

Этот документ — плод совместной работы группы экспертов. Пока это не часть политической программы, а вариант решения проблемы, предложенный участниками форума.

ТЕХНОЛОГИЧЕСКАЯ ПОЛИТИКА

Контекст

Россия войдет в период демократизации при слабых институтах. При этом страна накопила значительное отставание от мирового технологического развития и унаследовала обширную репрессивную инфраструктуру в сфере цифровых прав. Технологическая политика должна решать все эти проблемы одновременно.

Цифровые технологии будут развиваться намного быстрее, чем ожидает большинство людей. Темп развития тоже будет возрастать. Предсказать развитие конкретных технологий невозможно, но государство должно создавать для него все условия.

1. Транзитный период: десуверенизация Рунета

Следует признать неэффективность блокировок: они не позволяют пресечь преступную деятельность в сети и при желании могут обходиться пользователями. Преступления должны пресекаться путем ОРД, уголовного и судебного преследования тех, кто их совершает, а также, в определенных случаях, операторов серверов, платформ, владельцев доменов и т.д., если они содействуют преступлениям или препятствуют их расследованию. При этом правоохранные органы должны отказаться от требования ключей шифрования и других действий, направленных на ослабление шифрования.

Институциональные изменения

Упразднение Роскомнадзора. Его мелкие технические функции, включая распределение радиочастот и управление системой доменных имен/IP-адресации, передаются другим профильным ведомствам и общественным организациям.

Создание Офиса по цифровым правам — независимого органа под парламентским контролем. Функции: защита цифровых прав граждан, надзор за соблюдением этих прав со стороны ведомств и бизнеса, защита персональных данных, обеспечение баланса между безопасностью и приватностью.

Создание Агентства цифровой трансформации, которое отвечает за реализацию стратегии цифрового развития, в том числе цифрового равенства с помощью частно-государственного партнерства, и разрабатывает преференции для преодоления технологической отсталости.

Повышение цифровой компетенции силовых органов власти, ответственных за расследование утечек персональных данных, ликвидацию черного рынка данных и борьбу с компьютерными преступлениями.

Этот документ — плод совместной работы группы экспертов. Пока это не часть политической программы, а вариант решения проблемы, предложенный участниками форума.

Правовая база

Право на доступ к интернету и цифровой среде закрепляется в Конституции как фундаментальное право человека.

Следует принять Хартию цифровых прав (уровень ФЗ), которая включает:

- запрет блокировок, цензуры и отключений интернета;
- запрет использования технологий в целях дискриминации и массовой и внесудебной слежки;
- принцип сетевого нейтралитета — никаких привилегированных белых списков;
- право на доступные и безопасные цифровые госуслуги;
- право на шифрование данных;
- право на цифровую идентичность;
- все фундаментальные права человека должны также применяться в цифровой сфере.

Международная реинтеграция

- Возвращение в международное правовое поле в вопросах защиты цифровых прав (например, признание решений ЕСПЧ, возобновление участия в Совете Европы, ратифицировать Дополнительный протокол к Конвенции 108 Совета Европы ETS No.181 и Модернизирующий протокол 108+, CETS No. 223).
- Присоединение к Будапештской конвенции по киберпреступности и принятие мер, направленных на ее дальнейшее улучшение в соответствии с международными стандартами защиты цифровых прав.
- Выход из Ханойской конвенции либо принятие мер, направленных на ее радикальное изменение в соответствии с международными стандартами защиты цифровых прав.

Интеллектуальная собственность

- Реформа коллективного управления правами.
- Регулирование использования сиротских произведений.
- Расширение способов добросовестного использования.
- Регулирование произведений, создаваемых ИИ.
- Расширение исключений для предоставления правовой охраны (в т.ч. софтверные патенты).
- Сокращение срока охраны исключительных прав в некоторых случаях (например на софт и контент, сгенерированный компьютерами) до минимального срока, установленного Бернской конвенцией.

Этот документ — плод совместной работы группы экспертов. Пока это не часть политической программы, а вариант решения проблемы, предложенный участниками форума.

2. Программа привлечения высокотехнологичного бизнеса

- Пониженные налоги на прибыль высокотехнологичных компаний (IP Box);
- Нулевой налог на дивиденды венчурного капитала в сфере высоких технологий;
- Упрощенный визовый режим для высококвалифицированных специалистов, автоматическое предоставление им вида на жительство;
- Введение института e-residency.

3. Свободные технологические зоны

В регионах создаются свободные технологические зоны — площадки для тестирования и коммерциализации высокорисковых технологий: беспилотного транспорта, новых криптопротоколов, биотехнологий и других направлений.

Каждый кластер регионов определяет приоритетную технологическую специализацию исходя из имеющихся ресурсов, климатических условий и научной базы. Федеральный центр обеспечивает для этого институциональные льготы, выровненные условия конкуренции и защиту мелких рыночных игроков.

Приоритетные направления:

- Биотехнологии
- Искусственный интеллект
- Робототехника
- Software и IT-решения
- Беспилотный транспорт (наземный и авиационный).
- Дерегулирование малой авиации.

4. Искусственный интеллект: инфраструктура, занятость, применение технологии

Создание инфраструктуры

Необходимо сформировать условия для строительства дата-центров в холодных малонаселенных регионах с учетом привлекательности конкретных инвестпроектов. Это снизит операционные затраты для бизнеса и даст импульс для развития технологий в области искусственного интеллекта.

При этом стоит учитывать базовые экологические требования: питание от возобновляемых источников энергии, приоритет электроснабжения населения и критической инфраструктуры, использование тепла дата-центров для отопления близлежащих поселений.

Этот документ — плод совместной работы группы экспертов. Пока это не часть политической программы, а вариант решения проблемы, предложенный участниками форума.

ИИ в государственном управлении

У каждого ведомства должна быть локальная агентная система искусственного интеллекта с открытым исходным кодом и открытыми весами. Она оценивает качество принимаемых решений и дает рекомендации. Если действия ведомства систематически расходятся с рекомендациями системы, это должно быть основанием для рассмотрения его деятельности специальной парламентской комиссией. При этом исключается принятие государственных решений искусственным интеллектом или исключительно на основании рекомендаций ИИ.

Вызовы

На данный момент возможны различные пути развития искусственного интеллекта. Он может быть обычным технологическим переходом, случавшимся много раз в истории цивилизации, а может привести к радикальному переустройству рынка труда, включая массовый рост безработицы.

Во втором случае большая часть ВВП будет создаваться с участием ИИ, что даст огромный прирост добавленной стоимости, за счет перераспределения которой будет обеспечен **безусловный базовый доход**.

В условиях распространения ИИ-генерированной дезинформации и кризиса традиционных бизнес-моделей следует поддерживать медиа с помощью налоговых послаблений или иного стимулирования.

5. Цифровизация государства и криптотехнологии

Цифровизация

Развитие и реформирование платформы Госуслуг: усиление цифровизации государственных сервисов (включая суды), но при условии перехода на децентрализованные протоколы для предотвращения утечек данных и злоупотреблений.

Государственные ведомства получают, обрабатывают и передают персональные данные только на основе информированного согласия, которое пользователь вправе отозвать.

Следует внедрять ПО с открытым исходным кодом как стандарт для всех государственных органов.

Криптотехнологии

Криптографические методы нужно внедрять для распределения бюджетов всех уровней и учета государственных активов. Открытость реестров будет снижать коррупционные риски.

Должно быть легализовано свободное обращение криптовалют для повседневных (небольших) транзакций — в целях защиты приватности граждан.

Этот документ — плод совместной работы группы экспертов. Пока это не часть политической программы, а вариант решения проблемы, предложенный участниками форума.

Следует утвердить процедуру сертификации блокчейн-технологий и криптовалют для крупных транзакций частного сектора — при условии соответствия требованиям прозрачности и автоматической уплаты налогов.

Стимулировать применение смарт-контрактов: они исключают посредников и снижают риск мошенничества.

Демократические процедуры

Необходимо привлекать специалистов для разработки криптографических методов сбора и анализа данных, не нарушающих приватность.

Применять эти методы в голосовании на муниципальных выборах и в работе цифровых ассамблей — для обеспечения безопасности, прозрачности, приватности и снижения стоимости демократических процедур.

НАД ДОКУМЕНТОМ РАБОТАЛИ:

Роман Баданин, журналист-расследователь, основатель и главный редактор издания «Проект»

Саркис Дарбинян, киберадвокат, исполнительный директор RKS Global, правовой советник VPN Guild

Михаил Климарев, директор Общества защиты интернета

Наталья Крапива, юристка и экспертка по цифровым правам

Александр Лурье, IT-инженер, предприниматель

Павел Мунтян, сооснователь анимационной студии Toonbox и основатель ИИ-проектов

Анна Чехович, Freedom Tech Education Lead, Human Rights Foundation