ЦИПР

ЦИПР-2026 · АНАЛИТИКА

ИИ в ТЭК

Цифровые двойники, управление знаниями и киберустойчивость – обзор по материалам ЦИПР-2026

Нижний Новгород · май 2026 **diplatforms.ru**

Оглавление

Источник

> *По материалам деловой программы ЦИПР-2026 (diplatforms.ru). Все цифры и формулировки приведены строго по выступлениям спикеров.*

1. Краткое резюме и ключевые выводы

На ЦИПР-2026 тема ИИ в ТЭК прозвучала через четыре взаимосвязанные сессии: цифровые двойники, управление знаниями, киберустойчивость критической информационной инфраструктуры и киберстрахование. Вместе они дали редкий срез реального отраслевого опыта – без маркетинга, с конкретными кейсами и признанием незакрытых проблем. Ниже – главные выводы по фактуре выступлений спикеров.

1. **Газпром нефть: цифровой двойник бизнес-процесса даёт до 5% EBITDA.** При охвате только отдельных технологических объектов эффект ограничен долями десятых единиц процента; переход к цифровому двойнику ключевого бизнес-процесса («процесса ввода новых скважин») выводит эффект «на порядок больше». При этом компания бурит более 1200 скважин в год – около 20% от новых скважин по отрасли, а автоматизация достигает 98,9% эффективности инвестиций бурения (Маргарит Андрей, Газпром нефть).
2. **Транснефть обнаружила 8000 связей в онтологической модели одного узла учёта.** Конфигуратор онтологической модели объекта «Шишхарис» выявил 8000 связей в рамках единого узла: оборудование, функции, топология, композиция, ассоциации. Транснефть движется к описанию миллионов единиц оборудования с помощью ИИ-агентов, поскольку «конвенциональными методами это все не опишешь» (Гришанин Максим, Транснефть).
3. **До 80% корпоративных знаний в ТЭК лежат «мёртвым грузом».** Традиционные системы управления знаниями «превращаются в кладбище данных», а «уникальные инженерные знания уходят вместе с экспертами»; до 80% накопленных знаний не задействованы (Воробьев Константин, Российское энергетическое агентство Минэнерго).
4. **В половине компаний ТЭК Татарстана реализовано «недопустимое событие» в ходе кибериспытаний.** Пилот Positive Technologies в Татарстане в 2025 году охватил всю отрасль ТЭК региона; в 50% компаний-участников команде удалось достичь определённого самой компанией «недопустимого события». После закрытия выявленных уязвимостей «ТЭК Татарстана стал самым защищённым среди всех остальных регионов страны» (Серебрянников Дмитрий, Positive Technologies).
5. **Число кибератак на КИИ ТЭК выросло на 40% с 2024 по 2025 год.** Индекс угроз в ТЭК зафиксировал рост атак на критическую инфраструктуру на 40% в 2025 году по сравнению с 2024-м. Атаки носят не финансовый, а разрушительный характер – цель злоумышленников создать «неприемлемый ущерб» государству, а не получить финансовую выгоду (Головатый Артем, Росэнергоатом).
6. **Россети снизили IT-затраты на 40% за счёт цифровизации и унификации.** Переход к единым платформенным подходам и отказ от дублирующих систем позволил крупнейшей сетевой компании России существенно сократить операционные издержки в IT-блоке (Кравченко Константин, Россети).
7. **Рынок киберстрахования в России – менее миллиарда рублей при потенциале 2–3 млрд.** Объём фактических страховых сборов по корпоративным полисам кибербезопасности составляет «до миллиарда» рублей; рынок при этом «готов страховать бизнес на два-три миллиарда». На рынке около 200 корпоративных полисов; мировой рынок – $14–15 млрд в 2024

году с прогнозом роста до более $100 млрд к 2028 году (Еремеев Иван, РК Страховой Брокер; по данным Munich Re).

8. **«Налог на поиск» стоит промышленному предприятию полмиллиона рублей в неделю.** Инженер тратит порядка 20% рабочего времени на поиск информации. Для предприятия с 100 инженерами, каждый из которых тратит два часа в неделю на поиск, это порядка 500 тыс. рублей в неделю прямых потерь (Маевский Антон, Инвенторус).
9. **Для ТЭК главная угрозируемая субтехнология ИИ – машинное зрение, а не LLM.** В отличие от общей дискуссии вокруг языковых моделей, в промышленности и ТЭК ключевой субтехнологией является компьютерное зрение: безопасность людей, контроль качества продукции, мониторинг производственных процессов. «На площадке Цифры вообще не видел ни одного стенда с камерами» (Лещенко Владимир, КМ-альянс).
10. **Страховой дом ВСК: накануне атаки правление отказало в 100 млн руб. на кибербезопасность.** В ноябре 2025 года ВСК подвергся «одной из самых массированных кибератак на российском рынке» – утром сотрудники обнаружили, что «не работало ровным счётом ничего». За день до атаки правление отклонило дополнительные 100 млн руб. на кибербез. После инцидента руководитель информационной безопасности переведён в ранг члена правления (Фролов Роман, Страховой Дом ВСК).

2. Контуры темы: четыре сессии, одна повестка

ИИ в ТЭК на ЦИПР-2026 – не единая монолитная тема, а четыре взаимосвязанных разговора, каждый со своим фокусом и составом спикеров. Картина, складывающаяся из всех четырёх, гораздо полнее, чем любая из них по отдельности: данные питают двойников, знания – людей и ИИ-агентов, а вся система уязвима без киберзащиты и инструментов управления рисками.

2.1 «Цифровые двойники в ТЭК» (партнёрская сессия Транснефть, 18 мая)

Сессия объединила нефтетранспортную, нефтедобывающую и энергетическую компании: Транснефть, Газпром нефть, Сургутнефтегаз, Россети, а также Минэнерго и вендоров – Галактику и СКАД ТЕХ. Центральный вопрос – что такое цифровой двойник «на сто процентов» и как перейти от уровня отдельных объектов к уровню актива и бизнес-процесса. Газпром нефть описала трёхуровневую модель: двойник объекта → двойник бизнес-процесса → двойник актива, каждый уровень на порядок эффективнее предыдущего.

2.2 «Интеграция ИИ в корпоративные системы управления знаниями. Кейсы и вызовы в ТЭК» (сессия Минэнерго, 20 мая)

Сессия с участием Интер РАО, Сбера, КМ-альянса, Инвенторуса, НИИК, Ультиматека и Российского энергетического агентства. Фокус – как превратить накопленную информацию в работающее знание, и почему это не происходит само по себе: от «налога на поиск» до утраты экспертизы вместе с уходящими сотрудниками. Прозвучал ключевой тезис: ТЭК ежедневно генерирует 6 петабайт данных, однако «где они, кто их использует, где хранятся» – вопрос остаётся риторическим (Лещенко Владимир, КМ-альянс).

2.3 «От пилота к системе. Киберустойчивость КИИ ТЭК в масштабе страны» (сессия Минэнерго, 18 мая)

Сессия о переходе от разовых кибериспытаний к системной киберустойчивости отрасли. Участники – Минцифры, Минэнерго, Positive Technologies, Росэнергоатом, РАСУ, ИКС Безопасность, РЕД СОФТ,

Инностейдж, Транснефть. Разобран пилот в Татарстане: масштабные кибериспытания всего ТЭК региона с участием как региональных, так и федеральных компаний. Результаты легли в стратегическое видение цифровой трансформации ТЭК до 2036 года.

2.4 «Реальная проверка киберустойчивости и киберстрахование в технологическом и промышленном секторе» (18 мая)

Сессия с участием Positive Technologies, InfoWatch, АльфаСтрахования, ВСК, Гарды, АЙДЕКО, УЦСБ, РК Страхового Брокера и Северстали. Открылась кейсом ВСК – реальная кибератака в ноябре 2025 года – и далее развернулась в честную дискуссию о том, почему промышленные компании не покупают киберстрахование и что нужно изменить для роста рынка.

3. Цифровые двойники в ТЭК

Цифровые двойники на ЦИПР-2026 обсуждались не как технологический тренд, а как зрелая управленческая концепция. Центральным тезисом стало разграничение уровней зрелости – от двойника отдельного объекта до двойника всего актива, и только на высших уровнях эффект становится стратегически значимым.

3.1 Три уровня зрелости: объект, процесс, актив

Газпром нефть реализует цифровую трансформацию более шести лет и прошла путь через все три уровня. Первый уровень – цифровые двойники отдельных технологических объектов (пласт, скважина, система трубопроводов): позволяют оптимизировать отдельные операции, но «эффекты в масштабе бизнеса незначительны – доли десятых единиц процента». Второй уровень – цифровой двойник ключевого бизнес-процесса, например процесса ввода новых скважин: позволяет искать «глобальный оптимум» при одновременной оптимизации добычи, NPV, логистики, МТР. Именно здесь возникает эффект «до пяти процентов от EBITDA по году». Третий уровень – цифровой двойник актива из сотен элементов: позволяет принимать стратегические решения – выход в новый регион, продление жизни месторождения (Маргарит Андрей, Газпром нефть).

3.2 Транснефть: от ПКТС к онтологической модели

Транснефть движется к построению единой цифровой модели инфраструктуры. Конфигуратор онтологической модели описывает объект «едиными принципами» – оборудование, функции, топологию, состав и ассоциации. На примере узла учёта качества и количества нефти выявлено 8000 связей. В ПКТС (производственно-коммерческой системе Транснефти) содержится более 12 млн объектов. Первым практическим результатом стало ускорение проектирования, автоматическое создание проектной документации и верификация данных. Следующий шаг – написание ИИ-агентов, которые смогут описывать миллионы единиц оборудования (Гришанин Максим, Транснефть).

3.3 Сургутнефтегаз: определение термина как точка отсчёта

Сургутнефтегаз поставил принципиальный вопрос: прежде чем говорить о достижениях, нужно договориться о понятиях. Диспетчерский пульт с оперативной схемой энергосистемы «с шестидесятого года» – это уже цифровой двойник? Или нужна 3D-модель с возможностью «заглянуть внутрь»? Полный цифровой двойник – это IoT, SCADA, ERP/ЯМ, MES/PLM, описание бизнес-процессов и шина данных. BIM-модели нужны в объёме, определённом конкретным предприятием (Гимранов Ринат, Сургутнефтегаз).

3.4 Россети: снижение IT-затрат на 40% и новые свойства старых продуктов

Россети обратили внимание на измеримый экономический эффект цифровизации: унификация подходов позволила снизить IT-затраты на 40%. Одновременно Кравченко подчеркнул: наложение цифровой модели на уже существующие продукты (например, диспетчерский тренажёр) даёт им «новые свойства» – из инструмента обучения он превращается в «мини-двойник», позволяющий анализировать разнообразные эксплуатационные сценарии (Кравченко Константин, Россети).

3.5 Нормативы vs. предиктивная аналитика: главная дилемма

Ключевое ограничение для предиктивного обслуживания в энергетике – жёсткие регламенты. Предиктивная аналитика может показать, что «не все регламенты надо соблюдать или их надо соблюдать по-другому», но изменить нормативную базу – задача вендора, заказчика и регулятора совместно. На примере телекома экономия от предиктивного обслуживания составила «не проценты, а разы» (Телков Алексей, Галактика).

3.6 Минэнерго: проект «КиберТЭК» – цифровой двойник отрасли

Замминистра энергетики поддержал концепцию создания цифрового двойника ТЭК на уровне отрасли: он «сокращает процессы, ускоряет их, является серьёзным подспорьем для ИИ». Проект «КиберТЭК» – создание отраслевого двойника – должен охватить все три уровня, описанных Газпром нефтью. Цифровые двойники позволят «проектировать объекты в три-четыре раза быстрее» в ближайшие годы (Шереметцев Эдуард, Минэнерго России).

4. Управление знаниями и корпоративные данные в ТЭК

Сессия по управлению знаниями на ЦИПР-2026 вышла за рамки дискуссии об ИИ-инструментах и поставила принципиальные вопросы: зачем управлять знаниями, как доказать экономическую эффективность и почему промышленные предприятия до сих пор не решили эту задачу, несмотря на доступность технологий.

4.1 «Мёртвый груз»: 80% знаний не задействованы

До 80% корпоративных знаний в ТЭК лежат «мёртвым грузом»: традиционные системы управления знаниями превращаются в «кладбище данных», а уникальные инженерные знания «уходят вместе с экспертами». Первичный сбор знаний в промышленных кластерах «по большому счету уже произошел» – переход от бумажных журналов к цифровым библиотекам состоялся. Проблема – в качестве работы со знаниями: «из данных нужно извлекать знания, а это никакая модель ИИ не верифицирует, нужна экспертиза» (Воробьев Константин, Российское энергетическое агентство; Лещенко Владимир, КМ-альянс).

4.2 Налог на поиск: экономика потерь

Инженер тратит около 20% рабочего времени на поиск нужной информации. При двух часах в неделю на поиск и команде в 100 инженеров потери составляют порядка 500 тыс. рублей еженедельно. Тест «живого знания»: «может ли инженер за десять минут получить проверяемый ответ на конкретный технический вопрос со ссылками на источники?» Если нет – знание хранится неправильно (Маевский Антон, Инвенторус).

4.3 ТЭК: 6 петабайт данных в сутки

ТЭК генерирует ежедневно 6 петабайт данных. Где они хранятся, кто их использует – остаётся открытым вопросом. Действовать надо по принципу Парето: определить, какие знания критически

влияют на экономический результат, и работать только с ними. «Никаких вычислительных мощностей не хватит, если собирать все данные» (Лещенко Владимир, КМ-альянс).

4.4 Интер РАО: собственная платформа с датасетом внутри

Из-за чувствительности данных Интер РАО создала собственную AI-платформу с корпоративным датасетом. На её базе реализованы сервисы: сравнение подписанных документов с согласованными в СЭД, автоматическая подготовка протоколов совещаний, чат с базой знаний по внутренним регламентам. Сотрудники обучены создавать собственных ИИ-агентов. Начато тестирование решений от Сбера и Яндекса в режиме on-prem (Колодей Сергей, Интер РАО).

4.5 Сбер: GigaCowork как агентский слой для предприятий

Сбер представил агентскую платформу GigaCowork: агент обучается «на естественном языке», без программирования – через описание «скиллов», аналогичных должностным инструкциям сотрудников. Платформа доступна as-is из облака и on-prem; подключается к любым корпоративным системам – ERP, CRM, специализированным АСУ ТП. Ключевое ограничение: без управления доступами и логирования использование в «серьёзной корпоративной среде на sensitive данных просто опасно» (Кутуков Андрей, Сбер).

4.6 НИИК: RAG-база по технологии карбамида

Научно-исследовательский институт карбамида – один из четырёх мировых лицензиаров производства удобрения – создал индексированную RAG-базу знаний, загрузив в неё «классический труд по карбамидной технологии». Модель отвечает только с опорой на проверенные данные и «не стесняется сказать, что чего-то не знает». Это названо достижением, поскольку галлюцинации модели – главный барьер для доверия в высокоответственных производственных процессах (Колодеца Павел, АО НИИК).

4.7 Проблема формализации экспертизы

В R&D и НИОКР главный барьер – невозможность формализовать экспертизу: инженер «быстрее спросит коллегу, чем оформит и разместит знание». Росатом с 2010 по 2018 год разработал методологию извлечения и сохранения критических знаний, защищённую в МАГАТЭ. Принцип: «процесс извлечения – это не цифровой, а когнитивный процесс, человек к человеку» (Лещенко Владимир, КМ-альянс).

5. Киберустойчивость КИИ ТЭК

Сессия «От пилота к системе» стала одной из наиболее содержательных на ЦИПР-2026: разбор реального пилота в Татарстане, конкретные данные об успехах атакующей команды, честное признание нормативных пробелов и обсуждение пути к постоянным кибериспытаниям как стандарту для отрасли.

5.1 Пилот в Татарстане: 50% – реализованное «недопустимое событие»

В 2025 году Positive Technologies провела масштабный пилот кибериспытаний для ТЭК Татарстана: участвовали все региональные и федеральные компании отрасли. Каждая компания самостоятельно определила «недопустимое событие» и критерии его реализации. Ограничений было три: не атаковать подрядчиков, не удалять серверы со СЗИ, не применять физическое воздействие. В результате в 50% компаний команда достигла «недопустимого события». После устранения

уязвимостей «ТЭК Татарстана стал самым защищённым регионом страны» (Серебрянников Дмитрий, Positive Technologies).

5.2 Рост атак на КИИ ТЭК: +40% в 2025 году

Индекс угроз в ТЭК зафиксировал рост компоненты атак на критическую инфраструктуру на 40% с 2024 по 2025 год. Последствия атак – двух типов: прекращение функционирования объекта (экономический ущерб владельцу) и инцидент с воздействием на окружающую среду и жизнь людей. Злоумышленники «не будут размениваться на финансовую выгоду – они действуют с точки зрения разрушения». Симультанная атака на несколько энергетических компаний одного региона (генерация, передача, доведение до потребителей) способна нанести «неприемлемый ущерб» государству (Головатый Артем, Росэнергоатом).

5.3 Стратегия киберустойчивости ТЭК до 2036 года: три вектора

Утверждённое в феврале 2026 года стратегическое видение цифровой трансформации ТЭК до 2036 года включает три параллельных вектора: технологическая независимость; покрытие ИТ-ландшафта отечественными решениями (импортозамещение); опора на независимые объективные методы контроля. Именно третий вектор – новый: «кибериспытания как инструмент объективной валидации» и «внедрение рейтингов киберустойчивости» для стандартизации оценки (Серебрянников Дмитрий, Positive Technologies; Шереметцев Эдуард, Минэнерго).

5.4 Росэнергоатом: доверие ≠ импортонезависимость

Росатом разграничил импортонезависимость и доверие: «отечественные решения по умолчанию считаются доверенными» – это ошибочное допущение. Доверенное решение требует прозрачной верифицируемой производственной цепочки, управляемости на всём жизненном цикле, задокументированных результатов тестирований и аппаратного корня доверия. Для функций аварийной защиты реакторной установки нормативно установлен критерий надёжности – вероятность отказа 10^{-5}; такой показатель достигается только через архитектурные решения, а не через выбор одного «доверенного» компонента (Головатый Артем, Росэнергоатом).

5.5 Нормативные пробелы: регуляторы «должны быть на шаг впереди»

Пилот в Татарстане выявил необходимость изменения нормативной базы. Ключевые направления: синхронизация требований ФСТЭК, ФСБ и Минцифры; переход от самооценки к объективным методам контроля; конвертация показателей киберустойчивости в «финансовые количественные показатели» для принятия управленческих решений. Идея: обязательный экзамен для руководителей значимых объектов КИИ по кибербезопасности по аналогии с экзаменами Ростехнадзора для атомных объектов – «раз в три года» (Шереметцев Эдуард, Минэнерго; Головатый Артем, Росэнергоатом).

5.6 РЕД СОФТ: экосистема совместимости как фундамент безопасности

Построение экосистемы отечественного ПО – не разовая задача, а постоянный процесс. РЕД СОФТ работает над предсказуемостью версионирования: заранее согласовывает с партнёрами, «какой версии какой пакет будет стоять в операционной системе» – это устраняет несовместимость при обновлениях. Задача ближайшего будущего – объединить базы знаний нескольких вендоров (Р7, VK, РЕД СОФТ) для единой экосистемной поддержки с ИИ-ассистентом (Рустамов Рустам, РЕД СОФТ).

6. Киберстрахование и управление киберрисками

Дискуссия о киберстраховании на ЦИПР-2026 открылась кейсом, которого раньше на подобных площадках не было: страховая компания ВСК поделилась опытом собственной масштабной кибератаки. Это задало особый тон – честного разбора, почему рынок киберстрахования в России не растёт соразмерно угрозам и что изменится.

6.1 Кейс ВСК: атака в ноябре 2025 года

Страховой Дом ВСК в ноябре 2025 года подвергся «одной из самых массированных кибератак на российском рынке». Утром сотрудники обнаружили: «не работала почта, не работало ровным счётом ничего – работал только свет». Четыре блока потерь, чётко оцифрованных компанией: расходы на форензику и восстановление систем (включая сверхурочные); упущенная выгода и простой (основная статья потерь); восстановление информации из бэкапов; юридические расходы и рассылки клиентам. Урок: «DRP-план может быть шикарным, но когда начинаешь реально смотреть, 50% не работает» (Фролов Роман, Страховой Дом ВСК).

6.2 Рынок: «до миллиарда» при потенциале «2–3 миллиарда»

Объём корпоративного рынка киберстрахования в России – «до миллиарда рублей» фактических сборов; рынок при этом готов страховать бизнес на 2–3 млрд рублей по одному полису. На рынке около 200 осознанных корпоративных полисов. Для сравнения: глобальный рынок киберстрахования по данным Munich Re – $14–15 млрд в 2024 году, $20–22 млрд в 2025-м, прогноз к 2028 году – более $100 млрд. Российский прогноз к 2027–2028 году – 10 млрд рублей (Еремеев Иван, РК Страховой Брокер).

6.3 Почему промышленность не страхуется

Три главные причины отказа от киберстрахования в промышленности. Первая: основные простои и оборудование «уже застрахованы по движению», а там «есть определённое покрытие» киберрисков. Вторая: транзакционные операции покрываются полисами профессиональной ответственности. Третья: нет статистики для ценообразования – «каждый придумывает свои методики», «пока идём на ощупь». Дополнительный барьер – «культура замалчивания» киберинцидентов, не позволяющая накопить базу данных для актуарных расчётов (Гусев Сергей, Северсталь; Богданов Валентин, УЦСБ; Буза Алексей, АльфаСтрахование).

6.4 Киберриски как «неклассические» риски для страховщика

Киберриски не подчиняются классическим страховым моделям: информация «мгновенно копируется», «неконтролируемый доступ», а «пожар не может мгновенно распространиться на триста складов – взломать триста центров через одну точку можно в считанные секунды». Значит, стохастические вероятностные подходы «могут не работать», а одно событие способно «вынести весь рынок одним убытком» (Хайретдинов Рустэм, Гарда).

6.5 Импортозамещение как фактор страхового тарифа

Прозвучала идея о льготных страховых ставках для компаний, прошедших импортозамещение: «стек контролируется отечественной компанией», уязвимости закрываются оперативнее, регресс предъявим. Страховщики пока не выработали чёткой позиции – «нет понимания, как конкретно это влияет на ценообразование» (Арефьев Андрей, InfoWatch; Буза Алексей, АльфаСтрахование).

7. Практики внедрения: барьеры, культура, эффекты

Спикеры четырёх сессий ЦИПР-2026 по ТЭК сошлись в оценке главного барьера внедрения ИИ: проблема не технологическая. Технологии есть, доступны и работают. Проблема – в том, что «нельзя купить фабрику агентов и не знать, что с ней делать».

7.1 Данные до знаний, знания до агентов

Последовательность, которую обозначили практики: сначала – управление знаниями как фундамент, затем – ИИ как инструмент работы с этими знаниями. «Начинайте с менеджмента знаний», иначе любые инвестиции в ИИ-инструменты «уйдут в песок» (Лещенко Владимир, КМ-альянс). Компания не может получить эффект от RAG-системы, если документы «лежат, как положили», без структурирования и связанности по сущностям.

7.2 Нормативная база и регламентное мышление как тормоз

В энергетике «сто процентов всё по регламентам»: предиктивная аналитика может предложить более эффективный режим обслуживания, но изменить нормативную базу – задача, требующая взаимодействия вендора, заказчика и регулятора. Это «самая сложная дилемма – подвинуть нормативку под то, что даёт аналитика» (Телков Алексей, Галактика).

7.3 Три кита эффективной системы управления знаниями

Лещенко из КМ-альянса выделил три равнозначные составляющие: создание нового знания (инновации, антиплагиат, патентный ландшафт); эксплуатация знания (извлечённые уроки, журналы ошибок, мониторинг процессов); передача знания (обучение, патентование, капитализация). «На каждый из этих элементов есть кейсы применения и считаемый экономический эффект» (Лещенко Владимир, КМ-альянс).

7.4 Культура раскрытия информации как условие развития рынка

Страховой рынок и рынок кибербезопасности не могут развиваться без накопления статистики инцидентов. ВСК намеренно выбрала политику открытости: ежедневно принимают две-три крупных компании, рассказывают «по шагам, что нужно делать» при атаке. «Давайте не будем друг от друга ничего утаивать» – позиция, разделяемая не всеми. На Западе публичность появилась после регуляторного требования: публичные компании в США обязаны сообщать об инциденте в течение четырёх дней (Фролов Роман, Страховой Дом ВСК; Хомутов Дмитрий, АЙДЕКО).

7.5 «Вовлечь руководителя, говорить на его языке»

Ключевой практический вывод по продвижению кибербезопасности: «когда приходишь с терминами фишинг-шмишинг – ему ничего не говорит». Нужно переводить в категорию «недопустимых событий» на языке последствий для бизнеса: «что надо сделать, чтобы у тебя во рту начал ощущаться вкус сухарей?» Только так руководитель начинает понимать серьёзность угрозы (Шереметцев Эдуард, Минэнерго).

8. Отраслевой срез: нефтегаз и энергетика

Четыре сессии ЦИПР-2026 по ТЭК дали возможность сравнить позиции компаний разного масштаба и профиля: от нефтедобычи и трубопроводного транспорта до атомной и сетевой энергетики. Картина неоднородная – «на финиш вышли: один в модных кедах, другой в рваных калошах, третий босиком».

8.1 Газпром нефть: лидер по зрелости цифровых двойников

Газпром нефть – наиболее зрелый кейс: более шести лет системной реализации, охват всей цепочки создания ценности, переход на третий уровень (цифровой двойник актива). Ключевые показатели: эффект до 5% EBITDA при двойнике бизнес-процесса, 98,9% эффективности инвестиций бурения, более 1200 скважин в год (около 20% от новых по отрасли). Вывод: «таких показателей невозможно достичь без цифрового двойника» (Маргарит Андрей, Газпром нефть).

8.2 Транснефть: масштаб задачи – миллионы объектов

Транснефть работает в качественно иных масштабах: миллионы единиц оборудования, сотни тысяч типов. Именно поэтому «конвенциональными методами это все не опишешь» – нужны ИИ-агенты, способные строить онтологические модели автоматически. Уже реализован прототип конфигуратора для оборудования АСУ ТП и узлов учёта. Транснефть привлекает рыночных подрядчиков (СКАД ТЕХ, Галактика) для разработки агентов – «нас самих на всех не хватит» (Гришанин Максим, Транснефть).

8.3 Россети: IT-экономия 40% и новые сценарии для старых систем

Россети демонстрируют прагматичный подход: снижение IT-затрат на 40% – измеримый операционный результат цифровизации. Наложение цифровой модели на существующие системы расширяет их функциональность без замены оборудования: диспетчерский тренажёр превращается в аналитический инструмент для разбора «разнообразных эксплуатационных сценариев» (Кравченко Константин, Россети).

8.4 Сургутнефтегаз: осторожность и прагматизм

Сургутнефтегаз занял позицию методичного движения: акцент на договорённости об определениях, внимании к информационной безопасности («с развитием цифровых технологий каждый день появляются уязвимости») и реалистичной оценке сроков окупаемости цифровых двойников для разных типов объектов (Гимранов Ринат, Сургутнефтегаз).

8.5 Интер РАО: суверенная AI-платформа с внутренним датасетом

Интер РАО выбрала путь создания собственной AI-платформы «из-за чувствительных данных» – публичные облачные сервисы исключены. Сотрудники создают ИИ-агентов самостоятельно, ищут «сценарии эффективного использования ИИ». Тестирование решений Сбера и Яндекса ведётся уже в on-prem-режиме (Колодей Сергей, Интер РАО).

8.6 Росэнергоатом: атомный стандарт доверия как образец для отрасли

Росэнергоатом предложил транслировать атомный стандарт доверия на всю отрасль КИИ: не просто импортозамещение, а «прозрачная верифицируемая производственная цепочка, управляемость на всём жизненном цикле, задокументированные тесты». SCADA-система РАСУ получила сертификат первой категории значимости – пока единственная в стране; срок получения сертификата сокращён вдвое благодаря практике безопасной разработки (РБПО) (Головатый Артем, Росэнергоатом; Бутко Андрей, АО РАСУ).

9. Игроки сферы: компании и спикеры

Тему ИИ в ТЭК на ЦИПР-2026 формировали представители крупнейших отраслевых компаний, технологических разработчиков, страховщиков и регуляторов. Ниже – перечень участников четырёх профильных сессий.

- **Транснефть** – Гришанин Максим (первый вице-президент): онтологическая модель инфраструктуры, 8000 связей в единой модели узла учёта, ИИ-агенты для описания миллионов объектов.
- **Газпром нефть** – Маргарит Андрей (начальник управления программ повышения эффективности бизнеса): трёхуровневая модель цифровых двойников, эффект до 5% EBITDA, 98,9% автоматизации бурения, >1200 скважин в год.
- **ПАО Россети** – Кравченко Константин (заместитель генерального директора по цифровой трансформации): снижение IT-затрат на 40%, новые сценарии для существующих систем.
- **ПАО Сургутнефтегаз** – Гимранов Ринат (начальник управления ИТ): методичный подход к цифровым двойникам, акцент на информационную безопасность.
- **Минэнерго России** – Шереметцев Эдуард (заместитель Министра): проект «КиберТЭК», стратегия цифровой трансформации ТЭК до 2036 года, системный подход к кибербезопасности.
- **Минцифры России** – Шойтов Александр (заместитель Министра): эксперимент по повышению защищённости ГИС (постановление №860), ведётся с 2022 года.
- **ПАО «Интер РАО»** – Колодей Сергей (руководитель Центра информационных технологий): собственная AI-платформа с корпоративным датасетом, ИИ-агенты силами сотрудников.
- **СБЕР** – Кутуков Андрей (старший управляющий директор): GigaCowork – агентская платформа для корпоративного on-prem развёртывания.
- **КМ-альянс** – Лещенко Владимир (вице-президент): три составляющих эффективной системы управления знаниями, критика перекоса в LLM при игнорировании машинного зрения.
- **Инвенторус** – Маевский Антон (директор по стратегическому развитию), Хафизов Рустам (исполнительный директор): «налог на поиск», системы управления знаниями для R&D и НИОКР.
- **Российское энергетическое агентство Минэнерго** – Воробьев Константин (заместитель генерального директора): 80% знаний «мёртвым грузом», 6 петабайт данных ТЭК в сутки.
- **АО НИИК** – Колодеца Павел (заместитель генерального директора): RAG-база по технологии карбамида, модель, говорящая «я не знаю» при отсутствии данных.
- **ГК Ультиматек** – Растопшин Павел (генеральный директор): приземление ИИ в реальные производственные проекты с конкретными эффектами.
- **АО «Позитив Текнолоджиз»** – Серебрянников Дмитрий (Chief hacking officer): пилот кибериспытаний ТЭК Татарстана, 50% реализованных «недопустимых событий».
- **Росэнергоатом** – Головатый Артем (директор по информационным технологиям): стандарт доверия для КИИ, рост атак на ТЭК +40%, SCADA с сертификатом первой категории значимости.
- **АО «РАСУ»** – Бутко Андрей (генеральный директор): разработка и сертификация АСУ ТП для атомных станций, РБПО, сокращение срока сертификации вдвое.
- **ИКС Безопасность** – Ковалевский Александр (генеральный директор): отраслевые центры киберустойчивости, опыт взаимодействия с Минтрансом и Минстроем.
- **РЕД СОФТ** – Рустамов Рустам (заместитель генерального директора): экосистема совместимости отечественного ПО, предсказуемость версионирования.
- **Инностейдж** – Шепелявый Дмитрий (директор по международному бизнесу): управляемая защита как стандарт киберустойчивости ТЭК.

- **Транснефть-Технологии** – Темнякова Анна (начальник службы общественных коммуникаций): модерация дискуссии по цифровым двойникам.
- **АО«СКАД ТЕХ»** – Тафинцев Руслан (коммерческий директор): коммерческий ресурс для создания цифровой модели Транснефти.
- **Галактика** – Телков Алексей (генеральный директор): ERP/ЯМ в составе цифрового двойника, предиктивное обслуживание, экономия «в разы» в телекоме.
- **Страховой Дом ВСК** – Фролов Роман (член совета директоров, заместитель генерального директора): кейс кибератаки ноября 2025 года, открытая политика раскрытия опыта.
- **АльфаСтрахование** – Буза Алексей (руководитель направления по киберстрахованию): факторы ценообразования полисов, аудит клиентов.
- **РК Страховой Брокер** – Еремеев Иван (управляющий директор): объём рынка «до миллиарда», прогноз 10 млрд руб. к 2027–2028 годам.
- **Гарда** – Хайретдинов Рустэм (вице-президент): специфика киберрисков как «неклассических» для страховщика.
- **АЙДЕКО** – Хомутов Дмитрий (директор): промышленные NGFW в режиме мониторинга, а не разрыва сети.
- **ООО «УЦСБ»** – Богданов Валентин (генеральный директор): практика пентестов в промышленности, «окна возможностей» при плановых ремонтах.
- **Северсталь** – Гусев Сергей (заместитель директора по ИБ): практика реальных пентестов и red team, покрытие киберрисков существующими страховками.
- **GK InfoWatch** – Арефьев Андрей (директор по инновациям и продуктовому развитию): рынок киберстрахования ~4 млрд руб. (потенциал), «синяя линейка» промышленного NGFW.

10. Связка: суверенитет, инфраструктура, риски

Все четыре сессии ЦИПР-2026 по теме ИИ в ТЭК сходятся в одной точке: цифровая трансформация отрасли невозможна без одновременного решения трёх взаимосвязанных задач – суверенитета над данными и инструментами, масштабируемой инфраструктуры и управления принципиально новыми киберрисками.

Суверенитет в ТЭК сложнее, чем в потребительском сегменте. Данные АСУ ТП и технологических процессов «всегда имеют закрытый характер и ни в какие облака не поедут» – эта позиция не обсуждается, а принимается как аксиома. Публичный оператор обрабатывающий производственные данные крупнейших компаний ТЭК просто не может существовать в российских реалиях. Поэтому суверенитет здесь означает не просто «российское ПО», а on-prem инфраструктуру внутри закрытого корпоративного контура с собственным датасетом и возможностью развёртывания любых моделей внутри периметра.

Инфраструктурный вызов специфичен для ТЭК: речь идёт не о доступе к GPU-кластерам (хотя это тоже проблема), а о стандартизации данных. ТЭК ежедневно генерирует 6 петабайт данных, но они разрозненны, не связаны, не описаны. Онтологический подход Транснефти – 8000 связей в одном узле учёта – наглядно демонстрирует масштаб задачи описания всей инфраструктуры.

Риски в ТЭК приобрели системный характер: +40% атак за год, 50% «недопустимых событий» в ходе пилота, страховой рынок не успевает за ростом угроз. Ответом должна стать не точечная защита, а

«устойчивость как постоянный процесс» – по аналогии с «трое детей и ипотека»: кибериспытания как непрерывный режим, а не разовая проверка. Единственный способ вовлечь топ-менеджмент – говорить на его языке: «что нужно сделать, чтобы ты посидел и ощутил вкус сухарей?» (Шереметцев Эдуард, Минэнерго; Серебрянников Дмитрий, Positive Technologies).

11. Цитаты-якоря

Опорные высказывания спикеров ЦИПР-2026 по теме ИИ в ТЭК – из четырёх профильных сессий.

Цифровые двойники: уровни и эффекты

> *«Если вы ограничиваетесь уровнем цифровых двойников отдельных объектов, эффекты в масштабе бизнеса незначительны – это доли десятых единиц процента. Если объект управления – бизнес-процесс, вы уже на порядок больше эффекта можете получить. По нашим оценкам, до пяти процентов от EBITDA по году.»*
>
> **– Маргарит Андрей, начальник управления программ повышения эффективности бизнеса, Газпром нефть**
>
> *«Мы обнаружили восемь тысяч связей. Сюда погружено всё: оборудование инфраструктуры, технологическое оборудование самого узла, функции, топология, композиция, как он сгруппирован, куда он входит, и ассоциации.»*
>
> **– Гришанин Максим, первый вице-президент, Транснефть**
>
> *«У нас миллионы единиц оборудования. Описать все отдельно, а далее связать в единую систему, в такой очень многомерный граф – конечно, без помощи современных инструментов крайне затруднительно.»*
>
> **– Гришанин Максим, первый вице-президент, Транснефть**

Управление знаниями

> *«До восьмидесяти процентов этих знаний, к сожалению, часто лежат мёртвым грузом. Традиционные системы управления знаниями нередко превращаются в кладбище данных, а самое главное – уникальные инженерные знания уходят вместе с экспертами.»*
>
> **– Воробьев Константин, заместитель генерального директора, Российское энергетическое агентство Минэнерго**
>
> *«Менеджмент знаний является тем фундаментом, который позволит эффективно использовать ИИ. Если компания не занимается менеджментом знаний, то начинайте с него. Вот это первый шаг для того, чтобы потом покупать фабрику агентов и не знать, что с ней делать.»*
>
> **– Лещенко Владимир, вице-президент, КМ-альянс**

Киберустойчивость

> *«В половине компаний нам удалось дойти до недопустимых событий. После того как все закрыли обнаруженные уязвимости, отрасль ТЭК Татарстана стала самой защищённой среди всех остальных регионов нашей страны.»*
>
> **– Серебрянников Дмитрий, Chief hacking officer, АО Позитив Текнолоджиз**
>
> *«Компонента, связанная с атаками на КИИ, с двадцать четвёртого года в двадцать пятый выросла на сорок процентов. Это говорит о том, что риски, связанные с киберустойчивостью и кибер-инцидентами, растут.»*
>
> **– Головатый Артем, директор по информационным технологиям, Росэнергоатом**

> *«Киберучения – один раз пришёл и ушёл, а кибериспытание – это трое детей и ипотека. То есть это когда компании в постоянном режиме работают над мониторингом и своей безопасностью.»*
>
> **– Шереметцев Эдуард, заместитель Министра, Минэнерго России**

Киберстрахование

> *«Буквально за день до того, как у нас всё произошло, мы сидели на правлении и обсуждали, надо ли потратить на кибербез дополнительные сто миллионов рублей. И все члены правления сказали: ты с ума сошёл? А в это время уже кто-то был внутри нас.»*
>
> **– Фролов Роман, член совета директоров, Страховой Дом ВСК**

> *«Пожар не может мгновенно распространиться на триста складов по всей России. А взломать триста центров через одну точку – да пожалуйста, это можно сделать в считанные секунды. Поэтому классические вероятностные подходы здесь могут не работать.»*
>
> **– Хайретдинов Рустэм, вице-президент, Гарда**

12. Сводная таблица ключевых метрик

Числовые показатели сферы ИИ в ТЭК, прозвучавшие в выступлениях на ЦИПР-2026. Все значения приведены строго по материалам сессий.

Показатель	Значение	Источник
Газпром нефть: потенциальный эффект цифрового двойника бизнес-процесса	до 5% EBITDA	Маргарит Андрей, Газпром нефть
Газпром нефть: эффективность инвестиций бурения	98,9%	Маргарит Андрей, Газпром нефть
Газпром нефть: количество скважин в год	>1200 (около 20% от новых по отрасли)	Маргарит Андрей, Газпром нефть
Транснефть: связи в онтологической модели узла учёта	8000	Гришанин Максим, Транснефть
Транснефть ПКТС: объём объектов в системе	>12 млн	Гришанин Максим, Транснефть
Россети: снижение IT-затрат за счёт цифровизации	40%	Кравченко Константин, Россети
Доля знаний ТЭК, лежащих «мёртвым грузом»	до 80%	Воробьев Константин, Российское энергетическое агентство
ТЭК: ежедневная генерация данных	6 петабайт	Лещенко Владимир, КМ-альянс (данные Минэнерго)
Налог на поиск: потери предприятия с 100 инженерами	~500 тыс. руб./нед.	Маевский Антон, Инвенторус
Доля рабочего времени инженера на поиск информации	~20%	Маевский Антон, Инвенторус
Рост атак на КИИ ТЭК в 2025 году	+40%	Головатый Артем, Росэнергоатом
Пилот Татарстан: доля компаний с реализованным «недопустимым	50%	Серебрянников Дмитрий, Positive Technologies

Показатель	Значение	Источник
событием»		
Рынок киберстрахования в России (корпоративные сборы)	до 1 млрд руб.	Еремеев Иван, РК Страховой Брокер
Готовность страхового рынка к покрытию одного клиента	до 2–3 млрд руб.	Еремеев Иван, РК Страховой Брокер
Прогноз рынка киберстрахования России к 2027–2028 гг.	10 млрд руб.	Еремеев Иван, РК Страховой Брокер
Мировой рынок киберстрахования (2025)	$20–22 млрд	Munich Re (данные Еремеева Ивана)
Прогноз мирового рынка киберстрахования к 2028 г.	>$100 млрд	Munich Re (данные Еремеева Ивана)