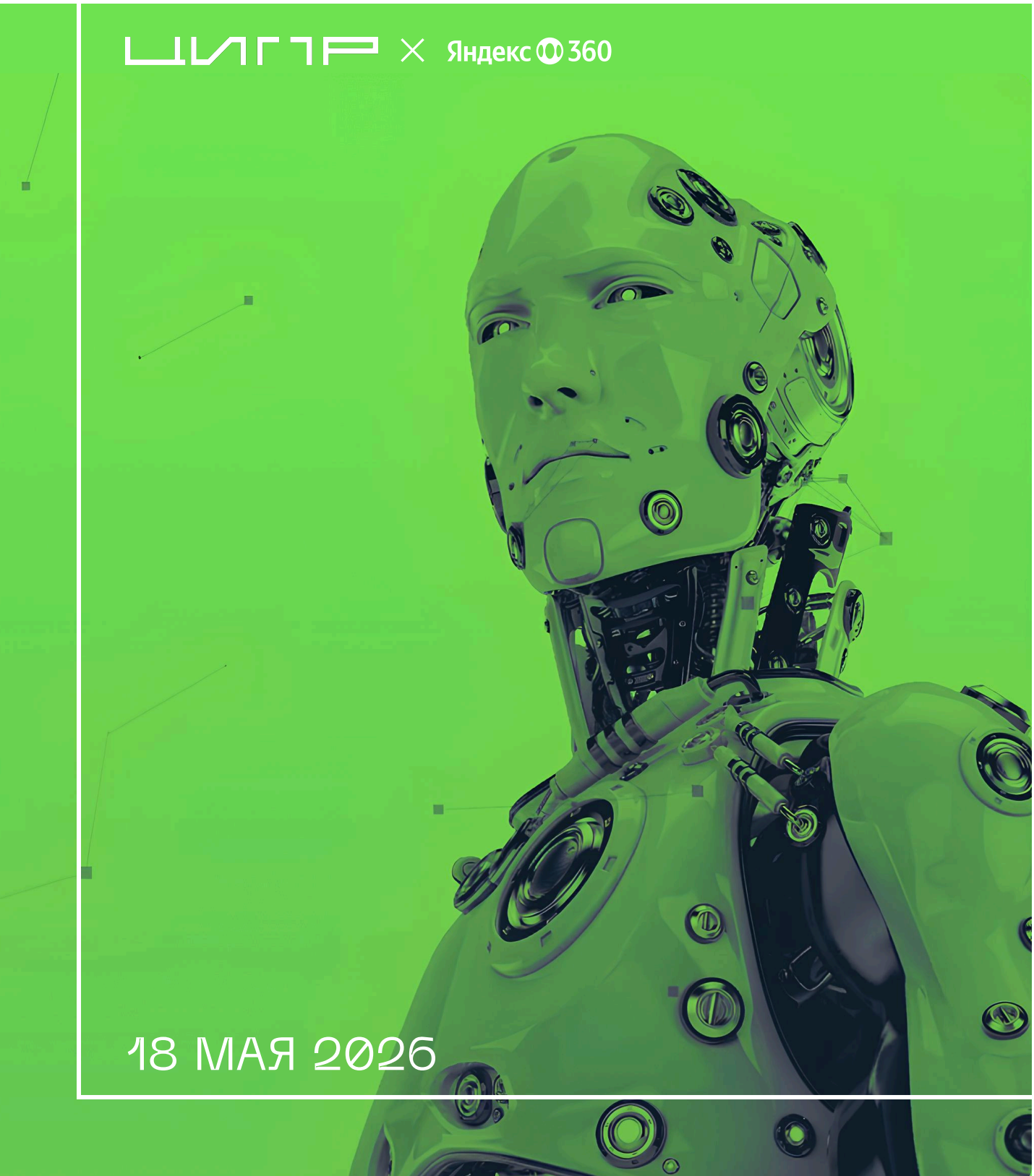
ОТ ПИЛОТА К СИСТЕМЕ. КИБЕРУСТОЙЧИВОСТЬ КИИ ТЭК В МАСШТАБЕ СТРАНЫ

Конспект встречи создан при помощи искусственного интеллекта и Яндекс Телемоста

ЦИПР × Яндекс 360



18 МАЯ 2026

МОДЕРАТОР

Эдуард Шереметцев, заместитель Министра энергетики Российской Федерации

УЧАСТНИКИ

- Александр Шойтов, заместитель Министра цифрового развития России
- Андрей Бутко, генеральный директор, АО «РАСУ»
- Артём Головатый, директор по информационным технологиям, Росэнергоатом
- Александр Ковалевский, генеральный директор, ИКС Безопасность
- Рустам Рустамов, заместитель генерального директора, РЕД СОФТ
- Дмитрий Серебрянников, Chief Hacking Officer, АО «Позитив Текнолоджиз»
- Иван Шальков, заместитель вице-президента, Транснефть
- Дмитрий Шепелявый, директор по международному бизнесу, Инностейдж

Сессия «От пилота к системе. Киберустойчивость КИИ ТЭК в масштабе страны» была посвящена итогам пилотного проекта по оценке киберзащищённости предприятий ТЭК Татарстана и перспективам масштабирования этого опыта на уровень всей страны. Участники обсудили переход от разовых проверок к системным непрерывным кибериспытаниям, вопросы доверенности отечественных решений, роль отраслевых центров киберустойчивости и необходимость вовлечения первых лиц компаний в вопросы информационной безопасности. Ключевым выводом сессии стало признание того, что киберустойчивость — это не одноразовое мероприятие, а постоянный динамичный процесс, требующий системного подхода, координации регуляторов, бизнеса и государства.

Эдуард Шереметцев (модератор, заместитель Министра энергетики) открыл сессию, обозначив контекст: в 2025 году Минэнерго совместно с Positive Technologies провело уникальный пилотный проект по оценке киберзащищённости отрасли ТЭК в Татарстане, охвативший региональные и федеральные компании. «Мы разговаривали, по сути дела, на языке руководителя организации», — отметил он, подчеркнув, что ключевым условием успеха стало вовлечение первых лиц компаний. В 2026 году ключевой задачей Минэнерго является развитие постоянного отраслевого механизма повышения защищённости объектов ТЭК, соответствующие предложения уже включены в стратегическое направление цифровой трансформации ТЭК до 2036 года.

Александр Шойтов (заместитель Министра цифрового развития) рассказал о развитии эксперимента по повышению защищённости государственных информационных систем (постановление Правительства № 860), который ведётся с 2022 года. Он выделил два ключевых направления: регулярный мониторинг с актуализацией принятых мер (чтобы исключить ситуацию, когда меры приняты лишь «для галочки»), и анализ безопасности систем искусственного интеллекта, который де-факто становится неотъемлемым элементом инфраструктуры. «Анализ защищённости является ключевым элементом в области обеспечения информационной безопасности систем», — подчеркнул спикер, добавив, что новый 117-й приказ ФСТЭК вводит понятие «нежелательных последствий» как основы для приоритизации защитных мер.

Дмитрий Серебрянников (Positive Technologies) представил итоги киберучений в Татарстане с точки зрения атакующей стороны. В пилоте участвовали как региональные, так и федеральные компании — все были уведомлены заранее и максимально подготовлены, что позволило проверить реальный уровень устойчивости при осознанной защите. «В половине компаний нам удалось дойти до недопустимых событий», — сообщил он, подчеркнув, что по результатам каждой успешной атаки компания немедленно получала детальные рекомендации. ТЭК Татарстана стал самым защищённым среди всех регионов страны после закрытия обнаруженных уязвимостей; следующий шаг — масштабирование через механизм кибериспытаний с привлечением всего исследовательского сообщества страны.

Дмитрий Шепелявый (Инностейдж) представил стратегическое видение системного перехода к киберустойчивости, утверждённое в феврале 2026 года на горизонт 10 лет. Он выделил три взаимосвязанных измерения: объективный независимый контроль через кибериспытания, рейтинги киберустойчивости для стандартизации оценки, а также экономика управления — перевод метрик кибербезопасности в финансовые показатели, понятные собственникам бизнеса. «Кибериспытание как инструмент объективной валидации — это точный шаг в сторону повышения киберустойчивости на основе объективного контроля», — резюмировал спикер, обозначив три принципа построения системы: определение недопустимых событий, приоритет объективных методов контроля над самооценкой, интеграция IT, ИБ и оценки непрерывности в единый контур управленческих решений.

Артём Головатый (Росэнергоатом) выступил с позиции главного конструктора систем автоматизации атомных станций и поставил под сомнение распространённое отождествление импортозамещения с безопасностью. «Импортозамещение без реальной доверенности — это иллюзия защиты», — заявил он, пояснив, что в Росатоме критерием доверия является не страна происхождения продукта, а управляемость и проверяемость всей производственной цепочки на протяжении жизненного цикла. Спикер призвал ввести обязательную сертификацию руководителей значимых объектов КИИ в части киберграмотности — по аналогии с действующим экзаменом Ростехнадзора для руководителей ядерных объектов. Дорожная карта Росэнергоатома: к 2027–2028 годам — защищённые СУТП с аппаратным корнем доверия, к 2030 году — полная конструктивно безопасная платформа АСУ ТП.

Андрей Бутко (РАСУ) описал системный подход Росэнергоатома к построению киберустойчивости: от категорирования КИИ и программы импортозамещения — к проактивной модели на основе недопустимых событий. Компания создала собственный SOC, работающий 24/7, и перешла от реактивной защиты к проактивной парадигме, фокусируясь на недопустимых событиях для критичных бизнес-процессов. Особо он отметил создание в рамках индустриального центра компетенций (ИЦК) полного IT-ландшафта архитектуры энергетических компаний, позволяющего расставлять приоритеты на уровне всей отрасли. «Системный подход очень важен, чтобы правильно спланировать работу — иначе к 2030 году мы просто ничего не успеем», — подчеркнул он.

Рустам Рустамов (РЕД СОФТ) рассказал о построении экосистемы совместимых российских решений на базе операционной системы РедОС. Главным вызовом он назвал обеспечение предсказуемой совместимости: сертификаты проходят на стенде, но в реальной эксплуатации при добавлении новых компонентов система может давать сбои. «Базы знаний пока не готовы к тому, чтобы на них применяли искусственный интеллект — это тяжёлая работа», — признал он, рассказав о планах объединить базы знаний нескольких вендоров с партнёрами (P7, VK) для создания бесшовной экосистемы технической поддержки с ИИ-агентами. В целом РЕД СОФТ чувствует хороший темп и уверен в зрелости российской экосистемы в ближайшей перспективе.