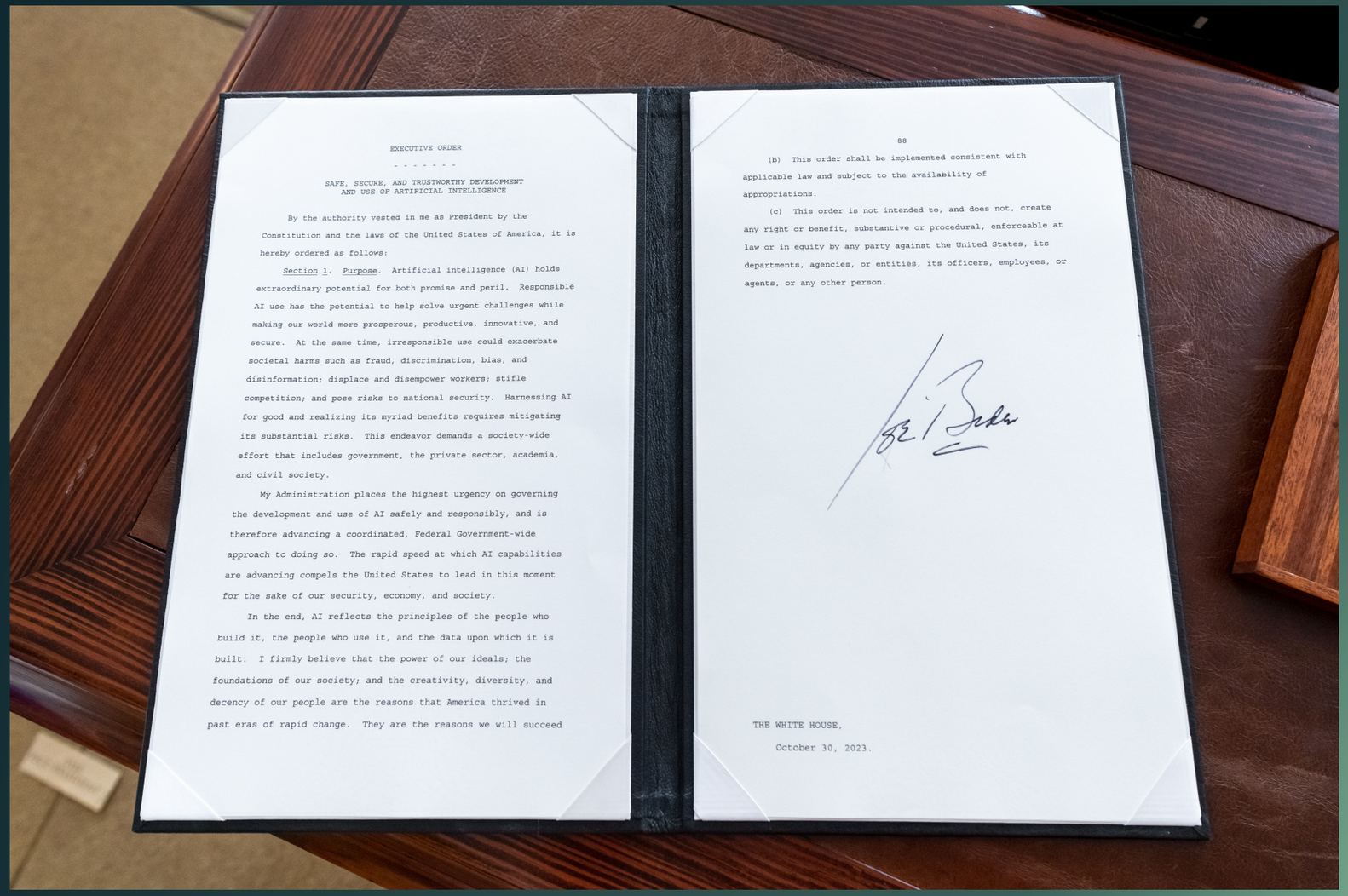
КОНСОРЦИУМ
ИССЛЕДОВАНИЙ
БЕЗОПАСНОСТИ
ТЕХНОЛОГИЙ
ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА

НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ • NATIONAL ASSOCIATION FOR INTERNATIONAL INFORMATION SECURITY • NAIIS • НАМИБ

Международные тренды регулирования вопросов безопасности ИИ

Павел Кузнецов
эксперт Консорциума ИБ ИИ, член НАМИБ

США



EXECUTIVE ORDER

- - - - - - -

SAFE, SECURE, AND TRUSTWORTHY DEVELOPMENT
AND USE OF ARTIFICIAL INTELLIGENCE

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.

My Administration places the highest urgency on governing the development and use of AI safely and responsibly, and is therefore advancing a coordinated, Federal Government-wide approach to doing so. The rapid speed at which AI capabilities are advancing compels the United States to lead in this moment for the sake of our security, economy, and society.

In the end, AI reflects the principles of the people who build it, the people who use it, and the data upon which it is built. I firmly believe that the power of our ideals; the foundations of our society; and the creativity, diversity, and decency of our people are the reasons that America thrived in past eras of rapid change. They are the reasons we will succeed

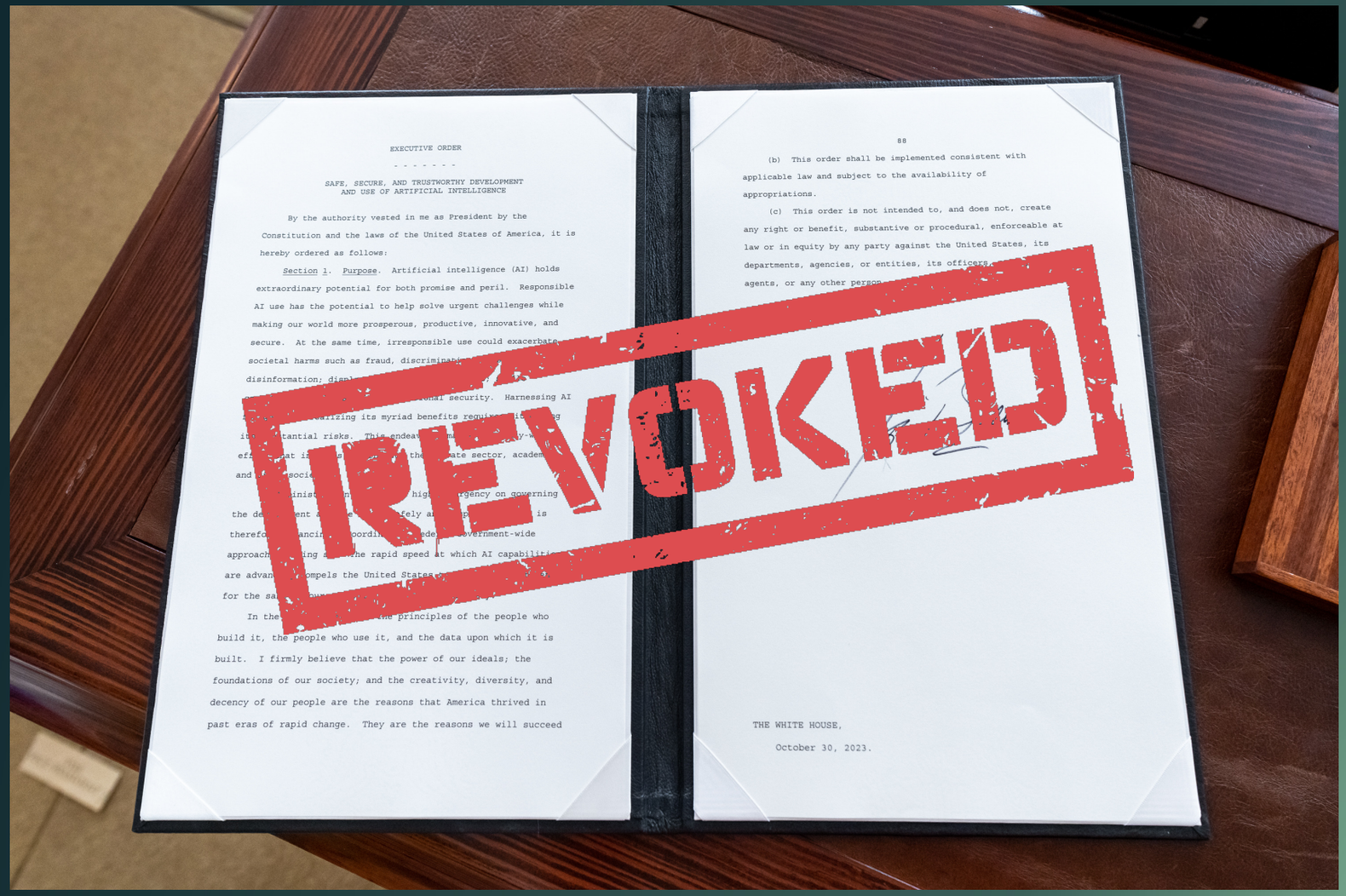
(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

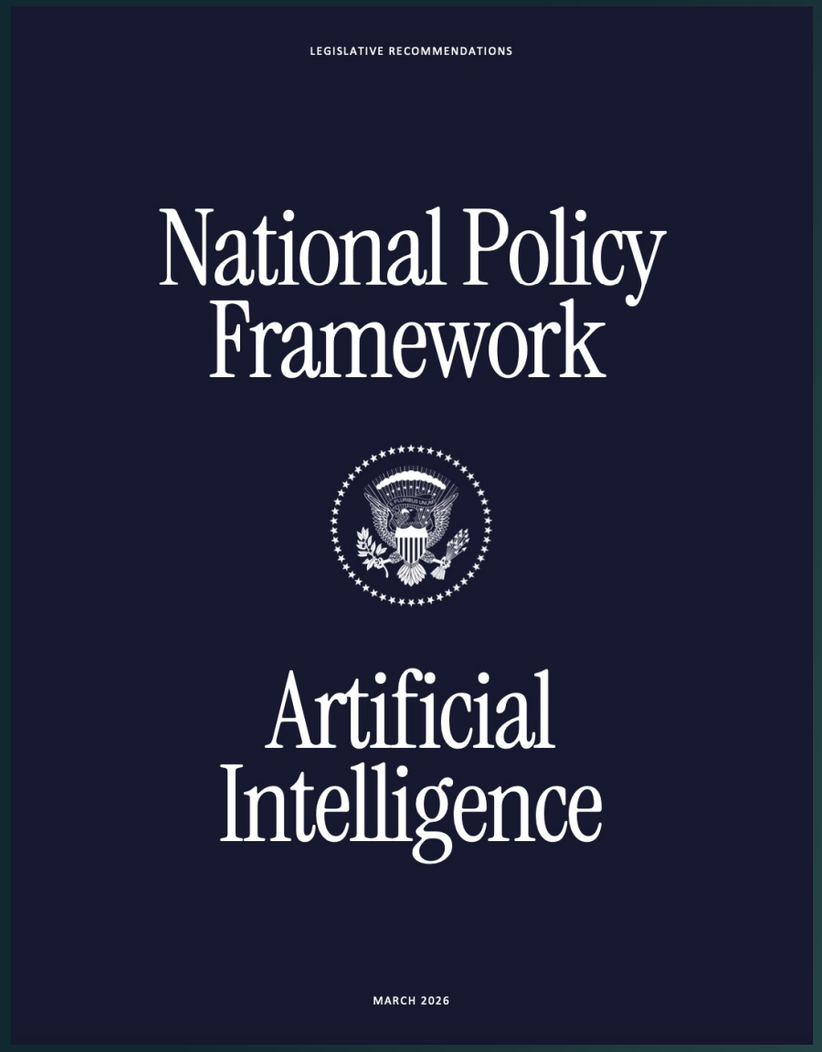
THE WHITE HOUSE,

October 30, 2023.

США


EXECUTIVE ORDER
- - - - - - -
SAFE, SECURE, AND TRUSTWORTHY DEVELOPMENT
AND USE OF ARTIFICIAL INTELLIGENCE
By the authority vested in me as President by the
Constitution and the laws of the United States of America, it is
hereby ordered as follows:
Section 1. Purpose. Artificial intelligence (AI) holds
extraordinary potential for both promise and peril. Responsible
AI use has the potential to help solve urgent challenges while
making our world more prosperous, productive, innovative, and
secure. At the same time, irresponsible use could exacerbate
societal harms such as fraud, discrimina
disinformation; dis
88
(b) This order shall be implemented consistent with
applicable law and subject to the availability of
appropriations.
(c) This order is not intended to, and does not, create
any right or benefit, substantive or procedural, enforceable at
law or in equity by any party against the United States, its
departments, agencies, or entities, its officers,
agents, or any other person
THE WHITE HOUSE,
October 30, 2023.
REVOKED

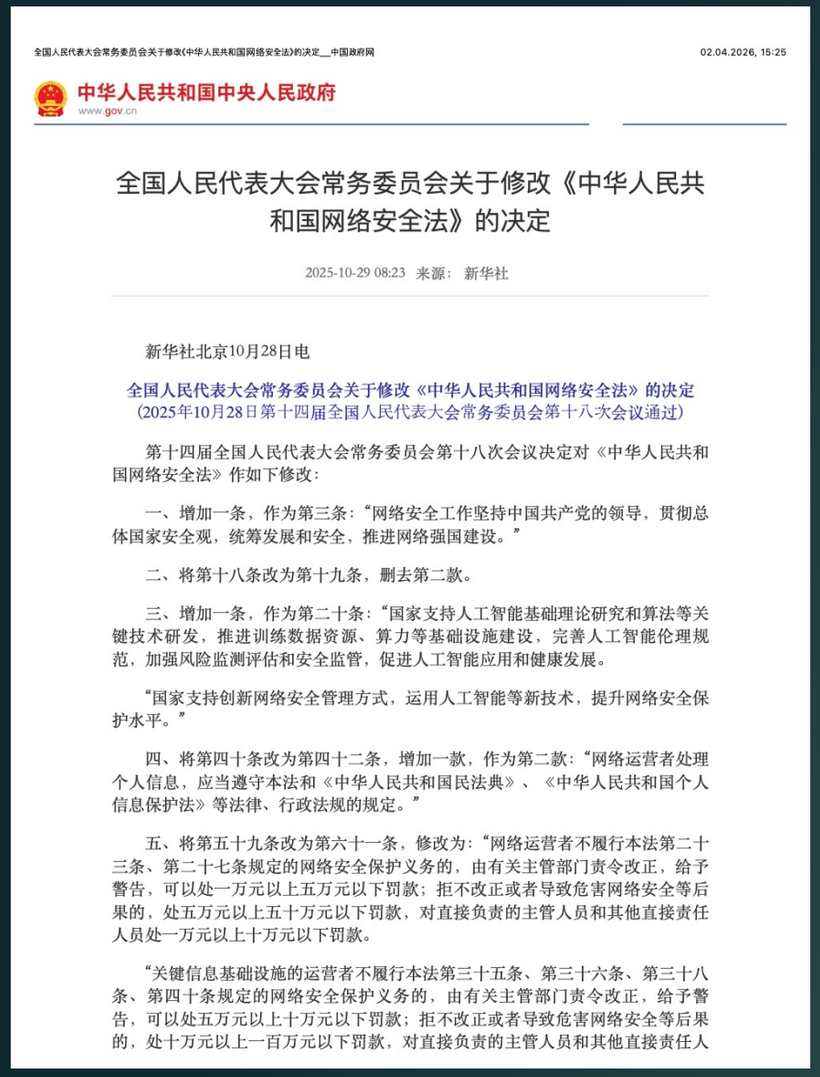
США



В контексте безопасности затрагиваются:

- **Защита детей от запрещённого контента, централизация роли родителей**
- **Конгрессу *следует* обеспечить федеральным исполнительным властям возможности противодействия мошенничеству с применением ИИ и угрозам национальной безопасности**
- **Защита свободы слова и интеллектуальной собственности в контексте творчества**

Китай



全国人民代表大会常务委员会关于修改(中华人民共和国网络安全法)的决定__中国政府网 02.04.2026, 15:25

中华人民共和国中央人民政府
www.gov.cn

全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定

2025-10-29 08:23 来源： 新华社

新华社北京10月28日电

全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定
（2025年10月28日第十四届全国人民代表大会常务委员会第十八次会议通过）

第十四届全国人民代表大会常务委员会第十八次会议决定对《中华人民共和国网络安全法》作如下修改：

一、增加一条，作为第三条：“网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。”

二、将第十八条改为第十九条，删去第二款。

三、增加一条，作为第二十条：“国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。

“国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。”

四、将第四十条改为第四十二条，增加一款，作为第二款：“网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。”

五、将第五十九条改为第六十一条，修改为：“网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

“关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人

1) Новейшее - поправки в Закон о кибербезопасности

В контексте ИИ затрагиваются:

- Содействие развитию
- Применение технологий для обеспечения сетевой безопасности

Довольно мягкий подход? ^_^

2) Ранее - значительное количество НПА, e.g.:

- Адм. положения в отношении DS IIS
- Набор НПА по разметке генерируемого контента
- etc.

Республика Корея

Принят Базовый (основной) закон об ИИ, в рамках которого, в контексте безопасности:

1) Создаётся отдельное ведомство, которому ставятся следующие задачи:
   - Определение и анализ рисков, имеющих отношение к безопасности ИИ
   - Ведение исследований по регулированию безопасности ИИ
   - Разработка критериев и методов оценки безопасности ИИ
   - Ведение исследований по технологиям и стандартизации безопасности ИИ
   - Международное сотрудничество и обмен информацией по вопросам безопасности ИИ

2) В отдельной статье прописаны обязанности организаций-операторов ИИ:
   - Идентифицировать, оценивать, и принимать контрмеры в отношении рисков на протяжении всего жизненного цикла систем ИИ
   - Создать и поддерживать в актуальном состоянии систему управления рисками, нацеленную на мониторинг и реагирование на инциденты безопасности ИИ

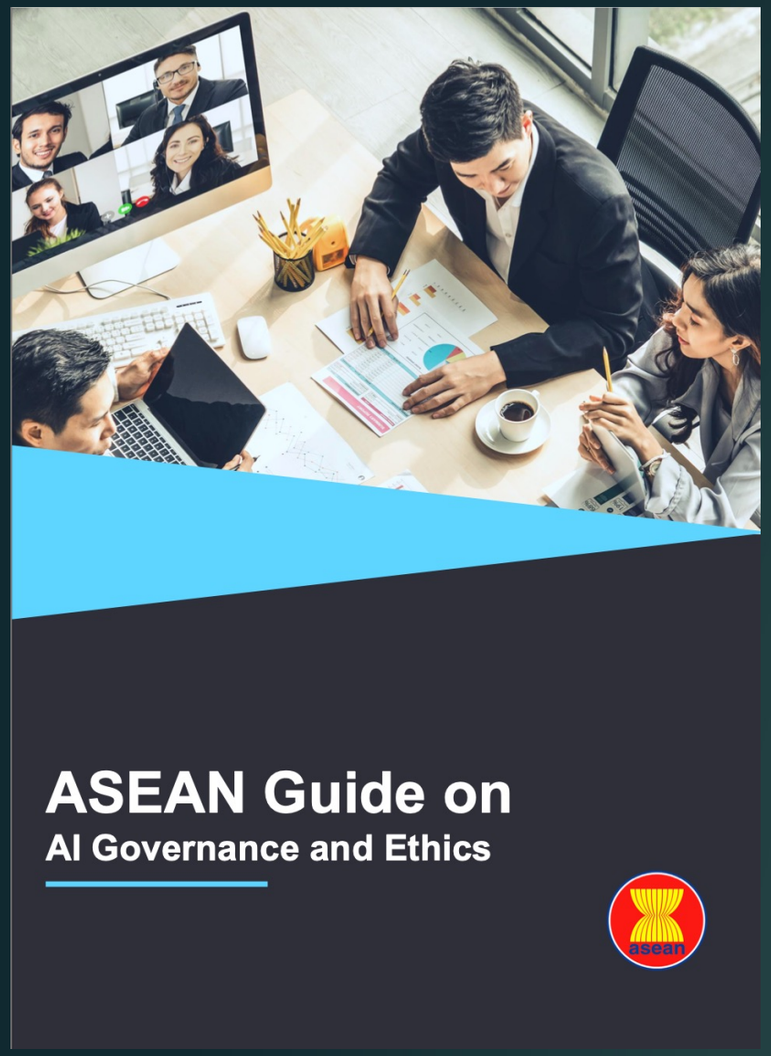
   NB. Операторы ⇔ МНИ

3) Определяет отдельно «Критический ИИ» – по сферам применения, при этом гармонизируя Закон с соответствующими НПА – проведённая работа очевидна

Международные объединения

EU Artificial Intelligence Act

Международные объединения



В контексте безопасности затрагиваются:

Стремление к обеспечению «Safety» – оценка рисков внедрения ИИ, разработка контрмер, ограничений – в контексте безопасности личности, общества и государства

Стремление к обеспечению «Security» – техническая защищённость систем ИИ, устойчивость к вредоносным воздействиям, т.е. компьютерная или «кибер-» безопасность

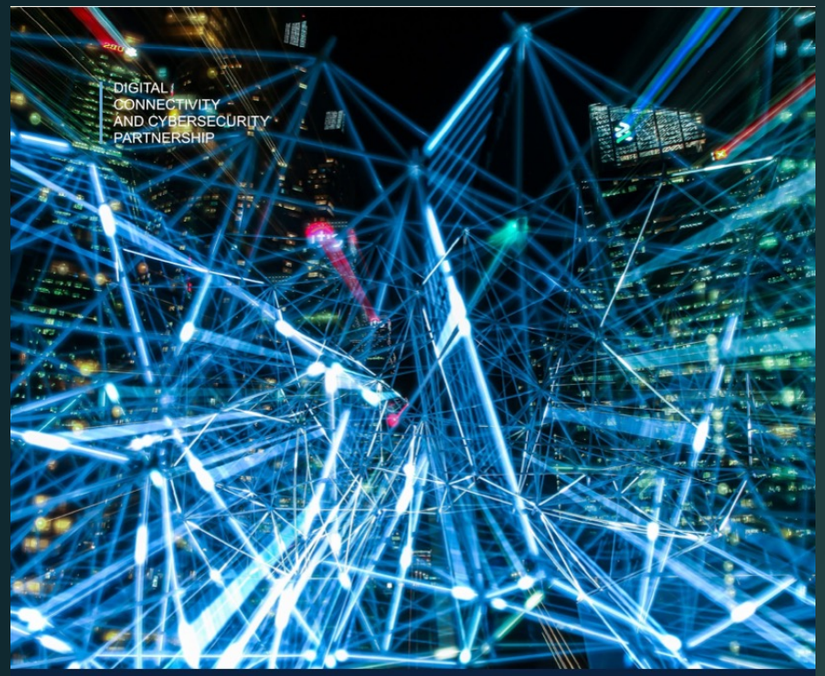
Отдельный блок посвящён охране ПДн

Международные объединения

Применительно к генеративным методам ИИ уточняет предыдущий документ, в части рисков:

- **Ошибки и «антропоморфизм»**
- **Фактически неточные ответы и дезинформация**
- **Deepfake’и, выдача себя за другое лицо, мошеннические и злонамеренные действия**
- **Правонарушения в сфере интеллектуальной собственности**
- **Конфиденциальность и защита личных данных**
- **Продвижение необъективных нарративов**

Международные объединения



ASEAN RESPONSIBLE AI ROADMAP
(2025-2030)

В контексте безопасности ставятся, в том числе, цели:

- **«Укрепить» набор инструментов кибербезопасности для снижения рисков, связанных с ИИ**
- **Нарастить возможности в области т.нз. инновационных технологий повышения конфиденциальности (PET)**
- **Усилить защиту ПДн в системах с использованием технологий ИИ**
- **Создать испытательный полигон/песочницу для технологий ИИ**
- **Предпринять набор конкретных шагов по обеспечению защиты ПДн**
- **Разработать и внедрить мониторинг и меры реагирования и предотвращения реализации рисков**

Международные объединения

В контексте безопасности определены 2 ключевых пути обеспечения безопасности систем, использующих технологии ИИ:

- **Риск-ориентированный подход**
- **Обеспечение «прослеживаемости» работы систем, использующих технологии ИИ**

Сквозная проблематика

Терминологическая неопределённость

В НПА разных юрисдикций определение понятия "искусственный интеллект" различается. E.g. Закон об ИИ ЕС, определение ОЭСР. Существуют юрисдикции, где полное определение до сих пор не выработано (Китай, Япония, РФ etc.)

Издаваемые НПА носят различающийся характер

От законов «прямого действия» до стратегий и рекомендаций

Стремление к гибкости создаёт больше неопределённости

Нацеленность на максимально обтекаемые формулировки делает НПА неприменимыми практически

Проблемы гармонизации НПА по ИИ с иными сферами законодательства

«Доверие», «Этика» и «Безопасность». «Суверенность», «Независимость» и «Национальность». «Сертификация», «Лицензирование», «Аттестация» и «Аккредитация»

КОНСОРЦИУМ
ИССЛЕДОВАНИЙ
БЕЗОПАСНОСТИ
ТЕХНОЛОГИЙ
ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА

НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
NATIONAL ASSOCIATION FOR INTERNATIONAL INFORMATION SECURITY
НАМИБ
NAIIS

СПАСИБО
ЗА ВНИМАНИЕ!