МАТЕРИАЛЫ КОНФЕРЕНЦИИ · 24 СЕНТЯБРЯ 2026, ЧЕТВЕРГ · 09:30–18:00

Код ИБ Новосибирск 2026: тезисы, записи и презентации

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

«Код ИБ» в Новосибирске прошёл 24–26 сентября на площадке Grand Autograph. Деловую часть 24 сентября открыли Ольга Поздняк и Дмитрий Домшинский. На сессиях говорили о цифровизации, искусственном интеллекте и связанных с ним рисках, о регулировании и защите персональных данных, о культуре кибербезопасности и безопасных настройках инфраструктуры. Отдельная секция была посвящена внедрению ИИ в бизнес-процессы. Затем состоялась деловая игра «ИИ под прицелом», а завершились день розыгрышем призов и неформальным ужином в ресторане «Коза и Лоза».

25 сентября прошла деловая игра со студентами НГТУ НЭТИ «Призрак Кода» и экскурсия в офис 2ГИС. 26 сентября — лекция «Как быть в ресурсе?» и забег «Кросс нации».

13
ВЫСТУПЛЕНИЙ

12
ЗАПИСЕЙ

1
ПРЕЗЕНТАЦИЯ

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Записи докладов
https://vkvideo.ru/playlist/-73689515_50

Фотографии
https://vk.ru/album-73689515_312143352

Страница отчёта на сайте
https://codeib.ru/event/kod-ib-novosibirsk-2026-1015/page/otchet-kod-ib-novosibirsk-2026-1015

Содержание

01 **Голос отрасли: Цифровизация, Кибербезопасность, Искусственный Интеллект**
Руслан Пермяков, Дмитрий Бойко, Руслан Копцев, Полина Сазонова, Руслан Поляков

02 **Диалог с регулятором**
Звягинцева Полина

03 **Как повышать культуру кибербезопасности?**
Руслан Бугаев

04 **Персональные данные в 2026 году**
Евгений Гергель

05 **TS Hard - комплексный хардининг от TS Solution**
Дмитрий Сигаев

06 **Управление безопасностью конфигураций ИТ-ресурсов**
Кирилл Евтушенко

07 **Комплекс ИБ САКУРА для построения ZTNA**
Александр Несов

08 **Как приручить ИИ-агента: с чего начать внедрение ИИ в бизнес**
Полина Сазонова

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

10 **Как мы создали ИИ-фабрику по созданию персонифицированных КП**
Ольга Поздняк

11 **Использование систем на базе ИИ для повышения продуктивности групповой работы экспертов на примере форсайта проводимого в рамках форума АСИ "Архипелаг**
Руслан Пермяков

12 **Использование ИИ при создании аннотаций судебных решений**
Евгений Бессонов

13 **Деловая игра: «ИИ под прицелом»**
Дмитрий Бойко, Руслан Поляков, Ольга Поздняк, Сергей Поздняк, Руслан Пермяков, Полина Сазонова

10:30 · 40 минут · Тезисы проверены редакцией · 07.10.2026

Голос отрасли: Цифровизация, Кибербезопасность, Искусственный Интеллект

Руслан Пермяков
Советник директора ИВМиМГ СО РАН, Заместитель директора ЦК НТИ ТДВ

Руслан Копцев
Руководитель Центра компетенций по цифровым технологиям и технологическому предпринимательству...

Руслан Поляков
CIO, Greenway Global

Дмитрий Бойко
Директор департамента безопасности, ГК Lime Credit Group

Полина Сазонова
И.о. руководителя Комитета по информационным технологиям Новосибирского областного отделения «ОПОР...

Запись доклада

Искусственный интеллект стал рабочим инструментом, но ускоряет только подготовленный бизнес

На панели сошлись, что ИИ уже встроен в бизнес-процессы. Руслан Поляков (Greenway Global) рассказал, что компания перестроила разработку: агенты помогают архитекторам, выполняют часть задач джунов, ускоряя работу на 30–40%, а на отдельных задачах до 70%. При этом ключевые решения остаются за командой. Дмитрий Бойко (ГК Lime Credit Group) видит плюс в обработке больших данных и прогнозах. Руслан Пермяков использует ИИ для транскрибации встреч и исследований через агентов. Полина Сазонова предупредила: ИИ должен ложиться на готовую инфраструктуру, данные, ERP и компетенции, иначе он добавит сумбур и ошибки вместо ускорения.

Теневое использование ИИ и утечки данных — новый контур риска для службы ИБ

Участники отдельно обсудили Shadow AI. Руслан Поляков сформулировал критерий готовности бизнеса: нужно понимать, где используется ИИ, какие данные куда уходят и кто отвечает за процесс. На практике сотрудники применяют внешние сервисы — ChatGPT, GigaChat, Claude и другие — вплоть до загрузки годовых отчётов и чувствительных данных. Дмитрий Бойко отметил: запрос на мониторинг взаимодействия с генеративными моделями есть, но готового решения вендоры пока не предложили; компании используют классический контроль рабочих станций, сетевого трафика и DLP. Руслан Копцев добавил, что базовый контроль утечек персданных есть, но контроль ИИ — длительная работа.

Стратегические и персональные данные нельзя отдавать в открытые модели без оценки риска

Руслан Поляков привёл кейс: информация об учебном проекте дрон-доставщика через 60 часов попала в украинские каналы, что показало скорость публичной утечки. Он подчеркнул: стратегические данные нельзя вываливать в нейросети, их нужно считать на защищённой инфраструктуре, а персональные данные требуют соответствия 152-ФЗ. Для безопасного использования ИИ он обозначил три варианта: локальное развёртывание, нейросеть в дата-центре с подписанным NDA или open-source-ресурсы. Задача IT и ИБ — определить, какие данные можно отдавать, а какие нельзя.

Скорость атак и уязвимостей растёт, а сертификация и резервирование отстают

Руслан Пермяков отметил, что скорость производства атак выросла в разы: при новых уязвимостях счёт идёт на дни, выпуск Zero Day — на минуты, а сертификация длится месяцами. Дмитрий Бойко напомнил про атаки на дата-центры и давление на инфраструктуру: такие сценарии нужно закладывать в модель угроз. Если у компании два независимых дата-центра, важно понимать, как быстро собраться, переехать и развернуть сервисы на новой площадке. Он привёл пример резервных каналов: формально они были, но из-за низкой пропускной способности выкачивание резервных копий заняло две недели.

Экономику ИИ нужно считать через прибыль и ускорение, а не только через экономию на людях

Руслан Пермяков рассказал, что разработка технологической документации и дрона-доставщика с нуля заняла 4 дня, 24 человеко-часа и около 600 тыс. рублей на токенах; уровень технологической готовности достиг 5–6. Аналогичный проект занял бы два месяца и соответствующий фонд оплаты труда. По его мнению, компаниям важно оценивать ИИ не через экономию, а через полученную прибыль и новые продукты; цель ускорения принятия бизнес-решений в 20 раз задаёт смысл, даже если не будет достигнута. Полина Сазонова добавила: иногда дешевле посадить джуна, чем использовать ИИ, а стоимость инфраструктуры растёт вместе с задачами.

Безопасное использование ИИ требует новых компетенций и обучения людей

Участники согласились, что ИИ не отменяет обучение. Руслан Копцев говорил, что рынку нужны люди, умеющие правильно формулировать задачи, задавать контекст и граничные условия, управлять качеством решения и превращать рассуждения в результат. Студентам нужно давать практические кейсы, чтобы к выпуску был опыт работы с моделями. Руслан Поляков призвал инвестировать в молодёжь сейчас, иначе через 5–10 лет возникнет кадровая яма. Полина Сазонова предупредила о риске завышенных ожиданий: ИИ — не волшебная кнопка, его нужно пробовать и отвечать за результат.

11:10 · 30 минут · Тезисы проверены редакцией · 08.10.2026 · Полные тезисы на сайте →

Диалог с регулятором

Звягинцева Полина
Начальник отдела
Управление ФСТЭК России по СФО

Запись доклада

Защита информации по 117 приказу — это непрерывный циклический процесс, а не разовое мероприятие

Звягинцева Полина подчеркнула, что по 117 приказу организация деятельности по защите информации должна представлять собой циклический процесс. Начинается он с разработки плана, в котором обозначены мероприятия, сроки и ответственные лица; план должен быть на бумаге — при проверке его предъявляют. Далее реализуются организационные и технические методы, после чего проводится оценка состояния защиты информации путем расчета показателей защищенности КЗИ и уровня зрелости.

Расчет показателя зрелости распространен и на подрядные организации

В августе 2026 года вышел долгожданный методический документ и изменения в 117 приказ, установившие требования по расчету показателя зрелости — в том числе для подрядных организаций, имеющих доступ к информационной инфраструктуре оператора-владельца.

Утвержден документ состава и содержания мер — «азбука» по защите информации

12 апреля 2026 года директор ФСТЭК утвердил документ состава, содержания мероприятий и мер по защите информации. Спикер называет его «азбукой по защите информации от несанкционированного доступа». Объемом более 180 страниц, он содержит подробное описание реализации мероприятий и мер; изучив его, можно квалифицированно разобраться в теме.

Аттестация остается обязательной только для ГИС, для остальных — контроль уровня защищенности

Вышли изменения в 77 приказ. Аттестация остается обязательной только для государственных информационных систем. Владелец ГИС вправе выставлять требования по аттестации к подключаемым к нему иным информационным системам.

Непредставление сведений о показателе защищенности влечет административную ответственность

Непредставление сведений о показателе защищенности, а также непроведение мероприятия и ненаправление сведений влекут ответственность по статье 13.12.1: штраф для должностных лиц — 10 тысяч рублей, для юридических лиц — от 50 до 100 тысяч.

Готовятся изменения 79 постановления, а также приказов 235 и 239

Готовятся изменения в 79 постановление о лицензировании технической защиты конфиденциальной информации: сейчас лицензиату достаточно заявить трех человек (руководитель и два инженерно-технических работника), а в проекте по каждому направлению услуг прописывается свое количество — от 9 до 15 человек.

12:00 · 20 минут · Тезисы проверены редакцией · 07.10.2026 · Полные тезисы на сайте →

Как повышать культуру кибербезопасности?

Руслан Бугаев
Руководитель отдела развития бизнеса
Secure-T

Запись доклада

Социальная инженерия — по-прежнему главный вектор атак, и защищённый периметр от неё не спасает

По статистике (по итогам 4 квартала 2024 года) 50% атак на организации в целом приходится на социальную инженерию, а 88% атак на частные лица также связаны с социальной инженерией. Докладчик подчёркивает: эти цифры «плюс-минус соединены» и повторяются из года в год, как бы мы ни старались.

Зрелость киберкультуры в организации делится на три типа — от «бумажного королевства» до настоящей киберкультуры

Первый уровень — «бумажное королевство»: всех подписали, всех обучили, все молодцы — и больше в эту сторону не смотрим. Второй — базовый процесс повышения уровня осведомлённости: базово обучаем, что-то проверяем, какая-то движуха в организации есть, но не более.

Базовый процесс осведомлённости строится от «печки» — приказов, регламентов и программы обучения, а измеряется метриками и проверкой фишингом

Отправная точка — приказы, регламенты и программа обучения: мы от чего-то отталкиваемся, что-то собрали и от этого двигаемся дальше. Форматы обучения — «на вкус и цвет»: кому-то тренинги, кому-то курсы в системе дистанционного обучения, кому-то плакаты и регламенты.

Платформа Secure-T закрывает базовый процесс силами одного-двух человек — вплоть до компании на 12 тысяч сотрудников

Обучающая платформа Secure-T собирает в одном месте фишинговый модуль, обучающий модуль и статистику: обучаем, проверяем, собираем статистику — удобный инструмент, позволяющий выстроить как минимум базовый процесс.

Для зрелых организаций киберкультура строится по трём трекам с отдельным циклом мероприятий и обязательной обратной связью

Сотрудников делят на три трека: технические специалисты, топ-менеджеры и безопасники. Для каждого трека — свой путь обучения, дальше начинаются более узконаправленные тренинги: один раз собрать и быстро обучить проще, чем каждый раз садиться заново.

Коммуникацию с сотрудниками строят вместе с HR, а зоны ответственности ИБ и HR нужно чётко разделять

Стратегия коммуникации — это мост между рядовыми сотрудниками и специалистами, отвечающими за безопасность, и строится он с помощью HR-департамента: очные встречи, программы мотивации, опросы, вебинары, рассылки. Метрики — удовлетворённости, осведомлённости, вовлечённости и успешности информационных материалов. Ориентир — на рядовых пользователей: фокус-группа, например, женщины 50+ из бухгалтерии, поэтому безопасникам курсы и кажутся простыми.

12:20 · 20 минут · Тезисы проверены редакцией · 07.10.2026 · Полные тезисы на сайте →

Персональные данные в 2026 году

Евгений Гергель
Менеджер по продажам
Information Security Lab

Запись доклада

Штрафы за нарушения в обработке персональных данных выросли до миллионов рублей, а за повторную утечку применяется оборотный штраф

Регулирование прошло путь от введения в 2024 году уголовной ответственности за незаконное использование и передачу персональных данных до шкалы штрафов, локализации баз данных и выделения согласия на обработку в отдельный блок в 2025 году. По ряду составов уже идут производства и есть прецеденты.

Согласие на обработку данных — теперь отдельный документ, а на сайте нужен чекбокс без предустановленной галочки

Раньше согласие можно было вписать в общие положения сайта, и было непонятно, есть оно или нет. Теперь оно выделено в отдельный документ: если согласие вшито в договор и переходной формы нет, его нужно переоформить отдельно — бумажный вариант в составе договора не работает.

Локализация баз данных: зарубежный хостинг и зарубежные трекеры — типичные нарушения

Запись, систематизация, накопление, хранение, уточнение и извлечение персональных данных не должны происходить за пределами российских серверов. Типичное нарушение — зарубежный хостинг или зарубежный сервер, куда данные уходят, там анализируются и считаются, но без соответствующего уведомления о трансграничной передаче данных. Сюда же попадают аналитические инструменты вроде Google Analytics и Meta Pixel: их использование без необходимых уведомлений Роскомнадзору также считается нарушением. Решение — локализовать сбор и все операции, предусмотренные требованием локализации, и оформить трансграничную передачу данных.

В 2026 году добавились реестр ЦОД, идентификация владельцев доменов и более жёсткие правила трансграничной передачи

Появился реестр центров обработки данных и требования к ним, причём требования стали довольно жёсткими и проверяются регуляторами. Больше нельзя найти нишевый дата-центр, где просто стоят серверы, и считать, что требования по локализации выполнены, — выбор площадки должен быть осознанным.

Крупные компании могут обязать обезличивать персональные данные по требованию Минцифры

Если компания обрабатывает большое количество персональных данных — под такую санкцию, например, попали банки, — Минцифра может обязать её обезличивать эти данные. Процесс довольно затратный: есть несколько путей обезличивания, статическое и динамическое, и каждый требует значительных ресурсов. Если есть понимание, что такое требование в принципе может грозить, думать об этом стоит заранее: и выбор решения, и само внедрение требуют большого объёма ресурсов и финансов.

Проверки регулятора начинаются с коврового сканирования сайтов, а ошибки у компаний типовые

Основной паттерн проверки — базовое ковровое сканирование российского сегмента на наличие на сайтах всех необходимых политик и файлов. Когда появляются данные о нарушениях, они переходят к профильному инспектору, который в ручном режиме всё перепроверяет и формирует предписание, дальше идут штрафные санкции. Проблемы у всех типовые, особенно когда сайтом занимаются подрядчики: шаблонная политика, предустановленные галочки, одна галочка на все цели вместо отдельной под каждый процесс, проблемные куки-баннеры, зарубежные трекеры и хостинги.

12:40 · 20 минут · Тезисы проверены редакцией · 07.10.2026 · Полные тезисы на сайте →

TS Hard - комплексный хардининг от TS Solution

Дмитрий Сигаев
Региональный менеджер продаж
TS Solution

Запись доклада

Информационная безопасность — не результат, а постоянный процесс: начинать надо с аудита, а не с закупки новых СЗИ

ИБ — это не проект с финальной точкой, а постоянный процесс с вливанием огромного количества денег. Злоумышленники постоянно адаптируются к средствам защиты, которые выпускают российские производители: атаки становятся более хитрыми, изощрёнными, глубокими и мощными. Сколько бы СЗИ ни было развёрнуто, всегда найдётся уязвимость, которую пропустили — из-за нехватки экспертизы, компетенций или потому, что «глаз замылился».

Харденинг TS Solution — комплекс услуг, который закрывает дыры в инфраструктуре «минимальной кровью»

Харденинг — это набор услуг и сервисов, позволяющих полностью закрыть дыры в инфраструктуре минимальной кровью: полностью избежать потерь нельзя, потому что злоумышленники не спят и постоянно изобретают новые способы ломать сервисы, торчащие наружу, и корпоративную почту.

Бесплатный аудит NetAudit длится 30 календарных дней и всегда что-то находит

NetAudit — лёгкое решение, которое разворачивается в инфраструктуре заказчика: само приложение компактное, анализ трафика не такой глобальный, но всё равно позволяет находить много интересного. Услуга бесплатная и длится порядка 30 календарных дней. Каждый раз, когда проводится NetAudit, находятся хвосты, дыры, уязвимости и сервисы, торчащие наружу.

TSECO — deception-платформа, которая ловит хакера, уже проникшего в инфраструктуру

TSECO — новинка TS Solution. Это deception-платформа, которая расставляет внутри инфраструктуры ловушки, приманки и «файлы-канарейки». Её задача — найти злоумышленника, который уже проник в инфраструктуру и может находиться там месяцами, ничего не делая; как только он начнёт активность, «эхо» его поймает, потому что его софт реагирует на сигнатуры, и сотрудники ИБ это мгновенно видят. Любой контакт с ложной целью — стопроцентный индикатор атаки.

С уже внедрёнными СЗИ можно работать: донастройка, рекомендации и статус Check Point в России

Если на предприятии уже стоят продукты Positive Technologies, TS Solution готов их посмотреть, помочь донастроить, порекомендовать, где что подкрутить или заменить, какие галочки поставить и какие политики расставить. Схема рабочая: «трезвый взгляд» со стороны помогает найти то, что пропустили из-за замыленного глаза.

13:00 · 20 минут · Тезисы проверены редакцией · 07.10.2026 · Полные тезисы на сайте →

Управление безопасностью конфигураций ИТ-ресурсов

Кирилл Евтушенко
Генеральный директор
Кауч

Запись доклада

Небезопасная настройка — это такая же уязвимость, только «тихий убийца»

Когда об уязвимостях говорят без уточнений, почти всегда имеются в виду вендорские: отсутствие патчей и ошибки разработчика, которые находит классический сетевой сканер и закрывает установкой патча. Небезопасная настройка — по сути такая же уязвимость, но вокруг неё меньше хайпа: нет ежедневных новостей и нет баз CVE и БДУ с идентификаторами, которые привлекали бы внимание.

Безопасных настроек требуют регуляторы, а бизнес-кейс создают атаки

Драйверов два. Первый — регуляторы: исторически самый активный из них — Банк России, который около 20 лет заставляет банки заниматься настройками, а теперь подгребает и страховые, и другие организации. Другой стек пока не очень активничал, но в этом году вышло уже шесть документов, регулирующих безопасную настройку, — регулятор явно нацелился и в эту сторону.

Настройки измеряются миллионами, и «волшебного патча» для них не существует

По международным практикам безопасного построения систем: Windows-сервер — около 550 настроек, влияющих на безопасность, Linux-дистрибутивы — 300–350, базы данных — 200–300. Суммарно на одном сервере набирается порядка 1000 настроек. Даже если взять только высокорисковые — 200–300 на хост, — для тысяч хостов это 300 тысяч настроек, а для крупных инфраструктур — миллионы.

Классический вулн-менеджмент упирается в узкое горлышко на каждом шаге

Типовой процесс универсален и для уязвимостей, и для настроек, и для комплаенса. В основе — сканер уязвимостей (в ведении подразделения ИБ или выделенной компании). При большой инфраструктуре отчётов получается очень много, и их нужно посмотреть, оценить, приоритизировать и разложить по группам — в IT этим занимаются разные администраторы: серверный сегмент, пользовательский, тестовый, разработка.

Готовые скрипты и сканер конфигов вместо «сырых» отчётов

Популярные сканеры (мировой референс — Nessus, российский — C-Max Quattro) изначально создавались под сетевое сканирование вендорских уязвимостей, а блок настроек добавился позже, поэтому анализ конфигов там ограничен матчами — «матч/не матч» для того, что взяли с хоста. Здесь написали движок, работающий именно с конфигами: сняли это ограничение и ускорили сканирование — один хост с любым количеством прикладного ПО проверяется примерно за 30 секунд.

13:20 · 20 минут · Тезисы проверены редакцией · 09.10.2026 · Полные тезисы на сайте →

Комплекс ИБ САКУРА для построения ZTNA

Александр Несов
Менеджер по работе с клиентами
ИТ-Экспертиза

Запись доклада | Презентация

САКУРА — российская платформа для анализа защищенности рабочих мест и активного реагирования: Zero Trust не на словах, а на деле

САКУРА — российский программный комплекс информационной безопасности, внесенный в реестр российского ПО. Продукт вырос из исторического ядра удаленной работы, но контролирует защищенность рабочих мест независимо от их расположения — и удаленных, и офисных. Это не коробочное решение, а гибкое конструирование политик безопасности: каждой группе устройств назначается профиль рабочего места — набор правил контроля и сценариев реагирования.

Проверка по принципу «светофора»: агент собирает, сервер выносит вердикт, шлюз выполняет

Архитектура — классическая клиент-серверная. Цепочка выглядит так: агент собирает параметры, сервер проверяет их по профилю и выносит вердикт по принципу светофора, а решение выполняет шлюз. Зеленый — проверка пройдена, рабочее место получает полный доступ; красный — проверка не пройдена, доступ не предоставляется, установленная сессия сбрасывается на шлюзе; желтый — некритичное нарушение, рабочее место получает ограниченный доступ к части ресурсов, пользователь и офицер безопасности получают уведомление с рекомендацией, как устранить.

С 2017 года: от проекта для Ростеха до 200 000 рабочих мест под контролем

Первый релиз состоялся в 2017 году, а продукт вырос из проекта для госкорпорации «Ростех»: холдинг развернул центральный сервер, дочерние организации — агентов (30 000 рабочих мест). Удаленка 2020 года ускорила тиражирование: сегодня САКУРА работает в ДИТ Москвы (более 45 000 рабочих мест), в государствообразующем банке (более 100 000 рабочих мест, совместное решение удаленного доступа с «Амиконом»), в банках и на промышленных предприятиях. Масштаб подтвержден нагрузочным тестированием: 105 000 рабочих мест, пиковая загрузка сервера — 15% CPU.

15:00 · 20 минут · Тезисы проверены редакцией · 09.10.2026 · Полные тезисы на сайте →

Как приручить ИИ-агента: с чего начать внедрение ИИ в бизнес

Полина Сазонова

И.о. руководителя Комитета по информационным технологиям Новосибирского областного отделения «ОПОРЫ РОССИИ», аналитик центра ИИ НГУ, член Общественного совета при Минцифры НСО

Запись доклада

ИИ-агент — это цифровой сотрудник, а не волшебная кнопка, и управлять им нужно через классический менеджмент

Полина Сазонова предлагает смотреть на ИИ-агента как на цифрового сотрудника. Он очень быстрый, дерзкий, активный и энергичный: может за короткое время наделать дел, которые людям придётся долго разгребать. Поэтому задачи ему нужно делегировать максимально чётко: формулировать цель («твоя цель — сделать такой-то результат»), передавать знания, которые разрешено использовать, выдавать доступ в инструменты и определять полномочия.

Сначала процесс, потом агент: автоматизация хаоса приводит к цифровому хаосу

Прежде чем внедрять ИИ-агента, нужно понять, какой процесс будет автоматизироваться, и чётко его описать. Полина Сазонова подчёркивает: если операция повторяется и имеет понятный результат, агента применять можно. Но многие компании слышат, что ИИ моден, и пробуют внедрять агента, не описав процесс, не разложив его на шаги и не определив KPI. Это ошибка номер один.

Ошибка агента масштабна, поэтому доступы, инструменты и автономность нужно ограничивать

Опасность в том, что агент часто воспринимается как волшебная кнопка от всего. Если человек ошибается, он ошибается один раз; если ошибается агент, ошибка становится масштабной. Полина Сазонова приводит пример: агент запустили, чтобы помочь настроить инфраструктуру, он нашёл в базе пароли от прода, вышел на прод, завалил сервер и вернулся с отчётом. На вопрос «зачем завалил прод?» он ответил: «не подумал».

Внедрение агента должно быть поступательным: от наблюдения и рекомендаций к масштабированию

Полина Сазонова описывает порядок внедрения: сначала описываем процесс, считаем экономику агента, запускаем его в режиме наблюдения и рекомендаций — «тебе нельзя действовать, наблюдай». Затем ограничиваем полномочия и наблюдаем. Если агент подтвердил свои возможности, выдаём полномочия и масштабируем. Это похоже на внедрение нового человека в отдел.

Безопасность данных и моделей: сотрудники могут обходить корпоративные ограничения

В кулуарах практически каждая компания может сказать, что уже в опасности, потому что неизвестно, какие модели используют сотрудники и как они с ними взаимодействуют. Даже если в компании есть система контроля трафика, ничто не мешает сотруднику переслать файл на личную почту и поработать с ним с помощью ИИ. Регулятор выпускает документы, которые запрещают обрабатывать ПДН и отдавать данные на серверы за пределами, но появляются инструменты обфускации и деанонимизации.

15:20 · 20 минут · Тезисы проверены редакцией · 09.10.2026 · Полные тезисы на сайте →

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

Сергей Поздняк
CEO
АльфаПи

Запись доклада

Текстовые правила для ИИ-агента не работают: ограничения нужно вшивать в код и инструменты

Сергей Поздняк прямо говорит: промпты и текстовые правила — вчерашний день. Агент может не выполнить правило, забыть его, обойти запрет или соврать, что документ исправлен, хотя он не менялся. MD-файлы с правилами он читает не полностью: может прочитать в начале, в конце, а может не прочитать вообще. Поэтому в продакшене опираться только на промпты опасно — агент уходит в сторону и действует непредсказуемо.

Боевому ИИ-агенту нужна файловая память, серверный таск-трекер и Вики с семантическим поиском

В системе Сергея Поздняка память разделена на слои. На ноутбуке — файловая память, где агент читает контекст проекта. На сервере — таск-трекер: вся деятельность раскладывается на проекты, задачи, подзадачи и вехи с ответственными, зависимостями, ТЗ, принятыми решениями и результатом. Агент, попадая в проектное пространство, сразу понимает, где он находится и что делает.

Управленческий учет можно построить с помощью ИИ-агента, но придется перелопатить всю систему учета

В компании АльфаПи управленческий учет сделали для Ольги Поздняк. Началось с просьбы помочь разместить банковскую выписку. Оказалось, что выписка привязана к контрагентам, контрагенты — к документам, а база заведена непонятно как, многое было заведено неправильно. Пришлось перелопатить и восстановить всю систему учета.

ИИ не заменяет автоматизацию: импорт 1600 позиций из Компаса сделали без ИИ, а ИИ применяют для проектирования производственного процесса

На производстве есть программа Компас, где хранятся чертежи и спецификации изделия, а также дерево продукта. Эти данные нужно перенести в систему производственного планирования и снабжения. Одно изделие содержит 1600 позиций, и три человека тратили на его заведение две недели. Сергей выяснил, что проприетарный формат Компаса можно разобрать: они раскрыли бинарник, извлекли чертежи и дерево продуктов и запихнули в систему производственного планирования.

Если агент имеет доступ к неверифицированным данным и права записи или удаления, он может нанести ущерб

Сергей Поздняк отдельно останавливается на безопасности использования ИИ-агента. Если пустить агента к данным и дать ему права чтения, записи и удаления, он может сделать с ними все что угодно. Нужно ограждать себя: один агент, например, деплоит и делает запись в папку на сервере, дальше штатная автоматизация подхватывает, третий агент заходит, смотрит, что получилось, и включает механизм. Это классический подход к безопасности использования ИИ-агента. Через MCP можно дать агенту сразу доступ к боевой инфраструктуре, поэтому во все инструменты надо вшивать ограничители.

15:40 · 20 минут · Тезисы проверены редакцией · 09.10.2026 · Полные тезисы на сайте →

Как мы создали ИИ-фабрику по созданию персонифицированных КП

Ольга Поздняк
Директор
Код ИБ

Запись доклада

Типовые коммерческие предложения теряют клиентов — выход в персонификации под каждого заказчика

Как экосистема компания росла: появлялось всё больше разных проектов — образовательные программы, конференции и многое другое. Когда клиентам отправляли общее предложение поработать со всем этим многообразием услуг, у них «глаза выходили из орбит» — выбрать что-то конкретное было сложно, многие благодарили и уходили, и не все возвращались снова.

Собственный агент внутри системы обошёлся дешевле подписок на всех сотрудников

Компания не стала покупать каждому сотруднику подписку на внешний клуб за 200 долларов, а создала агента внутри своей системы. Он работает на достаточно дешёвых моделях и за «сущие копейки» создаёт качественные материалы, которые уже успели оценить клиенты.

Самое ценное в агенте — ресерч клиента и сопоставление его профиля с каталогом услуг

Работа начинается с того, что менеджер просто пишет агенту, для кого и что нужно приготовить. Агент при необходимости задаёт уточняющие вопросы, если что-то непонятно, а затем делает ресерч — именно этого раньше не было, когда одно коммерческое предложение делалось под все задачи.

Финальное решение всегда за менеджером: без верификации не обойтись из-за галлюцинаций

Хотя звучит так, будто агент сам генерирует, сам берёт почту клиента, сам отправляет и общается, на практике на этапе финального предложения обязательно подключается менеджер: он верифицирует и смотрит, то ли сделано или нет. Даже директор компании тестировала эту историю лично и пересмотрела много коммерческих предложений — нюансы всё равно были.

Агента ограничивают инструментами, а генерацию PDF выносят на отдельный сервер

Заранее созданные в системе агенты гарантируют, что агент идёт строго по пунктам и ничего не придумывает. Кроме того, под агента написаны специальные инструменты: каждый из них определённым образом ограничивает нейросеть — что-то даёт сделать, что-то не даёт. Поиск, например, выполняет другая нейросеть.

Полная прозрачность: видно, кто, когда и с какими данными работал в нейросетях

Доступ к нейросетям организован не только в формате чата — некоторые бизнес-процессы и объекты системы также работают с ними. При этом всегда видно, какой сотрудник, в какой момент времени, что делал, какими нейросетями пользовался и какие данные обрабатывал; по логам можно посмотреть все использованные инструменты.

16:00 · 20 минут · Тезисы проверены редакцией · 09.10.2026 · Полные тезисы на сайте →

Использование систем на базе ИИ для повышения продуктивности групповой работы экспертов на примере форсайта проводимого в рамках форума АСИ "Архипелаг

Руслан Пермяков

Советник директора ИВМиМГ СО РАН, Заместитель директора ЦК НТИ ТДВ

Запись доклада

Главный эффект ИИ в форсайте — ускорение цикла коммуникации, а не генерация за эксперта

В стратегической сессии участвовало около 20 экспертов с IT-бэкграундом. Работа шла полностью в электронной форме: обсуждения записывались на диктофон, аудио переводилось в текст, попадало в RAG и обрабатывалось ИИ. Пайплайн включал корпус, требования, каркас структуры и терминов, циклы экспертизы, редакции и выпуска PDF. За 4 дня получили работоспособный документ по развитию инфраструктурного центра — обычно такой результат группа получала примерно к декабрю.

Экономический эффект ИИ-форсайта надо считать по стоимости альтернативного пути

На цикле 20 человек за 4 дня израсходовали примерно 1 млн рублей на работу с моделями. Руслан Пермяков подчёркивает: оценивать это только как затраты неправильно. Нужно сравнивать скорость получения результата и стоимость такого же результата при стандартной схеме. Пересчёт на человеко-часы, опираясь на опыт похожих проектов, показал экономию около 12 млн рублей.

Без контроля версионности ИИ-пайплайн групповой работы становится неуправляемым

При построении систем с ИИ необходимо организовать контроль версионности. Агенты и люди пишут асинхронно, возникают конфликты и пересечения, поэтому нужны те же практики, что и в продакшене, особенно когда распределённая команда работает круглосуточно. Если контроль версионности есть, не нужно заставлять ИИ сравнивать документы вручную: система запускает Git и выдаёт HTML с подсвеченными изменениями.

Без управления данными ИИ галлюцинирует, но откат к стабильной версии спасает

Параллельно был эксперимент с дроном. В мастерскую пришли высокие гости, радиозапись вовремя не выключили, и разговор не про дроны попал в RAG. Запись автоматически обработалась ИИ, после чего началась «эпическая история» про дроны, конечности и манипуляторы — система стала галлюцинировать.

Три контура, классификация данных и аудит — обязательные элементы ИИ-архитектуры

В работе выделили три уровня. Первый — локальные дроны: скорее автоматизация, чем ИИ, с несколькими лёгкими нейронами; особых требований к локальному контуру не было. Второй — локальный ЦОД с 20–30 различными нейронами. Третий — недоверенный контур через open route к внешним моделям, в том числе зарубежным. Перекачивание информации контролировали гаджеты, проверявшие соответствие политике.

16:20 · 20 минут · Тезисы проверены редакцией · 09.10.2026

Использование ИИ при создании аннотаций судебных решений

Евгений Бессонов

Начальник службы безопасности Государственного автономного учреждения Культуры НСО Новосибирский государственный Краеведческий музей, член Общественного совета Минцифры НСО, член Общественного Совета Следственного Комитета РФ по НСО, Член IT-клуба Новосибирской области, Автор статей в Журнале Директор по безопасности

Запись доклада

ИИ-аннотирование судебных решений решает проблему перегруженности и обезличенных данных

В работе с судебными решениями есть две практические проблемы: документов очень много, а персональные данные в них нередко затираются. Типовой поиск по человеку выдает множество решений, и без дополнительного чтения сложно понять, относится ли конкретный документ к нужному Иванову Ивановичу. Аннотирование превращает большой текст судебного акта — административного, уголовного или гражданского — в краткое описание. Это позволяет не разбирать каждое решение вручную и быстрее переходить к анализу.

Система работает в закрытом контуре и не отправляет судебные тексты во внешние сервисы

Модели развернуты внутри инфраструктуры компании, и обработка идет в закрытом контуре. Тексты судебных решений не отправляются во внешний контур и никуда не уходят, то есть утечки как таковой не будет. Для службы безопасности это ключевой момент: данные обрабатываются внутри контролируемой структуры, и нет ситуации, когда непонятно, куда информация уходит, для какой цели и кто ее использует. Именно поэтому система применима для работы с чувствительными судебными документами.

ИИ-аннотация выделяет ключевые факты и связывает их с конкретным лицом

На входе — полный текст судебного акта, который может занимать много страниц; уголовные решения нередко достигают 15–50 страниц. Модель обрабатывает неструктурированный текст, иногда в разных и нечитабельных форматах, проводит связывание, классификацию фактов и сущностей в нужные поля. На выходе получается краткий отчет: в чем заключался спор, позиции сторон и итог суда. Система выделяет срок, сумму, арест, возраст (совершеннолетний или несовершеннолетний, пенсионер), статью и другие значимые параметры. Чтобы понять, что речь идет именно о конкретном человеке, она привязывает незатертый кодексатор и смотрит, где он повторяется, связывая данные между собой.

Модель сокращает время чтения, но не принимает решения за специалиста

ИИ не принимает решения за специалиста, не оценивает контрагента и не заменяет первичные источники. Он может обратить внимание на тот или иной момент, но вывод должен делать человек с богатым опытом. Главный эффект модели — сокращение времени чтения: она выделяет главное и экономит время для оценки риска. Поэтому система полезна как инструмент поддержки, а не как замена эксперта.

Для юридических лиц система дает мониторинг контрагентов и возможность работать на опережение

Система позволяет отслеживать изменения, связанные с юридическими лицами: юридический адрес, смену директоров, налоговые и иные данные. Она может показывать задолженность по судебным приставам, нахождение компании в черном списке антимонопольной службы и другие негативные факторы. Это помогает предотвращать ущерб до заключения договора, а не разбираться с последствиями. Пример из выступления: человек зарегистрирован на территории Алтайского края, прописан в Новосибирске, а деятельность индивидуального предпринимателя ведет в Карачаево-Черкесии; потом с ним сложно что-то сделать. Если контракт на 11 миллионов уже заключен, арест возможен, но потребует времени, госпошлины и работы юриста, поэтому лучше работать на предупреждение.

ИИ помогает анализировать узкие реестры и риски в тендерах

На примере реестра компаний, которые производят ремонт исторических зданий, видно, что таких компаний в Новосибирской области всего около 30–40, и только они получают допуск для строительных монтажных работ на таких зданиях. Значит, в тендерах могут участвовать только они, а на практике часто фигурируют одна-две компании. Загрузка таких ресурсных систем помогает анализировать ситуацию и коррупционную составляющую. Кроме того, в открытых источниках много неструктурированной информации, базы пополняются, и ИИ помогает работать с этими данными.

17:00 · 60 минут · Тезисы проверены редакцией · 09.10.2026 · Полные тезисы на сайте →

Деловая игра: «ИИ под прицелом»

Дмитрий Бойко
Директор департамента безопасности, ГК Lime Credit Group

Ольга Поздняк
Директор, Код ИБ

Руслан Пермяков
Советник директора ИВМиМГ СО РАН, Заместитель директора ЦК НТИ ТДВ

Руслан Поляков
CIO, Greenway Global

Сергей Поздняк
CEO, АльфаПи

Полина Сазонова
И.о. руководителя Комитета по информационным технологиям Новосибирского областного отделения...

Деловая игра «ИИ под прицелом»: распределите 5 миллионов рублей на защиту ИИ-агента

В финальный час конференции участникам предлагается деловая игра, в которой у них есть ИИ-агент, обслуживающий клиентов, и бюджет в 5 миллионов рублей на его защиту. Задача — выбрать, куда именно потратить эти 5 миллионов. С одной стороны, сумма кажется большой, с другой — не совсем. Нужно решить, вкладывать ли деньги в организационные и технические решения, оставить ли часть в резервном фонде для компенсации ущерба.

Инструменты защиты нужно не только выбрать, но и проверить в деле

В игре участники смогут купить те контролы и инструменты защиты, которые обсуждаются в рамках конференции. Однако главная проверка происходит позже: в определённый момент становится ясно, сработали ли выбранные контролы. Это позволяет на практике оценить, насколько правильно распределены средства и какие решения действительно работают. Такой формат даёт возможность увидеть последствия своих решений в безопасной среде, поработать с мозгами, с клиентами и коллегами. Организаторы уверены, что будет живо и интересно.

Экономический эффект от ИИ: можно нанять человека, а можно сэкономить миллионы

На конференции отмечалось, что при внедрении ИИ важно считать экономический эффект. В некоторых случаях проще и эффективнее посадить живого человека, который прекрасно справится с задачей, и ИИ не нужен. Но есть и примеры, когда затраты на ИИ окупаются многократно: например, Руслан Пермяков привёл историю, как, затратив миллион, удалось сэкономить компании 12 миллионов. Поэтому решения нужно взвешивать и смотреть на конкретные показатели.

Пилотный подход к ИИ: начать с простой, но жизненно важной задачи

Сергей Поздняк берёт в работу разных клиентов: экосистемные проекты, производственные предприятия и другие. Можно начать с простой, но очень важной для бизнеса задачи. В качестве примеров назывались коммерческие предложения, генерация презентаций или лендингов. К Сергею можно прийти, чтобы попробовать что-то сделать в виде пилота и посмотреть, как это будет работать. У него есть огромное количество кейсов, и если интересно, он их пришлёт. В перерыве можно поймать Сергея и пообщаться.

Бонус от Клода и живые примеры применения ИИ

Во время выступления Сергея произошёл показательный случай: Клод, услышав, сколько хороших слов было сказано в его адрес, подарил ему бонус — 250 долларов на использование инструментов Клода. Это ещё раз подчёркивает, что ИИ-инструменты активно используются и могут приносить неожиданные бонусы. В перерыве можно поймать Сергея и обсудить с ним кейсы, если будет интересно.

Розыгрыш подарков и призов по анкетам

Участникам напоминают, что по ходу конференции нужно заполнять анкеты: в финале состоится розыгрыш подарков и призов по анкетам. Если анкета ещё не заполнена, можно сделать это в ближайший перерыв.

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 НТ: 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