

Код **ИБ** Екатеринбург 2026: тезисы, записи и презентации

Главное из выступлений конференции: ключевые тезисы каждого доклада, ссылки на записи и презентации спикеров.



17

ВЫСТУПЛЕНИЙ

12

ЗАПИСЕЙ

2

ЗАЛА

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Фотографии

https://vk.ru/album-73689515_312299495

Страница отчёта на сайте

<https://codeib.ru/event/kod-ib-ekaterinburg-2026-1016/page/otchet-kod-ib-ekaterinburg-2026-1016>



Содержание

- 01 Голос отрасли: Цифровизация, Кибербезопасность, Искусственный Интеллект**
Сергей Марков, Ольга Чернокоз, Вячеслав Касимов, Евгений Зеваков, Никита Дунов
- 02 Диалог с регулятором. Роскомнадзор.**
Ярослав Федулов
- 03 Бизнес игра: "Кризисный штаб"**
Арсений Бенин
- 04 Диалог с регулятором. НКЦКИ.**
Юрий Зубаиров
- 05 Диалог с регулятором. ФСТЭК.**
Дмитрий Щёкотов
- 06 Деловая игра "Чужой среди своих"**
Павел Блинов, Вячеслав Новоселов
- 07 Практика построения катастрофоустойчивой ИТ- инфраструктуры**
Виктор Емельянов
- 08 Персональные данные в 2026 году**
Кирилл Солодовников
- 09 Как повышать культуру кибербезопасности?**
Константин Шевченко
- 10 ИИ в закрытом контуре**
Никита Дунов
- 11 Что произошло с ИИ в России за 3 года (наши наблюдения)**
Александр Скаковский
- 12 Практика использования ИИ в процессах компании: от создания персонифицированных КП для клиентов до построения управленческого учета**
Сергей Поздняк
- 13 ИИ для управления рисками**
Вячеслав Касимов
- 14 Подходы к автоматизации обезличивания данных для работы с «внешними» LLM**
Евгений Зеваков
- 15 ИИ пентест в действии: Живое демо анализа периметра компании и поиска уязвимостей**
Дмитрий Пензов
- 16 От вопросов покупателей к продажам: как доработать B2B-сайт с помощью ИИ**
Дмитрий Южанин
- 17 Деловая игра: «ИИ под прицелом»**
Ольга Поздняк, Сергей Поздняк, Евгений Попов, Антон Наумов, Дмитрий Южанин

10:30 • 60 минут • Тезисы проверены редакцией • 28.10.2026 • [Полные тезисы на сайте →](#)

Голос отрасли: Цифровизация, Кибербезопасность, Искусственный Интеллект

**Сергей Марков**

Директор по развитию технологий ИИ, ПАО Сбербанк

**Вячеслав Касимов**

Директор по ИБ, Точка Банк

**Никита Дунов**

Руководитель Группы цифровой трансформации, ГК "Метран"

**Ольга Чернокоз**

Председатель Правления Ассоциации инновационных решений и искусственного интеллекта «Регионы XXI ВЕК»...

**Евгений Зеваков**

Основатель Zevakov Labs, постоянный эксперт Ассоциации инновационных решений и искусственного интеллекта...

Запись доклада

ИИ в кибербезопасности — нейтральный инструмент, но он ускоряет гонку снаряда и брони

Сергей Марков (ПАО Сбербанк) подчёркивает: ИИ — это область науки и технологий для автоматизации интеллектуальных задач, и сама технология нейтральна. Как молотком можно заколачивать гвозди или разбивать головы, так и ИИ в кибербезопасности может использоваться и защищающимися, и атакующими. Автоматизированные системы для атак, аудита, выявления уязвимостей и защиты применяются очень давно, поэтому прогресс не стоит воспринимать как мгновенный скачок: часто агентные системы просто проверяют то, до чего у людей не доходили руки.

Предприятия ищут доверенный контур внедрения ИИ и бесплатный аудит процессов

Ольга Чернокоз рассказала, что возглавляемая ею ассоциация выстраивает доверенный контур внедрения искусственного интеллекта в российских регионах и на промышленных предприятиях. Она объединяет экспертов по ИИ, предприятия, внедряющие технологии, и IT-/ИИ-компании с готовыми решениями. Фокус — работа именно с предприятиями, а не с органами госвласти, где всё сложнее.

Бизнес осторожно внедряет агентов, начиная с простых и «незаменимых» функций

Евгений Зеваков (Zevakov Labs) отмечает: экономические сложности диктуют первоочередные задачи — секретарские функции, документооборот и всё, что с ними связано. Но хайп вокруг агентов приводит к запросам от руководителей: почему часть работы до сих пор делают люди? Если полгода назад звучало «заменим 5 секретарей на 2», то сейчас спрашивают: «у нас 10 инженеров-экологов, можем ли оставить 3 и сделать систему, которая сама готовит экологическую экспертизу?»

Агента нужно воспринимать как сотрудника: разграничение прав, минимум доступов и контроль внешних каналов

Вячеслав Касимов (Точка Банк) предупреждает: как только в LLM загружают большие данные о компании и клиентах, она становится многопользовательской, а тем более получает доступ в интернет — риски резко возрастают. В обычной системе есть чёткие правила доступа, и корректная программа не даёт выйти за рамки. В многопользовательском ИИ доступы размываются: либо архитектурно продуманы изолированные домены, либо получается «коммунальная квартира». Дополнительно есть специфический набор угроз — OWASP Top 10 для генеративных моделей и агентских решений.

Готовые AI-файрволы уже появляются, но защиту можно переиспользовать или строить самим

На вопрос о готовых решениях Вячеслав Касимов ответил, что есть два пути. Первый — найти готовое решение: интеграторы уже предлагают «AI-файрволы», у кого-то они работают, у кого-то нет. Второй — сделать самому. В любом случае нужно понимать особенности своей инфраструктуры и использования ИИ. Если речь о внешних моделях, крайне нежелательно, чтобы в них попадала чувствительная информация, поэтому нужен шлюз. Но если обращение идёт через веб, разницы с обычным уходом на Google Диск может не быть: в компании и так должен работать DLP. Не нужно выращивать из ИИ «могучую химеру» — это такое же приращение, просто с другими алгоритмами. Можно переиспользовать накопленные процессы защиты.

Зал 1 · 12:00 · 20 минут · Тезисы проверены редакцией · 28.10.2026 · [Полные тезисы на сайте →](#)

Диалог с регулятором. Роскомнадзор.



Ярослав Федулов

Начальник отдела контроля и надзора за соблюдением законодательства в сфере персональных данных

Управление Роскомнадзора по Уральскому федеральному округу

Запись доклада

Оборотные штрафы за утечки персональных данных заработали, и суды поддерживают Роскомнадзор

С прошлого года вступили в силу изменения об оборотных штрафах за утечки персональных данных. Практика нарабатывается успешно: суды поддерживают доводы Роскомнадзора, поэтому вопрос ответственности встаёт перед операторами всё острее.

На объектах КИИ с обработкой персональных данных действует мультипликатор ответственности

Для объектов КИИ, где обрабатываются персональные данные, действует мультипликатор ответственности: контроль идёт и по линии ФСТЭК (187-ФЗ), и по 152-ФЗ. Если ИСПДн является ещё и объектом КИИ, будьте готовы, что на вас направят взор сразу два регулятора.

За действия подрядчика административную ответственность несёт владелец информационной системы

Если информационную систему обслуживает подрядчик, эти работы рассматриваются как поручение на обработку персональных данных, и ответственность изначально лежит на владельце объекта. При уязвимости у подрядчика вопросы придут к владельцу: оператор отвечает и за его действия, а к подрядчику требования можно предъявить лишь в рамках Гражданского кодекса.

Основной вектор надзора — проверки сайтов без взаимодействия с контролируемым лицом

Ключевой вектор надзора Роскомнадзора — мероприятия по контролю без взаимодействия с контролируемым лицом. Они регулируются постановлением № 1046, а не 248-м ФЗ, и проводятся без уведомления: о проверке оператор узнаёт из требования об устранении нарушения со сроком 10 рабочих дней. Неисполнение грозит ответственностью, чаще всего по части 1 статьи 13.11 КоАП.

Хранение баз данных вне России и использование Google форм ведут к штрафам в миллионы

Строгое требование части 5 статьи 18 закона о персональных данных: при сборе персональных данных хранение и последующая обработка должны обеспечиваться с использованием баз данных на территории Российской Федерации. Любое иное решение — автоматический триггер для выявления нарушения и основание для дела по части 8 статьи 13.11 КоАП, где штраф для юрлиц измеряется в миллионах.

Вход на сайт через иностранные сервисы запрещён — введён состав по статье 13.55 КоАП

Требования 149-го федерального закона по способам авторизации на сайте уже действуют, и таких способов четыре: номер телефона, госуслуги, единая биометрическая система либо российская информационная система. Вход через иностранные сервисы — Apple ID, аккаунты Google — под запретом.

Зал 2 · 12:00 · 60 минут · Тезисы проверены редакцией · 28.10.2026 · [Полные тезисы на сайте →](#)

Бизнес игра: "Кризисный штаб"



Арсений Бенин

Коммерческий директор
АСИЕ-Групп

Утечка базы через подрядчика: исходная точка игры

Сценарий игры — собирательный, из реальных инцидентов. Вы управляете кризисным штабом вымышленного сервиса, принимающего заказы в приложении и на сайте, а подрядчик сервиса поддерживает портал обратной связи и выгрузку данных. В 9:00 появляется сообщение о продаже клиентской базы: в открытом доступе образец на 200 строк с персональными данными, и он совпадает с частью клиентских обращений.

Сначала фиксация следов, а не переустановка сервера

Подрядчик готов переустановить сервер, но до уничтожения его локальных журналов должно произойти сохранение доказательств. Отдельно штаб решает, что можно остановить, не прерывая приём заказов: команда на защите объясняла, что сервер нельзя сносить, потому что на нём есть следы, нужно задействовать альтернативные каналы и уведомить об этом пользователей.

Главный урок: подрядчику — только необходимые данные

Ключевой вывод разбора: подрядчику нужно давать исключительно те данные, которыми он будет пользоваться, — не больше. Если есть возможность, распределить их между двумя-тремя подрядчиками так, чтобы ни у кого не было целой картины.

Публичное сообщение, легитимный канал и риск мошенников

Штабу нужно подготовить сообщение объёмом до 60 слов, определить канал публикации, подписанта и следующую контрольную точку, учесть обращения клиентов и риск мошеннических сообщений. В игре клиенту приходит SMS со ссылкой на оплату и фразой про «компенсацию за утечку»: клиент должен понимать, какой канал легитимный и куда переходить не стоит.

Закрывать все экспортные каналы и не оставлять старый токен

В третьем раунде нашёлся отдельный токен задания выгрузки — при первом решении один из каналов выгрузки остался не закрыт. Логика проверки: если все ключи подрядчика либо все экспортные каналы охвачены и мера исполнена (коды A02 и A03), запрос вторым токеном отклоняется, иначе он проходит. Штабу нужно свериться с фактическим текстом первого решения: закрыт ли этот путь и какая проверка подтверждает результат.

Параллельные процессы и тщательная фиксация решений

В кризисе действия приходится выстраивать параллельно: пока инцидент развивается, штаб одновременно ограничивает доступ, сохраняет доказательства, готовит сообщение клиентам и проверяет остаточный доступ. По опыту участников, времени на ознакомление и распределение ролей не хватает — и это отражает реальность.



Зал 1 • 12:20 • 20 минут • Тезисы проверены редакцией • 28.10.2026 • [Полные тезисы на сайте →](#)

Диалог с регулятором. НКЦКИ.

Юрий Зубаиров

Представитель
НКЦКИ

Запись доклада

С 2025 года обязанности по взаимодействию с ГосСОПКА расширены и распространены на руководителей госорганов и организаций независимо от наличия объектов КИИ

Представитель НКЦКИ Юрий Зубаиров напомнил, что с момента вступления в силу Федерального закона 58 в 2025 году сфера действия 187-го Федерального закона о безопасности КИИ существенно расширилась. У субъектов КИИ появились новые обязанности, в частности обязанность сообщать в ГосСОПКА о компьютерных атаках. Обязанности по взаимодействию с ГосСОПКА распространились также на руководителей государственных органов и организаций: они попадают под действие закона независимо от наличия у них объектов КИИ.

Приказ 546 вводит обязанность сообщать в НКЦКИ об атаках на других субъектов КИИ в течение 12 часов

Приказ 546 устанавливает порядок обмена информацией о компьютерных атаках и компьютерных инцидентах между субъектами КИИ внутри страны, а также между субъектами КИИ и зарубежными ведомствами и организациями в области реагирования на компьютерные инциденты.

Приказ 547 задает сроки информирования НКЦКИ: 3 часа для значимых объектов КИИ и 24 часа в остальных случаях

Приказ 547 определяет сроки направления материалов в НКЦКИ. Для субъектов КИИ при наличии значимых объектов КИИ срок направления информации о компьютерном инциденте — 3 часа. Для иных объектов КИИ — 24 часа. Срок направления информации о компьютерных атаках — 24 часа. Для руководителей государственных органов срок информирования о компьютерных атаках и инцидентах — 24 часа.

Приказ 548 обязывает подключиться к инфраструктуре НКЦКИ для непрерывного взаимодействия с ГосСОПКА

Приказ 548 устанавливает правила непрерывного взаимодействия с ГосСОПКА для субъектов КИИ, а также для руководителей государственных органов и организаций. Непрерывное взаимодействие осуществляется посредством подключения к технической инфраструктуре НКЦКИ. Субъекты КИИ, имеющие значимые объекты КИИ, а также государственные органы и организации обязаны подключиться к инфраструктуре НКЦКИ.

НКЦКИ разграничивает компьютерную атаку и компьютерный инцидент: квалификация зависит от наличия последствий

Понятия «событие ГосСОПКА» не существует; есть термины «компьютерная атака» и «компьютерный инцидент». На примере ДДОС-атаки на публичный сайт, когда ресурсы в локальной сети не пострадали, нужно уточнить, было ли нарушено функционирование сайта. Если да — это компьютерный инцидент, если нет — компьютерная атака. Если сайт или DNS-сервер является частью объекта КИИ, информация направляется в установленные сроки; если не является, обязанности нет, но НКЦКИ рекомендует направлять сведения для общей картины и предупреждения других субъектов.

Практические разъяснения НКЦКИ: момент обнаружения, инциденты по вине сотрудников, блокировка IP и сбор логов

Моментом обнаружения компьютерного инцидента считается выявление последствий или начало мер реагирования. Если специалисты изначально обнаружили факты несанкционированного доступа или изменение конфигурации, но изменения не зафиксированы, моментом обнаружения считается выявление несанкционированного доступа. Если ресурсы на аутсорсинге у центра мониторинга ГосСОПКА и центр выявил атаку в 2 часа ночи, а сообщил в 8 утра, временем начала считается 2 часа ночи — время выявления центром ГосСОПКА.

Зал 1 · 12:40 · 20 минут · Тезисы проверены редакцией · 28.10.2026 · [Полные тезисы на сайте →](#)

Диалог с регулятором. ФСТЭК.

Дмитрий Щёкотов

Начальник отдела

Управление ФСТЭК России по УФО

Запись доклада

ФСТЭК создаёт систему учёта и мониторинга защищённости значимых объектов и ГИС

9-е управление ФСТЭК России занимается учётом автоматизированных систем, включая государственные информационные системы. Создана и прошла проектную эксплуатацию информационно-аналитическая система «Кречет», к которой будут подключать всех субъектов КИИ со значимыми объектами и органы государственной власти. ФСТЭК уже рассылает рекомендации, в том числе обязательные в силу 250-го указа Президента, по устранению уязвимостей и работе с фишинговыми атаками. В 239-й приказ, скорее всего, со следующего года внесут изменения: субъекты КИИ будут в обязательном порядке предоставлять такие же сведения, какие сейчас по 117-му приказу предоставляют органы государственной власти.

Оценка защищённости строится на показателях, самооценке и верификации ФСТЭК

Мониторинг текущего состояния технической защиты информации и безопасности значимых объектов КИИ означает, что организация в силу закона должна не реже одного раза в полгода проводить у себя мониторинг. Оценка состояния защиты информации проводится оператором на основе показателей защищённости: изначально каждому показателю по умолчанию присваивается единица, а при рассмотрении материалов ФСТЭК проверяет, действительно ли нормы выполняются.

Организационные требования: ответственный за безопасность и подготовленные специалисты

Обязательно должно быть назначено должностное лицо, отвечающее за безопасность. Как правило, это заместитель руководителя, заместитель директора или иной руководитель по безопасности, который организует всю работу. Второй пункт — назначение специалистов отдела, которые должны соответствовать требованиям и иметь соответствующее образование. Речь может идти об одном-двух человек, но важна организованная структура. По первым двум пунктам подтверждение, как правило, пока не требуется.

Парольная политика и многофакторная аутентификация — зона особого внимания

Учётные записи с паролями должны соответствовать требованиям парольной политики. Каждое предприятие разрабатывает свою политику, но она должна соответствовать методикам, в том числе разработанным ФСТЭК. При проверке ФСТЭК смотрит, разработана ли политика, сверяет её с методическими документами; если она не соответствует показателю, присваивается ноль. В ходе контрольных мероприятий могут подойти к любому автоматизированному рабочему месту, подключённому к информационной системе, и проверить вход-выход по количеству знаков и выполнение требований парольной политики. Многофакторная аутентификация привилегированных пользователей и администраторов — слабое место на многих предприятиях: лучше всего требование выполняется в энергетике, хуже всего — в оборонно-промышленном комплексе. Предоставляются сведения о сервисных учётных записях, в том числе при привлечении подрядных организаций и аутсорсинге. При самооценке нужны подтверждающие документы; при контрольных мероприятиях ФСТЭК составляет таблицу, но по умолчанию считается, что всё проверено.

Уязвимости, сканирование и средства защиты: что проверяет ФСТЭК

Организации могут привлекать сторонние компании для проверки и сканирования информационной системы. Предприятия непрерывного цикла могут сканировать уязвимости только после остановки работ; ФСТЭК обычно согласовывает такие работы с работодателем, но организация может и отказать. В силу 250-го указа Президента ФСТЭК рассылает рекомендации по уязвимостям; все субъекты со значимыми объектами учтены, а дополнительными запросами ФСТЭК получает сведения о наличии программного обеспечения и определяет, какая уязвимость по какому продукту опасна для предприятия. Проверяются межсетевые экраны на периметре и их настройки, средства антивирусной защиты со снимками экрана панели управления и централизованным управлением, защита от отказа в обслуживании и DDoS (при доступе к информационным системам должен быть договор). Централизованный сбор событий безопасности должен быть на всех устройствах; принимаются только CIM-системы.



Зал 2 • 13:00 • 70 минут • Тезисы проверены редакцией • 28.10.2026 • [Полные тезисы на сайте →](#)

Деловая игра "Чужой среди своих"



Павел Блинов

Директор отдела продаж
SkyDNS



Вячеслав Новоселов

Генеральный директор
SkyDNS

Игра моделирует кризисный штаб крупного ритейлера в разгар «чёрной пятницы»

Условная компания — один из крупнейших федеральных ритейлеров: 45 тысяч сотрудников, 750 магазинов, распределительная сеть комплексов. Склады заполнены, компания вложила много денег в маркетинговую акцию, до старта «чёрной пятницы» считанные часы. Потери от кибератаки могут составлять от 30 до 50 миллионов в час. Штабы включают ключевые роли: CEO, CISO, CIO, CTO, коммерческого директора и другие функции. В каждом штабе есть инсайдер, играющий на стороне конкурента; генеральный директор инсайдером быть не может. В трёх раундах штаб получает новую информацию и четыре варианта ответа, на обсуждение — 5 минут, финальное решение принимает генеральный директор. Затем нужно восстановить цепочку атаки по пяти вопросам и вычислить инсайдера.

Атаку организовал конкурент, а техническая цепочка началась с логистического партнёра

За атакой стоял конкурент. Его цель — сорвать «чёрную пятницу» и ударить по продажам компании. Для этого конкурент нанял внешних хакеров и одновременно подкупил человека внутри кризисного штаба. Техническая цепочка началась с компрометации логистического центра. Затем сотрудник получил письмо от доверенного отправителя и перешёл на новый домен. Рабочее устройство было скомпрометировано. После этого активность появилась ещё на нескольких устройствах. Они начали обращаться к DGA-доменам — автоматически сгенерированным доменам, связывавшимся с C2-инфраструктурой атакующих. Через DNS формировался скрытый канал передачи данных и начался вывод конфиденциальной информации.

DGA-домены и DNS-туннелирование позволяют скрытно связываться с атакующими

Участники видели обращения к новым доменам, зарегистрированным менее суток назад и ранее не встречавшимся в инфраструктуре. EDR не реагировал и не классифицировал угрозы. Затем пять рабочих устройств начали с похожей периодичностью обращаться к неизвестным доменам, которые постоянно менялись. За 15 минут корпоративный сервер отправлял аномальное количество DNS-запросов к недавно появившимся доменам. В третьем раунде появились необычно длинные DNS-запросы с меняющимися поддоменами и неизвестный процесс на нескольких устройствах; одно устройство принадлежало сотруднику с доступом к конфиденциальной информации.

Проблемы с VPN и 80 000 DNS-запросов оказались ложными следами

В сценарии вокруг настоящего инцидента были ложные следы. 80 000 DNS-запросов генерировал легитимный сервис веб-аналитики, а проблемы с корпоративным VPN были связаны с изменением парольной политики. Эти события выглядели как значимые аномалии и могли отвлечь штаб от главного сценария. Участникам предлагалось решить, что могло ложно отвлечь от фокуса главного сценария: обращение одного устройства к новым доменам, пять устройств с похожими обращениями, аномальное количество DNS-запросов корпоративного сервера или появление неизвестного процесса. Это подчёркивает необходимость отделять отвлекающие маневры от истинной причины атаки.

Главный урок: самое громкое событие не обязательно самое опасное

Финальный вывод игры: в реальном инциденте важно не просто видеть отдельные аномалии, а уметь связывать их между собой и понимать, что происходит в инфраструктуре. Самое громкое событие не обязательно самое опасное. Штабу приходилось приоритизировать направления при ограниченных ресурсах: работать с корпоративным сервером, с VPN, с группой рабочих устройств или ждать дополнительных данных. В сценарии одновременно развивались три вектора: аномальные DNS-запросы к меняющимся доменам, проблемы с корпоративным VPN и обращения рабочих устройств к новым доменам. Цена ошибки особенно высока, когда под угрозой устройство сотрудника с доступом к конфиденциальной информации.

Зал 1 • 13:00 • 20 минут • Тезисы проверены редакцией • 28.10.2026 • [Полные тезисы на сайте →](#)

Практика построения катастрофоустойчивой ИТ-инфраструктуры



Виктор Емельянов

Заместитель коммерческого директора
RTCloud

[Запись доклада](#)

Уровень катастрофоустойчивости определяется допустимым временем простоя

Катастрофоустойчивая архитектура строится исходя из целей и ценности информационных систем и делится на три уровня. Для большинства систем и данных достаточно надёжного резервного копирования — базового уровня, без которого практически не обходится никто; время восстановления здесь составляет от нескольких часов до нескольких суток.

К техногенным и антропогенным угрозам добавились военные и террористические опасности

Стратегические предприятия, а также объекты транспортной и энергетической инфраструктуры сами по себе являются опасными объектами и всегда выступают основными целями при возможных атаках. При этом самые ценные информационные системы обычно размещаются ровно там же, где находится предприятие — практически в его сердце, — и тем самым в прямом смысле становятся целью военных и террористических угроз.

Схема 3-2-1 обязательна: без отчуждения копий простой может растянуться на неделю

Резервное копирование защищает от аппаратных и программных сбоев, ошибок и злонамеренных действий персонала и от шифровальщиков, но спасает только данные, а не инфраструктуру. Рекомендуется подход 3-2-1: три копии на носителях двух разных типов, причём одна копия должна отчуждаться — храниться не там, где лежат основные данные.

Active-Active исключает простой и позволяет проводить плановые работы без остановки систем

В схеме полного резервирования Active-Active нет выделенной основной или резервной площадки: существует два или более ЦОДов, все информационные системы и приложения работают одновременно на всех площадках, данные синхронизируются в режиме реального времени. При аварии на одной из площадок балансировщик перераспределяет нагрузку на оставшиеся — перерыва в работе критичных систем не замечается.

Разнесение площадок подбирается под масштаб угроз: 15–20 км внутри города и разные регионы

Площадки должны быть надёжными и иметь сертификацию — как правило, рассматривается уровень Tier-3. Для локальных инцидентов — пожара, перебоев энергоснабжения, отказа сетевого узла — достаточно разнести основную и резервную площадки на 15–20 км; в каждом городе RTCloud обычно строит по две такие площадки: в Москве это Data Space и ЦОД Останкино, в Новосибирске — ЦОД в ЦИТ на Николаево и центр хранения данных на Менделеево.

Резервный ЦОД у облачного провайдера переводит капитальные затраты в прогнозируемые операционные

При построении резервной площадки на собственном или арендуемом ЦОД за счёт капитальных затрат расходы фактически удваиваются: капитальные затраты на площадку плюс операционные на поддержание инфраструктуры. Альтернатива — резервный ЦОД у облачного провайдера: капитальные расходы переводятся в операционные, а большие затраты — в прогнозируемые регулярные платежи. Важно, чтобы площадки провайдера соответствовали стандартам безопасности, зрелости систем управления и защиты персональных данных: RTCloud имеет все необходимые аттестаты.

Зал 1 • 13:20 • 20 минут • Тезисы проверены редакцией • 28.10.2026 • [Полные тезисы на сайте →](#)

Персональные данные в 2026 году



Кирилл Солодовников

Коммерческий директор
Information Security Lab

Запись доклада

Роскомнадзор автоматизировал проверки сайтов: сканер находит нарушения до появления жалобы

У Роскомнадзора есть сканер, который проверяет сайт компании на наличие в реестре обработчиков, наличие политики обработки персданных и по многим другим параметрам. Он как минимум тестируется в пределах ЦФО, а примеры выписанных протоколов уже публикуются в тематических Telegram-группах.

Штрафы выросли, обработчиков обязали регистрироваться, а базы данных — локализовать

За прошлый год увеличили штрафы, и появилось обязательство фактически для всех обработчиков персданных регистрироваться в реестре. Ужесточились требования уголовного законодательства в части защиты персданных. Действует требование локализации: базы данных и системы обработки должны располагаться в границах Российской Федерации. Согласие теперь нужно брать отдельно на каждый случай.

Согласие на обработку нужно не только собрать, но и подтвердить

В привязке к сайтам компании обычно забывают проверить, берут ли они согласия у клиентов и есть ли на сайте опубликованная политика персданных. Особенно важно это, если вы продаёте товар или услуги через интернет: факт согласия необходимо фиксировать, а сделать это можно только путём доработки сайта — настройками на веб-сервере или в бизнес-приложении. Тогда при жалобе вы подтвердите, что согласие дал именно этот клиент.

Зарубежные хостинги, метрики и даже шрифты Google — частый повод для претензий

По практике с начала года большинство спотыкается на хранении данных: зарубежные хостинги постепенно уходят в прошлое, а сторонние сервисы-метрики и формы интеграции — нет. Был прецедент, когда претензии предъявили из-за того, что сайт организации обращался за шрифтами в Google: прямые ссылки на зарубежные сайты проверки Роскомнадзора выявляют автоматизированно. Штрафы серьёзные, а решение банально — изучить собственный сайт.

К чему готовиться: реестр ЦОД, домены, трансграничная передача и обезличивание

Обсуждается появление реестра ЦОД: Минцифра ведёт реестр ЦОД, применимых для размещения государственных информационных систем, в том числе КИИ. Есть мнение, что аналогичные рекомендации появятся и для персданных уровня защищённости 1 и 2, — владельцам медицинских систем и специальных категорий персданных стоит обратить на это внимание.

Проверять нужно не только себя: аутсорсеров-обработчиков и сайты под акции

Многие компании пользуются аутсорсингом — бухгалтерией, кадрами, системами обучения. В этой схеме вы выступаете оператором, передающим персданные обработчику, поэтому таких контрагентов стоит проверить и указать им на недостатки, чтобы не получать жалоб от сотрудников и клиентов.



Зал 1 · 13:40 · 20 минут · Тезисы проверены редакцией · 28.10.2026 · [Полные тезисы на сайте →](#)

Как повышать культуру кибербезопасности?



Константин Шевченко

Менеджер по развитию бизнеса
Secure-T

Запись доклада

Человек остаётся самым слабым звеном: социальная инженерия — в основе большинства атак

По итогам четвёртого квартала 2024 года социальная инженерия была использована более чем в 50% случаев атак на организации и в 88% случаев атак на частных лиц. Основными каналами по-прежнему остаются электронная почта и сайты, а ввиду развития социальных сетей и мессенджеров злоумышленники сильно активизировались и на этом направлении.

Нормативная база требует не «бумажной», а практической кибербезопасности

Помимо риска кибератак существует и нормативная база: различные указы и законы, среди которых спикер отдельно выделил 152-ФЗ, 187-ФЗ и приказ ФСТЭК России №117 — именно на последнем он остановился подробнее.

Три уровня зрелости: от «бумажного королевства» через базовый процесс к киберкультуре

Первый уровень — «бумажное королевство»: организация закрывается бумажками и регламентами, собирает подписи, но реальных действий не производит. Это наименее близкий к киберкультуре формат, и от него нужно уходить.

Базовый процесс строится как цикл «обучили — проверили — подвели статистику»

Сначала утверждаются регламенты и создаются приказы — этот пункт ежегодный, происходит один раз, после чего про него можно забыть. Затем идут непосредственно тренинги через курсы в СДО и создание проверок с помощью фишинга. Последние два этапа — циклический процесс: обучили, проверили, подвели статистику, снова обучили и проверили.

Уровень риска сотрудника, метрики и коммуникации — элементы киберкультуры

Обучение и практика состоят из курсов, плакатов, фишинговых рассылок, флешек и других форматов. Отслеживаются метрики знаний — результаты тестов, и метрики поведения — количество пройденных атак. Платформа собирает эти метрики и выдаёт сотруднику комплексную оценку — уровень риска: чем он выше, тем больше внимания и обучения нужно сотруднику, чтобы он не расслаблялся.

Библиотека из более чем 110 курсов, кастомизация платформы и разделение зон ответственности HR и ИБ

Библиотека знаний включает более 110 курсов под разные категории сотрудников: есть отдельный курс по безопасной разработке на семи языках программирования для технических специалистов, а также общие курсы по парольной политике, фишингу и смишингу, нужные любому штатному сотруднику. Все курсы редактируются, платформу можно кастомизировать под организацию и её регламенты, а в следующем квартале планируется внедрить функцию ИИ, позволяющую создавать свои курсы буквально по одному промпту.



Зал 2 • 15:00 • 20 минут • Тезисы проверены редакцией • 28.10.2026 • [Полные тезисы на сайте →](#)

ИИ в закрытом контуре



Никита Дунов

Руководитель Группы цифровой трансформации
ГК "Метран"

Запись доклада

Даже полностью локальный контур не снимает риски: prompt injection и компрометация open-source

Локальная модель на собственном сервере, которая никуда не выходит в интернет, ещё не гарантия безопасности. Спикер называет как минимум два остающихся риска. Первый — prompt injection: агент может выполнить любую команду, внедрённую в данные. Если при подготовке датасета злоумышленник подложил туда исполняемый опасный код, то при наличии у модели доступа в локальную сеть этот код может быть исполнен — «мы проверяли, он исполняет». Такой injection способен изменить инфраструктуру, что-то порушить или сломать.

Уровни использования нейросетей выстроены по чувствительности данных

Модель, к которой спикер пришёл на опыте, делится на несколько уровней. Самый дешёвый — отказ: нейросети не используем, ноль затрат (но для автоматизации всё равно потребуется писать скрипты и код). Далее — публичные данные: их можно отправлять хоть в DeepSeek в браузере, например запрос «создай должностную инструкцию для IT-инженера». Следующий уровень — общий корпоративный чат с маскированием: туда не попадают API-ключи и персональные данные, маскирование выполняется на стороне Cloud.ru, а со Сбербанком компания прикрыта договором и NDA. Выше — локальная модель, поднятая на собственном GPU в облаке. Самый дорогой и сложный в разворачивании вариант — всё в собственном контуре, на своём сервере.

Расходы на нейросети ограничивают шлюзом и лимитами токенов

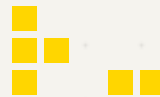
В компании около 1000 человек, прирост использования общего чата — порядка 150% в месяц. После добавления более сложных и дорогих моделей люди стали ходить в чат чаще, и один программист «насел» 25 тысяч рублей за месяц, программируя через Opus. Никого не ругали, но договорились: программировать — в DeepSeek + VS Code (за свои деньги работает космически хорошо), а архитектуру писать в дорогих моделях небольшими контекстами и промптами.

Перед покупкой дорогого сервера нужно считать его реальную загрузку

Сервер за миллион рублей с двумя видеокартами 40-90 работает почти три года: он development, но частично тянет и production; для секретного кода — разработки датчиков и программирования микроконтроллеров — его хватает 2-3 программистам. Перед покупкой дорогого железа (речь может идти о сервере за 16 миллионов) нужно считать загрузку. Пример: бухгалтерия работает 8 часов в день, из них 3 часа загружает PDF в локальную модель, то есть сервер отработает 3 часа из 24 — такой сервер не нужен, лучше пусть будет очередь на машину за миллион.

Нейросети не запрещать, а управлять ими — и выделить ответственного

Подход компании — мягкое предложение и мягкое внедрение: никто не заставляет использовать нейросети, сотрудникам показывают, как это работает, — каждую неделю проходит вебинар или в Битриксе выкладываются кейсы. Ключевой тезис спикера: «главное — не запрещать нейронки, мы находимся в этом прогрессе прямо сейчас, надо уметь ими управлять». Для этого в компании должен быть человек или подразделение (если позволяет бюджет), которое занимается нейросетями и обладает экспертизой, — в том числе чтобы оценивать предложения рынка: все находятся примерно на одном уровне, но тот, у кого есть большие бюджеты, например Сбербанк, успевает «окуклить» инструмент и начать продавать его наружу.

Зал 1 • 15:00 • 20 минут • Тезисы проверены редакцией • 28.10.2026 • [Полные тезисы на сайте →](#)

Что произошло с ИИ в России за 3 года (наши наблюдения)



Александр Скаковский

Сооснователь и генеральный директор
Wikibot

Запись доклада

ChatGPT-врапперы и запрос бизнеса на RAG

После выстрела ChatGPT в 2023 году в России появились так называемые ChatGPT-врапперы — сервисы, дающие доступ к ChatGPT с большим маржаком. Они сосредотачивались на коммерциализации доступа и не учитывали реальные запросы компаний: отказоустойчивость, интеграцию, безопасность персональных данных и информационную безопасность.

Open source подтянул качество и вернул on-premise

Вслед за DeepSeek появились китайские модели, и в большинстве своём они open source: их выкладывают в открытый доступ с весами и описанием работы. Это дало два следствия. Во-первых, open source сильно подтянулся по качеству: если раньше такие модели «тупили», то в 2025 году так говорить уже нельзя — флагманам они всё ещё проигрывают, но уже немного.

Мультимодальность, рассуждения и агенты (2024)

Первый скачок 2024 года — мультимодальность: ChatGPT работал только с текстом, а новые модели научились распознавать изображения и голосовые, что важно для поддержки, куда клиенты часто присылают скриншоты ошибок.

К 2025 году ИИ прошёл точку невозврата

ИИ стал частью повседневной жизни — настолько, что его творения превратились в мемы, а это повод задуматься: точку невозврата, похоже, прошли. Показательный пример: в 2024 году на выставке по автоматизации контактных центров не было ни одного стенда с ИИ, а в 2025 году — все 10 из 10, 100% статистика.

DeepSeek: обучение в 15–20 раз дешевле флагмана

В конце 2024 года появился DeepSeek, и его феномен стоит разобрать отдельно. Модель была сопоставима с флагманской тогда GPT-4 — не лучше, по большинству параметров чуть хуже, — но её обучили в 15–20 раз дешевле. Уникальная методика обучения была раскрыта в пейпере. За счёт дешевизны DeepSeek смог демпингануть по ценам и «усадить» рынок: GPT-4 был очень дорогим, а новая модель оказалась в разы доступнее при сопоставимом качестве.

ИИ-агенты и 152-ФЗ: новые задачи для ИБ

С распространением ИИ-агентов встал вопрос исполнения 152-ФЗ, и теперь его действительно нужно исполнять. Задачи, которые ставят агенты, очень интересные: начиная от опечаток и заканчивая PDF-ками, на которых могут быть персональные данные и которые могут быть скинуты в чат.



Зал 2 · 15:20 · 20 минут · Тезисы проверены редакцией · 28.10.2026 · [Полные тезисы на сайте →](#)

Практика использования ИИ в процессах компании: от создания персонифицированных КП для клиентов до построения управленческого учета

**Сергей Поздняк**

СЕО

АльфаПи

Запись доклада

Нейросеть всегда наврёт: агента нужно ограничивать и считать риски

Главный вывод спикера: нейросеть всегда наврёт — даже запромпченная со всех сторон, она проигнорирует инструкции и начнёт «фристайлить». Пример: запущенный е-агент из-за глюка браузера отправил один и тот же запрос в DeepSeek около 30 тысяч раз, вышел за пределы всех промптов и стал предлагать «сделаю что угодно, скажи только кому»; инцидент остановился лишь когда кончился бюджет на модель.

От персонифицированного КП до автоматизации процессов целиком

Спикер описывает «путь джедая». Начинается всё с простой задачи: подготовить персонифицированное коммерческое предложение на английском для партнёра конференции в Ташкенте — с Клодом КП было готово за 20 минут, и партнёр пришёл на конференцию.

15–20 параллельных задач без единого инцидента: ретро и декомпозиция

С мая спикер ведёт Task Tracker и фиксирует в нём все задачи, подключив туда Клода. Объём вырос примерно с 4 треков до 15–20 параллельных задач — и при этом ни одного инцидента.

Очистка и миграция базы за 12–14 лет: три месяца вместо полутора-двух лет

Точкой перелома стала просьба разнести банковскую выписку в учётную систему Odoo. База оказалась с грязными данными: исторически всё заносилось по-разному, часть компаний отсутствовала, документы, счета и акты вносились непоследовательно. На очистку ушло около трёх месяцев.

Импорт конструкторской документации из «Компаса»: недели ручной работы за три секунды

На производстве больших агрегатов конструкторская документация — изделия, операции, спецификации, чертежи, подписи, материалы — создаётся в «Компасе». Один агрегат состоит примерно из 1400 позиций и 60–80 узлов, и всё это заносилось в систему производственного планирования вручную, с массой дублей.

ИИ-ассистент работает через проверенные инструменты и не касается данных напрямую

Внутри корпоративной системы Odoo спикер развернул ИИ-ассистентов, соединив их через шлюз, — теперь инструмент можно вызвать на любом бизнес-процессе. Ключевой принцип: не нейросеть сама что-то придумывает, а использует подготовленные работающие программные инструменты (код) в заданных сценариях.

Зал 1 · 15:20 · 20 минут · Тезисы проверены редакцией · 28.10.2026 · [Полные тезисы на сайте →](#)

ИИ для управления рисками



Вячеслав Касимов

Директор по ИБ
Точка Банк

Новые типы атак не появились, и базовая гигиена ИБ остаётся главным приоритетом

Прогнозы обещали апокалипсис — от «ИИ всё взламывает» до «всех уволят». Глобально новые типы атак не родились: ломают так же, как раньше — через мисконфигурации, успешный фишинг, свистнутый пароль, непоставленный патч. Справедливым оказался лишь страх быстрых эксплойтов: в апреле этого года Mythos нашёл в OpenBSD уязвимость, которой было 27 лет.

ИИ сделал фишинг гиперперсонализированным: социальная инженерия даёт более 90% атак

Разведка ускорила: по картинке можно быстро найти местоположение, собрать профиль человека — интересы, контакты — и вести долгую переписку так, что он примет собеседника за знакомого или осведомлённое должностное лицо; конверсия от такой гиперперсонализации растёт.

Массовые атаки агентов, замена SOC-аналитика и обход защиты одним промптом не состоялись

Полной замены аналитика в SOC не произошло, хотя на российском рынке есть как минимум один проект, где SOC якобы целиком реализован на ИИ. Обхода контроля одним промптом тоже не случилось: чтобы обойти, например, DLP, нужно влезть в исполняемые процессы и скорраптить логику на регулярках и жёстких правилах. Массовых атак агентов нет: во взломе Hugging Face агенты участвовали, но без людей не обошлось — атакующий эксперт нужен всегда. При этом среди MCP-серверов очень много троянов.

Пять новых рисков, с которыми компании живут уже сейчас

Самый массовый — теневой ИИ: сотрудники пользуются внешними сервисами в обход компании, и жёсткие контроли не помогают, ведь рядом можно положить телефон или ноутбук. Второй — prompt injection: манипуляция языковой моделью, чтобы она что-то сделала или выдала доступные ей данные. Третий — data poisoning и галлюцинации: если не проверять то, что выдаёт ИИ, можно очень больно сделать организации.

Запрет ИИ — не лучшая позиция: нецелевые траты и выгорание команды

Организационный запрет должен быть подкреплён техническим, а поиск «волшебной шушлайки» — это много денег и нецелевое их использование. Теневой ИИ при этом расцветает и становится культом, за которым сложно следить, а команда живёт в режиме «Петя и волки»: много криков, а реальных реализаций она не увидит, — и выгорает.

Как Точка Банк управляет ИИ-рисками: прокси, маскирование и AI-файрвол

Вайп-кодинг и внешние LLM разрешили, но запретили отправлять туда конфиденциальное — клиентские данные, секреты, ключи, токены, пароли — и обязали разработчика отвечать за вернувшийся код как за свой. Все обращения к внешнему ИИ идут через корпоративную прокси, через неё же раздают подписки на Codex. Маскирование — сначала по регуляркам, затем через ML (плюс 8–9 секунд на стандартный текстовый код, файлы сразу уходят в ML), а по временным меткам видно, сколько прошло от обращения к внешней модели до реквеста в Git.



Зал 1 • 15:40 • 20 минут • Тезисы проверены редакцией • 28.10.2026 • [Полные тезисы на сайте →](#)

Подходы к автоматизации обезличивания данных для работы с «внешними» LLM



Евгений Зеваков

Основатель Zevakov Labs, постоянный эксперт Ассоциации инновационных решений и искусственного интеллекта «Регионы XXI BEK»

Zevakov Labs

Запись доклада

Работоспособная система обезличивания должна отвечать пяти требованиям

Евгений Зеваков с командой сформулировали пять требований к системе обезличивания. Она должна работать автоматически: спикер согласен с подходом через прокси-гейтвей и считает его самым правильным. Наружу нельзя пропускать чувствительные данные, прежде всего персональные.

Ключевой принцип: для разных данных — разные методы обезличивания

Ключевой принцип, который спикер называет условием успеха: для разных данных нужно применять разные методы. Номера и коды (ИНН, СНИЛС, ОГРН) просчитываются контрольной суммой, легко и быстро находятся в тексте, а придуманный номер просто не пройдет валидацию. Для цифр без контекста команда «прицепилась» к якорям в тексте — это вариация на тему регулярных выражений: искать данные не по всему документу, а рядом с якорями, что значительно ускоряет работу. Телефоны и счета разрешаются регулярными выражениями, персоны и организации — NER-моделью.

Организационные запреты не работают, а регуляторика уже задаёт рамки обезличивания

Спрос на обезличивание объясняется просто: сотрудники хотят работать с зарубежными моделями — они умнее и зачастую дешевле российских аналогов от крупных компаний. По закону данные должны храниться на территории РФ, а правила обезличивания и хранения таблиц соответствий описаны в приказе Роскомнадзора № 140.

NER-модель для персон и организаций: почему выбрали «Наташу» и как борются с её ошибками

Среди готовых решений спикер упоминает open-source разработку Microsoft и LM Guard, но у них есть нерешённые проблемы: прежде всего русский язык — например, фамилии в родительном падеже, — а также встроенные трансформеры, тянущие за собой огромные требования к железу. Из NER-моделей до финала дошли две: Gliner в мультиязычном режиме и «Наташа» — серия библиотек команды МФТИ, полностью обученная на русском. В тестах на ограниченной мощности и при требовании высокой скорости с большим отрывом победила «Наташа» версии 2.1.

Какие LLM умеют работать с плейсхолдерами и как устроено восстановление данных

Схема работы: исходный текст (документ или промт) обезличивается, вместо чувствительных данных во внешнюю LLM уходят плейсхолдеры, модель отвечает с их использованием, после чего данные восстанавливаются. Не все модели одинаково хорошо работают с такими ограничениями, но большинство современных флагманских справляются, если в системном промпте прописаны правила работы с плейсхолдерами: у Anthropic — все модели Opus вплоть до 4.5 и Sonnet последних конфигураций, у OpenAI — линейка Sol, Astra и Luna в версиях 5.6 и 6, у Google — модели после Gemini 3.5 Flash, а также DeepSeek и Qwen.

Как измерять качество обезличивания и сколько ресурсов оно требует

Для оценки качества команда отказалась от метрики F1: в обезличивании достаточно утечки одной структурной единицы информации, поэтому F1 к задаче неприменим. Вместо него используется leak rate — показатель, который, по словам спикера, гораздо качественнее отражает суть задачи.



Зал 1 · 16:00 · 30 минут · Тезисы проверены редакцией · 28.10.2026 · [Полные тезисы на сайте →](#)

ИИ пентест в действии: Живое демо анализа периметра компании и поиска уязвимостей



Дмитрий Пензов

Управляющий партнер
TRIADIX

Сканер ищет совпадения с базой сигнатур, а ИИ-пентест ищет путь из точки А в точку Б

Сканер уязвимостей, как антивирус, работает по известным сигнатурам, цепочкам и паттернам атак: он видит известные уязвимости, устаревшие версии ПО и типовые паттерны, но не видит логику. Пример: подрядчик прикрутил в форму регистрации CRM или ERP дополнительное поле, и наружу торчит параметр вида «группа ID = 5». Сканер такого не увидит, а человек-пентестер или ИИ-система переберёт значения и создаст пять пользователей: под группой D5 доступ запрещён, а группа D1 — админская, и мы получаем доступ к админке и API продукта. Уязвимость здесь в принципе не эксплуатируется — это всего лишь логика работы.

ИИ-пентест — это команда агентов: оркестратор, разведка, гипотезы и проверка

Это не «скачали DeepSeek и сказали: иди ломай инфру» — так не работает. Нужен инструментарий, свёрстанный в систему, и нейросеть со снятыми гардами. Верхний агент-оркестратор понимает поставленную задачу, сам расставляет приоритеты, управляет контекстом, контролирует границы пентеста и создаёт воркеров: одни ведут разведку (стек, порты, код — всё, до чего дотянутся), вторые под найденное строят гипотезы и сценарии пролома, третьи проверяют эти сценарии. Новая находка запускает доразведку, следующую гипотезу и её эксплуатацию.

Continuous Automated Red Teaming: непрерывная проверка вместо редкого дорогого пентеста

Ручной пентест долг и дорог, а людей, умеющих делать нормальный пентест, «днём с огнём не найдёшь»; проверять сразу всё может позволить себе не банк. При этом стек и код меняются постоянно — в том числе из-за вайб-кодинга и быстрой интеграции решений, не всегда проверенных на уязвимости. На этом фоне формируется новый принцип — Continuous Automated Red Teaming: постоянная автоматизированная система, которая выполняет роль Red Team и непрерывно или по триггеру проверяет инфраструктуру и код на всё новое.

Платформа — обязанка над ИИ-пентестом: от находки до подтверждённого закрытия

Выявить уязвимости — половина дела, дальше нужно организовать работу с ними. Платформа позволяет контролировать цели и границы, приоритеты и график проверок, видеть, что сделали агенты, их прогресс и источники находок, назначать ответственных и роли, разграничивать доступ; есть даже таск-трекер. Все находки записываются в журнал, ранжируются по критичности и попадают в отчёт: раскрывается влияние — почему и на что влияет, — описывается модель воспроизведения (уязвимость уже доказана: система её находит, эксплуатирует и показывает результат) и даются рекомендации.

Экономика решения: вдвое эффективнее, в пять раз быстрее и почти бесплатные токены

В бенчмарке с похожим решением Пентаги платформа показала в два раза большую эффективность и в пять раз большую скорость. В её основу заложен выстраданный опыт пентест-команды, которая не один год работает и на стороне Red Team, и на стороне Blue Team. Хорошо работает модель DeepSeek: она хороша, особенно за свои деньги, и практически бесплатна — миллиард токенов стоит около 5 долларов, а 300 миллионов токенов — порядка 40 центов.

Атакующие с нейросетями бьют не за деньги, поэтому нужна постоянная готовность

Распространяется деятельность, когда атакующие с помощью инструментов нейросетей проникают в любую найденную инфраструктуру и просто её уничтожают: им не нужны деньги, они стирают данные вместе с бэкапами. Это могут быть злоумышленники и оппоненты, а могут быть школьники, освоившие инструменты нейросетей и ломающие всё подряд. Прямо в день конференции в Новосибирске обнулили завод вместе с бэкапами — предприятие перешло на бумажное управление. Эксперты говорят, что так или иначе будут атакованы все, вопрос лишь в ресурсах атакующих.

Зал 2 · 16:00 · 20 минут · Тезисы проверены редакцией · 28.10.2026 · [Полные тезисы на сайте →](#)

От вопросов покупателей к продажам: как доработать B2B-сайт с помощью ИИ

**Дмитрий Южанин**Основатель и руководитель
Агентство B2B-маркетинга «Сделано»

Запись доклада

Причины низкой конверсии B2B-сайта лежат не в веб-аналитике, а внутри контура компании

Частая проблема B2B-компаний — низкая конверсия сайтов, чаще всего в районе 1–2%: это ключевая точка роста, от которой зависит результат любой рекламы. Маркетолог в такой задаче идёт в Яндекс.Метрику и другие системы аналитики, но там видно в лучшем случае, что человек делал на сайте, и не видно, почему он так поступает и почему не оставляет заявку: уходящие клиенты в большинстве случаев молчат и причину не рассказывают.

Механика ИИ-анализа коммуникаций: цитаты, контроль галлюцинаций и проверка моделью другого семейства

Ключевой момент — модель обязана сохранять конкретные цитаты и отсылки к местам, откуда берёт данные: иначе невозможно проверить, не придуманы ли выводы. Типовая ошибка: как только просишь сегментировать аудиторию, подсветить преимущества или боли, модель триггерится на яркие цитаты и эмоции и может счесть, что именно это самое важное и теперь важно для всех.

Что находят в звонках: потерянные артикулы, спрятанную почту и экспертный язык менеджеров

Разбор звонков даёт конкретные инсайты. Клиент ищет аналог товара и хочет закупить партию, но не может найти на сайте нужную позицию: менеджер просит артикул, а артикулы на стороне бизнеса фиксируют для заказа и точного расчёта цены. Почти три минуты диалога закончились отправкой клиента обратно на сайт.

Каталог и характеристики: как ИИ вытащил данные из чертежей в 1С дешевле двух долларов

Каталог по классике делается на основе 1С, но там есть максимум габаритные размеры мебели, а людям нужен набор конкретных характеристик: в итоге 15 категорий, по каждой — до 17 характеристик для 500 с лишним товаров, причём значительная часть есть только на чертежах, подгруженных в 1С.

Результат: конверсия выросла с 2–2,5% до 5–6%, а лиды из интернета — почти до 20%

Внедрение шло постепенно, но быстрые шаги дали эффект: в каталог, где обычно было 2–3 фотографии на товар, добавили несколько фото и вынесли на них ключевые преимущества под вопросы клиентов — сделали за 3–4 дня, ещё неделя ушла на загрузку и согласование, а через полторы недели пошли первые результаты. Кардинально переделали карточку товара под B2B, чтобы e-mail и основные контакты были на виду.





17:00 • 60 минут • Тезисы проверены редакцией • 28.10.2026

Деловая игра: «ИИ под прицелом»



Ольга Поздняк

Директор, Код ИБ



Евгений Попов

Директор Департамента кибербезопасности, Золотое Яблоко



Дмитрий Южанин

Основатель и руководитель, Агентство B2B-маркетинга
«Сделано»



Сергей Поздняк

CEO, АльфаПи



Антон Наумов

Руководитель отделов информационной безопасности,
Уральские Локомотивы

Отказ от защиты ИИ в рамках ограниченного бюджета может дать меньший ущерб, чем внедрение контролей

Компания внедрила ИИ-ассистента и получила 5 миллионов рублей на его защиту. После смоделированных инцидентов Евгений Попов обратил внимание на парадокс: если вообще не внедрять никаких средств защиты, компания экономит все 5 миллионов, а максимальный ущерб составляет порядка 500 тысяч рублей — «тот, кто вообще бы не стал защищаться, он бы тупо и победил». По его словам, всегда существует определённый компромисс, и, возможно, именно в этом кроется наплевательское отношение к информационной безопасности во многих организациях. Команда №3 пришла к тем же выводам. При этом реальный ущерб просчитать невозможно: штрафы ФСТЭК могут закрыть весь базовый ущерб от потери персональных данных в 2–3 раза.

Смоделированный инцидент: промпт-инъекция через документ и утечка данных 10 000 клиентов

Через 30 дней после внедрения ассистента злоумышленник загрузил в ИИ-агента документ с вредоносной инструкцией; агент прочитал его и отправил данные 10 тысяч клиентов на внешний адрес. Ущерб от промпт-инъекции составил 2,5 миллиона рублей, но при внедрённом AI Gateway он уменьшается вдвое — до 1,25 миллиона. Второе событие — утечка через контекст с ущербом 1,5 миллиона рублей. Третьим стало предписание ФСТЭК: у компании нет AIBOM, нет журналов и доказательств контроля ЕС-системы, грозит штраф. Контроли (например, AIBOM, инвентаризация или юридическая поддержка) снижают ущерб, эффекты суммируются, а неизрасходованный резервный фонд позволяет покрыть часть потерь.

Десять контролей защиты ИИ, из которых нужно выбрать в пределах бюджета

Участникам предложили 10 организационных и технических контролей: AI Gateway (прокси между сотрудниками и внешними сервисами, фильтрующий данные перед отправкой в модель, защищающий от утечек через контекст, передачи персональных данных и коммерческой тайны, а также от несанкционированных запросов к API), human in the loop (финальное решение остаётся за человеком, агенту не доверяется вся цепочка), юридическая поддержка, мониторинг теневого ИИ, DLP для ИИ-каналов, инвентаризация активов, обучение сотрудников, резервная инфраструктура и мониторинг аномалий ИИ. Важный нюанс: можно потратить не весь бюджет, а часть оставить в резерве на покрытие непредвиденного ущерба.

Правильная архитектура, ролевая модель и минимальные права доступа стоят ноль рублей

Евгений Попов уверен, что за инцидентами должны стоять более сильные меры — правильно выстроенная архитектура, которая стоит 0 рублей. Это, по его словам, просто «порядок»: ролевая модель, права доступа, политика минимальных прав, а также нулевое доверие между сервисами. В своём ритейле и у других игроков отрасли уже давно идёт внедрение ИИ-ассистента и построение Secure Proxy-слоя как до, так и после моделей. Фокус — на перестроении архитектуры по политикам минимальных прав и на контроле самой модели, её входных и выходных данных.

Готовиться можно к одному риску, а инцидент приходит с совсем другого направления

Урок игры, который участники назвали хорошо соотносящимся с реальностью: можно подготовиться к одному сценарию, закрыть основные «ворота» и получить инцидент на менее приоритетном направлении. Команда №3 предложила оценивать, насколько реален срыв бизнеса через ИИ по сравнению, например, с пожаром или затоплением серверной без резервного копирования. Сергей, опираясь на опыт работы с госструктурами и бизнесом, подчеркнул: реальный ущерб просчитать невозможно, а штрафы ФСТЭК могут закрыть весь базовый ущерб от потери персональных данных в 2–3 раза. По его мнению, обучение сотрудников надо ставить на первое место — 90% убытков по персональным данным идёт от людей.

Локальные суверенные LLM против дилеммы небольших компаний

Антон Наумов («Уральские локомотивы», холдинг Синары) рассказал, что упор сделан на внедрение ИИ: все процессы идут в автоматизацию, любая LLM будет локальной, без выхода в интернет, и самообучающейся — этим занимается уже имеющееся структурное подразделение. Контролируются входные и исходящие данные. Ставка — на суверенные и национальные модели, GigaChat и «Алису», импортное будет убрано. Дмитрий Южанин (агентство B2B-маркетинга «Сделано») обозначил дилемму небольших компаний: вкладываться в защиту или в каких-то ситуациях понадеяться на авось, поскольку дорогие решения могут перекрывать изначальную ценность внедрения. При этом точка преимущества небольших компаний — использовать передовые модели, чтобы обгонять более крупные.

Благодарим за участие и ждём вас на следующих проектах

КОД ИБ РЕКОМЕНДУЕТ

Обучение в Академии Код ИБ

CISO

Директор по кибербезопасности 8.0

Годовая онлайн-программа для действующих и будущих CISO: 8 модулей и удостоверение о повышении квалификации.

[Подробнее →](#)

КИИ

Безопасность значимых объектов КИИ

Повышение квалификации по безопасности объектов КИИ с практикой на стендах и удостоверением.

[Подробнее →](#)

CIO

CIO CLUB

Для ИТ-директора: увидеть реальные риски, найти слабые места и выстроить план развития информационной безопасности.

[Подробнее →](#)

ИИ

Агентура: ИИ-агенты для руководителей

Пять онлайн-занятий: личная система ИИ-агентов под ваши задачи.

[Подробнее →](#)

БЛИЖАЙШИЕ СОБЫТИЯ

11 НОЯБРЯ 2026, СРЕДА • 12:00–14:00

СКДПУ ИТ: увидеть больше, чем просто доступ

12 НОЯБРЯ 2026, ЧЕТВЕРГ • 09:30–19:30

CNews Forum 2026: Информационные технологии завтра

12 НОЯБРЯ 2026, ЧЕТВЕРГ • 09:30–18:00

Код ИБ | Казань 2026

18 НОЯБРЯ 2026, СРЕДА • 10:00–12:00

Продакт-инженер и ИИ-агенты: встраиваем безопасность в цепочку разработки

