- ПРАВА ЧЕЛОВЕКА -

Дата поступления рукописи в редакцию: 08.10.2025 г.
Дата принятия рукописи в печать: 02.11.2025 г.
DOI: 10.24412/2782-3830-2025-10-38-44

РЫБИН Михаил Дмитриевич,
аспирант кафедры
конституционного и муниципального права
Университета имени О.Е. Кутафина,
e-mail: misharibin14@gmail.com
Научный руководитель:

ТАЕВА Наталья Евгеньевна,
доктор юридических наук, доцент,
профессор кафедры конституционного и муниципального права
Университета имени О.Е. Кутафина (МГЮА),
e-mail: mail@law-books.ru

ЗАЩИТА ПРАВА НА ДОСТОИНСТВО ЛИЧНОСТИ ПРИ ИСПОЛЬЗОВАНИИ НЕЙРОННЫХ СЕТЕЙ: ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ

Аннотация. *Данное исследование анализирует проблемы защищенности, которые формируются при сохранении приватных материалов в ходе использования диалоговых систем, созданных на основе нейронных сетей. В научной работе рассматриваются потенциальные модели нарушения сохранности информации и анализируются технические и правовые особенности удаления данных из истории диалогов с искусственным интеллектом. Результаты проведенного анализа выявили необходимость разработки результативных механизмов, обеспечивающих конфиденциальность обрабатываемой информации.*

Ключевые слова: *нейронные сети, детальное обучение, конфиденциальность данных, защита персональной информации, уязвимости нейронных сетей, достоинство, безопасность в чат-ботах.*

RYBIN Mikhail Dmitrievich,
Postgraduate student in the Department
of Constitutional and Municipal Law
at O.E. Kutafin Moscow State Law University (MSAL)

TAEVA Natalya Evgenievna,
Doctor of Law, Associate Professor, Professor,
Department of Constitutional and Municipal Law,
O.E. Kutafina University (MSLA)

PROTECTING THE RIGHT TO PERSONAL DIGNITY WHEN USING NEURAL NETWORKS: PRIVACY ISSUES

Annotation. *This article analyzes the security issues that are formed when preserving private materials during the use of dialog systems based on neural networks. The scientific work examines potential patterns of information security breaches and analyzes the technical and legal features of deleting data from the history of dialogues with artificial intelligence. The results of the analysis revealed the need to develop effective mechanisms to ensure the confidentiality of processed information.*

Key words: *neural networks, deep learning, data confidentiality, protection of personal information, vulnerabilities of neural networks, dignity, security in chatbots.*

Введение

Современный этап технологического прогресса характеризуется активным развитием систем искусственного интеллекта, что способствует масштабному внедрению нейросетевых технологий в различные сферы профессиональной деятельности и частной жизни. Значительную популярность приобрела языковая модель ChatGPT, созданная компанией OpenAI, которая ранее добавила возможность сохранения истории диалогов. Однако отсутствие адекватного договорно-правового регулирования применения нейросетевых технологий приводит к многочисленным случаям несанкционированного распространения конфиденциальной информации и персональных данных. Использование этой информации в противоправных целях причиняет вред лицу, чье право на неприкосновенность частной жизни было нарушено, а также создает правовые риски для пользователей, сформулировавших запросы, поскольку их действия могут быть квалифицированы как неправомерная передача конфиденциальных сведений [13, с. 291]. Целью настоящей работы является анализ уязвимостей систем хранения информации нейронными сетями и выработка предложений по совершенствованию режима защиты приватных сведений.

Для ее достижения в исследовании были поставлены задачи: 1) проанализировать существующие правовые риски, возникающие при обработке персональных данных при использовании нейронных сетей; 2) классифицировать и описать методы утечки данных из языковых моделей с учетом международных стандартов кибербезопасности; 3) изучить актуальные технические протоколы и специализированные методики обеспечения конфиденциальности данных; 4) сформулировать рекомендации по развитию российского законодательства в области защиты права на достоинство личности и неприкосновенность частной жизни при использовании нейронных сетей.

Научная новизна исследования заключается в междисциплинарном синтезе технических и правовых особенностей защиты права на достоинство личности при использовании нейронных сетей. Благодаря исследованию криптографических и алгоритмических протоколов защиты конфиденциальности и анализу национального законодательства РФ в работе выявляется взаимосвязь между рассматриваемыми сферами. Продемонстрировано, как технические особенности нейронных сетей такие как отсутствие анонимности пользователя создают угрозу конституционному праву на достоинство личности.

Методологическая основа

Исследование основывается на совокупности общенаучных и частноправовых методов. В числе общенаучных методов использовались анализ научной литературы и официальных документов, изучение международных стандартов кибербезопасности (в частности, OWASP Top 10 for Large Language Model Applications), а также сравнительный анализ протоколов обеспечения конфиденциальности в машинном обучении, как, например, дифференциальная приватность, федеративное обучение и гомоморфное шифрование. Частноправовой метод был реализован через анализ нормативно-правовых актов Российской Федерации: Федеральных законов «О персональных данных», «О коммерческой тайне» и «Об информации». Материалами для исследования также послужили публикации, освещающие случаи утечек данных в крупных языковых моделях.

Основные проблемы и риски

Персональные данные представляют собой совокупность сведений, прямо или косвенно определяющих конкретное физическое лицо. К ним относятся имя, отчество, адрес места жительства, контактные телефоны, реквизиты документов, удостоверяющих личность, финансовые операции, биометрические параметры и другая информация. В соответствии с п. 1 ч. 1 ст. 6 Федерального закона «О персональных данных» [1] обработка перечисленных сведений допускается исключительно при наличии разрешения субъекта. Схожий правовой режим устанавливается для коммерческой тайны, доступ к которой не может быть предоставлен без разрешения ее правообладателя согласно п. 1 ч. 5 ст. 10 Федерального закона «О коммерческой тайне» [2]. В процессе взаимодействия с системами искусственного интеллекта пользователь часто сообщает сведения, содержащие его личные или коммерческие тайны. Нейронная сеть не реализует процедуру получения согласия на обработку подобных данных, из-за чего возникает правовой вакуум. Введенная информация инкорпорируется в саму конструкцию алгоритма, а у пользователя отсутствует техническая возможность для ее самостоятельного и полного удаления [13, с. 291].

Логические операции, выполняемые компьютерной системой, формализуются при помощи специальных языков программирования. Созданные алгоритмы демонстрируют значительное разнообразие, начиная с элементарных математических действий и заканчивая сложными процессами шифрования или прогнозиро-

вания экономических тенденций. Основная проблема состоит в трансформации персональных данных моделью машинного обучения, которая лишает субъекта возможности осуществлять контроль над их использованием. Сохраняется реальная опасность несанкционированного разглашения конфиденциальных данных. В случае недостаточной анонимизации информации на этапе обучения модели, злоумышленник способен применить специализированное программное обеспечение и методики анализа нейросетей для сопоставления генерируемых ответов с дополнительными данными и позднее восстановить приватные сведения.

Реальные примеры инцидентов

Рассмотрим несколько примеров нарушений конфиденциальности данных в сфере машинного обучения. В 2019 г. компания Google в рамках проекта «Nightingale» начала сотрудничество с сетью медицинских учреждений Ascension. В рамках проекта без уведомления пациентов осуществлялись сбор, обработка, и передача медицинских данных, включая имена, диагнозы, результаты лабораторных исследований, историю госпитализаций и других данных более 50 миллионов пользователей. Указанные сведения использовались в том числе для обучения нейросетей в целях автоматизации ведения медицинской документации, разработки инструментов анализа, прогнозирования, поддержки клинических решений. Отсутствие прозрачности и информированного согласия вызвало значительно общественный резонанс, а также расследование со стороны Министерства здравоохранения и социальных служб США. Инцидент продемонстрировал правовые и этические риски масштабной цифровизации различных сфер человеческой жизни, а также использования технологий машинного обучения [11].

В 2025 году была обнаружена утечка в рамках крупнейшей в мире нейросети «DeepSeek». В оставленной без защиты базе данных находились незашифрованные переписки пользователей, ключи API, системные логи и внутренние документы. Несмотря на то, что компания немедленно устранила данную проблему, данный инцидент поставил под угрозу конфиденциальность данных и право на достоинство миллионов пользователей платформы [3].

С 2019 по 2024 год компания Clearview AI осуществляла сбор, обработку, анализ изображений пользователей без их согласия для создания системы распознавания лиц. Цифровые данные включали фотографии, которые позволяли идентифицировать пользователей, а также информацию о времени и месте съемки. Накопленные данные использовались для обучения нейросети с целью повышения точности идентификации лиц для правоохранительных органов и частных компаний. Отсутствие прозрачности в ходе сбора и обработки информации привело к многочисленным расследованиям в отношении компании и штрафам со стороны регулирующих органов в Европе и США [9].

Указанные инциденты демонстрируют системные уязвимости и риски, присущие сбору и хранению значительных объемов личных данных для развития алгоритмов машинного обучения.

Механизмы утечки данных: анализ уязвимостей

Специалисты по защите информации выделяют основные каналы утечки данных при использовании нейросетевых сервисов. Среди основных рисков, описанных в руководстве OWASP Top 10 for Large Language Model Applications, можно выделить три следующих [6].

Первый риск – «Непреднамеренное раскрытие данных» – заключается в том, что нейросеть предоставляет пользователю данные другого пользователя. Причины подобных нарушений разнообразны, но основной признается некачественная анонимизация обучающих данных.

Второй риск представляет собой целенаправленные атаки «Инжектирование промптов», которые направлены на обход системных фильтров для получения конфиденциальной информации. Злоумышленник использует специально разработанные запросы, заставляющие алгоритм игнорировать ограничения, установленные разработчиками. Успешная атака может привести к раскрытию внутренних инструкций системы.

Потенциальная утечка сведений из массива данных для обучения представляет собой третью значительную проблему. Проникновение конфиденциальных сведений в тренировочный набор напрямую создает предпосылки для их последующего разглашения в ходе практического применения искусственного интеллекта. Как отмечает М.К. Редчиц, данный вид утечки также «относится к процессу дообучения модели, когда модель дополнительно обучают на корпоративных данных, необходимых для создания, например, чатбота консультанта» [14, с. 120].

Существующие и перспективные протоколы защиты

В числе специализированных механизмов, направленных на обеспечение конфиденциальности обучающих данных нейросетевых моделей, проект OWASP Top 10 for Large Language Model Applications выделяет несколько технологических решений, которые способствуют повышению уровня безопасности информационных масси-

вов, задействованных для тренировки алгоритмов искусственного интеллекта. К их числу относят федеративное обучение, организующее процесс на децентрализованных данных без их физического объединения, и дифференциальная приватность, которая вносит статистический «шум» в исходные массивы для блокирования попыток реинжиниринга. Дополнительные меры охватывают обучение конечных пользователей, обеспечение открытости процессов обработки информации и применение безопасных конфигураций программно-аппаратных комплексов. Более сложные методы защиты содержат гомоморфное шифрование, позволяющее производить вычисления с зашифрованными данными, токенизацию и процедуры целенаправленного редактирования обучающих выборок [14, с. 122].

Защита нейросетевых систем от кибератак требует применения специальных методов, обеспечивающих конфиденциальность данных на всех этапах работы алгоритма. Они формируют дополнительные барьеры для злоумышленников, пытающихся получить несанкционированный доступ к нейронным сетям. К числу наиболее действенных и распространенных можно отнести четыре следующих протокола:

Протокол дифференциальной приватности представляет собой систему, позволяющую осуществлять публичное распространение информации о массиве данных через описание групповых моделей при одновременном сокрытии сведений об отдельных людях. Каждый участник вычислительной процедуры размещает индивидуальную реализацию нейронной сети и выборочно интегрируется в отдельные сегменты общих вычислений [10, с. 1162]. Протокол одновременно функционирует на разнородных вычислительных платформах, а итоговый продукт формируется через консолидацию результирующих данных от всех участников. Для гарантии приватности пользователей применяется алгоритм DP, который обеспечивает независимую обработку информации, организует коммуникацию между нейросетевой моделью и различными узлами хранения и исключает совместное применение первоначальных данных.

Протокол SecureML обеспечивает защиту конфиденциальности в системах обмена данными и структурных элементах нейросетевых моделей посредством применения методов гомоморфного шифрования, схем обязательств и механизмов секретного распределения. Его разработка решает задачу обучения облачных сервисов на информации от множества пользователей без нарушения политики приватности [5]. SecureML задействует специальную функцию пользовательской активации для тренировки нейронной сети с использованием защищенных процедур аутентификации. Как следует из исследования С. Шарма и К. Чен К, результатом работы становится сетевая модель, фрагменты которой распределяются между отдельными пользовательскими профилями. Она подлежит последующему коллективному применению всеми участниками платформы с гарантированным соблюдением режима конфиденциальности передаваемой информации [8, с. 2295].

Протокол компании MiniONN позволяет трансформировать стандартную нейросеть в «незаметную» версию, минимизируя риски для конфиденциальности. Согласно мнению специалистов Цзянь Лю и Яо Лу, реализация протокола основана на применении гомоморфного шифрования на стадии офлайн-обработки через схему обязательств и метод секретного разделения на серверной стороне, обеспечивая режим взаимной неинформированности между клиентом и сервером относительно обрабатываемых данных друг друга [4, с. 29].

Протокол DeepSecure представляет собой технологическое решение для защиты конфиденциальных сведений при анализе с применением моделей глубинного обучения. Согласно исследованию Б.Д. Рухани, в его основе лежат схемы обязательств. Разработчики внедрили метод предварительной оптимизации данных и архитектуры нейросети, что ведет к ускорению вычислительных операций [7, с. 3-4]. Упомянутая подготовительная стадия является независимой от основного процесса обработки и может выполняться любым сегментом серверной инфраструктуры. Кроме того, протокол DeepSecure обеспечивает возможность безопасного делегирования управления учетными записями на вспомогательный сервер для клиентов, обладающих ограниченными техническими ресурсами.

Подводя итог, защита персональных сведений, задействованных при обучении нейронных сетей, представляет собой актуальную проблему, которая требует совместных усилий создателей технологий и законодателей. В Российской Федерации разработка действенных правовых инструментов для регулирования цифровых отношений имеет первостепенное значение. Государство последовательно развивает законодательное поле цифровой экономики, стремясь создать единые правовые принципы ко всем видам цифровых технологий в рамках федерального законодательства.

Одним из инструментов преобразования регулирования цифровых отношений выступают экспериментальные правовые режимы. Традиционная система правового регулирования часто не справляется с задачами в условиях быстрого распространения цифровых новшеств. Объективная потребность в государственном регулиро-

вании и контроле над этими процессами сохраняет свою остроту. Специальное регулирование в инновационной цифровой сфере, согласно зарубежной практике, демонстрирует высокую результативность и позволяет государству в рамках локальных экспериментальных режимов оценить действенность правовых норм для конкретных цифровых нововведений [12, с. 35]. В докладе Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека, который посвящен цифровой трансформации и защите прав граждан в цифровом пространстве 2.0, содержится положение, о том, что для успешной реализации стратегического курса цифрового развития и достижения целей по охране свобод человека в виртуальной среде требуется принятие специального кодифицированного акта. Создание Цифрового кодекса рассматривается в качестве основного метода для систематизации правовых норм, регулирующих отношения в цифровой области Российской Федерации [15]. Предложенный кодифицированный акт призван установить фундаментальные принципы и механизмы защиты прав человека в цифровом пространстве и инструменты обеспечения информационной безопасности государства. Формирование кодекса предлагается осуществлять поэтапно: первоначально через внесение поправок в действующее законодательство с последующей консолидацией в самостоятельный нормативный акт.

Кроме того, согласование технологических и правовых мер требует учреждения института «правозащитного аудита» и проведения независимой экспертизы цифровых технологий и систем хранения информации. Параллельно с этим необходимо повышать степень участия институтов гражданского общества в разработке документов стратегического планирования, относящихся к сфере цифровых технологий.

Результаты исследования

Развитие и внедрение нейросетей в различные сферы человеческой жизни и деятельности является общемировой тенденцией, которую невозможно остановить или игнорировать. Надлежащее использование и правовое регулирование нейросетей связано с рядом преимуществ, включая автоматизацию рутинных задач, повышение точности и скорости обработки данных, развитие новых отраслей экономики, улучшение качества жизни, оптимизацию производственных процессов и др. Однако, как показывают рассмотренные ранее примеры, исследуемые технологии связаны со значительными рисками для конституционных прав человека. Использование нейросетей возможно исключительно при условии обеспечения надлежащего уровня правовых гарантий, а также разработки и использования актуальных способов защиты информации. Научное сообщество и разработчики технологий должны прилагать совместные усилия в вышеуказанном направлении.

Важно отметить, что широкое распространение алгоритмов машинного обучения, особенно в системах, обрабатывающих большие объемы конфиденциальной информации, делает необходимым внедрение специализированных механизмов защиты, часть из которых была рассмотрена в ходе исследования. Применение устаревших средств безопасности не может считаться эффективной стратегией для систем на основе ИИ в условиях постоянного появления новых и усложнения существующих методов атак. При этом важно также учитывать, что использование даже современных криптографических протоколов, обеспечивающих конфиденциальность данных, не всегда защищает от уязвимостей, которые вызваны фундаментальной ограниченностью встроенных защитных механизмов нейросетевых архитектур.

Для преодоления выявленных в ходе исследования системных недостатков предлагается реализация следующих мер:

В качестве первоочередной законодательной инициативы возможно введение процедуры, обязывающей получать предварительное информированное согласие гражданина на использование нейросетевых технологий для обработки его персональных данных. Их изменение, являющиеся результатом работы алгоритмов искусственного интеллекта, также должны производиться с ведома и согласия субъекта. Кроме того, закон должен гарантировать каждому лицу право на доступ к актуальной версии его персональных данных и возможность их проверки.

Второй мерой выступает законодательное закрепление обязательности применения специального «шума» на этапе обучения, чтобы невозможно было идентифицировать отдельного человека, но сохранялись общие статистические закономерности.

В-третьих, в качестве дополнительной правовой гарантии, предлагается введение института обязательного независимого внешнего аудита и сертификации систем искусственного интеллекта, отнесенных к категории повышенного риска. Это предполагает создание разработчиками новых систем, обеспечивающих возможность контроля их функционирования физическими лицами, гарантирующих целевое использование и позволяющих нейтрализовать потенциальные негативные последствия на всех этапах жизненного цикла языковой модели.

Заключение

Проведенное исследование позволяет сделать следующий вывод – обеспечение защиты права на достоинство личности в цифровую эпоху требует скоординированных усилий законодателей, разработчиков и научного сообщества. Последовательная имплементация предложенных мер в рамках стратегии цифровой трансформации и разрабатываемого Цифрового кодекса позволит минимизировать существующие угрозы приватности и заложить основу для этичного и безопасного развития искусственного интеллекта в России.

Список литературы:

[1] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

[2] Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 08.08.2024) «О коммерческой тайне» // Собрание законодательства РФ. – 2004. – № 32. – Ст. 3283.

[3] База данных китайской нейросети DeepSeek оказалась в открытом доступе [Электронный ресурс] // URL: https://www.rbc.ru/life/news/679b32609a7947536994a238 (дата обращения: 26.09.2025).

[4] Liu J. et al. (2017) Oblivious neural network predictions via minionn transformations // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communi-cations Security. – C. 619-631.

[5] Mohassel P., Zhang Y. Secureml (2017), A system for scalable privacy-preserving machine learning // 2017 IEEE Symposium on Security and Privacy (SP). – IEEE – C. 19-38.

[6] OWASP Top 10 for Large Language Model Applications [Электронный ресурс] // URL: https://owasp.org/www-project-top-10-for-large-language-model-applications/ (дата обращения: 26.09.2025).

[7] Rouhani B. D., Riazi M. S., Koushanfar F. Deepsecure: (2018) Scalable provably-secure deep learning // Proceedings of the 55th Annual Design Automation Conference. – C. 1-6.

[8] Sharma S., Chen K. (2018). Privacy-preserving boosting with random linear classifiers // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security – C. 2294-2296.

[9] Фирма Clearview собрала в соцсетях миллиарды фото лиц [Электронный ресурс] // URL: https://www.bbc.com/russian/features-65090432 (дата обращения: 29.09.2025).

[10] Вавилова, А. С. Обзор существующих механизмов обеспечения конфиденциальности данных в системах на основе машинного обучения // Инновации. Наука. Образование. – 2021. – № 36. – С. 1159-1167.

[11] Google's secret cache of medical data includes names and full details of millions [Электронный ресурс] // URL: https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information (дата обращения: 26.09.2025).

[12] Минбалеев, А. В. Трансформация регулирования цифровых отношений // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2019. – № 12. – С. 31-36.

[13] Мустаева, Д. Р. Проблемы правовой защиты конфиденциальной информации и персональных данных при использовании нейронных сетей // Аграрное и земельное право. – 2024. – № 12. URL: https://cyberleninka.ru/article/n/problemy-pravovoy-zaschity-konfidentsialnoy-informatsii-i-personalnyh-dannyh-pri-ispolzovanii-neyronnyh-setey (дата обращения: 25.09.2025).

[14] Редчиц, М. К., Мельников Д.В. Безопасность персональных данных, на которых были обучены нейросети // Молодежь. Наука. Инновации. – 2025. – Т. 1. – С. 118-122.

[15] Цифровая трансформация и защита прав граждан в цифровом пространстве 2.0. Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека. – Москва, 2025 [Электронный ресурс] // URL: https://sovet-nko.ru/files/2025/06/doklad-spch-po-pch-v-tsifre-2.0-2025-06-27_15-54-14_624644.pdf (дата обращения: 29.09.2025).

References:

[1] Federal Law No. 27.07.2006 dated 152-FZ (as amended by 24.06.2025) " On Personal Data "// Collection of Legislation of the Russian Federation. – 2006. - No. 31 (1 hour). - Art. 3451.

[2] Federal Law of 29.07.2004 No. 98-FZ (as amended by 08.08.2024) " On Trade Secrets "//Collection of Legislation of the Russian Federation. – 2004. – № 32. - Art. 3283.

[3] The database of the Chinese neural network DeepSeek was in the public domain [Electronic resource]//URL: https://www.rbc.ru/life/news/679b32609a7947536994a238 (access date: 26.09.2025).

[4] Liu J. et al. (2017) Oblivious neural network predictions via minionn transformations // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communi-cations Security. - S. 619-631.

[5] Mohassel P., Zhang Y. Secureml (2017), A system for scalable privacy-preserving machine learning // 2017 IEEE Symposium on Security and Privacy (SP). - IEEE - PP. 19-38.

[6] OWASP Top 10 for Large Language Model Applications [Электронный ресурс] // URL: https://owasp.org/www-project-top-10-for-large-language-model-applications/ (дата обращения: 26.09.2025).

[7] Rouhani B. D., Riazi M. S., Koushanfar F. Deepsecure: (2018) Scalable provably-secure deep learning // Proceedings of the 55th Annual Design Automation Conference. - S. 1-6.

[8] Sharma S., Chen K. (2018). Privacy-preserving boosting with random linear classifiers // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security – С. 2294-2296.

[9] Clearview has collected billions of photos of people on social networks [Electronic resource]// URL: https://www.bbc.com/russian/features-65090432 (contact date: 29.09.2025).

[10] Vavilova, A. S. Review of existing data privacy mechanisms in machine learning-based systems//Innovations. Science. Education. – 2021. – № 36. - S. 1159-1167.

[11] Google's secret cache of medical data includes names and full details of millions [Электронный ресурс] // URL: https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information (дата обращения: 26.09.2025).

[12] Minbaleev, A.V. Transformation of the regulation of digital relations//Bulletin of the University named after O.E. Kutafina (MSLA). – 2019. – № 12. - S. 31-36.

[13] Mustaeva, D. R. Problems of legal protection of confidential information and personal data when using neural networks//Agrarian and land law. – 2024. – № 12. URL: https://cyberleninka.ru/article/n/problemy-pravovoy-zaschity-konfidentsialnoy-informatsii-i-personalnyh-dannyh-pri-ispolzovanii-neyronnyh-setey (дата обращения: 25.09.2025).

[14] Redchits, M.K., Melnikov D.V. Security of personal data on which neural networks were trained//Youth. Science. Innovation. – 2025. - VOL. 1. - S. 118-122.

[15] Digital Transformation and Protection of Citizens' Rights in the Digital Space 2.0. Report of the Presidential Council on the Development of Civil Society and Human Rights. - Moscow, 2025 [Electronic resource]//URL: https://sovet-nko.ru/files/2025/06/doklad-spch-po-pch-v-tsifre-2.0-2025-06-27_15-54-14_624644.pdf (accessed: 29.09.2025).

