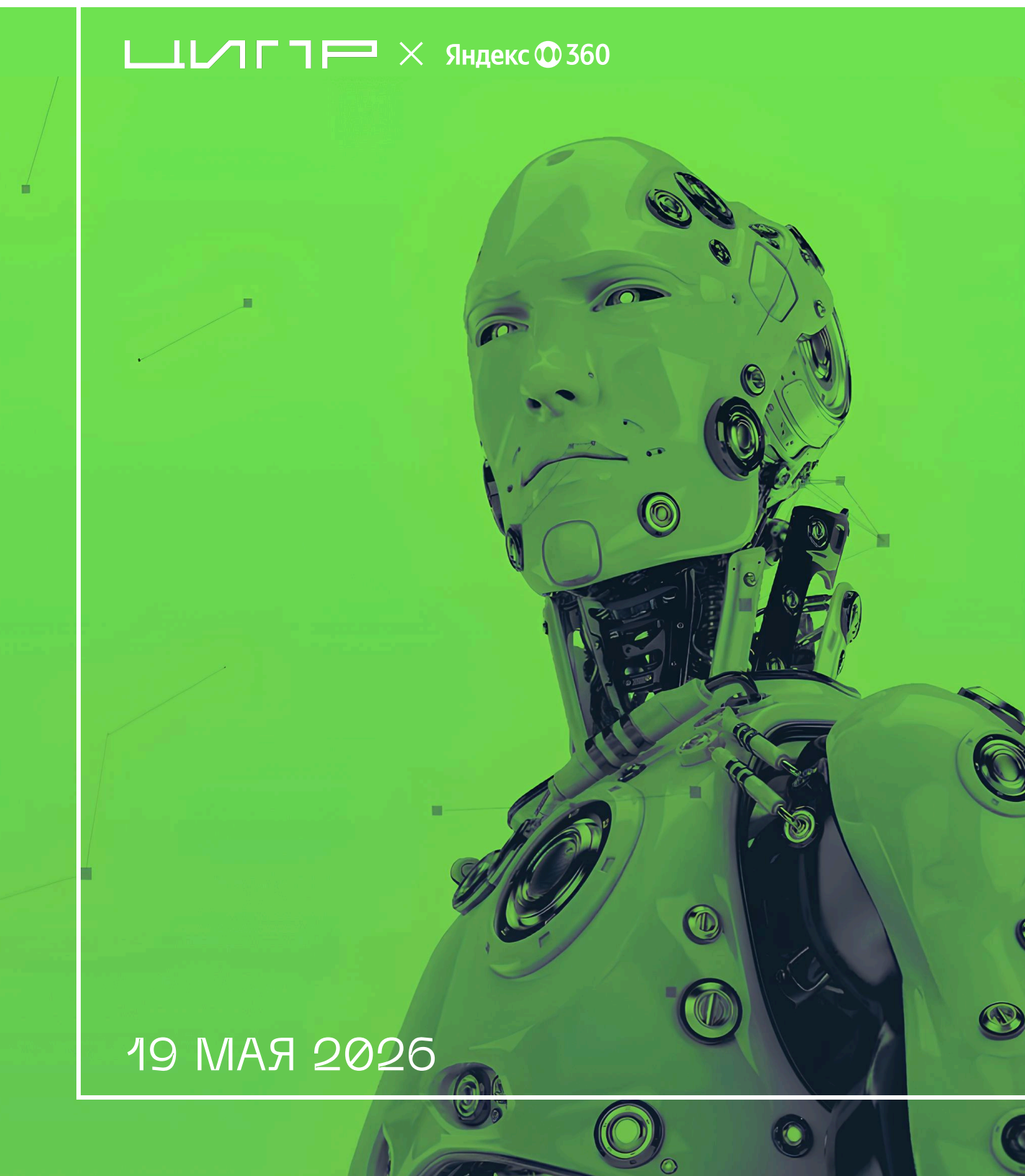


ДОВЕРЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ПОДПИСЬ КОДА В ПРОМЫШЛЕННОСТИ

Конспект встречи создан при помощи
искусственного интеллекта и Яндекс Телемоста

ЦИГТФ × Яндекс 360

19 МАЯ 2026



МОДЕРАТОР

Качалин Игорь, Генеральный директор, АНО "НТЦ ЦК"

УЧАСТНИКИ

- Аляутдин Роман, Директор департамента разработки ОС Аврора, ОМП
- Гусев Дмитрий, Заместитель генерального директора, АО "ИнфоТеКС"
- Деменев Алексей, Ведущий научный сотрудник, 8 Центр ФСБ России
- Смышляев Станислав, Генеральный директор, КриптоПро
- Соснин Юрий, Консультант, ООО "РусБИТех-Астра"
- Шевцов Дмитрий, Начальник управления, ФСТЭК России

Секция обсудила формирование единого пространства доверия для отечественного программного обеспечения через внедрение механизмов подписи кода на российских криптоалгоритмах. Участники пришли к выводу, что технической базы достаточно, но требуется унификация стандартов и интеграция процессов безопасной разработки. Ключевым вызовом остается создание правовой базы и регуляторики, позволяющей легально выпускать сертификаты безопасности для кода.

Слово берет **Дмитрий Гусев (АО "ИнфоТеКС")**. Он подчеркивает, что одной лишь криптографии недостаточно для обеспечения доверия, необходимо внедрение регламентов на всех этапах жизненного цикла ПО. «Важно подписать код не просто как получится, а как надо», — отмечает спикер, указывая на необходимость интеграции подписи в стандарты безопасной разработки, такие как ГОСТ Р 56939. По его словам, цель — создать культуру, где потребитель автоматически доверяет программному обеспечению, а разработчики четко контролируют заимствованные компоненты.

Своим опытом делится **Станислав Смышляев («КриптоПро»)**. «Наша отрасль криптографической подписью кода на российских алгоритмах пользовалась не года, а десятилетия», — заявляет он, подтверждая техническую готовность рынка. Спикер отмечает, что технические шероховатости уже устранены, и сейчас фокус смещается на стандартизацию и взаимодействие с регуляторами. Он уверен, что Россия имеет уникальную возможность создать единое пространство доверия с единым корнем, избежав сложностей, с которыми столкнулись зарубежные экосистемы.

Следом выступает **Юрий Соснин (ГК «Астра»)**. «Мы хотим, чтобы это было стандартом, чтобы разработчики прикладного ПО действительно не задумывались о том, для какой операционной системы целевой», — говорит он, призывая к унификации инструментов подписи. Соснин акцентирует внимание на том, что подпись кода должна стать индикатором качества разработки, а не просто формальностью. Он сообщает, что компания активно лоббирует включение требований по безопасной разработке в нормативную базу доверенного ПО.

Микрофон переходит к **Роману Аллаудину (ОМП)**. «Каждое приложение имеет подпись, при каждом старте приложения проверяется эта подпись», — описывает он архитектуру операционной системы «Аврора», где контроль целостности работает динамически. Спикер рассказывает о внедрении механизма «доверенного источника», позволяющего организациям замыкать экосистему на ограниченный круг приложений. По его словам, платформа готова к участию в едином пространстве доверия и уже тестирует совместимость с сертификатами других участников рынка.

Далее выступает **Дмитрий Шевцов (ФСТЭК России)**. «Мы недавно внесли изменения в положение о системе сертификации, где мы обязали всех наших разработчиков представлять сведения о программных компонентах», — сообщает он о новых мерах контроля. Спикер объясняет, что без инвентаризации компонентов и понимания их происхождения невозможно эффективно выявлять уязвимости. Он подтверждает, что ФСТЭК России поддерживает создание единой системы доверия и готово регулировать этот процесс через сертификацию и нормативные акты.