экономической жизни, а также те технологии, которые используются при разработке дипфейков, предлагая содержание обучения старших школьников и студентов [3].

В работах 2024 года Дунаева А.П. и Лисицын М.А. рассматривают зарубежный опыт определения и пресечения правонарушений, связанных с технологией дипфейка, исследуют судебную практику, приводят статистику преступлений, связанных с искусственным интеллектом, исходя из данных МВД России, анализируют отечественную законодательную базу [4,5].

В статьях 2023 года Ткалина А.А. рассматривает различные аспекты правового регулирования использования технологии дипфейк [6], Соловьев А.И. анализирует понятие «дипфейк» и описывает различные способы использования дипфейков, анализирует характеристики дипфейков [7], а Клевенский М.С. рассматривает дипфейк как средство информационного противоборства и утверждает, что дипфейк может быть для дискредитации того или иного политика и с целью введения в заблуждения противоборствующей стороны [8].

Вывод о необходимости научных исследований в сфере защиты прав человека делает Волкова Г.Е. в своей статье в связи с возросшими возможностями искусственного интеллекта [9].

Лаптев В.А. еще в 2021 году обратил внимание на технологии искусственного интеллекта, которые не способствуют развитию онлайн-правосудия [10].

Купка И.П. в своей статье осветил вопросы коммерческого применения технологии дипфейка в киноиндустрии, музыкальном производстве, рекламе и даже в военных целях [11].

Из анализа работ первой группы следует, что правоприменительная практика в сфере борьбы с дипфейками находится на пути своего развития. В УК РФ и КоАП РФ имеются правовые нормы, позволяющие привлекать к ответственности лиц, которые используют технологии дипфейка в противоправных целях.

Среди работ второй группы отметим следующие. В статье 2024 года Исакова А.Г. ставит вопрос о применении искусственного интеллекта для определения подлинности цифрового контента, используемого в качестве средства совершения мошенничества [12].

Ярокова А.О. в статье 2023 года указывает на такой инструмент как фактчекинг, который позволяет проверять сообщения и выявлять фейки [13].

Елизаров Д.А. в работе 2026 года рассматривает отличительные признаки дипфейков и методы их распознавания с использованием процедур машинного обучения и компьютерного зрения [14].

Березкин Ф.Е. в 2025 году указал на ряд технологий обнаружения дипфейков, разрабатываемых компаниями Reality Defender и Deep Media, основанных на обнаружении фактов неестественного моргания или аномалий в аудиоспектрах [15].

Интересной представляется работа Титова К.А. 2025 года, в которой представлена программа автоматического определения подлинности, использующая сверточную нейронную сеть (CNN) с архитектурой EfficientNetB0 [16].

Воронов С.А. в своей статье проанализировал существующие подходы к распознаванию дипфейков, сгенерированных с использованием технологий искусственного интеллекта, предложив классификацию дипфейков по типам генерации и по целям [17].

Никогда Д.К. в своей работе описала систему искусственного интеллекта, которая способна обнаруживать мошеннические схемы в социальных сетях [18].

Диреев И.Д. в 2025 году сформулировал проблему «методологического синтеза медиалингвистики и семиотики» как инструмента анализа мультимодальных медиатекстов и противодействия дипфейкам [19].

Роговой В. в 2024 году описал метод повышения точности классификации дипфейков, основанный на редукции цветовой палитры и спектральном анализе изображений [20].

Сафиуллин Р.Н. в 2023 году проанализировал влияние голосовых дипфейков на различные сферы общества и предложил методы их распознавания [21].

Иванов Д.Э. в 2023 году проанализировал различные методы дипфейков и обосновал необходимость

Таблица 1

Характеристики атак

ТИП АТАКИ	МЕХАНИЗМ ДЕЙСТВИЯ	ПОСТАВЛЕННАЯ ЦЕЛЬ	ПРИМЕР ИСПОЛЬЗОВАНИЯ
Дипфейки	Синтез контента с помощью ИИ	Манипуляция, шантаж, мошенничество	Поддельное видео с политическим деятелем
Атаки в TCP/IP	Использование уязвимостей сетевых протоколов	Перегрузка сети, перехват данных	SYN flood (отказ в обслуживании» — DoS, MAC-Spoofing (изменение физического адреса сетевого интерфейса — MAC-адреса)
Трояны	Маскировка под легитимное ПО	Кража данных, контроль над системой	Банковский троян для кражи паролей
Люки	Скрытые бэкдоры в алгоритмах	Обход защиты	Секретный доступ к зашифрованным данным
Эксплойты	Использование уязвимостей ПО	Получение контроля, установка вредоноса	Переполнение буфера
SQL-инъекция	Внедрение SQL-кода в запросы	Доступ к БД, изменение данных	Кража паролей из таблицы пользователей

разработки новых систем для борьбы с подделками, такими как лицевой обмен, синхронизация губ и манипуляция голосом [22].

Анализ перечисленных работ позволяет сделать вывод о том, что в настоящее время в российском праве отсутствует понятие «дипфейк». Вместе с тем, имеются разработанные технологии обнаружения дипфейков, которые могут использоваться в качестве учебного материала при подготовке специалистов в области информационной безопасности.

Решение поставленной задачи

Подготовка специалистов по борьбе с дипфейками требует комплексного подхода: сочетания технологических, правовых и образовательных мер, а также учета результатов международного сотрудничества, рассматривая синтетический контент как угрозу общественной стабильности, обуславливающей разработку новых технологических инструментов борьбы с технологиями дипфейков и мер ответственности.

Стратегия национальной безопасности Российской Федерации[11] подчеркивает важность создания безопасного информационного пространства и защиты российского общества от негативного информационно-психологического воздействия как одного из ключевых национальных интересов России.

Почему для решения этой проблемы недостаточно тех компетенций, которые прописаны в действующих ФГОС? Дело в том, что несмотря на наличие в образовательных стандартах по информационной безопасности большого количества компетенций, ни одна из них не предусматривает приобретения знаний и навыков по борьбе с этим новым явлением в цифровом мире — с дипфейками. Базовых мер цифровой гигиены становится недостаточно для борьбы с манипуляциями и фальшивой информацией. Наиболее близкой к рассматриваемой тематике является специальность высшего образования «Компьютерная безопасность»[12], поскольку именно в этой специальности предусмотрено привитие компетенций по противодействию компьютерным атакам. Среди таких атак изучаются: атаки в сетях TCP/IP; троянские программы; люки; эксплойты; атаки «противник в середине»; SQL-инъекции.

Каждая из этих атак характеризуется механизмом действия и поставленной целью (табл.1) и требует специфических, ориентированных на нее, методов защиты, например шифрования, обновления программного обеспечения, использования антивирусных программ и других методов.

Как следует из данных таблицы, дипфейки отличаются от других атак и механизмом действия и поставленной целью. Этим обстоятельством обусловлена необходимость разработки для обучаемых, будущих специалистов, новых компетенций.

Системный подход, учитывающий как технологические аспекты, так и правовые, применительно к формированию компетенций специалистов по противодействию дипфейкам можно структурно изложить следующим образом: специалист по дипфейкам должен обладать компетенциями в области технологий формирования дипфейков, методов их выявления, понимать

[11] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

[12] Федеральный государственный образовательный стандарт высшего образования — специалитет по специальности 10.05.01 Компьютерная безопасность. Утвержден приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1459. С изменениями и дополнениями от: 19 июля 2022 г., 27 февраля 2023 г.

и знать требования законодательства, регулирующего работу с дипфейками, учитывать этические аспекты.

Пример плана траектории формирования компетенций представлен на рис. 1.

Траектория формирования компетенций предусматривает в процессе подготовки специалиста получение знаний, условно разбитых на 4 взаимосвязанных блока, в следующих областях:

Блок А: Формирование технолого-аналитического интеллекта (От «насмотренности» к системному анализу);

Блок Б: Гуманитарно-психологическая экспертиза (Понимание «целевой аудитории» дипфейка — человека);

Блок В: Процедурно-операционный менеджмент (От личной компетенции к организационной практике);

Блок Г: Стратегическое прогнозирование и образование (Создание «иммунитета» будущего).

Содержание таких блоков определяется поставленной целью: подготовить специалиста нового типа, который способен не только обнаружить подделку, но и диагностировать уровень угрозы, понять её цель и смягчить последствия. Он выступает как кризис-менеджер цифровой реальности.

Блок А предусматривает:

- глубокое понимание экосистемы: Знание всей цепочки создания — от генеративных моделей (GAN, диффузионные) и фейк-аудио до инструментов синхронизации (Wav2Lip). Это позволяет предсказывать эволюцию угроз;
- многоуровневую верификацию, включая:
- аудиовизуальный слой: Поиск артефактов генерации (нефизичное отражение в глазах, неестественная динамика волос, отсутствие микродвижений головы, «ватный» голос без пауз на вдох);
- цифровой слой: Анализ метаданных файла, следов сжатия и повторной обработки, использование специализированных платформ (Intel's FakeCatcher, Sensity AI);
- контекстуальный слой: Сопоставление с архивами данных публичных выступлений человека, анализ фона, деталей одежды на предмет анахронизмов.

Блок Б предусматривает получение знаний в следующих областях:

- когнитивная психология: профессиональное знание механизмов, почему даже плохой дипфейк может сработать: эвристика доступности (яркий образ запоминается), эффект иллюзии правды (многократный повтор), предвзятость подтверждения (верим тому, что совпадает с нашими взглядами);
- нарративный и семиотический анализ: умение «читать» дипфейк как культурный текст. Какой миф он усиливает? Какую эмоцию эксплуатирует (страх, ностальгию, отвращение)? Какие культурные коды использует для правдоподобия?
- этическая и правовая карта: понимание тонкой грани между злонамеренной дезинформацией, сатирой, художественным высказыванием и научной реконструкцией. Знание правовых рамок в разных юрисдикциях (от законов о клевете до специфических, как статья 274.1 УК РФ Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации).

Блок В предусматривает получение знаний в следующих областях:

- разработка и внедрение протоколов: Создание внутренних стандартов проверки цифрового контента для медиакомпаний, государственных органов, корпораций. Чёткий регламент: кто, за сколько времени, с помощью каких инструментов и по какому чек-листу проводит проверку;
- кризисные коммуникации: Навыки не только внутреннего доклада, но и публичного объяснения. Как сообщить о фейке, не сея панику? Как восстановить доверие к пострадавшему институту или личности? Умение формулировать сообщения для разных аудиторий.
- управление цифровым наследием: Проактивные стратегии. Консультации по созданию «библиотеки эталонов» — защищённых аудио- и видеоматериалов ключевых персон для будущей верификации.

Блок Г предусматривает получение знаний в следующих областях:

- анализ трендов и сценарное планирование: Прогнозирование следующих рубежей (дипфейки в реальном времени на видео-звонках, массовая персонализированная дезинформация). Подготовка к ним.
- педагогика медиаграмотности: Умение не только самому разоблачать, но и обучать других. Разработка образовательных программ, мастер-классов, инфографики, которые объясняют угрозу на понятном языке, не требуя технического бэкграунда.

В результате на основе полученных знаний синтезируется образ специалиста как «архитектора доверия»:

- итоговый профиль — «гибридный аналитик». Его сила в синтезе: техническая подкованность служит глубокому гуманитарному анализу, который, в свою очередь, воплощается в чёткие процедуры и коммуникационные стратегии;
- его конечная цель — не вечная «гонка вооружений» с алгоритмами, а повышение цифровой устойчивости общества через образование, ясные протоколы и восстановление статуса проверенных источников;
- формирование такого специалиста требует принципиально междисциплинарной программы, где

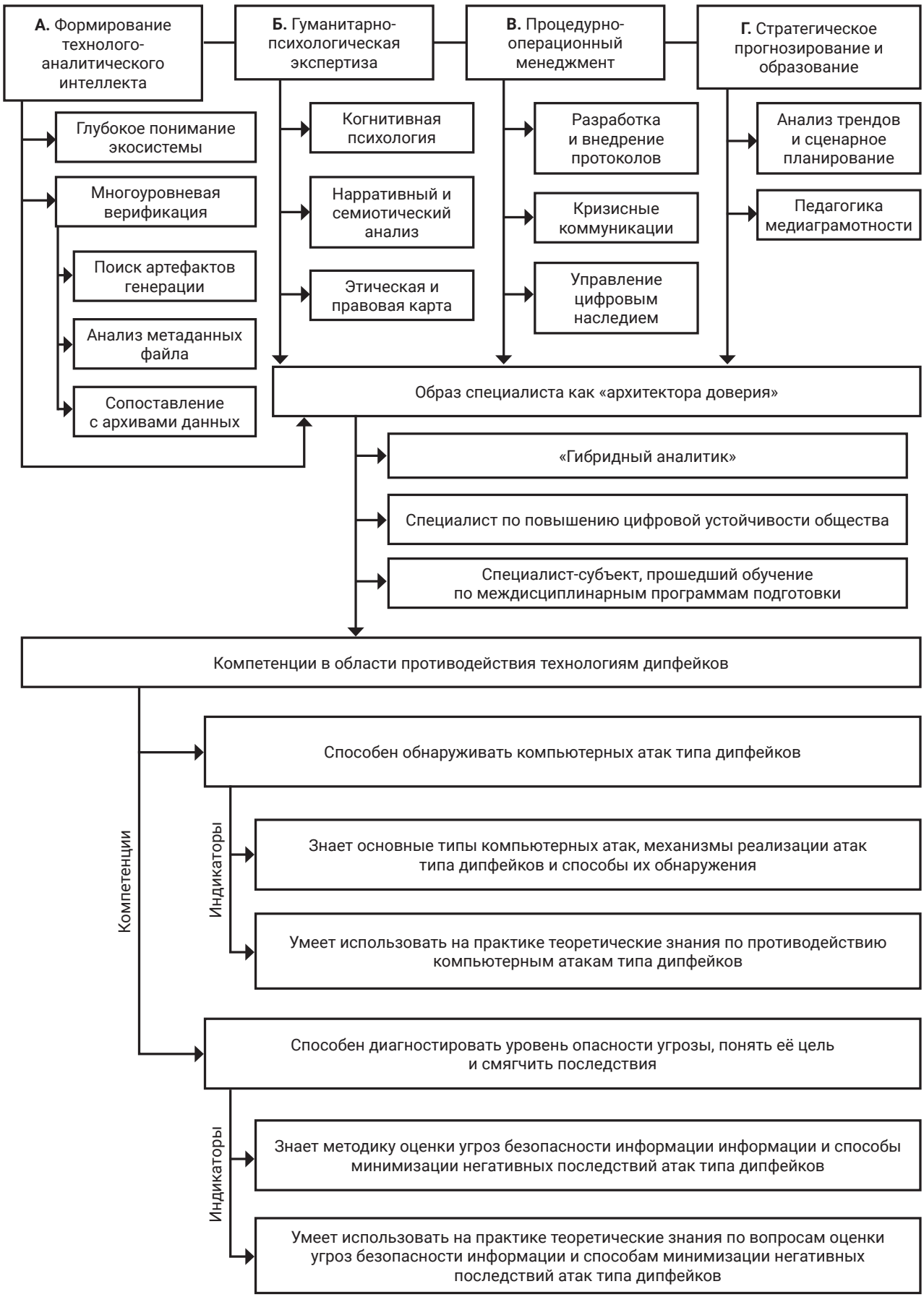

Рис. 1. План траектории формирования компетенций специалиста в области противодействия технологиям дипфейков

IT-модуль равен по весу модулям психологии, права, коммуникаций и этики. Именно на этом стыке рождается новое поколение защитников цифровой реальности.

Исходя из сказанного можно сформулировать компетенции, которыми должен обладать специалист:

1. Специалист способен обнаруживать компьютерные атаки типа дипфейков. В качестве индикаторов в этой компетенции используются следующие формулировки:

знает основные типы компьютерных атак, механизмы реализации атак типа дипфейков и способы их обнаружения;

умеет использовать на практике теоретические знания по противодействию компьютерным атакам типа дипфейков.

2. Способен диагностировать уровень опасности угрозы, понять её цель и смягчить последствия. В качестве индикаторов в этой компетенции используются следующие формулировки:

знает методику оценки угроз безопасности информации и способы минимизации негативных последствий атак типа дипфейков;

умеет использовать на практике теоретические знания по вопросам оценки угроз безопасности информации и способам минимизации негативных последствий атак типа дипфейков.

Выводы

В статье обоснована необходимость учета в образовательном процессе подготовки специалистов по информационной безопасности новых компетенций, заключающихся в умении разрабатывать и применять технологии обнаружения и противодействия дипфейкам.

В работе проведен анализ публикаций, в которых освещаются вопросы правовой основы борьбы с дипфейками и их опасности для общества. Проведен обзор публикаций, раскрывающих возможные подходы к обнаружению дипфейков. Предложен пример плана траектории формирования компетенций специалистов в области противодействия технологиям дипфейков, который включает в себя четыре фундаментальных блока необходимых знаний будущего специалиста: технолого-аналитический интеллект; гуманитарно-психологическая экспертиза; процедурно-операционный менеджмент и стратегическое прогнозирование и образование. Сформулированы компетенции, которыми должны обладать специалисты в области противодействия технологиям дипфейков и индикаторы достижения этих компетенций. Внедрение данных компетенций в практику позволит повысить уровень готовности выпускников к противодействию широкого спектра угрозам, в том числе технологиям дипфейков.

Достоверность полученных результатов основана на использовании при анализе данной проблемы официальных документов и научных работ специалистов в области борьбы с дипфейками.

Благодарности

Работа выполнена в рамках проекта РГГУ «Разработка программно-аппаратного комплекса для сертификации моделей искусственного интеллекта в интересах образовательного процесса РГГУ (на примере УГСН 10.00.00 Информационная безопасность)» (конкурс «Проектные научные коллективы РГГУ»)».

Литература

1. Клевенский М.С. Дипфейк: за и против // Российское общество сегодня: ценности, институты, процессы : материалы Всерос. науч. конф., Санкт-Петербург, 16—18 ноября 2023 г. СПб. : ООО Издательский дом «Сциентиа», 2023. С. 642—644.
2. Семененко В.А. Технико-криминалистические аспекты борьбы с технологией «дипфейк» // Следственная деятельность: проблемы, их решение, перспективы развития : материалы VII Всерос. молодёжной науч.-практ. конф., Москва, 27 ноября 2023 года. М. : Московская академия Следственного комитета Российской Федерации, 2024. С. 382—386.
3. Шатохина С.П. Дипфейк как метод применения искусственного интеллекта / С.П. Шатохина, Е.А. Варламова // Будущее науки 2024 : сб. научных статей 11-й Международной молодежной науч. конф. В 5 т. Курск, 18—19 апреля 2024 года. Курск: ЗАО «Университетская книга», 2024. С. 468—473.
4. Дунаева А.П. Дипфейк-технологии в России и в мире: актуальные проблемы правового регулирования / А.П. Дунаева, М.Л. Макаревич // Социально-экономическое развитие России: проблемы, тенденции, перспективы: Сборник научных статей участников XXIII Международной науч.-практ. конф., Курск, 15 мая 2024 года. Курск: ЗАО «Университетская книга», 2024. С. 511—516.

5. Лисицын М.А. Правовое регулирование технологии замены лица (дипфейк) // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». 2024. Т. 4. № 16. С. 189—195.
6. Ткалина А.А. Правовое регулирование цифровой технологии «дипфейк» // Цифровые технологии и право: Сборник научных трудов II Международной науч.-практ. конф. В 6 т. Казань, 22 сентября 2023 года. Казань : Познание, 2023. С. 360—372. EDN: IHBFEG.
7. Соловьев А.И. Дипфейк: развлечение, образование, манипуляция // В сб. материалов XXV Межд. науч.-практ. конф. «Журналистика — 2023: состояние, проблемы и перспективы», Минск, 22 ноября 2023 г. С. 481—484.
8. Клевенский М.С. Дипфейк: за и против // Российское общество сегодня: ценности, институты, процессы : материалы Всерос. науч. конф., Санкт-Петербург, 16—18 ноября 2023 г. СПб. : ООО Издательский дом «Сциентиа», 2023. С. 642—644.
9. Волкова Г.Е. К вопросу о защите прав личности в условиях распространения дипфейк-технологий // Юристъ-Правоведъ. 2023. № 3 (106). С. 15—22.
10. Лаптев В.А. Deepfake и иные продукты искусственного интеллекта на пути развития онлайн-правосудия // Актуальные проблемы российского права. 2021. Т. 16. № 11. С. 180—186.
11. Купка И.П. Дипфейк как информационное оружие современности / И.П. Купка, С.С. Щербаков // Динамика медиасистем. 2023. Т. 3. № 1. С. 375—381.
12. Исакова А.Г. Применение искусственного интеллекта в расследовании преступлений с использованием технологии «дипфейк» / А.Г. Исакова, А.В. Осин // Вестник науки. 2024. Т. 3. № 1(70). С. 235—242.
13. Ярокова А.О. Дипфейк как угроза индивидуального медиапотребления // Курсантские исследования: сборник научных работ. Могилев: Могилевский институт МВД Республики Беларусь, 2023. С. 266—268.
14. Елизаров Д.А. Определение признаков детектирования дипфейков для формирования входного вектора распознавания / Д.А. Елизаров, А.С. Окишев, А.В. Микунов // Инженерный вестник Дона. 2026. № 1 (133).
15. Междисциплинарные аспекты развития трансформационных технологий : сб. материалов I Межд. науч.-практ. конф., Геническ, 26—28 февраля 2025 г. СПб. : Наукоемкие технологии, 2025. С. 120. 814 с.
16. Титов К.А. Разработка программы для автоматического выявления дипфейков / К.А. Титов, Е.В. Корчемкина, Н.Л. Харина // Общество. Наука. Инновации (НПК-2025). Гуманитарные, общественные, физико-математические, компьютерные, химико-биологические и технические науки: сб. мат. XXV Всерос. (национальной) науч.-практ. конф., Киров, 22—30 мая 2025 г. Киров : Вятский государственный университет, 2025.
17. Воронов С.А. О подходах в распознавании дипфейков и синтетических медиа / С.А. Воронов, А.Д. Косолапов, А.В. Скробач // Информация и безопасность. 2025. Т. 28. № 1. С. 103—110.
18. Никогда Д.К. ИИ-система для обнаружения мошеннических схем в социальных сетях // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. 2025. Т. 2. С. 875—880.
19. Диреев И.Д. Медиалингвистика и семиотика: методология анализа мультимодальных медиатекстов // Актуальные вопросы современной филологии и журналистики. 2025. № 2 (57). С. 169—182.
20. Роговой В. Разработка метода выявления дипфейков: применение частотного анализа и уменьшения цветового пространства изображения для повышения точности классификации / В. Роговой, В.М. Коржук, О.А. Кокорина // V Межд. конф. по нейронным сетям и нейротехнологиям (NeuroNT'2024) : сб. докл. конф., Санкт-Петербург, 20 июня 2024 г. СПб. : Санкт-Петербургский государственный электротехнический университет ЛЭТИ, 2024. С. 45—49.
21. Сафиуллин Р.Н. Распознавание голосовых дипфейков: методы, сферы применения и влияние // Тенденции развития современной науки в свете исследований молодых ученых : сб. статей межд. науч. конф., Вологда, 29 ноября 2023 г. СПб. : Гуманитарный национальный исследовательский институт «Нацразвитие», 2023. С. 46—49.
22. Иванов Д.Э. Методы и вызовы в обнаружении дипфейков // IV Межд. науч. конф. по междисциплинарным исследованиям : сб. статей, Екатеринбург, 15 декабря 2023 г. Екатеринбург: ООО «Институт Цифровой Экономики и Права», 2023. С. 462—466.

SECTION:
REGULATORY INFORMATICS

FORMATION OF COMPETENCIES OF SPECIALISTS IN THE FIELD OF COUNTERING DEEPFAKE TECHNOLOGIES

***Shevtsova G.A.*[13], *Los V.P.*[14], *Tyshuk E.D.*[15]**

Keywords: *deepfake, legal framework for counteraction, artificial intelligence, detection methods, competencies.*

Abstract

Objective: *to analyze and develop the competencies of specialists in the field of countering deepfake technologies.*

Method: *the study is based on the analysis of the existing regulatory framework for combating deepfakes, assessing the danger and the degree of development of technologies for their detection.*

Results: *The article analyzes publications that highlight the legal framework for combating deepfakes and their danger to society. A review of publications that reveal possible approaches to detecting deepfakes is carried out. An example of a trajectory plan for the formation of competencies of specialists in the field of countering deepfake technologies is proposed, which includes four fundamental blocks of competencies: Block A. Technological and analytical intelligence; Block B. Humanitarian and psychological expertise; Block C. Procedural and operational management and Block D. Strategic forecasting and education.*

References

1. Klevenskii M.S. Dipfeik: za i protiv // Rossiiskoe obshchestvo segodnia: tsennosti, instituty, protsessy : materialy Vseros. nauch. konf., Sankt-Peterburg, 16—18 noiabria 2023 g. SPb. : OOO Izdatel'skii dom "Stsientia", 2023. S. 642—644.
2. Semenenko V.A. Tekhniko-kriminalisticheskie aspekty bor'by s tekhnologiei "dipfeik" // Sledstvennaia deiatel'nost': problemy, ikh reshenie, perspektivy razvitiia : materialy VII Vseros. molodezhnoi nauch.-prakt. konf., Moskva, 27 noiabria 2023 goda. M. : Moskovskaia akademiia Sledstvennogo komiteta Rossiiskoi Federatsii, 2024. S. 382—386.
3. Shatokhina S.P. Dipfeik kak metod primeneniia iskusstvennogo intellekta / S.P. Shatokhina, E.A. Varlamova // Budushchee nauki 2024 : sb. nauchnykh statei 11-i Mezhdunarodnoi molodezhnoi nauch. konf. V 5 t. Kursk, 18—19 aprelia 2024 goda. Kursk: ZAO "Universitetskaia kniga", 2024. S. 468—473.
4. Dunaeva A.P. Dipfeik-tekhnologii v Rossii i v mire: aktual'nye problemy pravovogo regulirovaniia / A.P. Dunaeva, M. L. Makarevich // Sotsial'no-ekonomicheskoe razvitie Rossii: problemy, tendentsii, perspektivy: Sbornik nauchnykh statei uchastnikov XXIII Mezhdunarodnoi nauch.-prakt. konf., Kursk, 15 maia 2024 goda. Kursk: ZAO "Universitetskaia kniga", 2024. S. 511—516.
5. Lisitsyn M.A. Pravovoe regulirovanie tekhnologii zameny litsa (dipfeik) // Vestnik studencheskogo nauchnogo obshchestva GOU VPO "Donetskii natsional'nyi universitet". 2024. T. 4. No. 16. S. 189—195.
6. Tkalina A.A. Pravovoe regulirovanie tsifrovoi tekhnologii "dipfeik" // Tsifrovye tekhnologii i pravo: Sbornik nauchnykh trudov II Mezhdunarodnoi nauch.-prakt. konf. V 6 t. Kazan', 22 sentiabria 2023 goda. Kazan' : Poznanie, 2023. S. 360—372. EDN: IHBFEG.
7. Solov'ev A.I. Dipfeik: razvlechenie, obrazovanie, manipuliatsiia // V sb. materialov XXV Mezhd. nauch.-prakt. konf. "Zhurnalistika — 2023: sostoianie, problemy i perspektivy", Minsk, 22 noiabria 2023 g. S. 481—484.
8. Klevenskii M.S. Dipfeik: za i protiv // Rossiiskoe obshchestvo segodnia: tsennosti, instituty, protsessy : materialy Vseros. nauch. konf., Sankt-Peterburg, 16—18 noiabria 2023 g. SPb. : OOO Izdatel'skii dom "Stsientia", 2023. S. 642—644.
9. Volkova G.E. K voprosu o zashchite prav lichnosti v usloviiakh rasprostraneniia dipfeik-tekhnologii // Iurist"-Pravoved". 2023. No. 3 (106). S. 15—22.

[13] ***Galina A. Shevtsova***, *Ph.D. (History), Associate Professor, Director of the Institute of Information Sciences and Security Technologies, Russian State University for the Humanities, Moscow, Russia.*
E-mail: shevtsova-g@mail.ru

[14] ***Vladimir P. Los***, *Dr.Sc. (Military), Professor, Principal Researcher, Russian State University for the Humanities, Moscow, Russia.*
E-mail: los-vladimir@yandex.ru

[15] ***Ekaterina D. Tyshuk***, *Senior Researcher, Russian State University for the Humanities, Moscow, Russia.*
E-mail: umo.azi@mail.ru

10. Laptev V.A. Deepfake i inye produkty iskusstvennogo intellekta na puti razvitiia onlain-pravosudiia // Aktual'nye problemy rossiiskogo prava. 2021. T. 16. No. 11. S. 180—186.
11. Kupka I.P. Dipfeik kak informatsionnoe oruzhie sovremennosti / I.P. Kupka, S.S. Shcherbakov // Dinamika mediasistem. 2023. T. 3. No. 1. S. 375—381.
12. Isakova A.G. Primenenie iskusstvennogo intellekta v rassledovanii prestuplenii s ispol'zovaniem tekhnologii "dipfeik" / A.G. Isakova, A.V. Osin // Vestnik nauki. 2024. T. 3. No. 1(70). S. 235—242.
13. Iarokova A.O. Dipfeik kak ugroza individual'nogo mediapotrebleniia // Kursantskie issledovaniia: sbornik nauchnykh rabot. Mogilev: Mogilevskii institut MVD Respubliki Belarus', 2023. S. 266—268.
14. Elizarov D.A. Opredelenie priznakov detektirovaniia dipfeikov dlia formirovaniia vkhodnogo vektora raspoznavaniia / D.A. Elizarov, A.S. Okishev, A.V. Mikunov // Inzhenernyi vestnik Dona. 2026. No. 1 (133).
15. Mezhdistsiplinarnye aspekty razvitiia transformatsionnykh tekhnologii : sb. materialov I Mezhd. nauch.-prakt. konf., Genichesk, 26—28 fevralia 2025 g. SPb. : Naukoemkie tekhnologii, 2025. S. 120. 814 s.
16. Titov K.A. Razrabotka programmy dlia avtomaticheskogo vyiavleniia dipfeikov / K.A. Titov, E.V. Korchemkina, N.L. Kharina // Obshchestvo. Nauka. Innovatsii (NPK-2025). Gumanitarnye, obshchestvennye, fiziko-matematicheskie, komp'iuternye, khimiko-biologicheskie i tekhnicheskie nauki: sb. mat. XXV Vseros. (natsional'noi) nauch.-prakt. konf., Kirov, 22—30 maia 2025 g. Kirov : Viatskii gosudarstvennyi universitet, 2025.
17. Voronov S.A. O podkhodakh v raspoznavanii dipfeikov i sinteticheskikh media / S.A. Voronov, A.D. Kosolapov, A.V. Skrobach // Informatsiia i bezopasnost'. 2025. T. 28. No. 1. S. 103—110.
18. Nikogda D.K. II-sistema dlia obnaruzheniia moshennicheskikh skhem v sotsial'nykh setiakh // Nauchno-tekhnicheskoe i ekonomicheskoe sotrudnichestvo stran ATR v XXI veke. 2025. T. 2. S. 875—880.
19. Direev I.D. Medialingvistika i semiotika: metodologiia analiza mul'timodal'nykh mediatekstov // Aktual'nye voprosy sovremennoi filologii i zhurnalistiki. 2025. No. 2 (57). S. 169—182.
20. Rogovoi V. Razrabotka metoda vyiavleniia dipfeikov: primenenie chastotnogo analiza i umen'sheniia tsvetovogo prostranstva izobrazheniia dlia povysheniia tochnosti klassifikatsii / V. Rogovoi, V.M. Korzhuk, O.A. Kokorina // V Mezhd. konf. po neironnym setiam i neirotekhnologiiam (NeuroNT'2024) : sb. dokl. konf., Sankt-Peterburg, 20 iiunia 2024 g. SPb. : Sankt-Peterburgskii gosudarstvennyi elektrotekhnicheskii universitet LETI, 2024. S. 45—49.
21. Safiullin R.N. Raspoznavanie golosovykh dipfeikov: metody, sfery primeneniia i vliianie // Tendentsii razvitiia sovremennoi nauki v svete issledovanii molodykh uchenykh : sb. statei mezhd. nauch. konf., Vologda, 29 noiabria 2023 g. SPb. : Gumanitarnyi natsional'nyi issledovatel'skii institut "Natsrazvitie", 2023. S. 46—49.
22. Ivanov D.E. Metody i vyzovy v obnaruzhenii dipfeikov // IV Mezhd. nauch. konf. po mezhdistsiplinarnym issledovaniiam : sb. statei, Ekaterinburg, 15 dekabria 2023 g. Ekaterinburg: OOO "Institut Tsifrovoi Ekonomiki i Prava", 2023. S. 462—466.