Регламент ЕС по ИИ

А.Л. Тюльканов

Специалист по регулированию ИИ и данных,
Ассоциированный исследователь Центра международных исследований интеллектуальной собственности Страсбургского университета

RIGF, апрель 2024

Подходы к регулированию применения ИИ

I

Саморегулирование, в том числе на основе рекомендаций ЮНЕСКО, ОЭСР и др.

II

Тематическое и секторальное регулирование
Illinois Artificial Video Interview Act, NYC AI Bias Law

III

Закон, детализируемый подзаконными актами
Проект Artificial Intelligence and Data Act (Канада)

IV

Детальный закон
Регламент ЕС по искусственному интеллекту

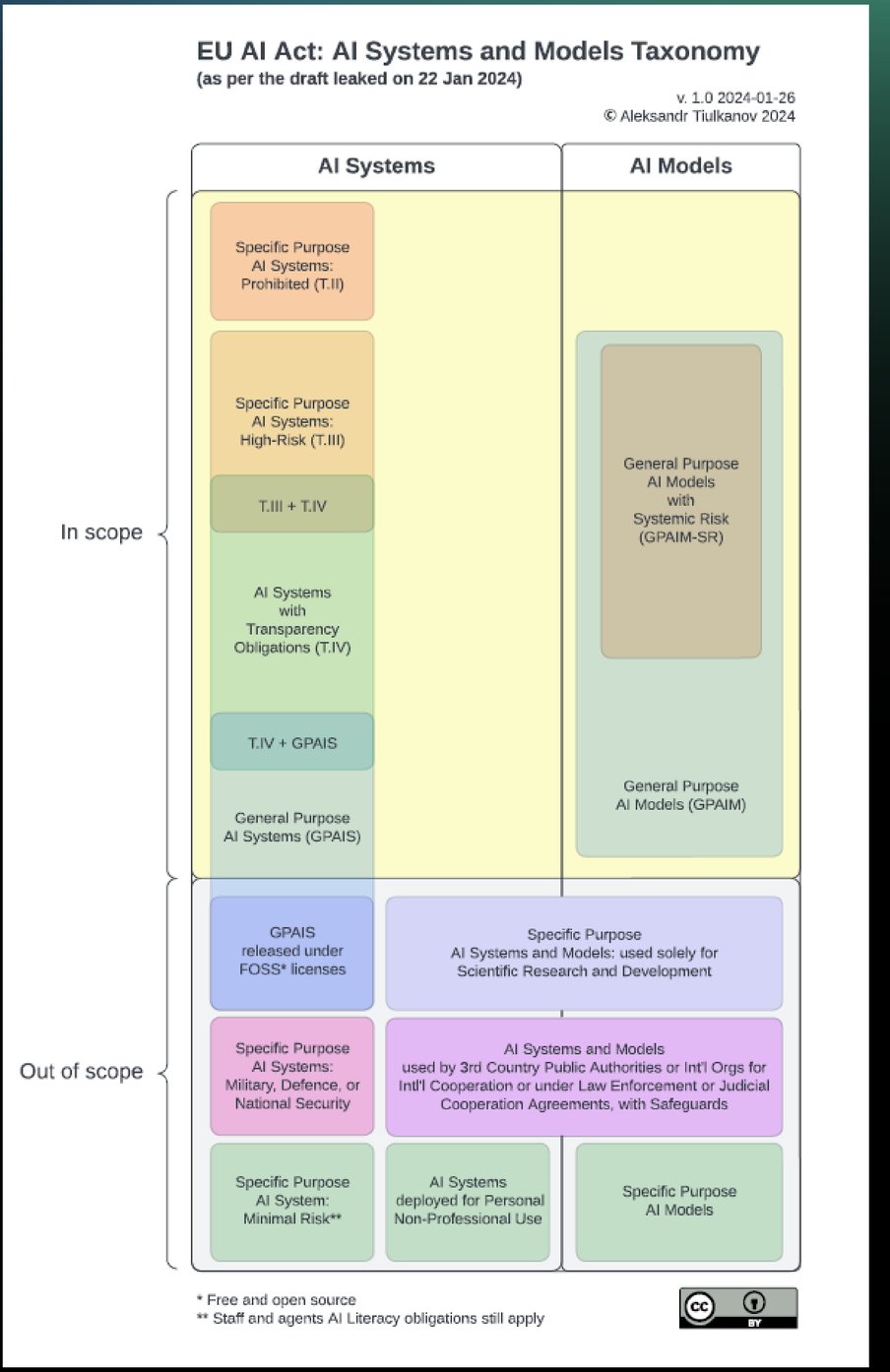
Регламент ЕС по ИИ

01 Не регулирует большинство ИИ-систем

02 Устанавливает случаи, когда применение систем ИИ **требует гласности** (дипфейки, робозвонки, биометрическая категоризация…)

03 Устанавливает требования для систем ИИ **повышенной опасности** и запрещает применение **недопустимо опасных систем**

04 Устанавливает требования для перспективных **ИИ-моделей общего назначения**, в особенности с системными рисками для общества



Перечень систем повышенной опасности

1. Системы, сами по себе являющиеся продукцией, подлежащей оценке соответствия (медицинские изделия, игрушки, машинное оборудование и др.), либо обеспечивающие безопасность такой продукции.

2. Биометрические системы для дистанционной идентификации, для категоризации и для распознавания эмоций.

3. Системы, обеспечивающие безопасность критической инфраструктуры.

4. Системы, применяющиеся для отбора на учебу или работу или для последующей оценки результатов, а также для принятия юридически значимых решений, включая распределение задач или заказов на основе поведения и характеристик отдельных сотрудников или самозанятых.

5. Системы, применяющиеся для решений о предоставлении социального обеспечения, государственных услуг или жизненно важных услуг в частном секторе, в том числе для кредитного и страхового скоринга.

6. Системы, применяемые для оценки рисков рецидивизма, для оценки доказательств по делу и для ряда других задач в области обеспечения правопорядка.

7. Системы, применяемые для контроля миграции, пограничного контроля и решения вопросов о предоставлении убежища.

8. Системы, обеспечивающие отправление правосудия и альтернативных процедур разрешения споров либо влияющие на результат выборов, референдумов или на поведение избирателей.

В чём специфика европейского подхода?

- **Повышенную опасность создаёт не только применение ИИ, связанное с повышенным риском вреда для жизни и здоровья граждан, но и с повышенным риском их фундаментальным (конституционным) правам**
- **Во избежание избыточной регуляторной нагрузки на бизнес, базовые правила устанавливаются едиными для всех 27 стран Союза**
- **Если ИИ-система уже является регулируемым продуктом (например, ПО - медицинские изделия, SaMD), разработчику не нужно дублировать усилия и техническую документацию**

Что для систем повышенной опасности?

- **Требования к качеству данных и управлению ими** (качество и репрезентативность обучающей выборки и предотвращение незаконной дискриминации)
- **Требования к важнейшим характеристикам таких систем** (соблюдение заявленной точности, робастность, информационная безопасность, подконтрольность человеку, протоколирование работы)
- **Поддержание актуальной технической документации на систему** и информационная поддержка эксплуатантов для успешной интеграции системы в их ИТ-инфраструктуру
- **Мониторинг производительности, инцидентов и корректирующие действия** после выпуска системы в обращение и ввода в эксплуатацию
- **Внедрение системы менеджмента качества (СМК)** и **системы управления рисками** (пропорционально рискам)
- **Испытания и подтверждение соответствия** (как правило на основании самоконтроля и декларирования, без сертификации)
- **Регуляторные песочницы** с послаблениями в части условий обработки персональных данных для создания систем ИИ

Требования к системам повышенной опасности будут применяться **по истечении двух лет** с момента вступления Регламента ЕС в силу (для медицинских изделий и других регулируемых продуктов из Приложения II срок составляет три года).

CEN/CENELEC ведёт работу над стандартами (на базе стандартов ISO/IEC с адаптацией), соблюдение которых разработчиком ИИ-системы даёт презумпцию соблюдения требований Регламента ЕС.

Этический компас для вашей организации

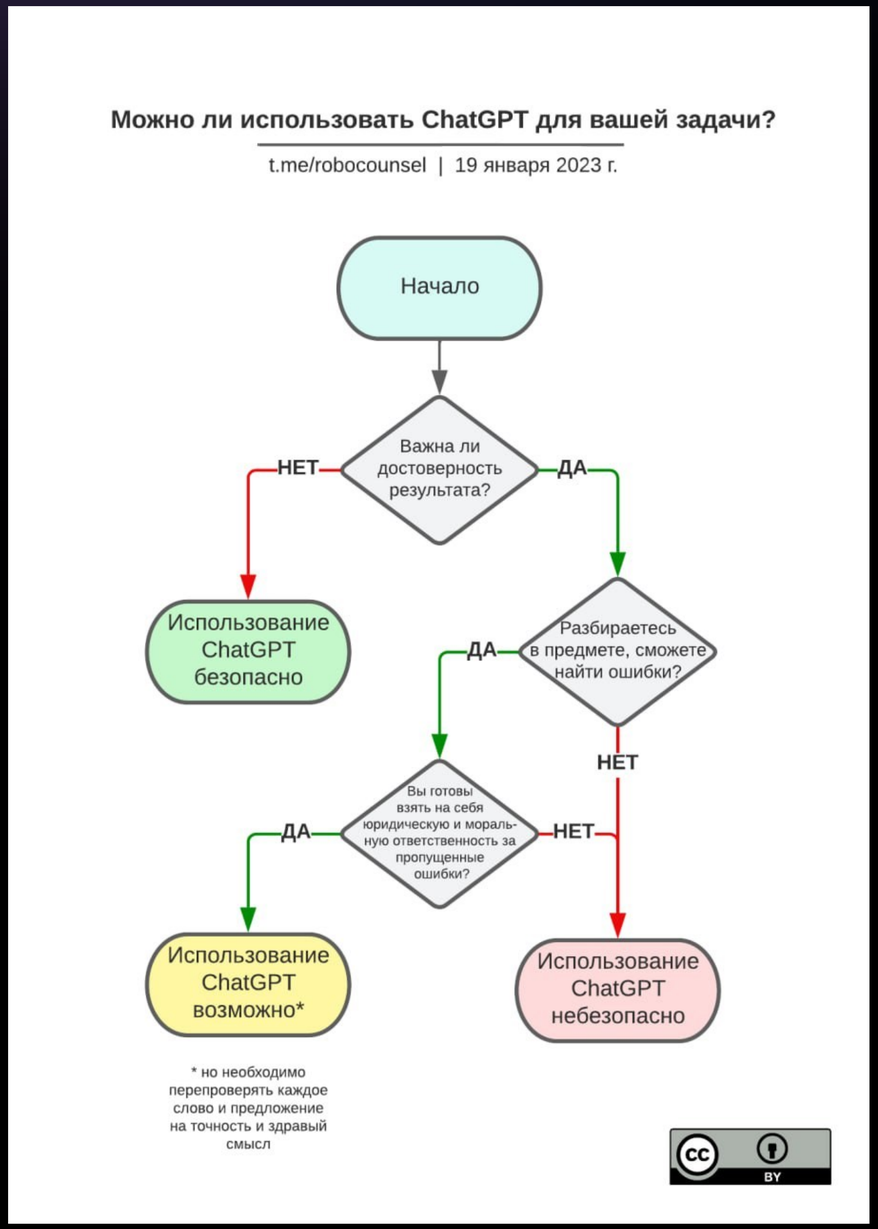
01 Технология, которую вы планируете применить, оптимальна для вашей задачи? Чем вы это докажете?

02 Использование вами этой технологии законно и соответствует общепринятым этическим нормам? Чем вы это докажете?

03 Кто несёт личную ответственность за результаты и как регламентирован процесс разработки и (или) применения?

04 Если завтра обо всех деталях процесса расскажут СМИ, вы будете этим гордиться?

Личный компас пользователя генеративного ИИ



Реакции