Военная академия Генерального штаба Вооруженных Сил Российской Федерации

Угрозы информационной безопасности Российской Федерации в области науки и образования в условиях развития технологий искусственного интеллекта

Ведущий научный сотрудник
научно-исследовательского института (информационной безопасности)
кандидат технических наук
Чернышов Владимир Иванович

Москва 2026

АКТУАЛЬНОСТЬ

«Искусственный интеллект — это будущее не только России, это будущее всего человечества. Здесь колоссальные возможности и трудно прогнозируемые сегодня угрозы. Тот, кто станет лидером в этой сфере, будет властелином мира. И очень бы не хотелось, чтобы эта монополия была сосредоточена в чьих-то конкретных руках…» - Владимир Путин, 1 сентября 2017 года.

Технологии искусственного интеллекта - комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать **результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека** при решении задач компьютерного зрения, обработки естественного языка, распознавания и синтеза речи, поддержки принятия решений и других практически значимых задач обработки данных

ГОСТ Р 59277–2020

Победа в гонке искусственного интеллекта положит начало новому золотому веку процветания человечества, экономической конкурентоспособности и национальной безопасности для американского народа.

Искусственный интеллект позволит американцам открывать новые материалы, синтезировать новые химические вещества, производить новые лекарства и разрабатывать новые методы использования энергии – промышленная революция. Он позволит создавать принципиально новые формы образования, средств массовой информации и коммуникации – информационная революция. И он позволит совершать совершенно новые интеллектуальные достижения: расшифровывать древние свитки, которые когда-то считались нечитаемыми, совершать прорывы в научной и математической теории и создавать новые виды цифрового и физического искусства – ренессанс.

Промышленная революция, информационная революция и ренессанс – всё одновременно. Таков потенциал, который открывает искусственный интеллект. Открывающиеся перед нами возможности одновременно вдохновляют и заставляют задуматься. И от нас зависит, воспользуемся ли мы ими или упустим.

«Американский план действий в области искусственного интеллекта» июль 2025 г.,
Дональд Дж. Трамп, 45-й и 47-й Президент Соединенных Штатов

ФАКТОРЫ, ВЛИЯЮЩИЕ НА УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Современное состояние информационной безопасности характеризуется внедрением искусственного интеллекта практически во все сферы человеческой деятельности – творчество, медицину, транспорт, банковский и финансовый секторы, торговлю, охрану правопорядка

ТЕХНОЛОГИЧЕСКИЕ

- существенный рост динамики развития технологий искусственного интеллекта
- сложность прогнозирования результатов применения технологий искусственного интеллекта
- высокий темп внедрения и простота масштабируемости технологий искусственного интеллекта
- технологическая политика государств
- тенденции дальнейшего развития технологий искусственного интеллекта

Угрозы информационной безопасности Российской Федерации в условиях развития технологий искусственного интеллекта

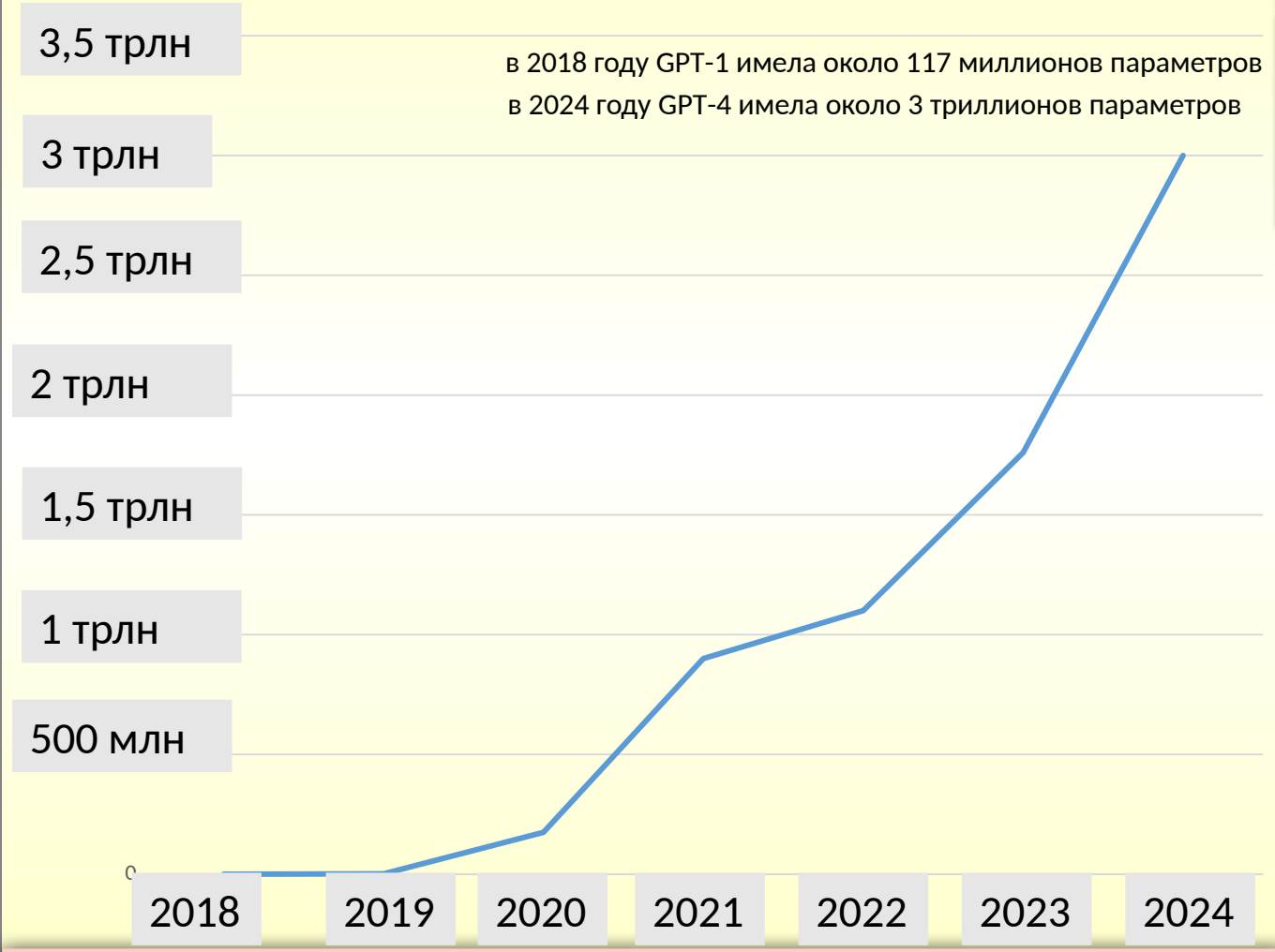
ФУНКЦИОНАЛЬНЫЕ

- возможность создания цифровых двойников человека и цифровых сообществ
- возможность создания виртуальных экспертов
- доступность генерации фото-, аудио- и видео- контента
- реализация автоматизированных кибератак
- генерация адаптивных вредоносных программ и фишинговых кампаний
- усиление возможностей технической разведки
- увеличение автономности действий робототехнических комплексов
- создание роевых технологий
- создание антропоморфных роботов
- формирование единой цифровой среды

ФАКТОРЫ, ВЛИЯЮЩИЕ НА УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Применение технологий искусственного интеллекта с одной стороны развивает экономику и совершенствует функционирование общественных и государственных институтов, а с другой стороны порождает новые угрозы информационной безопасности

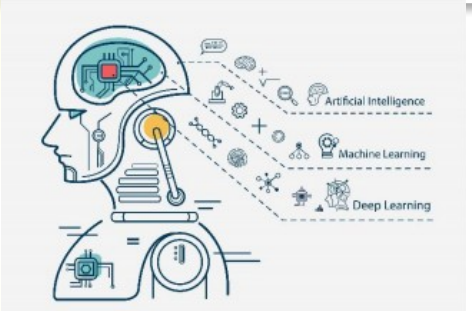
Количество входных параметров больших языковых моделей



*в настоящее время наблюдается **существенный рост** возможностей больших языковых моделей благодаря развитию вычислительных мощностей, масштабированию генеративных моделей и появлению новых архитектур*

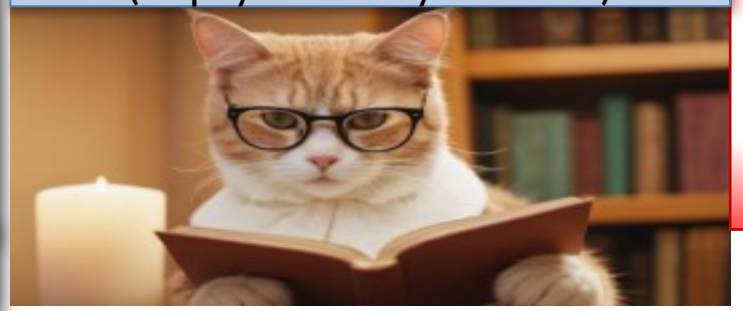
высокий темп внедрения и простота масштабируемости технологий искусственного интеллекта

Для того, чтобы охватить 100 миллионов пользователей:
Интернет – около 6-7 лет
Мобильные устройства (iPhone) – около 5 лет
ТИИ (чат-бот «ChatGPT») – всего 2 месяца



*высокий темп внедрения и масштабируемость не может быть многосторонне обеспечена информационной безопасностью, что резко увеличивает количество **потенциальных угроз***

возможность создания виртуальных экспертов (виртуальных учителей)



*при внедрении в обучение ТИИ способны значительно расширить **возможности персонализации образования**, выступая в роли индивидуального наставника для каждого ученика и позволяя создавать учебные планы **с учетом уникальных особенностей обучаемых***

При внедрении в обучение ТИИ:

получение недостоверной, ошибочной информации;

нарушение конфиденциальности персональных данных обучаемых;

негативное влияние на когнитивное развитие детей при неконтролируемом использовании виртуальных учителей;

манипуляция мнением обучаемых;

создание цифровых сообществ, негативно влияющих на обучаемых

привыкание к технологии искусственного интеллекта

ВЫВОДЫ

1. Будущее технологий искусственного интеллекта связано с созданием более универсальных, автономных, персонализированных систем, с широким применением в медицине, индустрии, повседневной жизни и комплексных интеллектуальных экосистемах, с акцентом на улучшение взаимодействия человека и машины, а также интеграцию новых вычислительных технологий. Такое развитие информационной среды приближает человечество к переходу в киберфизические среды, в которых информационная среда сопоставима с физической

2. При внедрении технологий искусственного интеллекта необходимо учитывать не только значительную пользу от их применения, но и угроз информационной безопасности возникающие вследствие этого

3. Необходимо внедрять в обучение работу с технологиями искусственного интеллекта. Так как массовое внедрение в производство, требует специалистов не только в своей сфере, но и навыков работы с технологиями искусственного интеллекта

СПИСОК ИСТОЧНИКОВ

1. Милорадович Е.А. Большие языковые модели в 2024 году: полное сравнение. – URL: https://gptunnel.ru/blog/llm-full-comparison-of-2024/ (дата обращения 2025–11–13).

2. These Countries, Companies Are In An AI Patent Frenzy: Report. – URL: https://mescomputing.com/news/ai/ these-countries-companies-are-in-an-ai-patent-frenzy-report / (дата обращения 2025–11–11).

3. Селянин Я.В. Приоритеты госфинансирования и перспективы развития отрасли искусственного интеллекта в США. Анализ и прогноз. Журнал ИМЭМО РАН №3. – 2021. с. 65-93.

4. Мельников В.Б., Поздняков Н.И. Искусственный интеллект и военное образование // Информационные технологии в современном инженерном образовании. – 2021. – С. 232–238.

5. База угроз безопасности информации ФСТЭК. – URL: https://bdu.fstec.ru/threat (дата обращения 2023–12–13).

6. Ломако А.Г., Менисов А.Б. Ландшафт угроз безопасности информации технологий искусственного интеллекта // Сборник 31-й научно-технической конференции методы и технические средства обеспечения безопасности информации. – 2022. – С. 49.

7. Отчет счетной палаты США. – URL: https://gao.gov/products/gao-23-106453/ (дата обращения 2025–12–02).

8. Салунов А.А. Почему искусственный интеллект вызывает споры: возможности, риски и мнение экспертов. Российская газета. – URL: https://rg.ru/2025/08/11/pochemu-iskusstvennyj... (дата обращения 2025–12–02).

9. Богатырева Ю.И., Кузнецова С.И. Педагогические аспекты применения искусственного интеллекта в образовании: факторы риска и угрозы в цифровой образовательной среде // Международный научно-исследовательский журнал №7. – 2025. 157 с.

10. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики №5. – 2025. 87 с.

11. Эльяс В.П. Изменения характера угроз в информационной сфере в современных условиях и в обозримой перспективе// Сборник материалов НПК…25 ноября 2021 г. – М: ВАГШ ВС РФ, 2021. Совершено секретно. Инв. № 189966. С.5-15

12. Кайзер В.А., Котов Д.В. Современные угрозы НБ в условиях применения ТИИ в информационной сфере / НС ВАГШ № 91. – М: ВАГШ ВС РФ, 2022. Секретно. Инв. № 190514. С.5-14

13. Подберезкин А.И. Современная стратегия национальной безопасности России: Монография. – М.: МГИМО, 2023. Изд. дом «Международные отношения», 2023. – 1594 с

14. Князев А.В., Добриков Ю.С., Холодов В.А., Применение технологий искусственного интеллекта в военной сфере: преимущества и угрозы// Военная мысль. – 2025. – №7. – С. 63-70

Военная академия Генерального штаба Вооруженных Сил Российской Федерации

Угрозы информационной безопасности Российской Федерации в области науки и образования в условиях развития технологий искусственного интеллекта

Ведущий научный сотрудник
научно-исследовательского института (информационной безопасности)
кандидат технических наук
Чернышов Владимир Иванович

Москва 2026