МИНОБРНАУКИ РОССИИ
Институт проблем передачи информации им. А.А. Харкевича РАН
Юго-Западный государственный университет
Институт программных систем им. А.К. Айламазяна РАН
Институт информационных технологий, Баку, Азербайджан

ОБЛАЧНЫЕ И РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

ОРВС – 2023

В РАМКАХ

НАЦИОНАЛЬНОГО СУПЕРКОМПЬЮТЕРНОГО ФОРУМА (НСКФ – 2023)

Сборник трудов 4-й международной научно-технической конференции

28 ноября – 1 декабря 2023 года

Редакционная коллегия:
И.И. Курочкин, Э.И. Ватутин, А.П. Афанасьев,
Р.М. Алгулиев, И.Н. Григоревский

Переславль-Залесский 2024

УДК 621.383.68.3: 681.785
ББК 32.971.35

Редакционная коллегия:
И.И. Курочкин, кандидат технических наук;
Э.И. Ватутин, доктор технических наук, доцент;
А.П. Афанасьев, доктор физико-математических наук, профессор;
Р.М. Алгулиев, действительный член НАНА Азербайджана,
доктор технических наук, профессор;
И.Н. Григоревский, кандидат технических наук, доцент.

Облачные и распределенные вычислительные системы в электронном управлении. ОРВС – 2023: сборник трудов 4-й международной научно-технической конференции (28 ноября – 1 декабря 2023 года) / ред. кол.: И.И. Курочкин [и др.]; ИПС РАН. Переславль-Залесский. – Курск: Изд-во ЗАО «Университетская книга», 2024. - 127 с.

ISBN 978-5-00261-018-1
DOI 10.47581/2024.Oblokj-Raspredelenie-OPBC-2023

Сборник содержит труды 4-й международной научно-технической конференции «Облачные и распределенные вычислительные системы» (Переславль-Залесский, 28 ноября – 1 декабря 2023), проводимой в рамках Национального суперкомпьютерного форума (НСКФ – 2023). Целью конференции является ознакомление с имеющимися достижениями по созданию облачных и распределенных вычислительных систем и их внедрение в научные исследования, учебный процесс и промышленность.

Сборник предназначен для научных сотрудников, преподавателей, аспирантов и студентов вузов.

Издание осуществлено с авторских оригиналов.

Редакция не несет ответственности за ошибки авторов.

Материалы для публикации одобрены программным комитетом Международной научно-технической конференции.

ISBN 978-5-00261-018-1

УДК 621.383.68.3: 681.785
ББК 32.971.35

© Институт проблем передачи информации им. А.А. Харкевича РАН;
© Юго-Западный государственный университет;
© Институт программных систем им. А.К. Айламазяна РАН;
© Институт информационных технологий, Баку, Азербайджан, 2024

Содержание

1. Hochreiter S., Schmidhuber J. Long short-term memory // Neural computation. Vol. 9, № 8. 1997. pp. 1735-1780.
2. Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. Deep learning. MIT press, 2016.
3. Nielsen M. A. Neural networks and deep learning. San Francisco, CA, USA: Determination press. Vol. 25. 2015. pp. 15-24.
4. Goodfellow I. et al. Deep Learning-Ian Goodfellow, Yoshua Bengio, Aaron Courville // Adapt. Comput. Mach. Learn. 2016.
5. Alguliyev R. M., Aliguliyev R. M., Abdullayeva F. J. Deep learning method for prediction of DDoS attacks on social media // Advances in Data Science and Adaptive Analysis. Vol. 11, №. 01n02. 2019. pp. 1950002.
6. Gers F. A., Schmidhuber J., Cummins F. Learning to forget: Continual prediction with LSTM // Neural computation. Vol. 12. №. 10. 2000. pp. 2451-2471.
7. Schmidhuber J. Deep learning in neural networks: An overview // Neural networks. Vol. 61. 2015. pp. 85-117.

Махмудова Р.Ш.

Институт информационных технологий, Баку, Азербайджан

УГРОЗЫ ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, СОЗДАВАЕМЫЕ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ, И МЕТОДЫ ИХ СНИЖЕНИЯ

Аннотация. В результате широкого применения технологий нового поколения, таких как искусственный интеллект, в обществе происходят большие изменения. Возможности искусственного интеллекта уже широко используются в финансах, национальной безопасности, здравоохранении, транспорте, сельском хозяйстве, городском управлении и других сферах. Применение искусственного интеллекта в значительной степени способствует социально-экономическому развитию общества и приводит к ряду положительных изменений в плане повышения производительности труда, снижения затрат на рабочую силу, оптимизации структуры человеческих ресурсов и создания новых рабочих мест. Но, как и все технологические инновации, искусственный интеллект имеет ряд негативных последствий и проблем. Одна из проблем, создаваемых искусственным интеллектом, связана с безопасностью персональных данных. В статье анализируются проблемы, создаваемые искусственным интеллектом, связанные с безопасностью персональных данных и методы их снижения.

Ключевые слова: искусственный интеллект, угрозы, защита персональных данных, конфиденциальность.

Введение

В настоящее время технологии искусственного интеллекта позволяют получать полезные знания из больших объемов информации. Например, с помощью камер он следит за нарушителями дорожного движения, распознает преступников из толпы, диагностирует заболевания и прогнозирует распространение вирусов.

Кроме того, искусственный интеллект лежит в основе рекомендательных сервисов для интернет-магазинов, голосовых помощников, фильтрует контент, пишет сценарии и даже музыку для фильмов, распознает речь и лица людей. Компании все чаще используют чат-боты для общения с клиентами через Интернет. Анализируя поведение потребителей и заранее прогнозируя спрос людей, искусственный интеллект позволяет предприятиям зарабатывать огромные суммы денег.

Помимо всех этих преимуществ, искусственный интеллект создает обществу ряд проблем. К потенциальным рискам, создаваемым искусственным интеллектом, эксперты относят технические проблемы, проблемы безопасности, проблемы совместимости, отсутствие прозрачности, юридические и этические проблемы, социально-экономическое неравенство и другие проблемы.

Опубликовано письмо некоммерческой организации Future of Life, подписанное генеральным директором Tesla, SpaceX и Twitter (X) Илоном Маском, соучредителем Apple Стивом Возняком, соучредителем Pinterest Эваном Шарпом и более тысячи экспертов в области искусственного интеллекта. В петиции говорится, что системы с интеллектом, сравнимым с человеческим, представляют большой риск для общества. Они настаивают на приостановке внедрения технологий искусственного интеллекта до тех пор, пока не будут созданы общие протоколы безопасности [1].

Джеффри Хинтон, один из основателей нейронных сетей, после ухода из Google пополнил ряды тех, кто считает развитие искусственного интеллекта угрозой для человечества. По его словам, Интернет будет наполнен контентом (фото, видео, тексты), созданным искусственным интеллектом, и люди не смогут отличать правдивую информацию

от ложной. В то же время он заявил, что технологии со временем изменят рынок труда и заменят людей в некоторых областях.

Поэтому считается, что для устойчивого развития этих технологий очень важно установить принципы и стандарты, которые помогут в первую очередь обеспечить безопасное и этичное использование искусственного интеллекта.

Угрозы безопасности персональных данных

Сбор и распространение больших объемов данных является одним из важных факторов развития технологий искусственного интеллекта. Однако сбор, интеграция и анализ больших объемов данных о физических лицах приводит к сужению сферы конфиденциальности. В настоящее время сбор данных осуществляется способами, которые обычный человек даже не может себе представить. Во многие потребительские товары (бытовая техника, детские игрушки, автомобили, трекеры здоровья, телефоны и т.д.) уже встроен искусственный интеллект. Все эти продукты передают данные, в том числе персональные, на облачные платформы своих производителей, разработчиков ПО и сервисных компаний.

В какой степени гарантируется конфиденциальность передаваемых данных? Наблюдения показывают, что случаев передачи собранных данных третьим лицам достаточно. Конфиденциальность в своей самой простой форме — это право любого человека не подвергаться слежке. Люди используют разные методы для защиты своей конфиденциальности, например, закрывать двери, вешать шторы на окна, носить солнцезащитные очки, использовать в некоторых религиях закрытую одежду и т.д. [2]. Конфиденциальность важна по нескольким причинам: она позволяет людям принимать собственные решения без принуждения, совершать решения и действия, не соответствующие определенным социальным нормам. Обеспечение конфиденциальности связано с вопросом неприкосновенности частной жизни.

Конфиденциальность уже давно является спорным вопросом между правительством и гражданами. Точно так же, как люди традиционно борются за право не подвергаться слежке, правительства часто борются за право слежки за своими гражданами.

Сбор персональных данных значительно облегчили такие технологии как Интернет, смартфоны, камеры видеонаблюдения и т.д. Сегодня в принципе можно отслеживать каждый шаг пользователей, даже еду, которую они едят в ресторане. Люди фотографируют места, где они находятся, и еду, которую они едят в ресторанах и выкладывают их в Интернет. Большая часть этих данных теперь загружается в облачные сервера, что значительно расширяет возможности отслеживания персональных данных.

Более того, добровольно загружая свои персональные данные на эти платформы, пользователи социальных сетей невольно передают авторские права на эти данные провайдеру платформы. Facebook и другие сети владеют этими данными, используют их и даже продают другим [3].

Одним из факторов успеха Google в сборе персональных данных является то, что люди не могут скрыть свои интересы при поиске информации. В обычной жизни многие люди вынуждены вводить соответствующие термины в строку поиска, чтобы получить информацию по теме из Интернета, скрывая при этом информацию, касающуюся деликатных личных вопросов. В результате в Интернете собираются даже самые сокровенные желания и сомнения пользователей.

В эпоху искусственного интеллекта конфиденциальность становится очень сложной проблемой. Поскольку и государство, и различные компании собирают и анализируют большой объем данных, в результате личная информация людей подвергается большому риску.

Системы искусственного интеллекта предназначены для обучения и совершенствования путем анализа больших объемов данных. В результате объем персональных данных, собираемых системами искусственного интеллекта, продолжает расти, что вызывает обеспокоенность по поводу конфиденциальности и защиты данных. Чтобы понять, как используются наши данные (статьи, изображения, видео и т.д.) достаточно рассмотреть принципы работы ChatGPT, Stable Diffusion и других генеративных инструменов искусственного интеллекта [4]. Создание нового информационного продукта этими инструментами происходит без согласия и участия владельца информации, что приводит к нарушению авторских прав и создает ряд угроз безопасности.

Еще одна проблема использования персональных данных в системах искусственного интеллекта заключается в том, что этот процесс непрозрачен. Поскольку алгоритмы, используемые в этих системах, сложны, обычные люди не понимают, как их данные используются при принятии решений. Эксперты полагают, что отсутствие прозрачности заставляет людей чувствовать себя неловко и не доверять системам ИИ [3,4].

В плане конфиденциальности еще одна проблема, возникающая при применении технологий искусственного интеллекта, заключается в том, что за человеком постоянно ведется слежка. Системы наблюдения на основе искусственного интеллекта открывают широкие возможности для деятельности правоохранительных органов. С другой стороны, это противоречит принципам конфиденциальности и гражданских свобод.

Известно, что компания Google отслеживает местоположение своих пользователей, даже если они не давали явного разрешения на раскрытие своего местоположения. Одной из самых больших проблем, связанных с практикой отслеживания местоположения Google, является потенциальное неправомерное использование персональных данных. Данные о местоположении невероятно чувствительны, и если они попадут в чужие руки, их можно использовать для отслеживания перемещений людей, наблюдения за их поведением и даже для преступной деятельности.

В настоящее время широко используются системы «умный дом». Эти системы и даже отдельные устройства постоянно собирают информацию об оффлайн-действиях, происходящих дома у пользователя. Такой тип сбора данных часто происходит из-за незнания пользователей и пренебрежения конфиденциальностью информации. Вызывает большую обеспокоенность тот факт, что технологии искусственного интеллекта могут быть использованы преступниками. Например, используя эти технологии для манипулирования общественным мнением и распространения дезинформации, вы можете создавать фейковые изображения и фейковые видео.

Киберпреступники уже используют нейронные сети, называемые «Deep fake», для создания откровенно сексуального контента в целях шантажа. Даже в даркнете предлагаются инструменты и сервисы для создания «глубоких фейков». Эти услуги включают создание видео на основе искусственного интеллекта для различных целей, таких как мошенничество, шантаж и кража конфиденциальной информации. Цена минуты такого видео варьируется от 300 до 20 тысяч долларов [5].

Система VoCo, представленная Adobe в 2016 году, может прослушивать разговор около 20 минут и имитировать голос любого говорящего человека. Такие технологии крайне опасны с точки зрения конфиденциальности [3]. Например, мошенники использовали этот метод, имитируя голос главы британской энергетической компании, велевшего генеральному директору одной из дочерних компаний компании срочно отправить 220 000 евро, и сумели перевести указанную сумму.

Способы снижения опасности искусственного интеллекта

Решение проблем, связанных с технологиями искусственного интеллекта, в настоящее время волнует весь мир. На ряде реальных примеров видно, что бесконтрольное

использование искусственного интеллекта может привести к негативным результатам. Потенциальные угрозы искусственного интеллекта для общества можно уменьшить несколькими способами.

Правовое и этическое регулирование. В целях обеспечения защиты персональных данных принимаются законодательные акты, регулирующие контроль за персональными данными. Первой страной, принявшей закон в этой области, были США – «Закон о конфиденциальности», принятый в 1974 году. В Европе в 1981 году была открыта для подписания Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Конвенция № 108). В настоящее время в европейских странах и большинстве стран мира действуют национальные законы, касающиеся регулирования персональных данных. К одной из реакций на увеличение оборота персональных данных и случаев их утечки следует отнести утверждение единого регламента General Data Protection Regulation (далее – GDPR), который с 2018 г. распространяется на все страны, входящие в Евросоюз [6]. Данное постановление существенно расширяет права физических лиц по контролю своих персональных данных и их обработке, а также ужесточает требования к ИТ-компаниям, осуществляющим обработку персональных данных. Это касается и нарушения требований по соблюдению конфиденциальности персональных данных. Крупные штрафы были наложены на такие компании как British AirWays, Google и т.д. [7].

Решение этих проблем требует реализации комплексных мер. В 2021 году Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) опубликовала «Рекомендации по этике искусственного интеллекта» [8]. Он устанавливает первую глобальную нормативную базу, одновременно возлагая на государства ответственность применять ее на своем уровне. Целью Рекомендации является реализация преимуществ, которые ИИ приносит обществу, и снижение рисков, которые он влечет за собой. В нем говорится, что все люди должны иметь возможность получить доступ к своим личным данным или даже стереть их. Он также включает в себя действия по улучшению защиты данных, а также знаний человека и его права контролировать свои собственные данные.

Осведомленность и образование. Одним из важных условий обеспечения защиты персональных данных является повышение уровня информированности людей всех групп населения. Чтобы гарантировать, что общество готово управлять последствиями ИИ, важно, чтобы общественность была информирована о преимуществах и потенциальных рисках ИИ. При этом независимо от специализации очень важно обучение таким темам, как сущность искусственного интеллекта, принципы его работы, области применения, потенциальные риски, связанные с искусственным интеллектом, защита и конфиденциальность персональных данных, юридическая ответственность при использовании искусственного интеллекта, этические вопросы и т.д.

Культура информационной безопасности. Защита персональных данных является проблемой информационной безопасности. С этими проблемами сталкиваются различные предприятия, компании и частные лица. Кража персональных данных может подвергнуть владельца финансовой и моральной опасности [9]. Социальные сети считаются основным источником доступа к личной информации. Пользователи социальных сетей раскрывают информацию о своих интересах, важных событиях, потребностях и зависимостях, тем самым теряя контроль над своей информацией. Кроме того, каждый регистрируется и добровольно предоставляет личную информацию, чтобы воспользоваться различными программами и дополнениями, сервисами.

С этой точки зрения повышение уровня поведения людей с информацией и повышение их культуры информационной безопасности является очень важным вопросом.

Заключение

Очень важно, чтобы компании и политики предприняли необходимые шаги для установления четких руководящих принципов и норм, гарантирующих, что технология искусственного интеллекта разрабатывается и используется таким образом, чтобы соблюдались основные права человека и ценности.

Развитие и применение новых технологий, особенно искусственного интеллекта, в различных сферах приводит к тому, что угрозы конфиденциальности персональных данных считаются одной из основных проблем искусственного интеллекта. Необходимость обеспечения безопасности персональных данных сегодня является реальностью. Не имея культуры информационной безопасности, современный человек не способен противостоять вмешательству в его личную жизнь.

Библиографический список

1. https://habr.com/ru/companies/inferit/articles/745230/
2. J. Van den Hoven. Information technology privacy and the protection of personaldata. In: J. Van den Hoven & J. Weckert (Eds.), Information technology and moralphilosophy (Cambridge studies in philosophy and public policy). Cambridge: CUP, 2008: 301–321.
3. Bartneck, C., Lütge, C., Wagner, A., Welsh, S. Privacy Issues of AI. In: An Introduction to Ethics in Robotics and AI. SpringerBriefs in Ethics. Springer, Cham., 2021, https://doi.org/10.1007/978-3-030-51110-4_8
4. https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/
5. https://ru.rayhaber.com/2023/05/darkwebde-deepfake-olusturma-fiyatlari-dakika-basina-20-bin-dolara-ulasti/
6. Литвин И.И. Особенности сбора, обработки и защиты персональных данных искусственным интеллектом // Вестник Уральского Юридического Института МВД России, 2021, №4, с. 112-118.
7. Соколова М. Е. Первые успехи нового европейского общего Регламента по защите персональных данных // Современная Европа. 2020. № 2. С. 61.
8. Recommendation on the Ethics of Artificial Intelligence, https://unesdoc.unesco.org/ark:/48223/pf0000386510?posInSet=3&queryId=0f54d193-642a-45af-8dcd-14e546cf3628
9. Махмудова Р.Ш. О проблемах формирования культуры информационной безопасности в обществе // Problems of Information Society, 2013, no.1 (7), с. 32-38. (азерб.)