УДК 004.056

А.Ж. НИЗАМОВ[1], А.М. НИЗАМОВА[2]

[1]*Финансовый университет при Правительстве России, Москва*
[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

СОЦИОТЕХНИЧЕСКИЙ ПОДХОД К ЗАЩИТЕ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЕКТА

Искусственный интеллект (ИИ) стал неотъемлемой частью цифрового общества. ИИ обрабатывает массивы данных, в том числе персональных и биометрических, что делает задачу обеспечения приватности крайне важно [1, 2].

Дополнительную угрозу представляют когнитивные воздействия, создаваемые ИИ. Которые могут включать вредоносные закладки, скрытые алгоритмы сбора данных или механизмы влияния на мышление пользователей.

Введение

Искусственный интеллект (ИИ) ускоряет анализ и принятие решений в образовании, здравоохранении и управлении, но повышает риски нарушения приватности. К персональным данным относятся сведения, позволяющие идентифицировать человека, включая биометрические и поведенческие.

Использование ИИ из недружественных юрисдикций создаёт угрозы: возможные закладки (backdoors), скрытая телеметрия и когнитивные манипуляции через искажённые ответы и рекомендации.

Постановка задачи

Основная цель исследования – определить методы и подходы к защите персональной информации, а также выработать критерии выбора безопасных систем для анализа данных. Для этого необходимо решить следующие задачи:

1. Определить угрозы, связанные с использованием зарубежных ИИ-платформ, включая риск утечек и когнитивных воздействий.
2. Описать методы защиты персональной информации на основе отечественных технологий.
3. Установить, какие ИИ целесообразно использовать для получения количественных данных и проведения вычислительных экспериментов.
4. Провести сравнительную оценку ИИ-платформ по скорости отклика и надёжности защиты данных.

Пути решения задачи

Для решения предлагается использовать комплексный подход:

1. Применение отечественных ИИ-систем. Использование российских решений (например, ЯндексGPT, SberAI, ruGPT, Kandinsky, GigaChat) снижает риски.

2. Выбор ИИ для расчётов и анализа данных.

Для проведения статистических расчётов целесообразно использовать:

– Python-библиотеки с интегрированными моделями машинного обучения (scikit-learn, NumPy, PyTorch);

– отечественные решения на базе СберКлауд и Яндекс Облака;

– локальные развертывания моделей LLM для автономной аналитики без передачи информации в сеть.

3. Методы защиты персональных данных.

– Применение принципов privacy by design (встроенная защита данных при проектировании);

– Federated learning – распределённое обучение без передачи исходных данных;

– Гомоморфное шифрование для безопасных вычислений над зашифрованной информацией.

4. Оценка оперативности и надёжности ИИ.

Эффективность ИИ для защиты информации определяется не только уровнем безопасности, но и скоростью реакции на запрос. Средняя оперативность отечественных ИИ (ЯндексGPT, GigaChat) составляет 2–6 с при простых запросах и до 20 с при сложных.

Заключение

Использование ИИ должно сопровождаться созданием безопасной цифровой среды, где персональные данные защищены от утечек, а когнитивное воздействие сведено к минимуму. Реализация принципов privacy by design, внедрение отечественных ИИ- и обучение специалистов —условия информационной независимости России.

Список литературы

1. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Цифровая безопасность. URL: https://digital.gov.ru/ru/activity/directions/1003./

2. Stanford Institute for Human-Centered Artificial Intelligence (HAI). Privacy in an AI Era: How Do We Protect Our Personal Information? — Stanford University, 2023. URL: https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information.