Aggregion

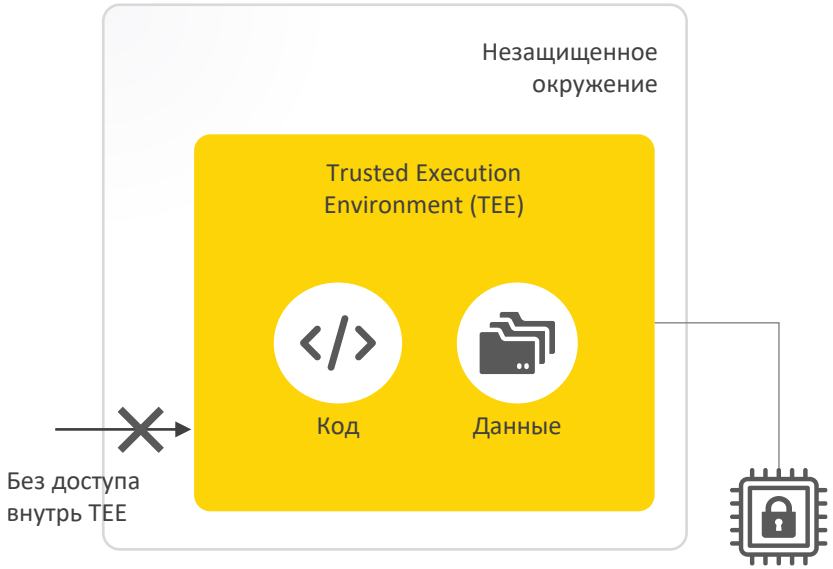
Конфиденциальные вычисления:

технологии и кейсы применения

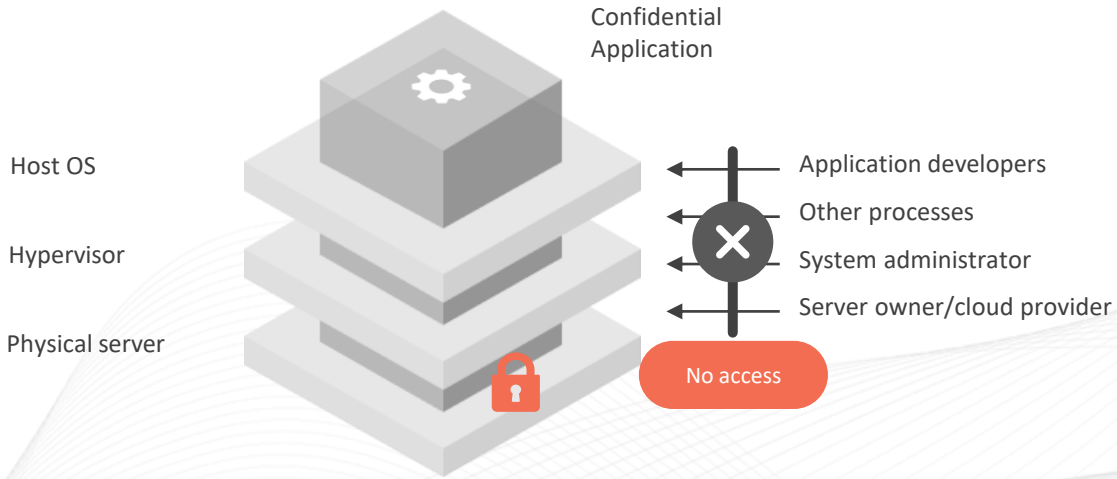
AGGREGION

Конфиденциальные вычисления

Защищают данные при их обработке с использованием шифрования и изолирования области памяти.
Ключ шифрования – не извлекаемый, секретный, встроен в процессор.



При шифровании встроенным ключом процессора никто не может получить доступ внутрь TEE



Ключевые владельцы технологий TEE

Технология доступна на рынке, автономна и локализована. Используется в промышленных внедрениях.

Конфиденциальные вычисления – недостающий элемент для полной защиты данных

Конфиденциальные вычисления позволяют реализовать сквозную защиту данных на всех этапах обработки: во время хранения, передачи и обработки

Защита при хранении

Шифрование данных в СУБД, файловой системе

Защита при передаче

Шифрование данных при передаче по сети

NEW

Конфиденциальные вычисления

Защита при использовании

Защита данных в RAM и при вычислениях

Существующая защита

Полная сквозная защита данных

Конфиденциальные вычисления обеспечивают:

Конфиденциальность данных

Невозможность просмотра данных внутри TEE

Целостность данных

Невозможность изменения/удаления данных внутри TEE

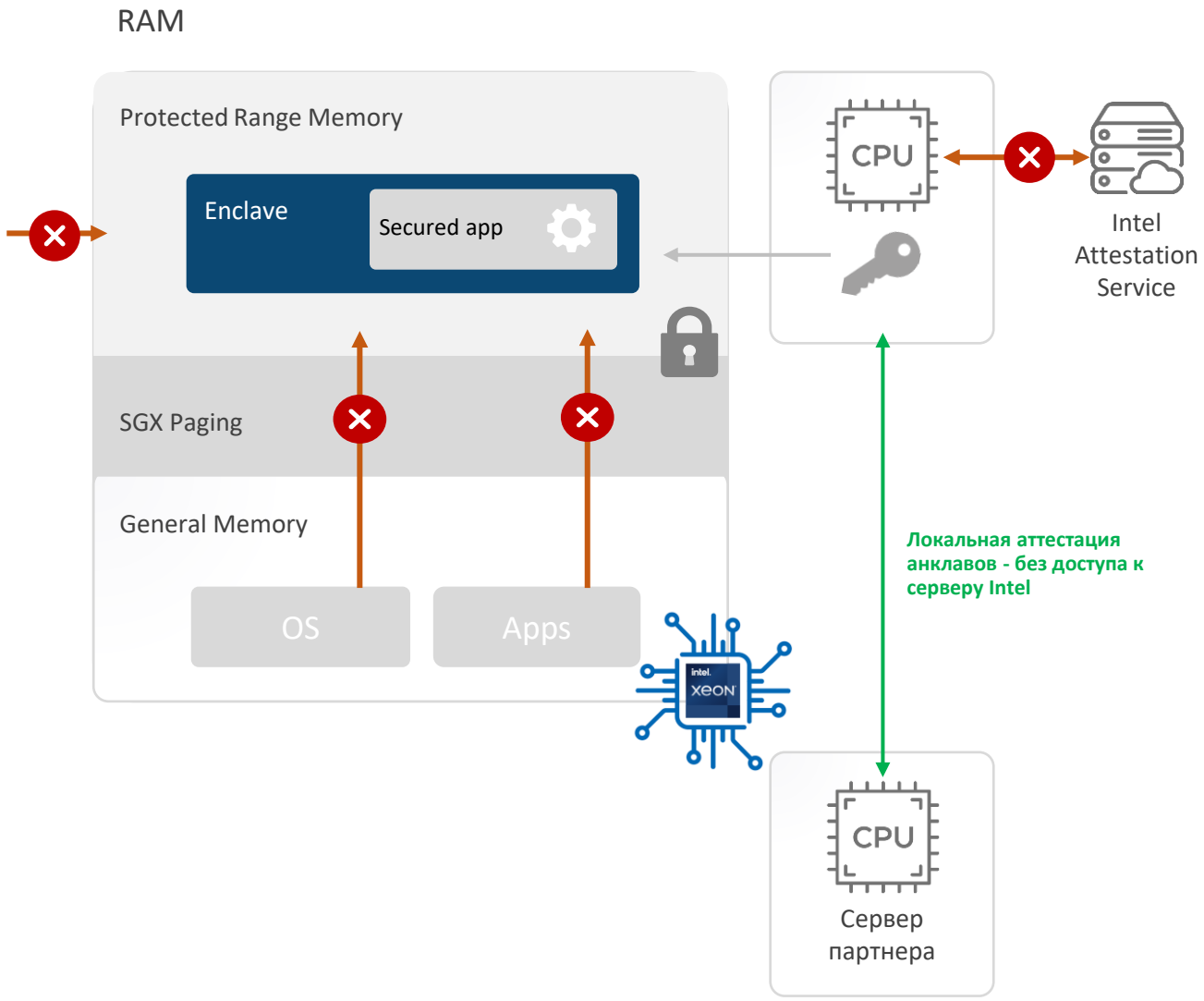
Целостность кода

Невозможность изменения/удаления исполняемого кода TEE

Сравнение TEE на различных технологиях

	Intel SGX	Intel TDX	AMD SEV	NVIDIA H100	Huawei Qintian	Amazon Nitro
Защищаемая область	Процесс	ВМ	ВМ	ВМ + GPU	ВМ	ВМ
Корень доверия	CPU	CPU	CPU	CPU + GPU	Cloud Provider/Hypervisor	Cloud Provider (Amazon Only)
Аттестация анклавов	Да	Частично	Частично	Частично	Да	Да
Специальное аппаратное обеспечение	Да (поддержка инструкций SGX на уровне CPU)	Да (поддержка инструкций TDX на уровне CPU)	Да, процессоры AMD с поддержкой SEV	Да, процессоры AMD с поддержкой SEV + чип NVIDIA H100	Уточнение	Нет
Поддержка в облаках	Selectel, MS Azure, GCore, CloudSigma, OVH	OVH	MS Azure, Google Cloud	MS Azure	Huawei Cloud	Amazon

Intel SGX: технология доступна на рынке, автономна и используется в промышленных кейсах



- SGX – набор инструкций работы с шифрованной памятью, встроен в процессор при его производстве. Нет зависимостей от Intel после производства процессора.
- Технология поддерживается всеми современными серверными моделями.
- При использовании локальной аттестации анклавов нет необходимости доступа к серверу Intel.

Полная автономность при использовании:

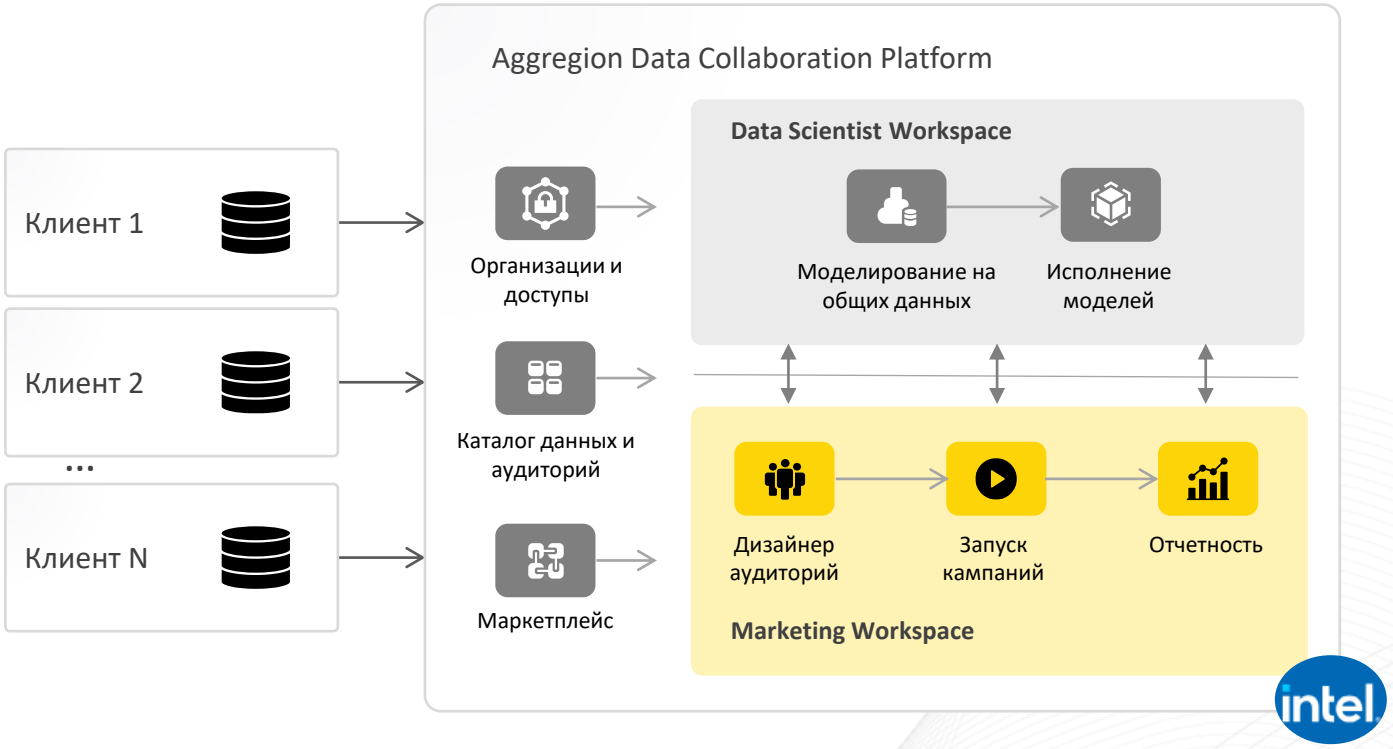
✓ Процессоры свободно доступны на рынке и в облачных сервисах

✓ Локальная аттестация анклавов без обращения к серверу Intel

Проверено на промышленном использовании в крупной финансовой группе

Aggregion Data Collaboration Platform

Единая платформа для совместной безопасной работы с данными и управления коммуникациями на их основе



Готовые решения для экосистем:

- Групповой Customer ID
- Customer Profile 360
- Управление согласием
- Моделирование и аналитика

Готовые решения для Retail Media:

→ Интеграция с рекламными платформами

→ Sales Lift отчетность

→ Верификация на основании фактовых данных

→ Отчетность и биллинг

- Сквозной цикл работы с данными на одной платформе: от публикаций в каталоге до моделирования и промышленного эксплуатации моделей
- Единая среда работы аналитиков и маркетологов
- Фиксация всех операций и биллинг партнеров

Технология конфиденциальных вычислений Aggregion

На примере использования анклавов у каждого из партнеров

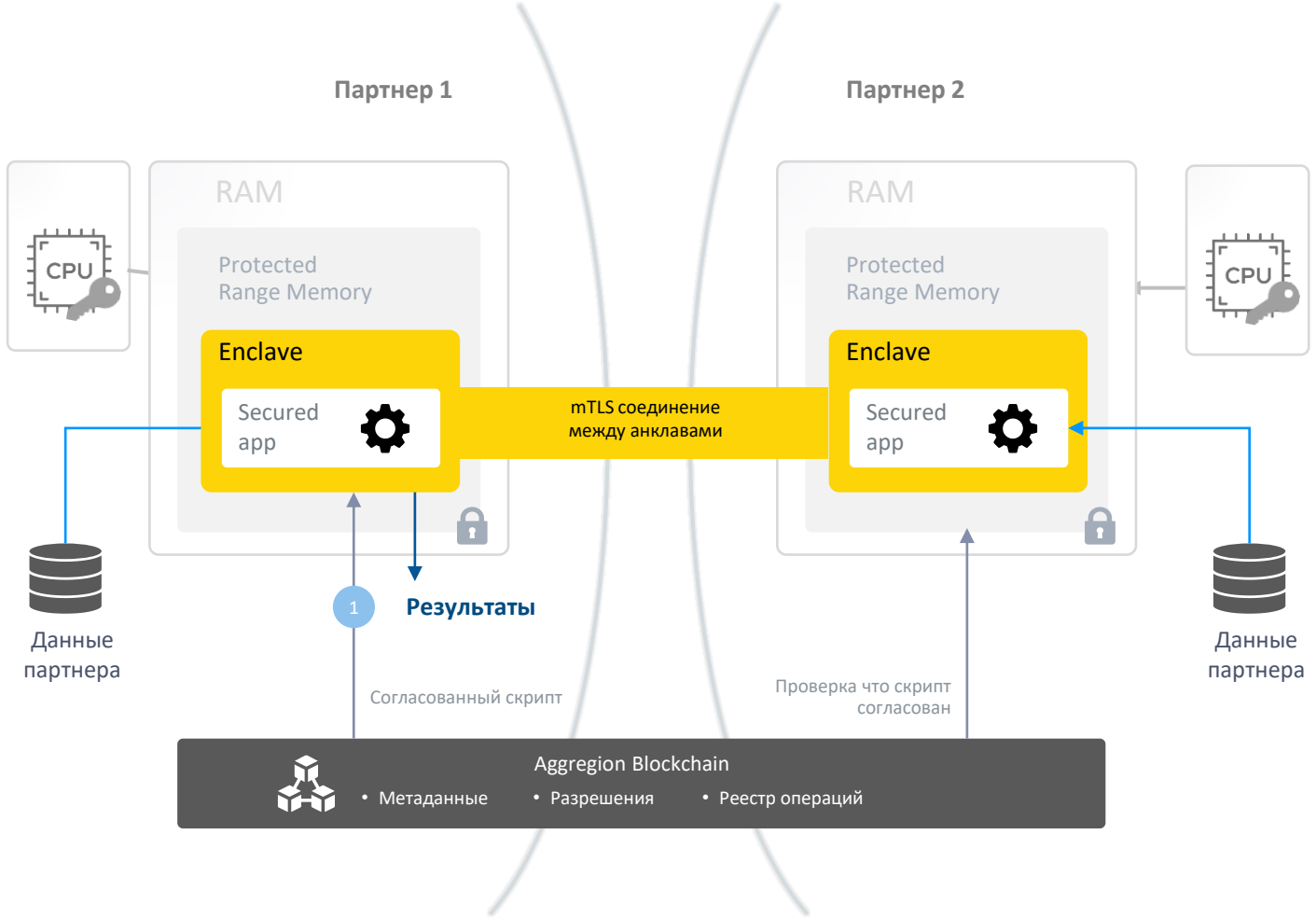
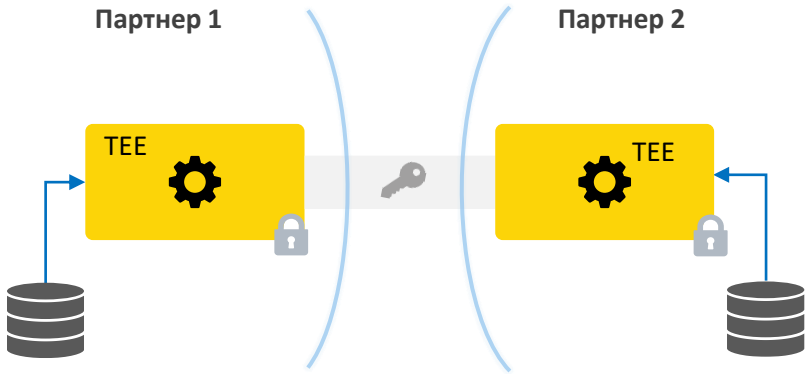


Схема работы:

1. Скрипты вычислений согласуются партнерами и подписываются в блокчейн.
2. Защищенный анклав запускается на стороне каждого партнера, между анклавами устанавливается защищенное соединение.
3. На стороне партнеров извлекается скрипт, проверяется, что он подписан партнером и помещается в анклав
4. Скрипт на стороне партнера извлекает данные для исполнения
5. Данные обрабатываются в каждом анклаве параллельно. Общая часть обработки происходит у одного из партнеров (как указано в параметрах скрипта)
6. Результаты обработки передаются одному из партнеров или во внешний сервис в соответствие с логикой скрипта
7. Фиксируется факт запуска скрипта в распределенном реестре. Анклавы завершаются и удаляются.

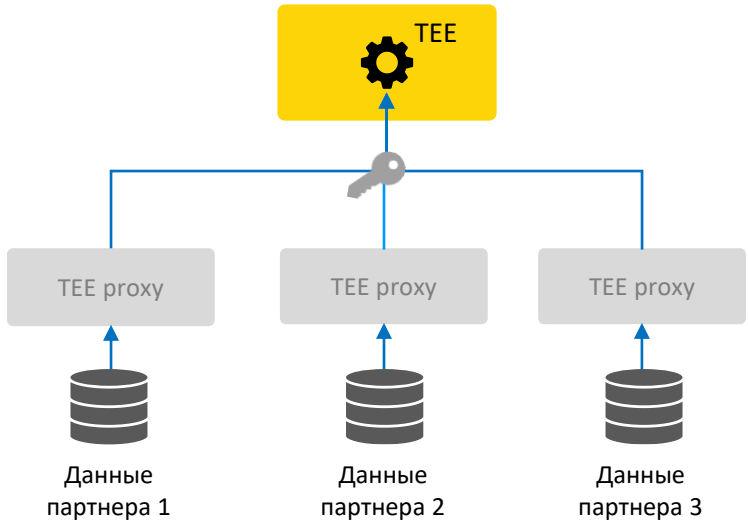
Варианты организации доверенных сред исполнения

Децентрализованный



- TEE в контуре партнеров
- Защищенное mTLS-соединение между TEE
- Возможность выбора TEE-исполнителя для каждого вычисления

Единый TEE-обработчик

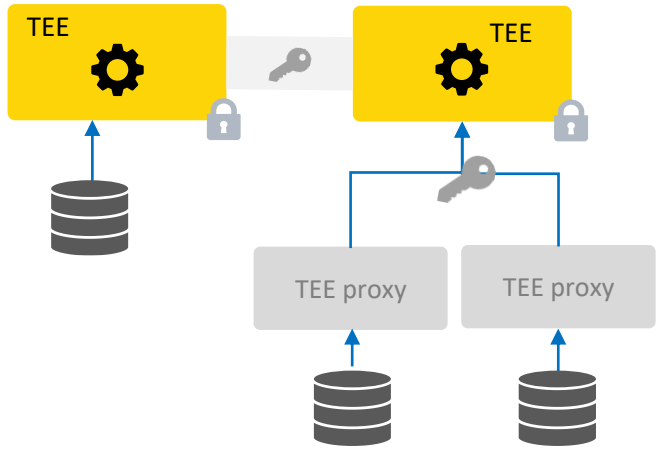


TEE Proxy – клиентское приложение или расширение в браузере.

Функции TEE proxy:

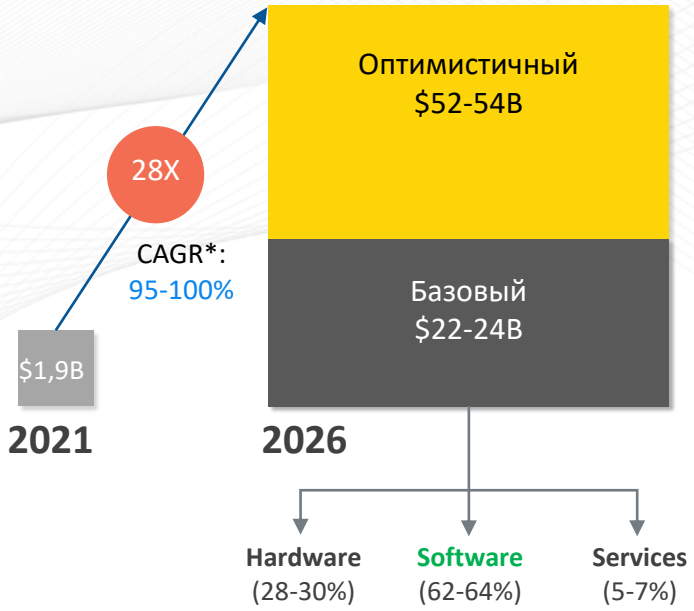
1. Аттестация TEE
2. Установка защищенного соединения с TEE

Гибридный



Отдельные TEE, например, для наиболее крупных компаний/с особыми требованиями к данным (тайна связи и пр.), TEE proxy – для остальных

Рынок конфиденциальных вычислений



- Privacy-enhancing calculations is a **top strategic technology trend** 2022 (Gartner)
- Gartner expects **60% of large organizations to use one or more privacy-enhancing computation techniques** by 2025. (Gartner)
- Privacy enhancing technology market is expected **to grow by a CAGR of 27% and reach a value of $ 25.8 billion** by 2033 (WEForum)

до **40%** рынка –

Банки и финтех

- Дек.23 – MS Azure добавляет поддержку NVIdia GPU для Confidential AI
- Окт.23 – Huawei выпускает Qingtian enclave в своем клауде
- Сен.23 – Google Cloud добавляет поддержку Intel TDX
- Окт.22 – NVidia выпускает H100 с поддержкой TEE для Confidential AI

* Confidential computing consortium

Всё ещё не доверяете Конфиденциальным вычислениям?

Microsoft использует Intel SGX для обеспечения безопасности данных в облачных средах. В Azure Confidential Computing SGX помогает изолировать чувствительные данные и вычисления. Intel SGX and TDX Use Case

Alibaba Cloud внедрила Intel SGX для защиты финансовых данных и улучшения безопасности своих облачных сервисов.Trenton Systems

Fortanix использует Intel SGX для создания решений в области управления ключами и шифрования, предлагая своим клиентам усиленную защиту данных на уровне аппаратного обеспечения. Fortanix - Intel SGX in Action

Google Cloud внедряет Intel TDX (Trust Domain Extensions) для обеспечения безопасности своих виртуальных машин. Google Cloud - Intel TDX Use Case

Министерство туризма Индонезии реализовало конфиденциальный обмен наборами данных между двумя операторами мобильной связи через TEE. Целью проекта было получение статистики туризма на основе объединенных обезличенных данных двух сотовых операторов. Intel SGX

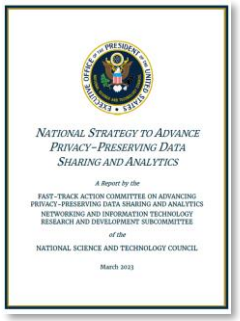
Компания Bosch использует Intel SGX для защиты данных при обучении моделей машинного обучения. Они используют реальные данные, которые остаются неизменными внутри анклава Intel SGX, что позволяет ускорить процесс и улучшить качество результатов, при этом соблюдая законы о защите данных Intel SGX

UK

Организация по экономическому развитию и сотрудничеству

Гайд по технологиям защиты privacy - ООН

Стратегия офиса Президента США по развитию конф. вычислений



Beeline Big Data

Совмещайте лучшее

Компании развивают партнерства, создавая ценности в совместной работе

Спиридонов Артём,
Program manager
Open Ecosystem and Big Data
AAspiridonov@beeline.kz
+77072117946

@ARTSELVIK