Суверенитет данных и безопасный ИИ: ключевые смыслы CyberDSA 2026

В Куала-Лумпуре (Малайзия) с 5 по 7 октября 2026 года прошла международная выставка и конференция Cyber Digital Services, Defence & Security Asia (CyberDSA). Мероприятие состоялось в выставочном центре MITEC и стало ключевой региональной площадкой для обсуждения вызовов кибербезопасности и доверенной цифровой трансформации.

Тема форума — «Продвижение безопасного ИИ, укрепление цифрового доверия и защита суверенитета данных». Организаторы сделали акцент на том, что в мире, где цифровые системы становятся всё сложнее, а искусственный интеллект меняет правила игры, критически важно обеспечить безопасность ИИ-решений, выстроить доверие в цифровых экосистемах и защитить контроль наций над своими данными.

По оценкам, в мероприятии приняли участие более 9000 профессионалов из 46 стран. Среди гостей — представители государственных структур, силовых ведомств, руководители служб информационной безопасности (CISO), исследователи, а также лидеры технологических компаний.

Помимо конференций, работала выставка, где компании демонстрировали решения в самых разных направлениях: защита сетей и дата-центров, облачные технологии, криптография, блокчейн, защита конечных устройств, концепция Zero Trust, разведка угроз и технологии безопасного ИИ. Также в рамках события провели флэш-токи (краткие экспертные выступления) и вручили премию Malaysia Cyber Security Award.

Среди партнёров и спикеров были представители Google, CyberSecurity Malaysia, Национального агентства кибербезопасности (NACSA), Вооружённых сил Малайзии, Индонезийского флота, Международного союза электросвязи (ITU), а также отраслевых советов (например, MOGSC — Malaysian Oil, Gas & Energy Services Council).

Организаторы ставили целью создать платформу для обмена знаниями, ускорить реализацию программ киберзащиты в регионе, укрепить партнёрства между государством и бизнесом, а также повысить глобальную конкурентоспособность за счёт усиления кибербезопасности. Для Малайзии событие также стало очередным шагом в укреплении роли страны как регионального центра кибердипломатии и планирования устойчивости инфраструктуры.

На CyberDSA 2026 чётко оформились три главных тренда, на которые стоит обратить внимание:

Безопасный ИИ как приоритет. Участники сошлись на том, что внедрение ИИ без встроенных механизмов защиты — это риск для всей экосистемы. В фокусе — «доверенный ИИ»: прозрачность моделей, контроль за обучением, защита от отравлений данных и атак через промпт-инъекции.

Суверенитет данных как новая норма. Государства всё чаще требуют, чтобы чувствительные данные оставались в пределах юрисдикции. На форуме

обсуждали, как это совместить с глобальной связностью и облачными сервисами, и какие архитектурные решения (например, федеративные вычисления) помогают соблюдать требования без потери эффективности.

Устойчивость критической инфраструктуры. Тема стала сквозной: от энергетики и водоснабжения до финансовых систем и умных городов. Акцент сделали на тестировании устойчивости (в том числе с помощью киберучений) и на том, как быстро восстанавливать работу после инцидентов.

На выставочной части CyberDSA представили несколько показательных решений, которые уже пилотируются в регионе:

Платформа для киберучений в реальном времени — позволяет моделировать атаки на сегменты инфраструктуры и отрабатывать реагирование без риска для действующих систем.

Система обнаружения аномалий на базе ИИ — выявляет отклонения в сетевом трафике и поведении пользователей, снижая нагрузку на SOC-команды.

Решения для Zero Trust в гибридных средах — помогают внедрять модель «никому не доверяй» в условиях, когда часть сервисов работает в облаке, а часть — в собственных ЦОДах.

В целом CyberDSA 2026 показала, что регион активно ищет ответы на новые вызовы: как развивать ИИ, не создавая уязвимостей, как защищать критически важные системы и как балансировать между открытостью данных и национальным суверенитетом.

Целуйко А.В., Балицкий П.С.
Финансовый университет при Правительстве РФ