Рецензия
на статью «Искусственный интеллект и национальная кибербезопасность России: вызовы, угрозы и пути технологического суверенитета»
Султанов Г.С., Курбанова А.М.

Характеристика и актуальность темы
Тема исследования обладает высокой актуальностью, поскольку ускоренное внедрение технологий искусственного интеллекта в государственные и корпоративные контуры управления одновременно расширяет возможности киберзащиты и усиливает спектр киберугроз. В условиях геополитической напряжённости, санкционных ограничений и повышенного риска атак на критическую информационную инфраструктуру проблематика сочетания ИИ-развития, правового регулирования и технологического суверенитета закономерно относится к приоритетам национальной безопасности.

Анализ содержания исследования
Авторы корректно формулируют цель и логику работы: систематизация угроз применения ИИ в киберпространстве, выделение уязвимостей правового поля и зависимости от технологических цепочек «недружественных» государств, а также разработка направлений укрепления суверенной ИИ-экосистемы. Содержательно статья выстраивает понятный причинно-следственный контур: правовая неопределённость снижает управляемость рисков и затрудняет распределение ответственности; технологическая зависимость усиливает уязвимость КИИ и ограничивает масштабирование отечественных решений; параллельно возрастает роль ИИ как инструмента атак (фишинг, дипфейки, автоматизация поиска уязвимостей) и защиты (анализ аномалий, интеллектуальные средства мониторинга, подходы Zero Trust).

При этом ряду положений требуется более строгая операционализация и уточнение доказательной базы. Так, в части «правовой неопределённости» целесообразно чётче развести стратегические документы и нормы права прямого действия, а также показать, какие именно правовые режимы предлагается вводить: риск-ориентированную классификацию ИИ-систем, требования к сертификации/аттестации для применения в КИИ, правила аудита моделей и данных, а также режим ответственности с указанием субъектов и оснований. В технологическом блоке стоит усилить раздел о «суверенной ИИ-экосистеме» конкретизацией архитектуры: вычислительная база, отечественные платформы/фреймворки, контуры доверенных данных, импортонезависимые цепочки поставок и механизмы контроля безопасности ИИ-компонентов в КИИ. Отдельные примеры и утверждения об использовании конкретных open-source/коммерческих решений в качестве угрозы требуют аккуратной формулировки, чтобы избежать терминологической и фактической неоднозначности.

Теоретическая и практическая значимость
Теоретическая значимость статьи проявляется в попытке связать три уровня анализа — технологический, правовой и институциональный — в единую рамку национальной киберустойчивости на фоне ИИ-трансформации.

Практическая значимость заключается в выдвижении набора мер, ориентированных на создание условий технологического суверенитета: развитие отечественных вычислительных платформ и кадров, формирование национальной системы сертификации ИИ-решений, усиление регуляторных механизмов и международная кооперация с дружественными странами. Работа может быть полезна при разработке дорожных карт по ИИ-безопасности для организаций, работающих с КИИ, а также при совершенствовании нормативных подходов к риск-ориентированному регулированию ИИ.

Заключение

Статья соответствует тематике научного обсуждения вопросов кибербезопасности и технологического суверенитета, обладает актуальностью и логичной структурой. Для усиления научной строгости рекомендуется: уточнить юридический статус используемых дефиниций и механизмов регулирования, конкретизировать модель риск-классификации ИИ для КИИ и систему метрик эффективности предлагаемых мер, а также усилить технологический раздел описанием архитектуры суверенной ИИ-инфраструктуры и контуров доверия.
Рекомендую данную статью к публикации в научном журнале.

Рецензент - Зотикова Ольга Николаевна, доктор экономических наук, профессор,
Российский государственный университет имени А.Н. Косыгина
г. Москва, Россия

Reviewer - Zotikova Olga Nikolaevna, Doctor of Economics, Professor,
Kosygin Russian State University, Moscow, Russia