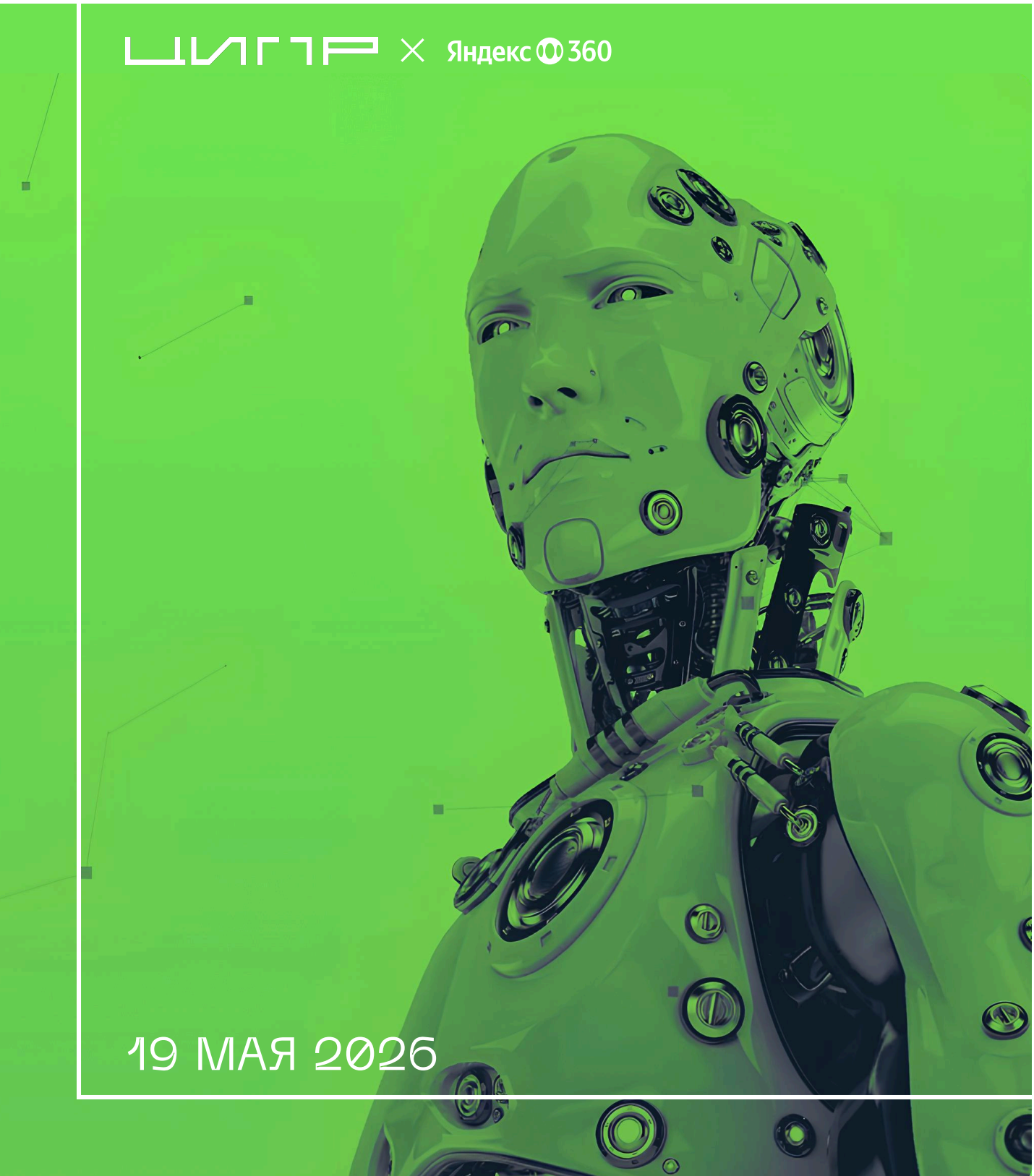
КИБЕРБЕЗОПАСНОСТЬ КАК НОВАЯ РОСКОШЬ ОТВЕТСТВЕННОГО БИЗНЕСА

Конспект встречи создан при помощи искусственного интеллекта и Яндекс Телемоста

ЦИТАТА × Яндекс 360



19 МАЯ 2026

МОДЕРАТОР

Глушенков Аркадий, Ведущий, Телеканал РБК

УЧАСТНИКИ

- Шойтов Александр, Заместитель Министра, Минцифры России
- Королев Андрей, Заместитель директора по информационным и цифровым технологиям, Госкорпорация «Росатом»
- Скворцов Владимир, Генеральный директор, АО АльфаСтрахование
- Соколов Андрей, Президент, АО ГК "МЕДСИ"
- Новиков Алексей, Управляющий директор, Positive Technologies
- Зайков Максим, Заместитель генерального директора по корпоративному бизнесу, Билайн

Сессия РБК «Кибербезопасность как новая роскошь ответственного бизнеса» собрала представителей государства, бизнеса и технологических компаний для обсуждения реальных угроз и методов защиты. Спикеры пришли к единому мнению: кибербезопасность перестала быть опцией и стала базовым условием выживания компании в цифровой среде. Ключевыми вызовами названы рост атак через подрядчиков, использование искусственного интеллекта злоумышленниками и необходимость внедрения принципа Security by Design.

Александр Шойтов (Минцифры РФ) открывает дискуссию обзором нормативного поля и главных угроз. «Государственное регулирование и сами атаки привели к тому, что критическая инфраструктура стала защищаться существенно лучше», – отмечает он, указывая на усиление контроля за цепочками поставок. Заместитель министра подчеркивает, что искусственный интеллект стал системным вызовом, позволяя хакерам быстрее находить уязвимости и строить атаки, что требует от бизнеса аналогичного использования ИИ для защиты своих систем.

Владимир Скворцов (АО "АльфаСтрахование") переводит тему в плоскость финансовой ответственности и управления рисками. «Кибербезопасность – это не роскошь, а ключевой элемент архитектуры любого бизнеса», уверен генеральный директор страховой компании, отмечая значительный рост спроса на киберстрахование. Он приводит примеры возмещения ущерба в размере от 10 до 100 миллионов рублей и подчеркивает, что страховщики не только компенсируют убытки, но и проводят аудиты для минимизации вероятности наступления страховых случаев.

Андрей Соколов (АО ГК "МЕДСИ") делится опытом медицинской отрасли, где утечка данных несет критические репутационные риски.

«Задача реализовывать стратегию кибербезопасности, потому что если этого не произойдет, то просто вопрос: через сколько это по тебе ударит», – заявляет он, сравнивая задержки с защитой с риском для жизни пациентов. Президент группы компаний акцентирует внимание на необходимости строгого контроля за подрядчиками и обучения сотрудников кибергигиене, так как человеческий фактор остается главным вектором атак.

Максим Зайков (Вымпелком) рассказывает о роли телеком-операторов в борьбе с мошенничеством и сетевыми атаками. «Мы видим, что более 98% мошеннических звонков теперь блокируются антифрод-платформами», – приводит он статистику эффективности регуляторных мер. Заместитель генерального директора описывает кибербезопасность как непрерывное соревнование, где операторы объединяют усилия для защиты инфраструктуры клиентов, предупреждая, что без создания союзов и обмена данными противостоять современным угрозам будет невозможно.

Андрей Королев (Госкорпорация «Росатом») раскрывает подход госкорпорации к безопасности в условиях жестких требований к критической инфраструктуре. «Внутренняя оценка риска – это сегодня самое ключевое, на базе чего строятся все технологические платформы», – утверждает он, описывая внедрение сертифицированных платформ безопасной разработки для контроля как внутреннего кода, так и решений подрядчиков. Заместитель директора по ИТ подчеркивает важность технологического суверенитета и добровольной сертификации радиоэлектронной продукции для минимизации рисков, заложенных в поставках из-за рубежа.

Алексей Новиков (Positive Technologies) дает экспертную оценку текущей ситуации, называя промышленность лидером по числу инцидентов. «Для большинства компаний кибербезопасность – это прямая и очень дорогая роскошь, потому что раньше они не тратились на базовый минимум», – констатирует он, приводя аналогию с пропущенным медицинским чекапом. Новиков предупреждает, что главная угроза сегодня – не остановка производства, а скрытое хищение коммерческой тайны и стратегических планов, и призывает компании делиться данными для создания эффективных национальных моделей защиты.

В финале участники резюмируют, что кибербезопасность и киберстрахование являются базовым минимумом, необходимым для любого ответственного бизнеса. Спикеры сошлись во мнении, что время на «технологический долг» исчерпано: компании должны переходить к модели Security by Design, где защита закладывается на этапе проектирования, а не добавляется постфактум. Регуляторы и бизнес готовы к формированию новых механизмов, включая государственные сервисы проверки дипфейков и обязательные стандарты, чтобы обеспечить устойчивость экономики в эпоху искусственного интеллекта.