

Перспективы развития технологий обеспечения доверия и безопасности программного обеспечения, в том числе с использованием технологий искусственного интеллекта

Арутюн Ишханович Аветисян

Директор Института системного программирования им. В.П. Иванникова РАН,
академик РАН

Email: director@ispras.ru

14.08.2026

Основа ИСП РАН – постоянно развивающаяся научная школа

С.А. Лебедев



В.А. Мельников



БЭСМ-6 в Музее науки Лондона



В.П. Иванников



Л.Н. Королёв



ИСП РАН сегодня – это:

>30 лет успешной работы

>30 направлений работы

>1000 сотрудников

**>200 компаний используют
наши технологии**



Открытая конференция ИСП РАН 2025
Около 2000 участников

Устойчивая модель развития: наука — образование — инновации

Устойчивое воспроизводство кадров и технологий требует единства науки, образования и **постоянной обратной связи** от решения реальных задач.



Наука

Фундаментальные исследования и научные школы



Образование

Подготовка кадров через участие в реальных исследованиях



Инновации / индустрия

Практические задачи и **обратная связь** для развития технологий



ИСП РАН: устойчивая модель в меняющихся условиях

НАУКА + ОБРАЗОВАНИЕ + СЛОЖНЫЕ ПРАКТИЧЕСКИЕ ЗАДАЧИ + ОБРАТНАЯ СВЯЗЬ → РАЗВИТИЕ ТЕХНОЛОГИЙ

1990-е — 2000-е

Международные технологические компании

Сложные R&D-задачи и обратная связь от глобальной индустрии

2010-е

Российские и международные заказчики

Расширение промышленного применения собственных технологий

2020-е

Российская индустрия, государство и профессиональные сообщества

Совместное развитие технологий, апробация и обратная связь от множества пользователей

Меняются заказчики, рынки и внешние условия — ИСП РАН сохраняет научную модель и адаптирует механизмы получения задач и обратной связи, необходимые для развития технологий.



Технологическая независимость ≠ технологическая изоляция

Участие в мировой науке

Передовые технологии невозможно развивать вне глобального научного контекста.

Международная кооперация

Совместные исследования, лаборатории, образовательные проекты и технологические сообщества.

Экспорт технологий и компетенций

Выход на внешние рынки не только с продуктом, но и с научными инновациями, образованием и центрами компетенций.



За последний год ИСП РАН:

- Подписал соглашение с Национальным суперкомпьютерным центром в Цзинане о создании Китайско-Российской совместной лаборатории искусственного интеллекта.
- Совместно с Институтом общественных наук Президентской академии выступил соорганизатором единственного российского национального мероприятия в рамках Глобального диалога ООН по управлению ИИ — международной сессии о доверии и управлении генеративным ИИ в Женеве.
- Представил разработки в области цифровой медицины на крупнейшей технологической выставке Африки GITEX Africa 2026 в Марракеше.

..и многое другое!

Сложность современного ПО

Сейчас программы:

- Быстро растут
- Усложняются
- Сочетают множество разнородных технологий
- Не обладают базовым доверием

В то же время программам необходимы:

- Эффективность
- Продуктивность
- Доверенность*

*Доверенность в данном контексте = безопасность



Инструменты РБПО: технологически независимый стек

ИСП РАН

SAFEC

безопасный компилятор

Аналоги: компоненты компиляторов GCC/Clang, исследовательские компиляторы и рандомизаторы (CompCert C, kcc, Selfrando, Oxyoron, Shuffler)

SVACE

инструмент статического анализа

Аналоги: Klocwork (Perforce, США), Coverity (Synopsys, США), Fortify (MicroFocus (прежде HP), США).

Открытые инструменты: Clang Static Analyzer, SpotBugs

CRUSHER

комплекс динамического и статического анализа

Аналоги: Peach Fuzzer (США, Peach Tech), Synopsys Defensics (Synopsys, США), MAYHEM (ForAllSecure, США).

Открытые инструменты: angr, AFL, Honggfuzz, Driller (США)

NATCH

инструмент определения поверхности атаки

Аналоги: инфраструктуры Panda, Decaf (без интроспекции), Panorama (исследовательский инструмент для Windows)

kaspersky

SAMSUNG



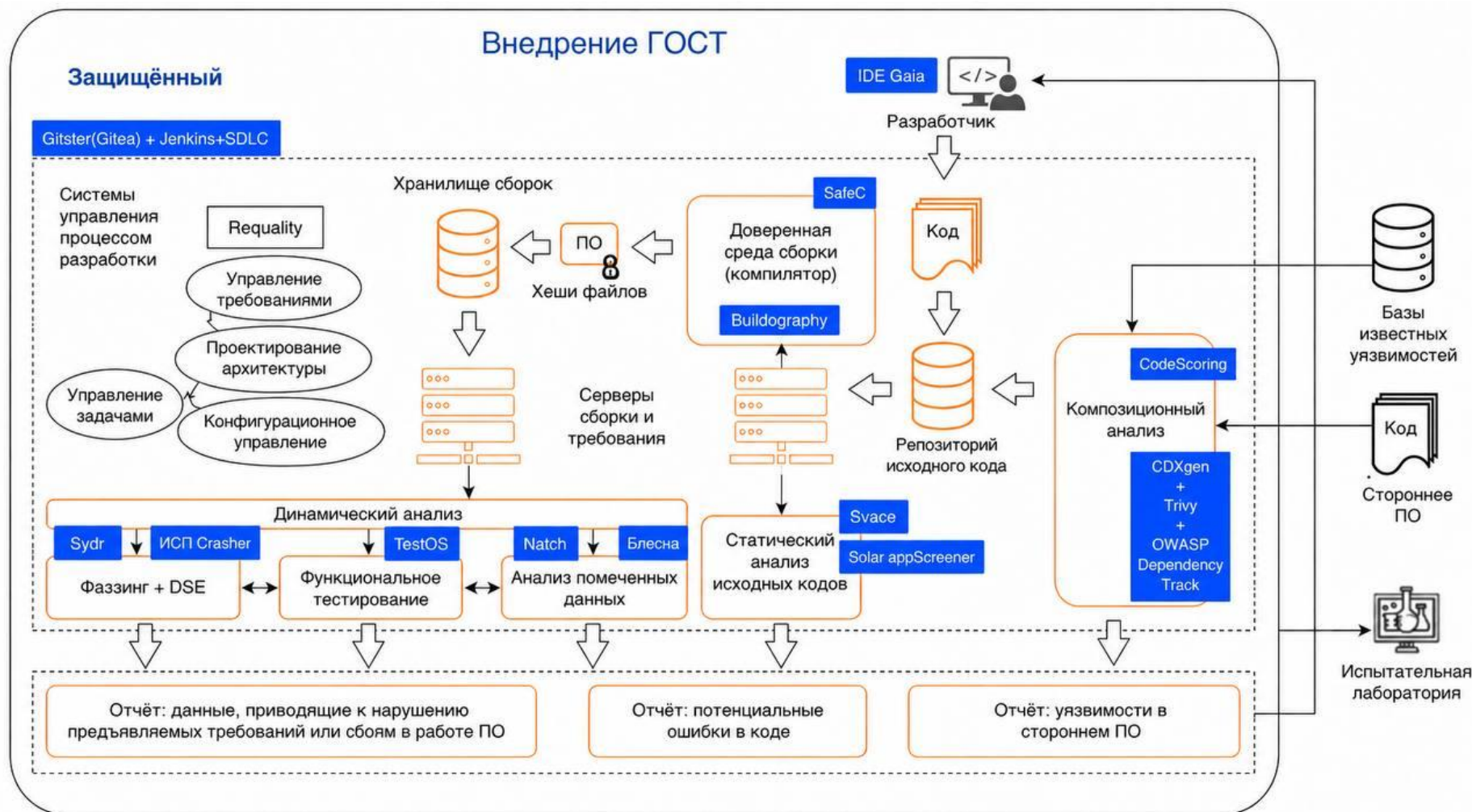
... и многие другие

200+

компаний используют
наши технологии

Жизненный цикл разработки безопасного ПО (РБПО)

Мы развиваем полный стек технологий для обеспечения жизненного цикла РБПО и обеспечиваем безопасность продукции всемирно известных компаний.



- РБПО специализируется для каждой отрасли (авиация, автомобили, космос, госсектор) под нормативные документы и специфику ПО
- Технологический стек ИСП РАН развивается с 2002 г. на базе результатов фундаментальных научных исследований по контрактам
- Совместно с ФСТЭК России создан портал **РБПО.РФ** — информационный ресурс Центра компетенций ФСТЭК России и ИСП РАН, объединяющий нормативные, методические, научные и практические материалы по разработке безопасного ПО.



Центр исследований безопасности системного ПО:

ИСП РАН

Создан на базе ИСП РАН по инициативе ФСТЭК России
Исследования ведут **>70** компаний и вузов



ИСП РАН - центр компетенций
ФСТЭК России и Росфинмониторинга

Результаты:

- ведётся сопровождение трёх веток ядра Linux, основанных на стабильных версиях 5.10, 6.1 и 6.10;
- проведён анализ более 45 тысяч предупреждений инструмента Svasc;
- подготовлены более 650 исправлений, уже принятых в основную ветку ядра Linux;
- подготовлены более 200 исправлений, принятых в основные ветки компонентов OpenSSL, Qemu, libvirt, CPython, Lua, .NET Runtime;
- ведутся работы по исследованию не только ядра Linux, но и других критических компонентов с открытым исходным кодом;
- подготовлены рекомендации по конфигурированию ядра и настройке доверенной загрузки для повышения безопасности;
- сформировано профессиональное сообщество исследователей безопасности системного ПО из компаний, вузов и научных организаций.



Создана масштабируемая экосистема, которая обеспечивает генерацию кадров и методологий и, как следствие, технологическую независимость

Стандартизация требований к разработке безопасных систем искусственного интеллекта



- ФГБУН «ИСП РАН» под руководством ФСТЭК России разработан проект **национального стандарта «Защита информации. Разработка безопасного в программного обеспечения реализующего технологии искусственного интеллекта»**.
- Проект национального стандарта разработан в рамках деятельности технического комитета по стандартизации **ТК 362 «Защита информации»**.
- Проект национального стандарта определяет требования к процессам разработки безопасного ПО, реализующего технологии искусственного интеллекта, и применяется **совместно с ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»**. [Плановый срок завершения - декабрь 2026 года.](#)

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ		
	НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ	ГОСТ Р (проект, первая редакция)

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ,
РЕАЛИЗУЮЩЕГО ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Общие требования

Настоящий проект стандарта не подлежит применению до его утверждения

Москва

202X

Платформа доверенного ИИ: безопасность на всем жизненном цикле

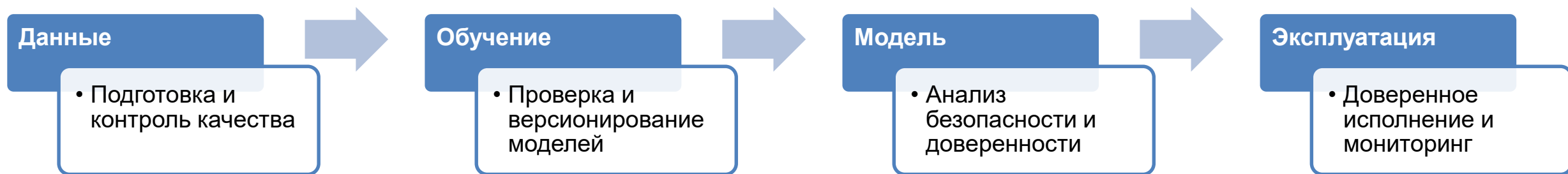


ИСП РАН

Для разработки безопасных систем ИИ недостаточно отдельных инструментов: необходимы безопасная инфраструктура и контроль данных и моделей на всех этапах жизненного цикла.

MLSecOps-платформа ИСП РАН

Единая среда обеспечения доверия на всем жизненном цикле ИИ



Доверенная технологическая основа
TrustTorch и **TrustFlow**: Версии PyTorch и TensorFlow, прошедшие через методики РБПО.



Безопасность ИИ обеспечивается не отдельными инструментами, а контролем всего жизненного цикла — данных, обучения, моделей и эксплуатации. MLSecOps-платформа объединяет их в единый технологический контур

РБПО — часть широкого технологического стека ИСП РАН

ИСП РАН создаёт широкий спектр программных технологий — от системного ПО и вычислительной инфраструктуры до анализа данных, цифровой медицины и математического моделирования. Разработки Института используются в промышленности, авиации, космической отрасли, здравоохранении и крупных научных проектах.



Операционные системы ответственного назначения

JetOS — операционная система реального времени для авионики гражданских воздушных судов, разработанная совместно с ГосНИИАС; установлена на MC-21.

БОСРВ — бортовая операционная система реального времени для непилотируемых космических аппаратов.



Цифровая медицина и биотехнологии

Анализ ЭКГ — интеллектуальный анализ цифровых электрокардиограмм; диагностическое ПО зарегистрировано Росздравнадзором как медицинское изделие.

Melanoscope AI — система интеллектуального анализа изображений новообразований кожи.

Персонализированные мРНК-вакцины — программный конвейер для автоматизированного поиска неоантигенов и персонализированного определения последовательности мРНК-вакцины по генетическим данным. В 2025 году программа зарегистрирована как ПО для ЭВМ. ИСП ведет работу в рамках консорциума под руководством НИЦЭМ им. Н. Ф. Гамалеи.



Анализ данных

Talisman — платформа построения интеллектуальных информационно-аналитических систем: сбор и обработка данных, автоматическое формирование баз знаний и анализ информации.



Облачная инфраструктура и ресурсоёмкие вычисления

Asperitas — платформа организации ресурсоёмких вычислений и хранения данных; используется в научных и прикладных проектах, в том числе как основа инфраструктуры для задач класса «мегасайенс».



Защита информации и маркирование документов

DocMarking — система внедрения цифровых водяных знаков в текстовые документы для противодействия анонимности при утечках. Позволяет идентифицировать пользователя и устройство по цифровой метке даже в изображении документа.



Широкий спектр работ в таких областях, как:

- обработка естественных языков;
- верификация моделей;
- анализ сетевого трафика;
- ..и других

Широкий технологический стек позволяет ИСП РАН объединять компетенции разных научных направлений для решения комплексных отраслевых R&D-задач.

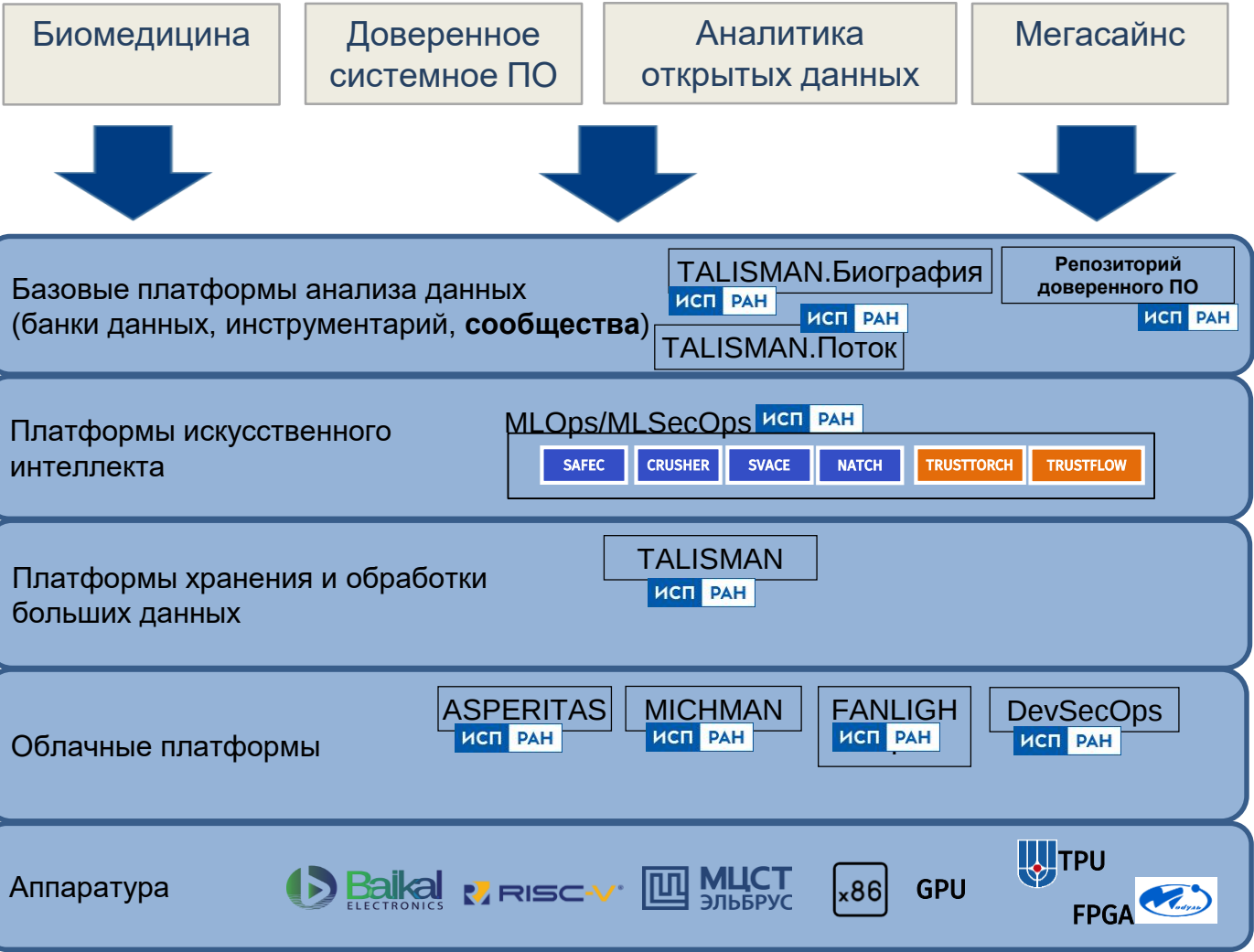
Доверенная экосистема ИСП РАН



Взаимодействие с регуляторами

- Центра компетенция ФСТЭК России на базе ИСП РАН (2019), Центр исследований безопасности системного программного обеспечения (2019)
- Исследовательский Центр доверенного ИИ (2022)
- Лаборатория федеративного обучения (2024)
- Консорциум «Исследования безопасности технологий ИИ»
- Центр компетенций Росфинмониторинг на базе ИСП РАН (2025)
- Платформа Внешнеполитической деятельности МИД России

Инновации в Государственном управлении



Научные Сообщества

- Консорциум РДИГ-М
 - НТЦ развития мРНК-технологий
-

Индустриальное партнёрство

- MLSecOps Платформа (Ростелеком)
- TALISMAN Платформа анализа открытых данных (ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ, ЗАРУБЕЖНЕФТЬ, РОССЕЛЬХОЗБАНК)
- Консорциум безопасности ключевых компонент СПО (более 30 компаний...) (KASPERSKY)
- Консорциум RODOO – Открытая платформа ERP (CODE SCORING)
- Облачная среда Asperitas – база коммерческого продукта Moncloud (moncloud системные решения)
- Гетерогенная ВС исследования на базе ИИ и ММ (РНО, РОСАТОМ)

Образовательное партнёрство (более 20)



Развитие РБПО: от технологического стека к сообществу

Модель устойчивого долгосрочного развития и **технологическая независимость** — это передовые Центры компетенций по генерации наукоёмких инноваций, создание и модерирование под их руководством соответствующих **сообществ**.



Следующий этап развития РБПО — формирование сообщества вокруг технологий ИСП РАН и партнёров, в котором открытый код и постоянная обратная связь от пользователей становятся источником новых задач и дальнейшего развития технологического стека.

ИСП РАН открыт к сотрудничеству с компаниями и организациями, заинтересованными в применении и совместном развитии технологий РБПО.

Открытая конференция ИСП РАН 2026: наука, технологии, индустрия



ИСП РАН

Открытая конференция ИСП РАН — ежегодная научно-практическая площадка, объединяющая представителей научных и образовательных организаций, ведущих ИТ-компаний и государственных ведомств. Основная задача — обмен результатами фундаментальных исследований и практическим опытом их внедрения, развитие взаимодействия науки и индустрии.

2026: новая площадка · развитие бизнес-выставки · партнёрские конференции и отраслевые встречи (встреча АРПП «Отечественный софт» и другие)

В 2026 году Открытая конференция ИСП РАН впервые пройдет на новой площадке — в Университете науки и технологий МИСИС. Обновление площадки станет частью развития формата конференции: наряду с научной программой особое внимание будет уделено взаимодействию с индустрией и технологической выставке.

Сайт
конференции:



Спасибо за внимание!