



Соблюдение требований и управление в цифровой экономике

Сипин Ли

Доцент

Сямэньский национальный институт
бухгалтерского учета





Содержание

Введение в цифровую экономику

Нормативно-правовая база в цифровой экономике

Соблюдение требований и управление в цифровом Китае

Практический пример: Проект «mBridge»



Содержание

Введение в цифровую экономику

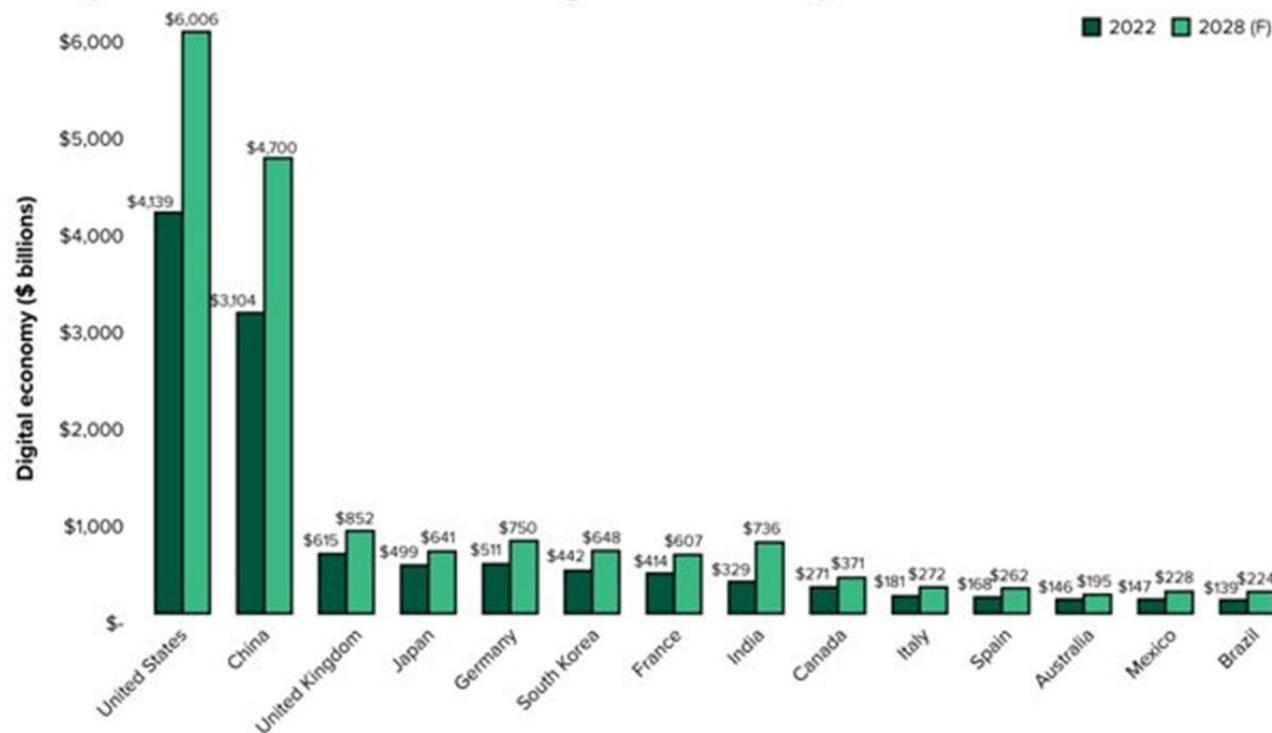
Нормативно-правовая база в цифровой экономике

Соблюдение требований и управление в цифровом Китае

Практический пример: Проект «mBridge»

- **Цифровая экономика:** Конвергенция цифровых технологий с традиционными экономическими практиками.
- Она охватывает широкий спектр отраслей и секторов: от электронной коммерции и цифрового маркетинга до финтеха и цифровых носителей.

Projected Growth Of The Digital Economy 2022 To 2028



Основные достижения: Электронная коммерция



- Расширение электронной коммерции
 - Например: Алибаба

Бизнес	Электронная коммерция	Облачный интеллект	Местные услуги	Логистическая сеть	Цифровые медиа и развлечения	Международная цифровая коммерция
Типичные примеры	Taobao, Tmall	Alibaba Cloud	Ele.me, Koubei	Cainiao Network	Youku	AliExpress

淘宝
Taobao

Alibaba Cloud

饿了么

菜鸟
Cainiao

YOUKU 优酷

AliExpress

天猫
TMALL.COM

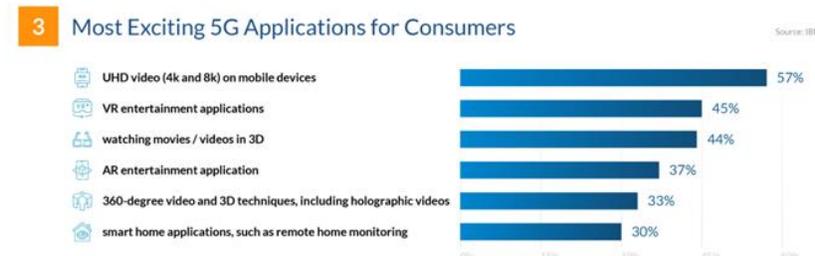
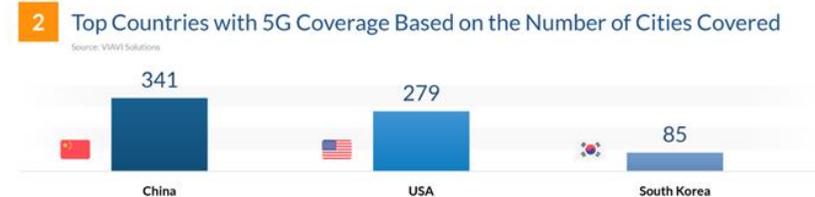
口碑
Koubei



Ключевые достижения: сети 5G



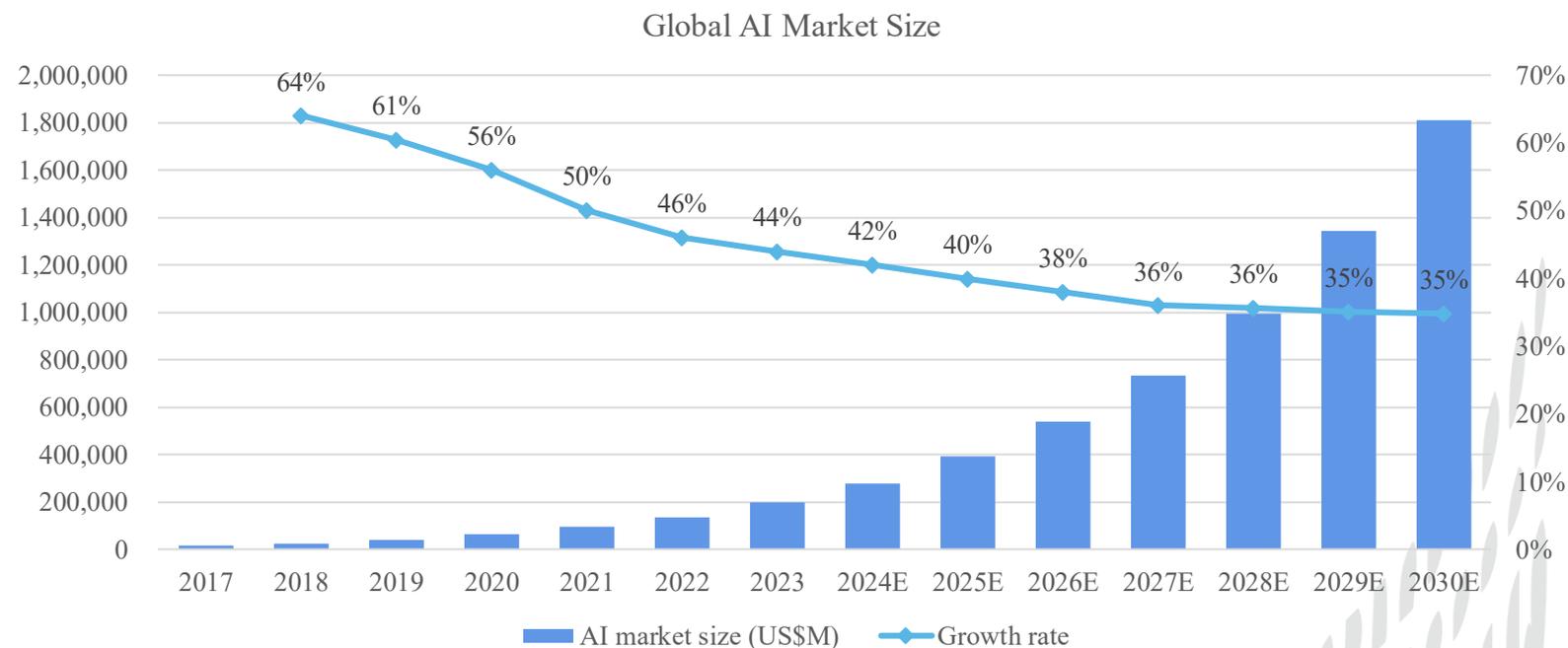
- Коммерческие запуски сетей 5G
 - Китай: построил крупнейшую в мире автономную сеть 5G
 - США: достигнуто почти 98% покрытие сети с использованием низкочастотных сетей
 - Европа: большинство стран быстро расширили покрытие сети 5G
 - В целом глобальное развертывание и внедрение приложений 5G ускорилось.



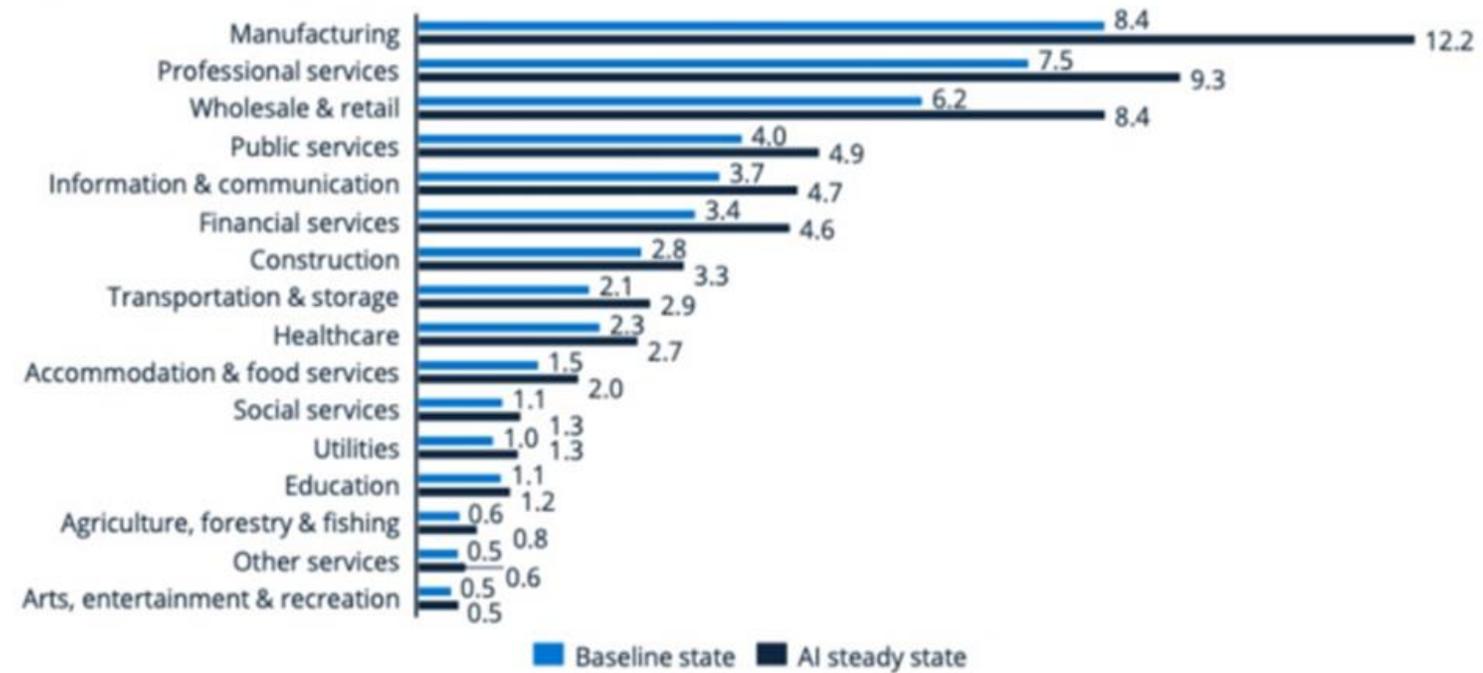
Основные достижения: искусственный интеллект



- Искусственный интеллект (ИИ) и машинное обучение (МО): глобальная индустрия ИИ быстро растет



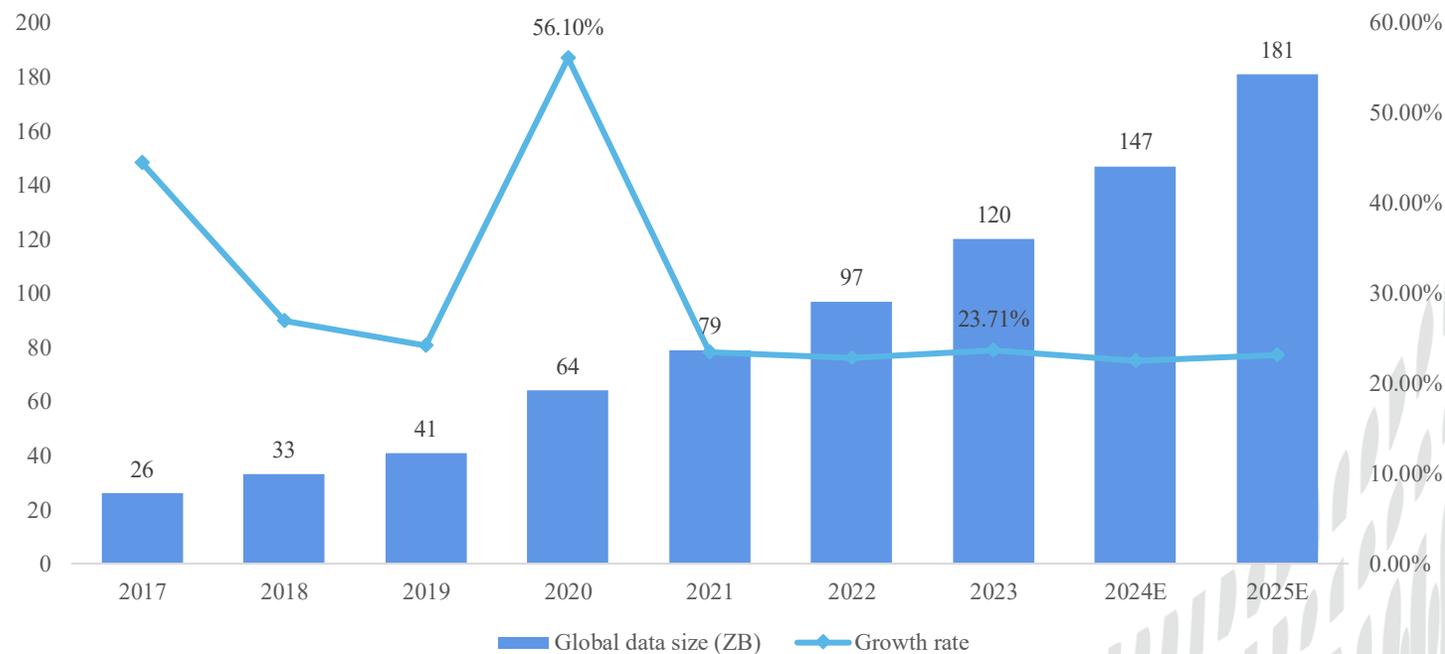
Impact of AI on industry output in 2035 in trillion US\$



Ключевые достижения: Большие данные



- Характеристики 5V: Объем, Разнообразие, Скорость, Достоверность, Ценность
- От данных к ценности



Данные как актив



- Ключевые аспекты:
 - Принятие решений на основе данных
 - Информация о клиентах и персонализация
 - Инновации и новые источники доходов
 - Повышение операционной эффективности
 - Управление рисками
- Проблемы и соображения: конфиденциальность, безопасность, управление данными, этические соображения и т. д.



- Данные — это новый тип **фактора производства**.
- Трехлетний план действий (2024-2026 гг.) для элементов данных ×
 - **Применение элементов данных в областях:** производство, сельское хозяйство, торговля и коммерция, транспорт, финансовые услуги, технологические инновации, туризм, здравоохранение, управление в случае чрезвычайных ситуаций, метеорологические службы, городское управление, зеленые низкоуглеродные инициативы.
 - **Эффект мультипликатора элементов данных**

Ключевые достижения: технология блокчейн



- Цифровые финансы и технология блокчейн
- **Блокчейн** — это технология распределенного реестра, которая позволяет создавать безопасную, прозрачную и защищенную от несанкционированного доступа запись транзакций. Транзакции группируются в блоки, которые затем криптографически связываются и защищаются. Эта цепочка блоков поддерживается в децентрализованной сети компьютеров (узлов) посредством механизма консенсуса.

- Ключевые особенности блокчейна
 - Технология распределенного реестра (DLT): каждый узел независимо проверяет и регистрирует транзакции
 - Децентрализованная сеть: нет единой точки отказа
 - Неизменность: записи транзакций постоянны и защищены от несанкционированного доступа
 - Безопасность и прозрачность: криптографические методы защиты транзакций; все участники сети имеют доступ к одним и тем же данным, которые обновляются в режиме реального времени
 - Анонимность: совершение транзакции, не раскрывая свою реальную личность
 - Прослеживаемость: легко отследить историю любого актива или данных, записанных в блокчейне



Содержание

Введение в цифровую экономику

Нормативно-правовая база в цифровой экономике

Соблюдение требований и управление в цифровом Китае

Практический пример: Проект «mBridge»

Проблемы цифровой экономики



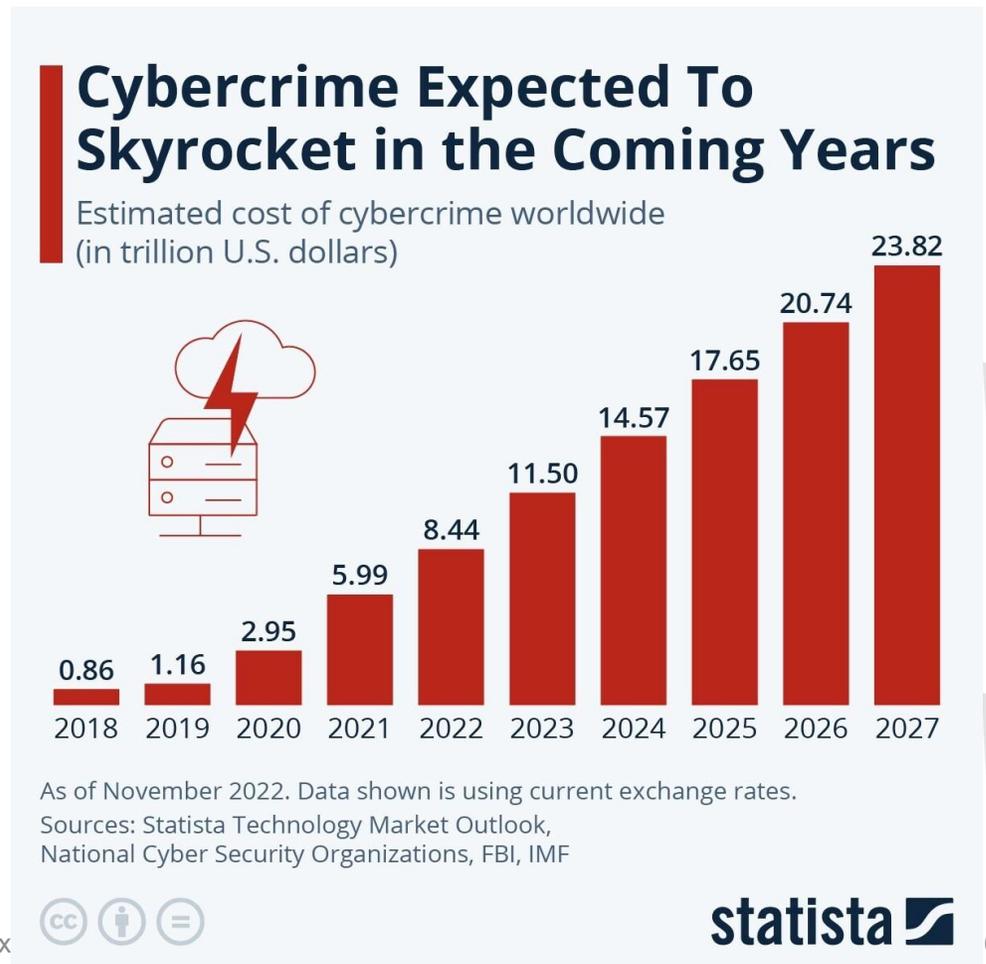
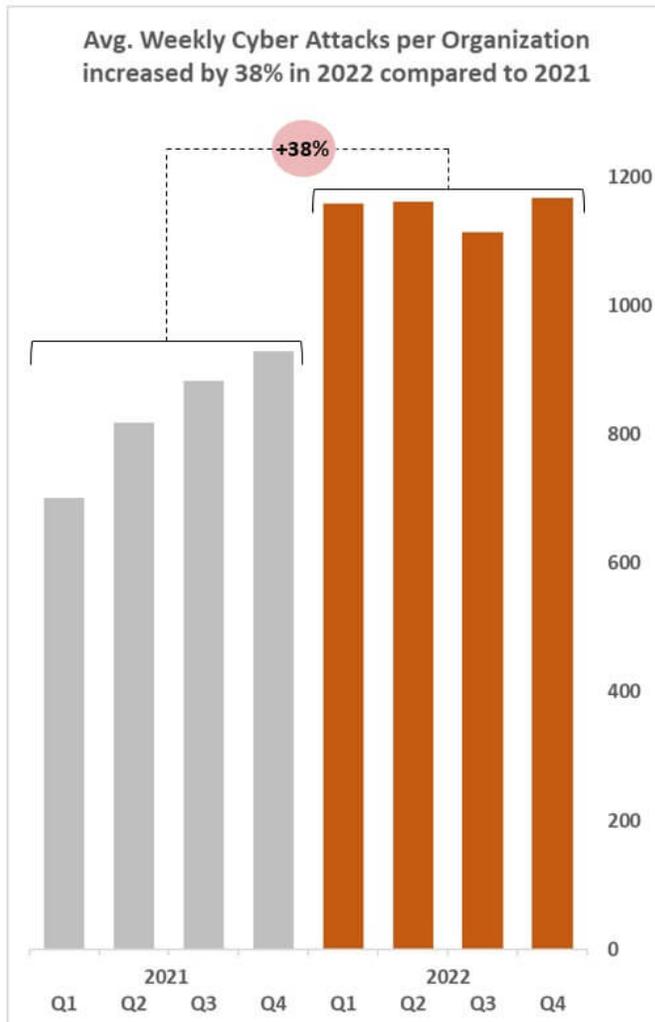
- Конфиденциальность и безопасность данных
 - Угрозы кибербезопасности: утечки данных, вредоносное ПО, фишинг и социальная инженерия.
 - Для борьбы с трансграничными киберугрозами необходимы гармонизация мировых стандартов и укрепление международного сотрудничества.
 - Человеческий фактор и обучение также имеют решающее значение.



ИИ и кибербезопасность



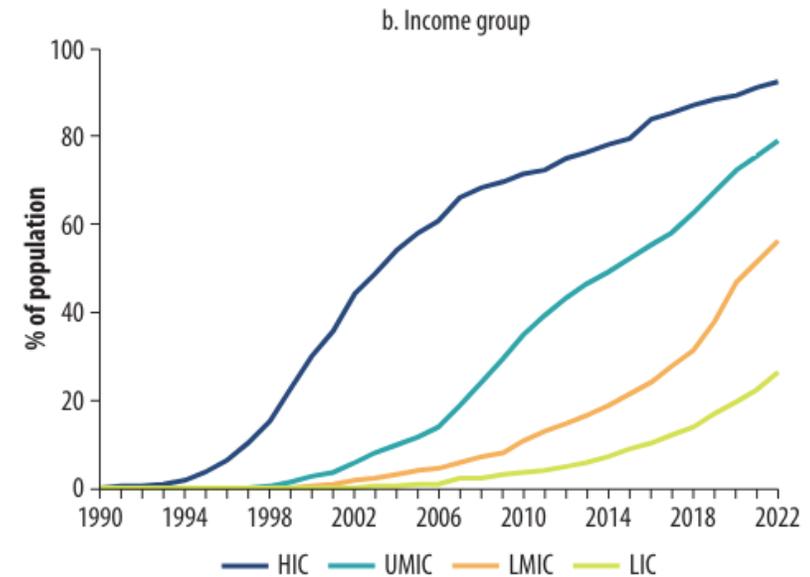
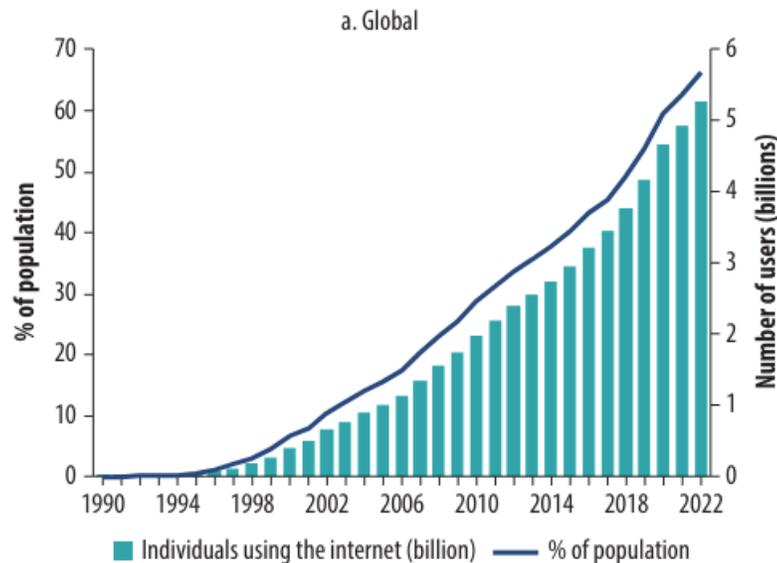
- Развитие технологий искусственного интеллекта, вероятно, приведет к увеличению числа кибератак.



Проблемы цифровой экономики



- Цифровой разрыв и неравенство: не у всех есть равный доступ к цифровым инструментам и подключению к Интернету.



Проблемы цифровой экономики



- Зависимость от технологий и системные риски
 - Пример: глобальный сбой в работе ИТ-систем



Проблемы цифровой экономики



- Нормативно-правовые сложности
 - Быстрый рост цифровой экономики и надлежащие нормативные рамки
 - Различная нормативно-правовая база в разных регионах
- Смещение рабочих мест и разрыв в навыках
- Этические и социальные последствия
 - алгоритмическая предвзятость, потеря конфиденциальности и т.д.
- Новые технологии необходимо регулировать.

Соблюдение требований и управление в цифровой экономике



- Стремительный рост цифровой экономики несет с собой как возможности, так и проблемы, делая **соответствие требованиям, риски и управление (CRG)** важнейшими компонентами для устойчивых и этичных деловых операций.
 - Обеспечение соблюдения законодательства и защиты данных: соблюдение нормативных требований, безопасность данных
 - Защита интересов заинтересованных сторон: доверие потребителей, доверие инвесторов
 - Поддержание операционной эффективности и безопасности: управление рисками, непрерывность работы
 - Содействие инновациям и этичным практикам: баланс между соблюдением требований и инновациями



- **Правила конфиденциальности и защиты данных**
 - Управление данными: определение порядка сбора, обработки, хранения и использования данных.
 - Конфиденциальность данных: анонимизация данных, шифрование данных, безопасное хранение и т. д.
- Глобальные правила: например, Общий регламент по защите данных (GDPR) в Европейском Союзе, Закон штата Калифорния о защите конфиденциальности потребителей (CCPA) в США и Закон о защите личной информации (PIPL) в Китае.
- Отраслевые правила: например, Стандарт безопасности данных индустрии платежных карт (PCI DSS) в сфере финансовых услуг.
- Местные законы



Общий регламент по защите данных



- **Общий регламент по защите данных (GDPR):** самый строгий закон о конфиденциальности и безопасности в мире
 - Вступил в силу 25 мая 2018 года
- **Ключевые цели**
 - **Усиление защиты данных:** усиление защиты персональных данных физических лиц на территории ЕС.
 - **Гармонизировать законы о конфиденциальности данных:** стандартизировать правила защиты данных в ЕС, чтобы упростить нормативную среду для бизнеса.
 - **Повысить подотчетность и соблюдение требований:** обеспечить ответственность организаций за защиту персональных данных и соблюдение принципов защиты данных.



- GDPR определяет:
 - Основные права физических лиц в цифровую эпоху
 - Право быть информированным
 - Право доступа
 - Право на исправление
 - Право на удаление
 - Право на ограничение обработки
 - Право на переносимость данных
 - Право на возражение
 - Права в отношении автоматизированного принятия решений и профилирования
 - Обязанности лиц, обрабатывающих данные
 - Методы обеспечения соблюдения требований
 - Санкции для тех, кто нарушает правила



- **Стандарты и положения по кибербезопасности**
 - Необходим для защиты цифровой инфраструктуры и конфиденциальных данных.
 - Глобальные правила: например, Закон о кибербезопасности и обмене информацией (CISA) в США, Директива о сетевой и информационной безопасности (NIS) в Европейском Союзе и Закон о кибербезопасности (CSL) в Китае.
 - Отраслевые нормативные акты: например, Закон о переносимости и подотчетности медицинского страхования (HIPAA) в здравоохранении и Стандарт безопасности данных индустрии платежных карт (PCI DSS) в сфере финансовых услуг.

Закон об обмене информацией о кибербезопасности



- Закон об обмене информацией о кибербезопасности (CISA): повышение устойчивости кибербезопасности путем содействия сотрудничеству между частными компаниями и государственными учреждениями для обмена информацией о киберугрозах.
 - Принят в 2015 году
- Ключевые цели
 - **Содействовать обмену информацией о киберугрозах:** создать правовую основу для добровольного обмена данными о киберугрозах.
 - **Снижение юридической ответственности:** обеспечение защиты от ответственности компаний, добросовестно обменивающихся информацией.
 - **Поддержка критической инфраструктуры:** фокус внимания на защите важнейших секторов, таких как энергетика, здравоохранение и финансы.
 - **Поощрение сотрудничества:** поощрять двусторонний обмен информацией об угрозах между правительством и частным сектором.

- **Регулирование цифровых финансов и криптовалют**
 - **Борьба с отмыванием денег (AML) и принцип «Знай своего клиента» (KYC):** Обеспечить проверку пользователей и отслеживание транзакций для предотвращения незаконной деятельности.
 - **Предотвращение мошенничества и защита прав потребителей:** защита от мошенничества, обеспечение безопасности активов клиентов и защита инвесторов.
 - **Соблюдение налоговых требований:** убедиться, что цифровые транзакции и прибыль от криптовалюты отражаются в отчетности для целей налогообложения.
 - **Добросовестность и стабильность рынка:** решать такие проблемы, как манипулирование ценами, особенно для стейблкоинов и других высокорисковых активов.



- **Положения о криптовалюте**
 - В некоторых странах создана нормативная база для криптовалюты.
 - Агентство финансовых услуг Японии (FSA) требует от криптовалютных бирж регистрации и соблюдения стандартов **AML** и **KYC**
 - Швейцария: швейцарский закон о блокчейне в 2021 году
 - Китай запретил децентрализованные криптовалюты, но разработал свою цифровую валюту центрального банка (ЦВЦБ)



- **Руководящие принципы в области искусственного интеллекта и этики**
 - Прозрачность: объяснимые решения ИИ для укрепления доверия.
 - Справедливость и недискриминация: минимизация предвзятости для предотвращения несправедливого обращения.
 - Подотчетность и человеческий надзор: обеспечение возможности человеческого надзора или вмешательства в высокорисковые системы ИИ.
- Примеры структур ИИ: Закон ЕС об ИИ; Директива об автоматизированном принятии решений в Канаде; Принципы использования ИИ в Японии.

Закон ЕС об искусственном интеллекте: новаторская концепция



- **Классификация на основе рисков:** приложения ИИ классифицируются как имеющие минимальный, ограниченный, высокий или неприемлемый риск.
 - **Минимальный и ограниченный риск:** основные требования к прозрачности для приложений с низким уровнем риска, таких как чат-боты или игры на базе искусственного интеллекта.
 - **Высокий риск:** строгие стандарты для таких чувствительных областей, как здравоохранение и финансы, включая качество данных и человеческий надзор.
 - **Неприемлемый риск:** Запрещенные приложения, такие как социальный скоринг.
 - Меры подотчетности.



Другие глобальные подходы к этике ИИ



- **Соединенные Штаты Америки:** Закон о правах искусственного интеллекта определяет такие принципы, как конфиденциальность данных и свобода от дискриминации.
- **Канада:** Директива об автоматизированном принятии решений для ИИ в государственном секторе, уделяющая особое внимание прозрачности и подотчетности.
- **Япония:** Принципы использования ИИ поощряют этичную разработку ИИ с добровольным подходом к соблюдению требований.



Содержание

Введение в цифровую экономику

Нормативно-правовая база в цифровой экономике

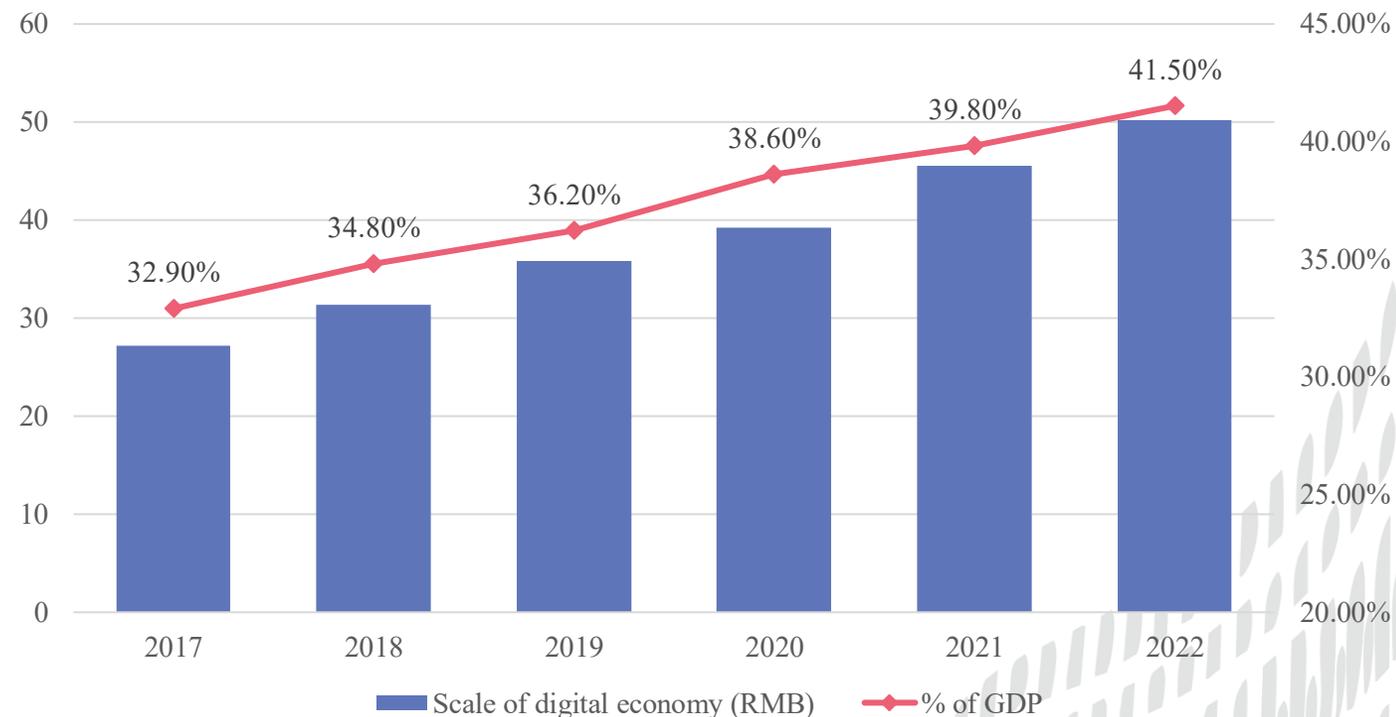
Соблюдение требований и управление в цифровом Китае

Практический пример: Проект «mBridge»

Цифровая экономика в Китае



- Цифровая экономика в Китае внесла основной вклад в ВВП
- XX Съезд КПК: Ускорить развитие цифровой экономики, содействовать глубокой интеграции цифровой экономики и реальной экономики, а также создать цифровой промышленный кластер с международной конкурентоспособностью.



Производительные силы нового качества



厦门国家会计学院
XIAMEN NATIONAL ACCOUNTING INSTITUTE

- Производительные силы нового качества: высокие технологии, высокая эффективность и высокое качество
- Технологические инновации являются «основным элементом развития производительных сил нового качества»
- Производительные силы нового качества и цифровая экономика тесно взаимосвязаны



- Основные достижения цифровой экономики Китая
 - **Цифровая инфраструктура:** развертывание 5G, цифровая валюта центрального банка (e-CNY)
 - **Инновационный потенциал цифровой индустрии:** ИИ, большие данные, облачные вычисления и т. д.
 - **Промышленная цифровая трансформация:** интеллектуальное производство, платформенная экономика
 - **Доминирование электронной коммерции и цифровых платежных систем**
 - **Цифровизация государственных услуг:** электронное правительство, проекты умных городов
 - **Сетевая безопасность и управление данными:** кибербезопасность, управление данными
 - **Международное сотрудничество в области цифровой экономики:** Глобальное партнерство



Существующие структуры соблюдения требований и регулирования



- **Закон о защите личной информации (PIPL):** Закон о защите данных
 - Вступил в силу 1 ноября 2021 года.
 - Область применения: Регулирует сбор, использование, хранение и передачу персональных данных.
 - PIPL применяется к обработке персональных данных физических лиц на территории Китая, независимо от того, где находится обработчик данных.
- Индивидуальные права: доступ и копирование, исправление и удаление, переносимость и отзыв согласия.
- Обязанности обработчиков данных: прозрачность, меры безопасности, минимизация данных, сохранение данных.



Существующие структуры соблюдения требований и регулирования



- **Закон о кибербезопасности (CSL)**
 - Вступил в силу 1 июня 2017 года.
 - Область применения: Устанавливает комплексные требования к безопасности сети и защите данных.
 - CSL распространяется на сетевых операторов, в число которых входят владельцы, администраторы и поставщики услуг, использующие сети на территории Китая.
- **Обязательства по обеспечению безопасности сети:** меры по обеспечению безопасности сети, реагирование на инциденты.
- **Критическая информационная инфраструктура (КИИ):** операторы КИИ должны внедрять усиленные меры безопасности, проводить регулярные оценки безопасности и проходить проверки со стороны соответствующих органов.
- **Локализация данных:** персональная информация и важные данные, собранные в Китае, должны храниться внутри страны.

Существующие структуры соблюдения требований и регулирования



- **Закон о безопасности данных (DSL):** Комплексная структура для усиления защиты данных, обеспечения национальной безопасности и регулирования практики обработки данных в различных секторах.
 - Вступил в силу 1 сентября 2021 году.
- **Ключевые компоненты**
 - **Классификация и сортировка данных:** классифицировать данные по чувствительности и важности – «основные», «важные» или «общие».
 - **Трансграничная передача данных:** Ограничить трансграничную передачу данных, особенно критически важных и конфиденциальных данных.
 - **Меры безопасности данных:** Реализация надежных мер безопасности.
 - **Соблюдение требований и подотчетность:** Создать внутреннюю систему управления безопасностью данных.

- В Китае нет единого закона об ИИ, но разработано множество нормативных актов, влияющих на ИИ, уделяя особое внимание безопасности данных, конфиденциальности, прозрачности и государственному надзору.
- Этические принципы:
 - **Надежный ИИ:** Подчеркивает надежность, справедливость и прозрачность, гарантируя, что ИИ принесет пользу обществу, минимизируя риски.
 - **Согласование с правительством:** Этические нормы для ИИ нового поколения (2021 г., Министерство науки и технологий)
 - Справедливость и отсутствие дискриминации; Прозрачность и подотчетность; Защита конфиденциальности
 - **Алгоритмическое регулирование** (2022 г., Администрация по киберпространству Китая)

- Основные нормативные рамки:
 - **Закон о безопасности данных (DSL):** Регулирует обработку данных и трансграничную передачу данных, обеспечивая безопасное управление данными для систем ИИ.
 - **Закон о защите личной информации (PIPL):** фокусирует внимание на конфиденциальности данных, требует согласия на сбор данных и защищает личную информацию, используемую в приложениях ИИ.
 - **Закон о кибербезопасности:** Устанавливает основополагающие требования к кибербезопасности, особенно касающиеся ИИ в критически важной инфраструктуре.
- Направления деятельности: защита данных, контроль конфиденциальной информации и согласование ИИ с национальными приоритетами.

- Общий схематический план для построения цифрового Китая

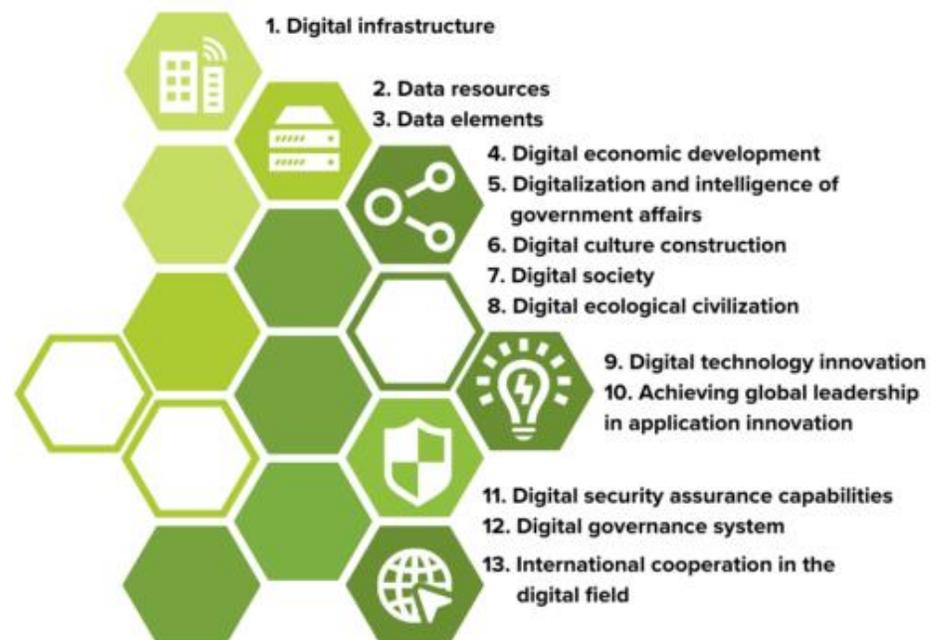
Development goals

By 2025

an integrated advancement pattern of horizontal access, vertical connectivity, and strong coordination will be basically formed, and important progress will be made in building a digital China.

By 2035

China's level of digital development will have been at the world's forefront, and major achievements will have been made in the construction of a digital China.



- **Общий схематический план для построения цифрового Китая: структура «2522»**
 - **Укрепление двух основ:** цифровая инфраструктура и система ресурсов данных.
 - **Содействие глубокой интеграции цифровых технологий с:** цифровой экономикой, цифровыми государственными услугами, цифровой культурой, цифровым обществом, цифровой экологической цивилизацией.
 - **Улучшение двух основных потенциалов:** системы инноваций в области цифровых технологий и структуры цифровой безопасности.
 - **Оптимизация двух сред:**
 - Создание справедливой и стандартизированной экосистемы цифрового управления
 - Улучшение международного цифрового сотрудничества

Две основы > Интегрированный план по 5 сферам > 2 основных потенциала > 2 среды



Прокладываем путь к цифровому Китаю



- В общем схематическом плане для построения цифрового Китая особое внимание уделяется **соблюдению требований и управлению/регулированию**.
 - Цифровой сектор необходимо регулировать.
 - Сектор обеспечения соблюдения требований необходимо оцифровать.
- Основные требования к соблюдению требований и управлению:
 - Совершенствование правовой и нормативной системы
 - Создание системы технологических стандартов
 - Повышение уровня управления
 - Очищение киберпространства





Содержание

Введение в цифровую экономику

Нормативно-правовая база в цифровой экономике

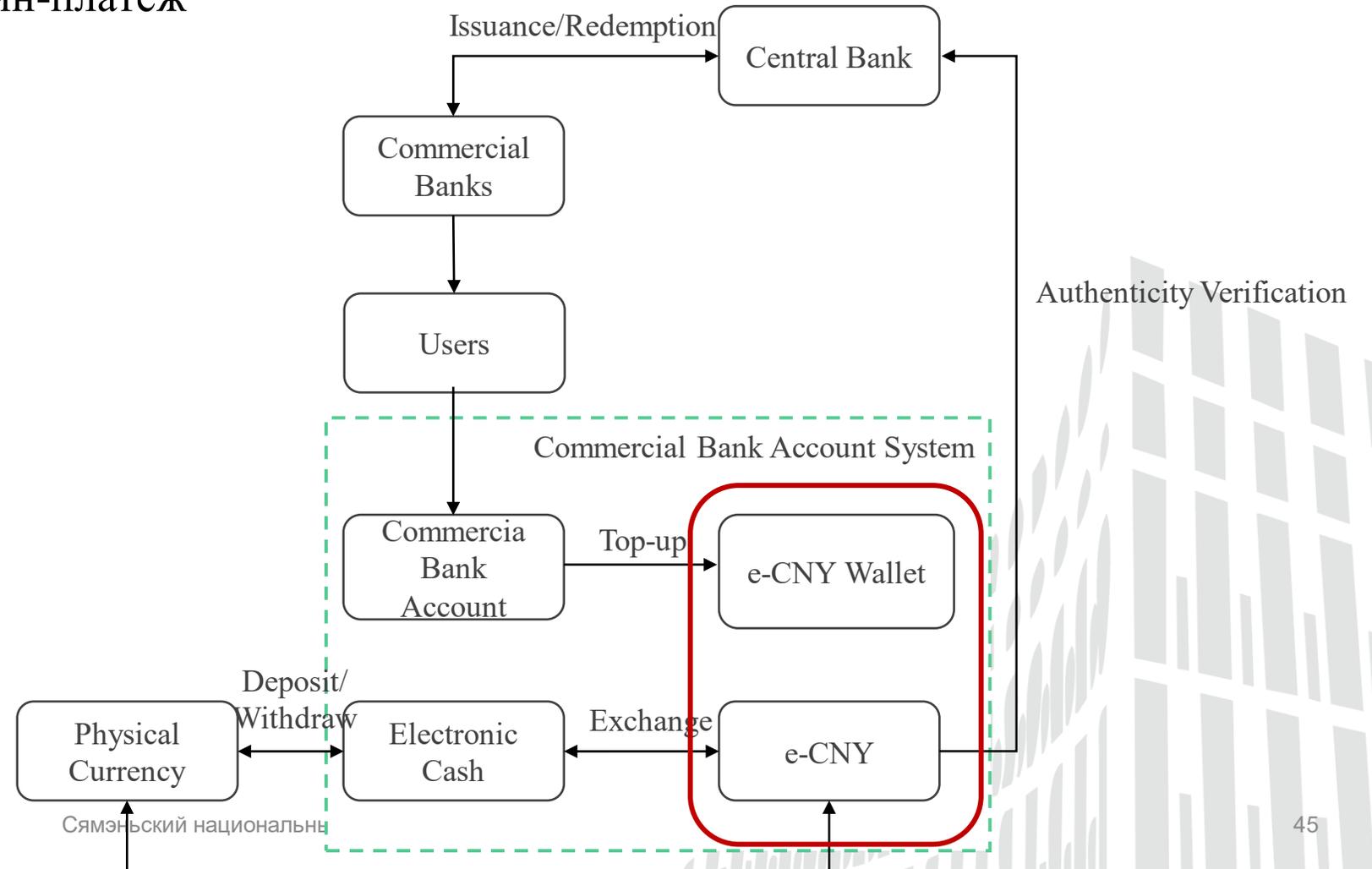
Соблюдение требований и управление в цифровом Китае

Практический пример: Проект «mBridge»

- Электронные платежи в цифровой валюте (DC/EP): e-CNY, или цифровой юань, представляет собой централизованную цифровую валюту, похожую на наличные деньги, которую можно использовать для розничных платежей и/или оптовых расчетов.
- Китай стал первой крупной экономикой, выпустившей цифровые валюты центрального банка.
- Факторы, способствующие развитию e-CNY



- Двухуровневая операция: Центральный банк и коммерческие банки
- Управляемый анонимный
- Двойной офлайн-платеж



ЦВЦБ в трансграничных платежах



- В октябре 2020 года G20 одобрила дорожную карту по совершенствованию трансграничных платежей и изучению того, как ЦВЦБ могут потенциально улучшить трансграничные платежи.
- Основные преимущества:
 - **Повышенная эффективность и скорость:** отсутствие посредников
 - **Улучшенная прозрачность:** транзакции, совершаемые с использованием ЦВЦБ, регистрируются в блокчейнах.
 - **Нормативно-правовая база:** надзор со стороны Центрального банка



ЦВЦБ в трансграничных платежах



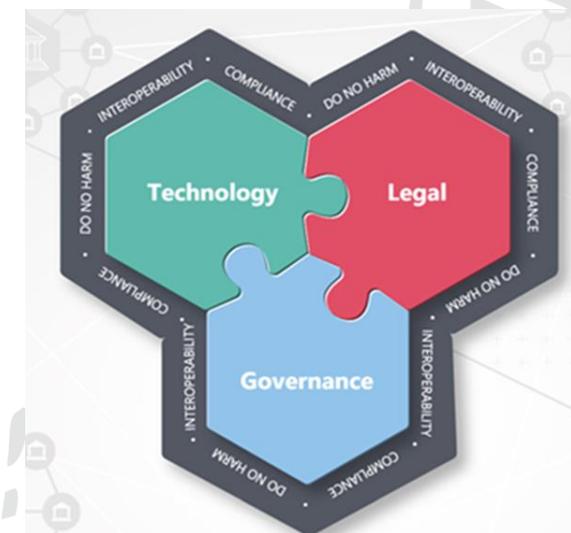
- **Проект «mBridge»:** инициирован Центром инноваций BIS (Банка международных расчетов), Институтом цифровой валюты Народного банка Китая, Управлением денежного обращения Гонконга, Банком Таиланда и Центральным банком Объединенных Арабских Эмиратов.
- Цель: изучить единую платформу для оптовых трансграничных платежей, объединяющую несколько ЦВЦБ (цифровых валют центральных банков).
- Цели проекта:
 - Устранить основные проблемы трансграничных платежей, такие как высокие издержки, риски расчетов и низкая скорость.
 - Авансовые трансграничные расчеты деньгами центрального банка.
 - Поддерживать использование местных валют в трансграничных транзакциях.
 - Создать возможности для новых и инновационных платежных продуктов и услуг.



Принципы проекта «mBridge»



- **Соблюдение требованиям:** платформа, разработанная для проекта «mBridge» соответствует международным стандартам и нормам различных юрисдикций, таким как ПФТ/ОД.
- **Не навреди:** центральные банки по-прежнему могут осуществлять контроль обменного курса и меры по управлению потоками капитала на платформе.
- **Операционная совместимость:** платформа поддерживает операционную совместимость с существующими финансовыми инфраструктурами участников.

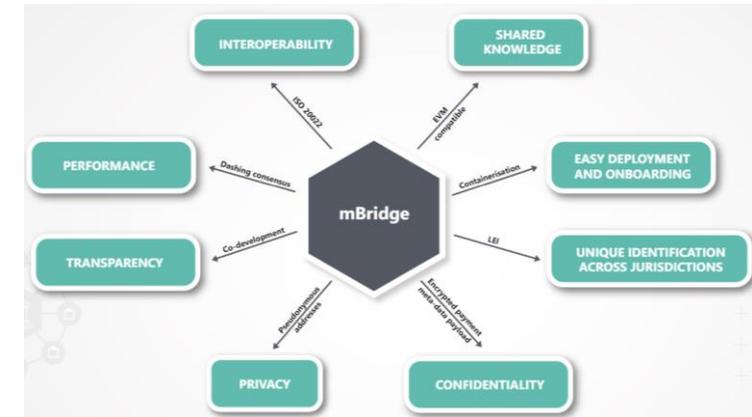


Проект «mBridge» и управление



Как «mBridge» помогает снизить риски при трансграничных платежах?

- Подход Lego-Bricks: модулирование таких функций, как платежи, обмен валюты, управление капиталом и функции ПФТ/ОД.
- Создан на основе технологии распределенного реестра (DLT)
 - Нет единой точки отказа
 - Повышенная безопасность
 - Прозрачно для уполномоченных сторон
 - Защита конфиденциальности
- Взаимодействие с собственными системами участников
 - Наличие внутренней системы ЦВЦБ **не является** обязательным условием для присоединения к платформе mBridge.



Развитие проекта «mBridge»



- В ходе пилотного этапа 2022 года платформа mBridge успешно обрабатывала транзакции на реальные суммы.
 - 20 банков в Гонконге (САР Китая), Таиланде, материковом Китае и ОАЭ использовали платформу mBridge для проведения 164 платежных и валютных операций на общую сумму более 22 миллионов долларов США.
- По состоянию на середину 2024 года проект «mBridge» достиг этапа минимально жизнеспособного продукта (MVP).
 - Означает полностью функциональную платформу, готовую к более широкому использованию.
 - Включает такие функции, как трансграничные платежи в режиме реального времени, операции с иностранной валютой и проверки соответствия.
- Проект «mBridge» теперь приглашает частные компании предлагать новые решения и варианты использования, которые помогут развивать платформу и продемонстрировать весь ее потенциал. Заинтересованные компании могут подать заявку на участие.

Будущие тенденции в цифровом управлении



- Суверенитет и локализация данных
- Регулирование ИИ и этическое управление
- Конфиденциальность и кибербезопасность
- Стандартизация новых технологий
- Прозрачность и подотчетность

- Цифровая экономика: экономический рост, эффективность и удобство, глобальный охват
- Важность соблюдения требований и управления для обеспечения этических и законных операций в цифровой экономике
- Роль технологий в повышении уровня соответствия требованиям посредством автоматизированного мониторинга и отчетности
- Интеграция технологий в обеспечение соответствия создает как проблемы, так и возможности

Вопросы и комментарии?



厦门国家会计学院
XIAMEN NATIONAL ACCOUNTING INSTITUTE

