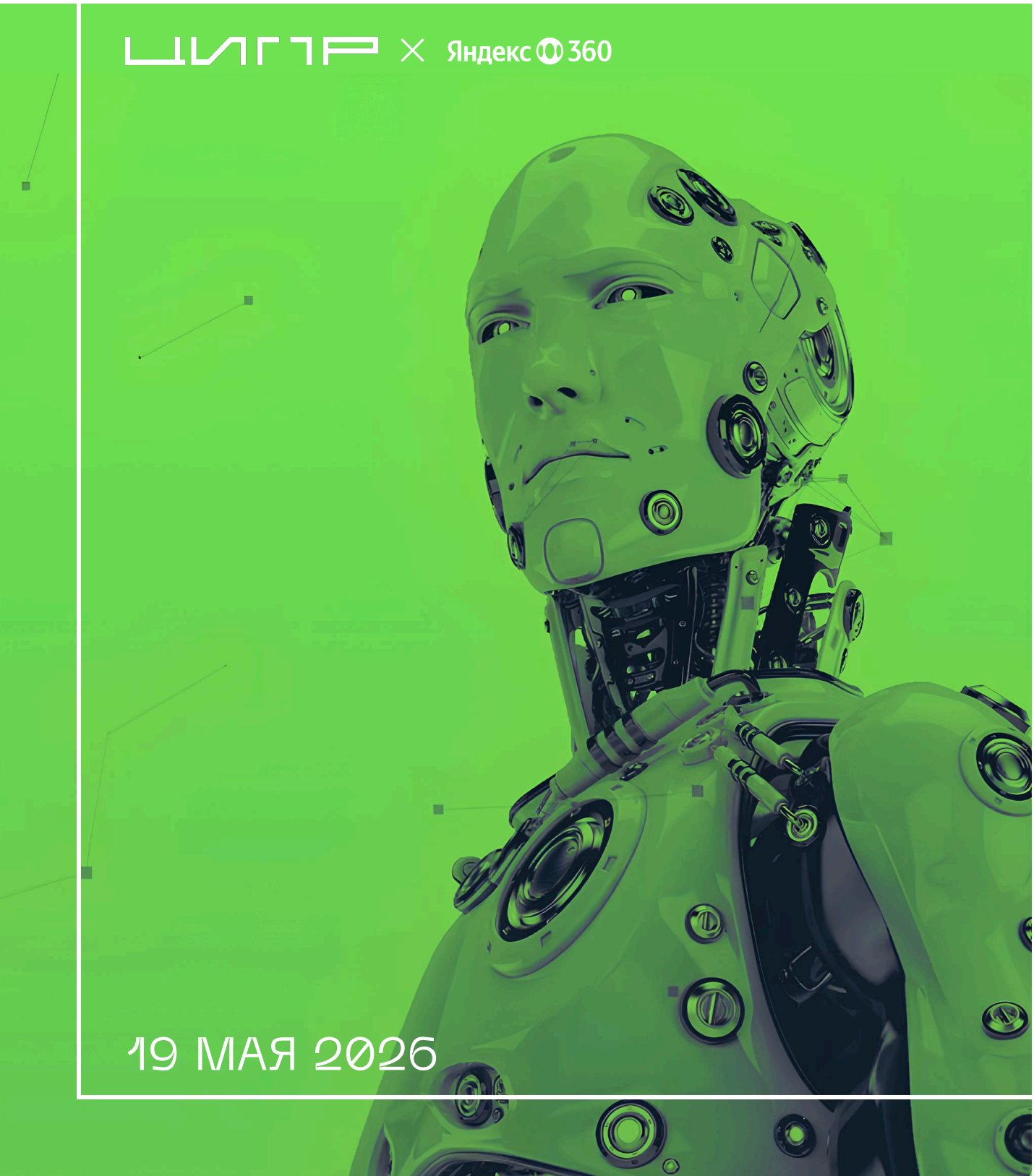
ПРАКТИЧЕСКАЯ КИБЕРБЕЗОПАСНОСТЬ И ИИ. РЕАЛЬНОСТЬ И ПЕРСПЕКТИВЫ

Конспект встречи создан при помощи искусственного интеллекта и Яндекс Телемоста

ЦИФРА × Яндекс 360



19 МАЯ 2026

МОДЕРАТОР

Кулашова Анна, Вице-президент по развитию бизнеса в России и странах СНГ, Kaspersky

УЧАСТНИКИ

• Аристов Виктор, Директор по информационной безопасности, ОАО "РЖД"

• Шапиро Роман, Руководитель направления информационной безопасности, АО "ПОЧТА РОССИИ"

• Мартынцев Алексей, Директор Департамента защиты информации и IT-инфраструктуры, ПАО "ГМК "Норильский никель"

• Курицин Владимир, Начальник Управления информационных технологий, АО "Зарубежнефть"

• Жуков Алексей, Директор Дирекции информационной безопасности, ООО "ГПМ Цифровые инновации"

• Никишов Дмитрий, Директор по информационной безопасности Дом.РФ

• Черкасов Сергей, Заместитель директора по экономической безопасности АО "Апат, АПАТИТ

• Бондаренко Алексей, Руководитель Департамента цифровизации, ГК УРАЛХИМ

Сессия объединила лидеров ИБ крупнейших инфраструктурных и технологических компаний для обсуждения влияния искусственного интеллекта на кибербезопасность. Спикеры обсудили переход от периметровой защиты к поведенческому анализу, роль ИИ в автоматизации SOC и риски, связанные с генеративными моделями. Ключевой вывод заключается в том, что ИИ стал необходимым инструментом для выживания в условиях роста атак, но требует строгого контроля и сохранения человеческого фактора в принятии решений.

Виктор Аристов (РЖД) открывает дискуссию с жесткой статистики: за четыре месяца текущего года компания зафиксировала 4,5 миллиона компьютерных атак, что превышает показатели прошлого года. «Мы делаем все, чтобы атака не состоялась, но не менее важно минимизировать ущерб и быстро восстановиться», — подчеркивает он. РЖД перешла к сегментации инфраструктуры на контуры критической информации, коммерческой тайны и обычных данных, чтобы сдерживать каскадные атаки. Особое внимание уделяется внедрению ИИ-агентов для поиска аномалий и угроз нулевого дня, так как скорость хакерских атак с использованием ИИ стремительно растет.

Роман Шапиро (Почта России) делится опытом создания консорциума из 19 вендоров для построения единой системы безопасности. «Искусственный интеллект — это не серебряная пуля, а инструмент, который поможет получить результат за меньшее количество ресурсов», — говорит он.

Почта России использует ИИ для трансформации скучных регламентов в понятные комиксы для сотрудников и для автоматизации проверки соответствия нормативным требованиям. Роман отмечает, что внедрение ИИ эффективно только при высокой зрелости бизнес-процессов, иначе компания получит «цифровизованный хаос».

Алексей Мартынцев (Норникель) проводит параллель между технологическим неравенством регионов и внедрением ИИ в бизнесе, утверждая, что будущее наступает неравномерно. «Будущее наступает неравномерно: где-то уже небоскребы, а где-то люди думают, как не попасть в пасть льву», — приводит он пример разрыва между технологическими центрами и отдаленными районами. Он призывает отказаться от ретроградного подхода и использовать ИИ для ускорения разработки продуктов и процессов. По его мнению, ИИ должен работать как помощник, повышающий эффективность команд, а не как замена человеческому интеллекту.

Владимир Курицин (АО "Зарубежнефть") скептически оценивает готовность ИИ принимать самостоятельные решения в критических системах, отмечая риски «черного ящика» и возможных сбоев. «Если процесс не выстроен, то в автоматизацию, цифровизацию или искусственный интеллект мы получим хаос, пусть и более красивый», — предупреждает он. Банк использует ИИ преимущественно во вспомогательных процессах: для предиктивной аналитики, обработки больших данных и снижения нагрузки на первую линию SOC. Владимир подчеркивает, что окончательное решение по критическим инцидентам всегда должно оставаться за человеком.

Алексей Жуков (МТС) рассказывает о росте атак прикладного уровня на 35% и переходе от защиты периметра к поведенческому анализу трафика. «Мы не можем гарантировать 100% защиты, но мы должны внедрять процессы, чтобы не проиграть в гонке вооружений», — заявляет он. МТС активно использует ИИ в SOC для фильтрации ложных срабатываний и обучения моделей на индикаторах компрометации из внешних баз. Также компания внедряет ИИ в управление уязвимостями и безопасность разработки (DevSecOps), чтобы контролировать качество кода, генерируемого с помощью ИИ-инструментов.

Дмитрий Никишов (Дом.РФ) видит в ИИ мощный инструмент для разгрузки аналитиков SOC, который может обрабатывать до 70–80% рутинных задач. «ИИ должен восприниматься как цифровой сотрудник, за которым нужно следить и которого нужно защищать», — считает он. Он прогнозирует развитие федеративного обучения для обмена моделями угроз между банками без передачи чувствительных данных и использование ИИ в Purple Team для моделирования атак. Дмитрий также отмечает риски использования сотрудниками непроверенных публичных ИИ-сервисов и рекомендует внедрять корпоративные защищенные модели.