Владимир Соловьев
Руководитель группы

// 2026

ДиалогНаука

Системная интеграция и консалтинг в сфере информационной безопасности

с 1992 года
на рынке информационной безопасности

34 года
практического опыта

Компетенции и стандарты

ФСТЭК / ФСБ · PCI DSS · SWIFT · ISO

ДиалогНаука

О компании

Более 30 лет помогаем организациям выстраивать надежную систему информационной безопасности

Оказываем консалтинговые услуги, разрабатываем и поставляем комплексные решения по информационной безопасности, сопровождаем их внедрение и эксплуатацию

Прошли путь от поставщика отдельных программных продуктов до компании, специализирующейся на системной интеграции решений по защите информации

Ключевые отрасли

- **Топливно-энергетический сектор**
- **Финансово-кредитный сектор**
- **Страховой сектор**
- **Промышленность**
- **Пенсионное обеспечение**

Анализ защищенности

оцениваем текущий уровень защиты инфраструктуры и данных

Проектирование защиты

разрабатываем модели угроз, архитектуру и документацию

Внедрение ИБ-решений

поставляем и интегрируем средства защиты информации

Соответствие требованиям

помогаем выполнять требования регуляторов и стандартов

Сопровождение

обеспечиваем техническую поддержку, аудит и развитие решений

ИИ вышел из чата в бизнес-процессы*

Positive Technologies

Инструмент Microsoft Prompty для работы с промптами LLM оказался уязвим: критическая брешь CVE-2026-73299 — 10 из 10 баллов по CVSS (сентябрь 2026).

Обычный .prompty-файл (из открытого репозитория или сгенерированный самой нейросетью) позволял выполнить произвольный код на сервере.

Новый вектор — атака через цепочку поставок ИИ. Брешь нашла российская команда Positive Technologies

УЦСБ и ГК «Солар»

Опрос 102 российских компаний (июль 2026): 50,5% подозревают или уже фиксировали утечки данных через ИИ-инструменты — из них 8,1% подтвердили реальные инциденты.

При этом 33,3% не применяют никаких специальных мер защиты ИИ, а 63,6% признают нехватку обучения и внутренних политик AI Security. Половина компаний даже не догадывается, что утечка может произойти изнутри

ГК «Солар»

Аналитики ГК «Солар» изучили трафик 150 российских компаний. За 2025 год объём данных, уходящих в общедоступные нейросети, вырос в 30 раз.

В чат-боты уходят презентации, аналитика, фрагменты кода и внутренняя переписка. Около 60% организаций до сих пор не имеют политик работы с ИИ

Дипфейки

ИИ атакует не только данные, но и людей: 41% организаций уже сталкивались с попытками выдать себя за руководителя через дипфейк (iProov).

Кейс инженерной компании Arup: сотрудник перевёл $25 млн после видеозвонка, где «руководители» были сгенерированы ИИ. Объём синтетики растёт ~900% в год

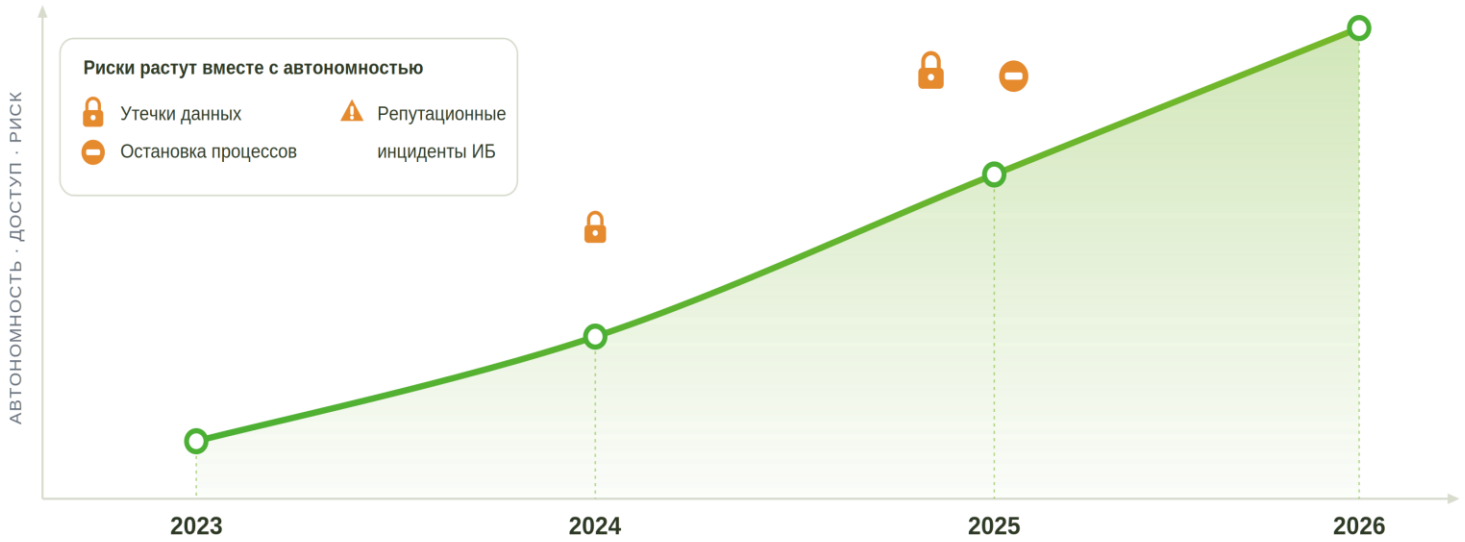
*Информация за 2026 год

ДиалОгНаука

Прошлое и настоящее ИИ-систем

Рост автономности ИИ и поверхности атаки

От изолированного чат-бота к агенту с правами сотрудника, 2023 — 2026



2023 Изолированный чат-бот

Копирование текста вручную, пилотные проекты. Нет доступа к системам.

2024 Подключение · RAG

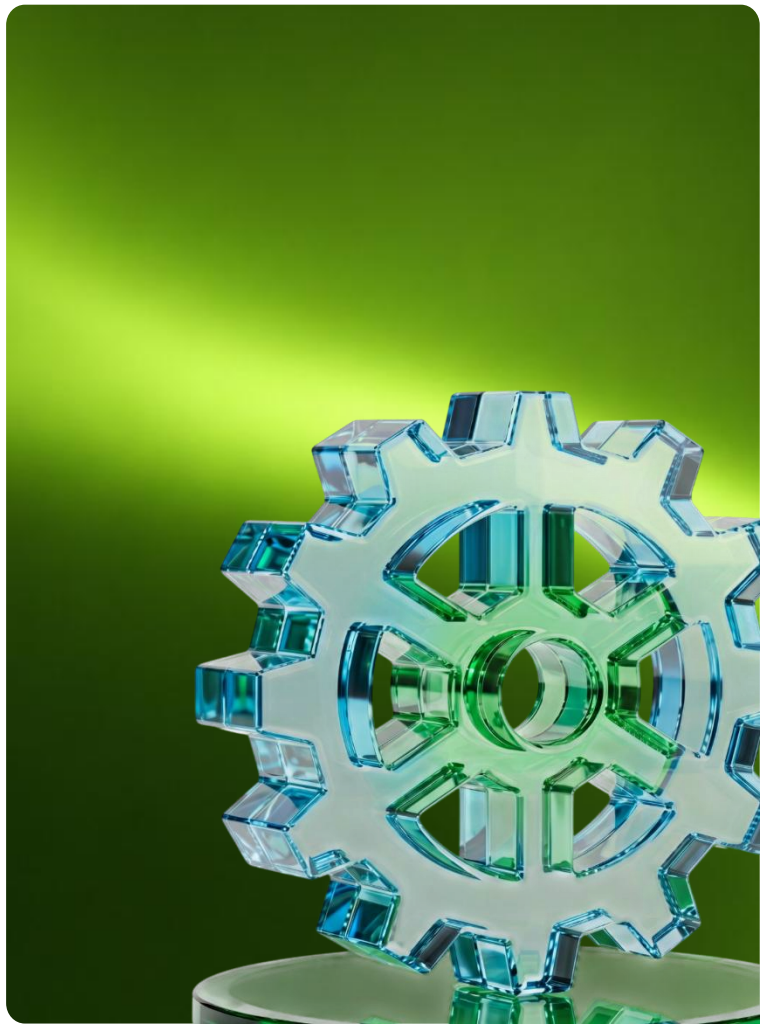
Корпоративные ассистенты и копилоты: доступ к базам знаний, документам, почте.

2025 ИИ-агенты · действие

Вызовы инструментов и API. ИИ не отвечает, а выполняет действия в системах.

2026 Встроены везде

Агенты в CRM, CI/CD, почтовых шлюзах и ноутбуках — с правами сотрудника.



ДиалОгНаука

Кризис классических подходов к защите

Традиционный софт

Детерминированная. Жесткие алгоритмы: «Если А, то Б»	**Логика работы**
Ошибки в коде. (CVE, инъекции SQL, переполнение буфера)	**Природа уязвимостей**
Взлом хостов. Нужен эксплойт: вредоносный код, уязвимости, ВПО	**Вектор атаки**
Сервисные аккаунты. Принцип минимальных привилегий	**Идентичность и права**
Прозрачные логи в журналах. Видно: кто, когда, какую команду/API вызвал	**Аудит и расследование**

ИИ-системы

Вероятностная. Интерпретация смысла, контекста и намерения
Когнитивные искажения. Манипуляция смыслом, слепые зоны логики
Инъекция в промпт (prompt injection). Вредоносные инструкции, скрытые в легитимных письмах, документах и данных
Наследование прав. Агент работает с правами самого сотрудника (доступ ко всему, что есть у пользователя)
«Черный ящик». Сложно понять, почему модель приняла решение отдать данные или выполнить действие