



AI, LLM и ПДн: как сотрудники уже сливают ПДн в ChatGPT и что с этим делать юридически и технически

Модератор и спикер: Калиничева Анастасия, Консультант по информационной безопасности АКТИВ.CONSULTING

Спикер: Воронова Елизавета, старший консультант по защите персональных данных, Б-152.

Спикер: Андюков Егор, старший специалист по информационной безопасности, Б-152.

Ассоциация пользователей стандартов по ИБ АБИСС

Объединяем профессионалов для создания
цивилизованного рынка аудита информационной безопасности

О нас

Ассоциация пользователей стандартов по информационной безопасности АБИСС – это сообщество профессионалов, основной задачей которого является развитие и совершенствование сферы применения стандартов информационной безопасности за счет постоянного взаимодействия членов, партнеров и поднадзорных организаций.

Мы объединяем

- ✓ Регуляторов ИБ
- ✓ Поднадзорные организации
- ✓ ИТ/ИБ компании
- ✓ Ассоциации и СМИ

Пятая межотраслевая конференция по регуляторике в сфере информационной безопасности, объединяющая на своей площадке специалистов, деятельность которых сопряжена с обеспечением соответствия ИБ-требованиям.





Не взлом, а копипаст:

новая реальность утечек ПДн



Калиничева Анастасия

Консультант по информационной безопасности АКТИВ.CONSULTING

О чем пойдет речь

01

Что такое ИИ и как с ним складываются отношения в мире

02

Ретроспектива законодательства об ИИ в России – от планов до первого НПА

03

Почему «слив» данных в ИИ – это утечка?

04

Что будет Оператору, который вовремя не задался вопросами безопасности ПДн

05

Как подразделения объединиться перед лицом ~~врага~~ утечки



Что такое ИИ?



Простыми словами это технологии и методы, которые помогают машинам выполнять задачи, требующие человеческого мышления



Законодательство транслирует термин ИИ как комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их

Мировое регулирование ИИ - положения



AI Act (Евросоюз)

Особенности:

Риск-ориентированный подход

Четыре уровня риска:

неприемлемый, высокий,
ограниченный, минимальный

Запреты:

- неконтролируемый сбор базы биометрических ПДн (социальный скоринг);
- определение эмоционального состояния человека;
- классификация физических лиц по их биометрическим ПДн (раса, религия и т.п.)



Казахстан, закон «Об искусственном интеллекте»

Особенности:

Риск-ориентированный подход

Три уровня риска: минимальный,
средний, высокий

Запреты:

- неконтролируемый сбор базы биометрических ПДн (социальный скоринг);
- определение эмоционального состояния человека;
- классификация физических лиц по их биометрическим ПДн (раса, религия и т.п.)
- нарушение законодательства о ПДн



Китай, комплекс НПА

Особенности:

От меньшего к большему

Региональные НПА

Риск-ориентированный подход

Пять уровней риска: низкий,
средний, значительный,
крупный, чрезвычайно
серьезный

Запрет:

нарушение права на
изображение, репутацию, честь,
неприкосновенность частной
жизни и персональных данных
(нарушение законодательства о
ПДн)

Мировое регулирование ИИ - санкции



AI Act (Евросоюз)

- нарушение запретов – до 35 млн евро (либо 7% годового мирового оборота)
- несоблюдение иных обязательств – до 15 млн евро (3% оборота)
- за предоставление недостоверных сведений регуляторам – до 7,5 млн евро (1,5% оборота)



Казахстан, закон «Об искусственном интеллекте»

нарушение
законодательства об ИИ
– 20-100 месячных
расчетных показателей



Китай, комплекс НПА

при квалификации дела
как нарушение
законодательства о ПДн
– до 50 млн юаней или
5% годового оборота

Ретроспектива законодательства об ИИ в России

Стратегическое планирование 2019-2021 годы

Указ Президента РФ от 10 октября 2019 года №490
«О развитии искусственного интеллекта в Российской Федерации»



- государственная поддержка;
- отраслевые ограничения;
- поправки в КоАП

Этические нормы 2021-2025 годы

Кодекс этики в сфере ИИ
Кодекс этики в сфере разработки и применения
искусственного интеллекта на финансовом рынке

Первый НПА 2026 год

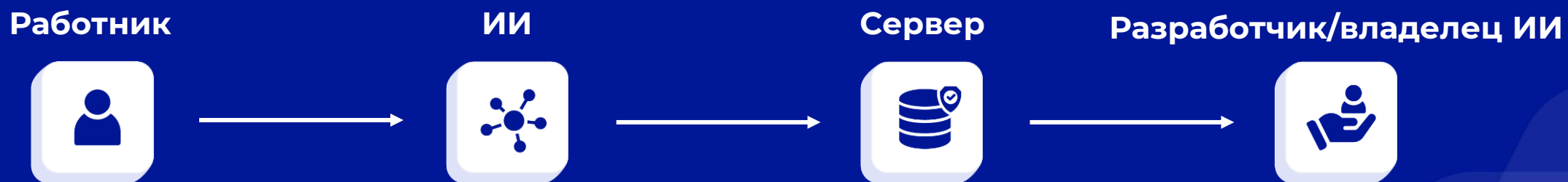
Федеральный закон от 26.07.2026 г. № 243-ФЗ
«О поддержке развития технологий искусственного интеллекта в
Российской Федерации»



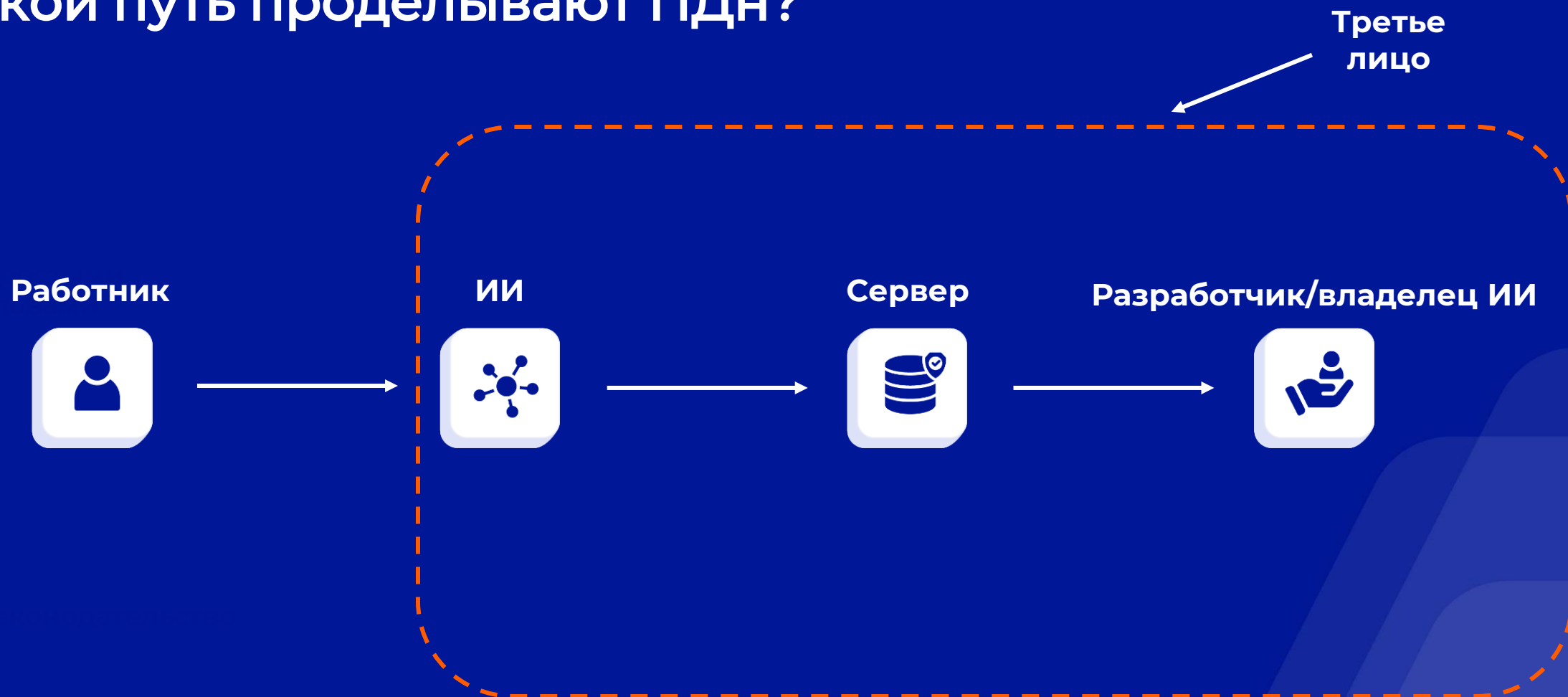
Законодательство
об ИИ

Законодательство
о ПДн

Какой путь проделывают ПДн?



Какой путь проделывают ПДн?



Почему это утечка?

Утечка ПДн – получение доступа к персональным данным третьим лицом, не имеющим на это полномочий (законное основание, согласие, т.п.)

Какие вопросы следует задать себе:

- ? Трансграничная передача, локализация
- ? Согласие на передачу третьему лицу
- ? Не относятся ли ПДн к биометрическим

Почему это утечка?

Утечка ПДн – получение доступа к персональным данным третьим лицом, не имеющим на это полномочий (законное основание, согласие, т.п.)

Какие вопросы следует задать себе:

- ? Трансграничная передача, локализация
- ? Согласие на передачу третьему лицу
- ? Не относятся ли ПДн к биометрическим

Что будет, если ответ не соответствует законодательству:

- ! Штраф до 6 (при повторе 18) млн. руб., отягчающее обстоятельство для уголовной ответственности
- ! Штраф до 300 тыс. руб.
- ! Штраф о 20 млн. руб. (при повторе – оборотный), уголовная ответственность

Ответственность за утечки ПДн и не только



Дорожная карта реагирования

Утечка произошла **только что**.
Как это понять?

ИБ зафиксировали
аномальную активность
в логах



Дорожная карта реагирования

Утечка произошла **только что**.
Как это понять?

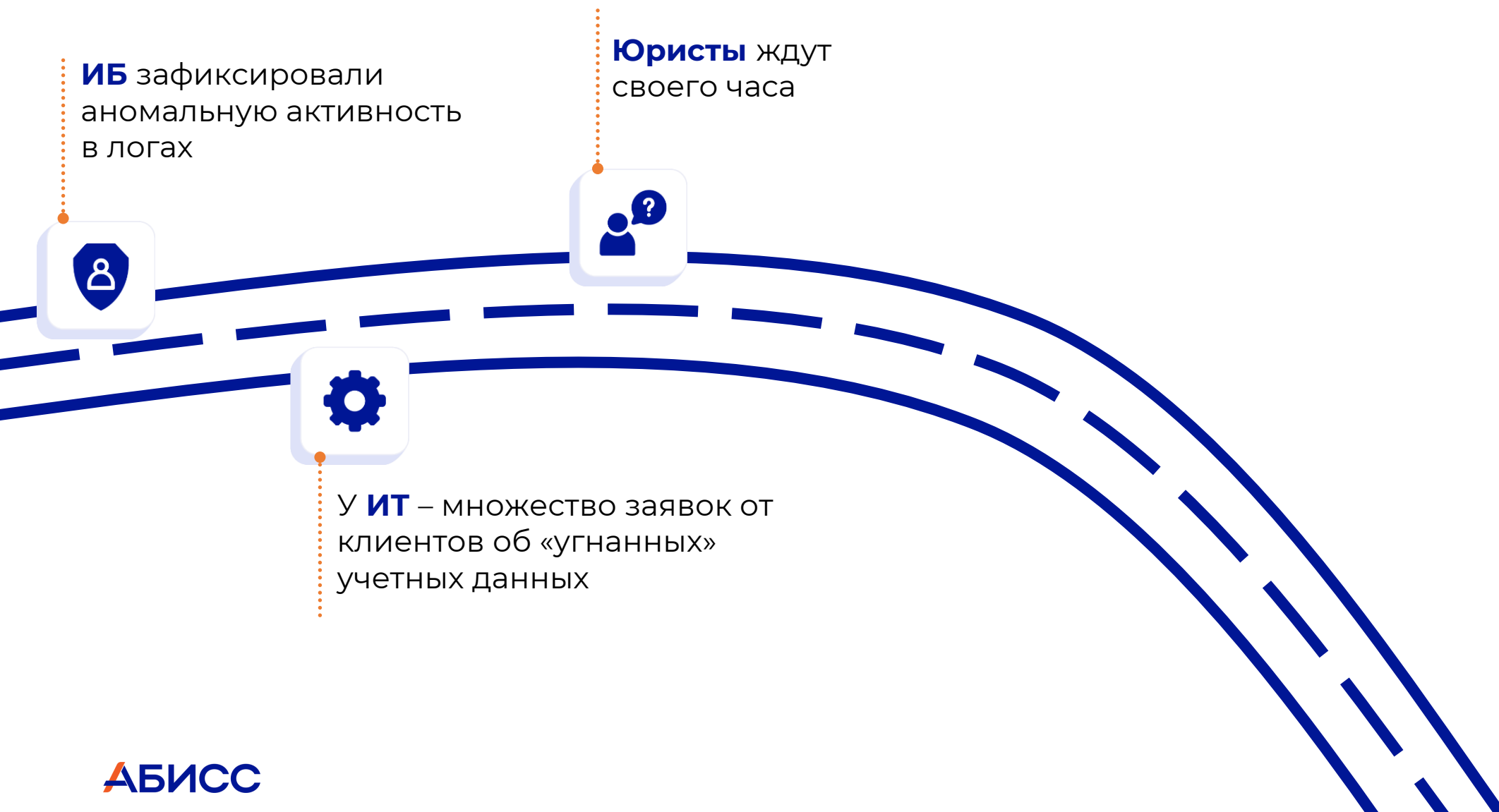
ИБ зафиксировали
аномальную активность
в логах



У **ИТ** – множество заявок от
клиентов об «угнанных»
учетных данных

Дорожная карта реагирования

Утечка произошла **только что**.
Как это понять?



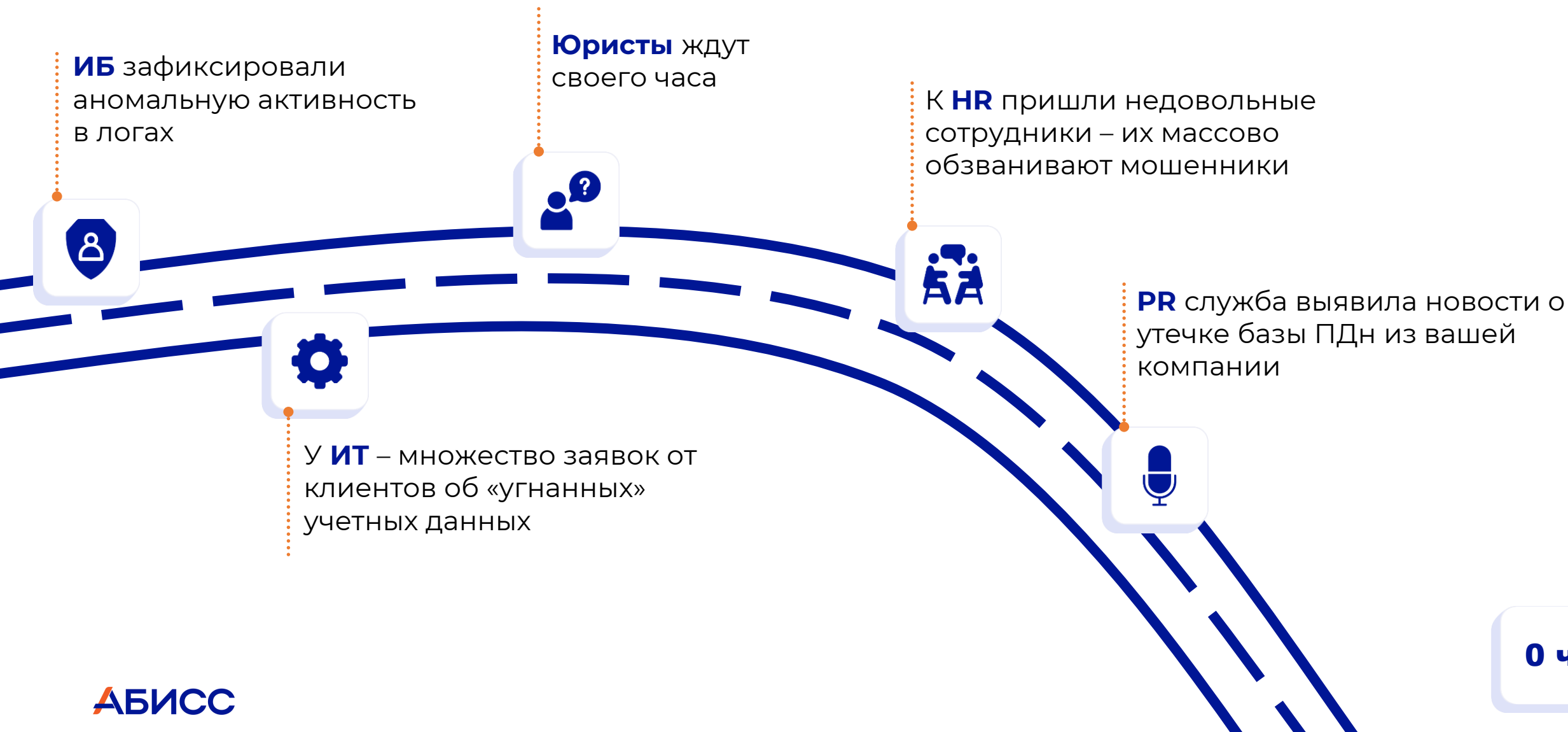
Дорожная карта реагирования

Утечка произошла **только что**.
Как это понять?



Дорожная карта реагирования

Утечка произошла **только что**.
Как это понять?



Дорожная карта реагирования

ИБ фиксирует все, что прямо или косвенно относится к инциденту



Дорожная карта реагирования

ИБ фиксирует все, что прямо или косвенно относится к инциденту



ИТ производит снятие логов прокси, DLP и дампов трафика

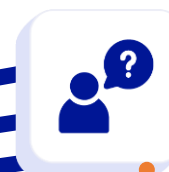


Дорожная карта реагирования

ИБ фиксирует все, что прямо или косвенно относится к инциденту



ИТ производит снятие логов прокси, DLP и дампов трафика



Юристы (DPO)
собирают информацию для уведомления РКН и проводят правовую оценку

Дорожная карта реагирования

ИБ фиксирует все, что прямо или косвенно относится к инциденту



ИТ производит снятие логов прокси, DLP и дампов трафика



PR мониторит СМИ и соцсети, проводит первичную оценку репутационных рисков



Юристы (DPO) собирают информацию для уведомления РКН и проводят правовую оценку

Дорожная карта реагирования

HR собирает письменные объяснительные с работников

PR мониторит СМИ и соцсети, проводит первичную оценку репутационных рисков

ИТ производит снятие логов прокси, DLP и дампов трафика

ИБ фиксирует все, что прямо или косвенно относится к инциденту

Юристы (DPO) собирают информацию для уведомления РКН и проводят правовую оценку

Дорожная карта реагирования



ИБ подготавливает
техническое заключение и
проводит оценку вреда

Дорожная карта реагирования

ИТ идентифицирует все устройства и учетные записи, производит дальнейший анализ трафика



ИБ подготавливает техническое заключение и проводит оценку вреда

Дорожная карта реагирования

ИТ идентифицирует все устройства и учетные записи, производит дальнейший анализ трафика



Юристы (DPO)
направляют уведомление в РКН



ИБ подготавливает техническое заключение и проводит оценку вреда

Дорожная карта реагирования



Дорожная карта реагирования



ИБ завершает
расследование

Дорожная карта реагирования

ИБ завершает
расследование



ИТ настраивает DLP и прокси-
шлюз для контроля ИИ-
трафика

Дорожная карта реагирования

ИБ завершает
расследование



ИТ настраивает DLP и прокси-
шлюз для контроля ИИ-
трафика



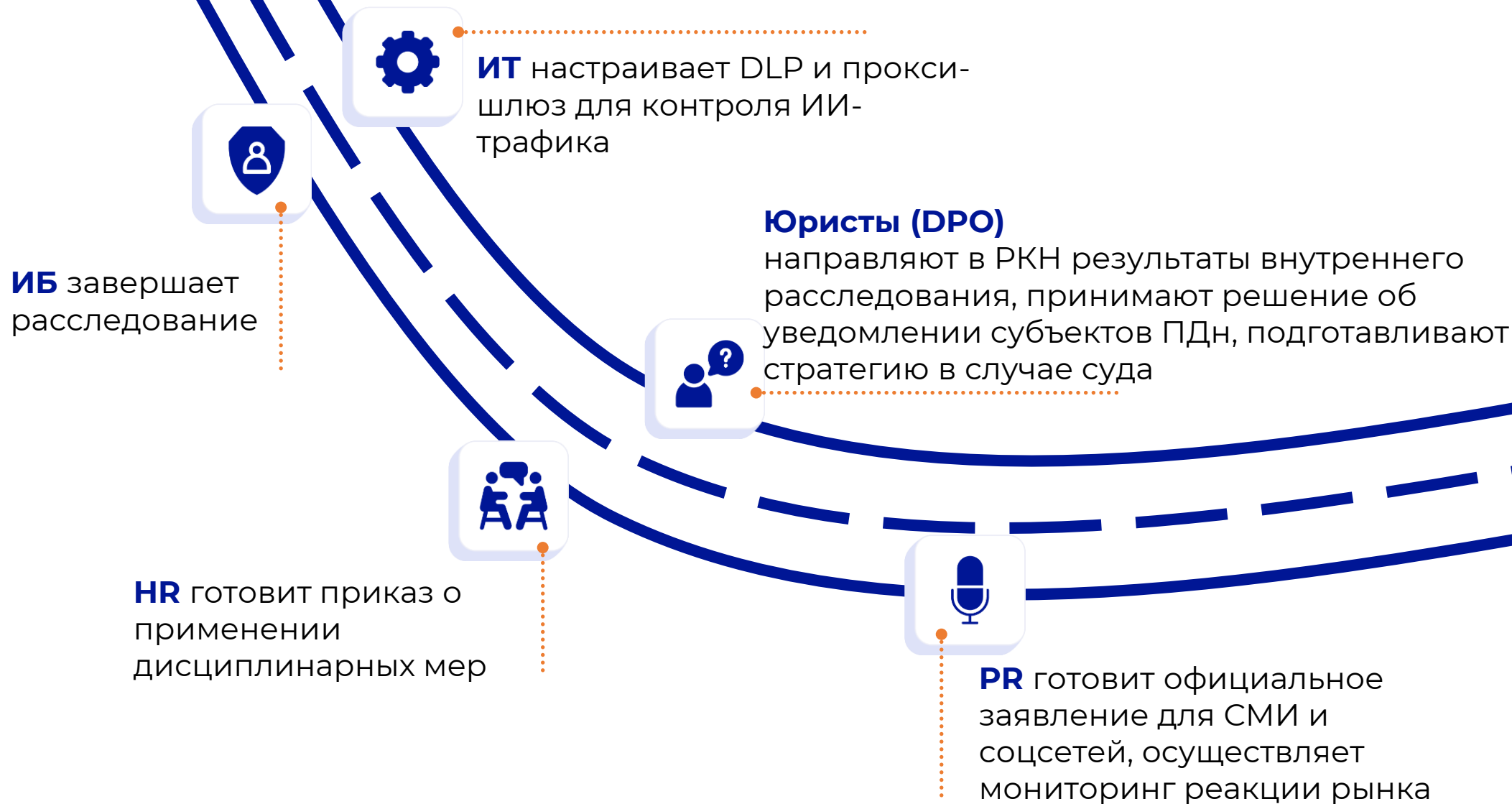
Юристы (DPO)

направляют в РКН результаты внутреннего
расследования, принимают решение об
уведомлении субъектов ПДн, подготавливают
стратегию в случае суда

Дорожная карта реагирования



Дорожная карта реагирования



Выводы

01

Мировая практика придерживается риск-ориентированного подхода

02

Российское законодательство заложило фундамент для развития ИИ технологий

03

Важно понимать, что за «лицом» ИИ находятся реальные третьи лица, и если они незаконно получают доступ к ПДн, то это полноценная утечка и к ней нужно быть готовым



АБИСС



Благодарю за внимание!

Калиничева Анастасия

Консультант по информационной безопасности
AKTIV.CONSULTING

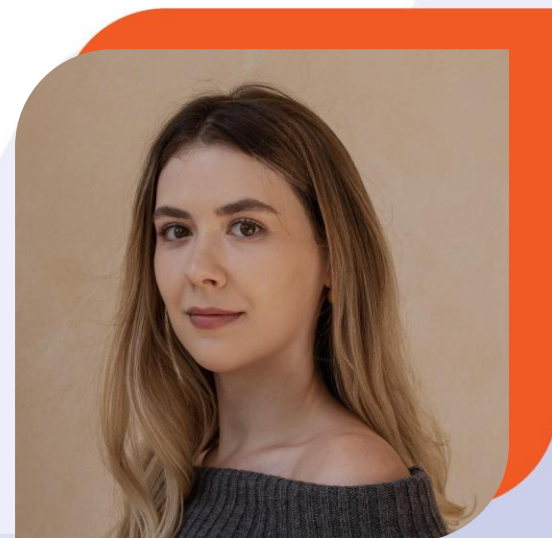
@ kalinicheva@aktiv.consulting

aktiv.consulting



Юридический каркас использования ИИ:

ОТ ОСНОВАНИЙ ДО ОТВЕТСТВЕННОСТИ



Елизавета Воронова, Старший консультант по защите персональных данных ООО «Б152» • 24.09.2026

Что разберём дальше

01

Правовые основания обработки ПДн
Согласие, договор и законный интерес — какое основание закрывает работу с ИИ

02

Договорная архитектура: иностранный SaaS,
русский SaaS или локальная модель

03

Автоматизированные решения
Ст. 16 152-ФЗ и риск для поставщика ИИ-
решения (кейс *Mobley v. Workday*)

04

Смежные правовые режимы: тайны,
исходный код и интеллектуальные
права

05

Внутренняя правовая инфраструктура
AI Governance, DPIA-подход и комплаенс чек-
лист

06

Ответственность сотрудника: кейс об
увольнении за разглашение тайны через ИИ

Правовые основания обработки ПДн

01

Согласие

Классическое основание - но требует информирования и не покрывает молчаливую передачу данных в чат-бот

02

Договор / поручение на обработку

Лицензионное соглашение вендора либо поручение по ст. 6 152-ФЗ - без него основания просто нет

03

Законный интерес

Работает только при балансе интересов и разумных ожиданий - обычно не покрывает передачу в публичный сервис



Договорная архитектура: три сценария

01

Иностранный SaaS

OpenAI, Anthropic, Google и т.п.
Учитывайте юрисдикцию серверов, тип аккаунта (личный/enterprise) - и то, что вендор часто не прописывает основания для ИИ-обработки прямо в privacy policy



02

Российский SaaS

YandexGPT, GigaChat, T-Pro AI.
Классическая конструкция: поручение на обработку по ст. 6 152-ФЗ, обязательства по конфиденциальности, распределение прав на результат генерации



03

Локальная модель

Self-hosted / open-weight. Данные не покидают периметр, но остаются вопросы хостинга (свой ЦОД или внешний) и лицензионных ограничений на коммерческое использование



Автоматизированные решения и права субъекта

- ✓ Ст. 16 152-ФЗ: если результат работы ИИ влияет на права и интересы человека - отказ в найме, скоринг, модерация контента - закон требует человеческого контроля и права субъекта оспорить такое решение
- ✓ В судах РФ бремя доказать, что решение принято именно в автоматизированном порядке, обычно лежит на самом пострадавшем субъекте - это снижает риск для работодателя
- ✓ Кейс Mobley v. Workday (2024): суд признал, что поставщик HR-tech решения на основе ИИ может нести ответственность как «агент» работодателя за дискриминационные результаты подбора
- ✓ Для российских компаний, использующих зарубежные ИИ-инструменты в найме или модерации, это ориентир на то, куда движется регулирование и договорная практика с вендорами
- ✓ Там, где ИИ участвует в решениях, влияющих на людей, нужен зафиксированный human-in-the-loop и понятная процедура обжалования - а не только основание для обработки данных

Смежные правовые режимы — не только 152-ФЗ



Коммерческая тайна

- ✓ Финансовый отчёт в промпте - разглашение тайны
- ✓ Банковская и врачебная тайна - вне 152-ФЗ
- ✓ Код в промпте - риск для коммерческой тайны, а не только для ПДн
- ✓ Без режима тайны и пункта в NDA привлечь сотрудника к ответственности почти невозможно



Интеллектуальные права

- ✓ Передача РИД без согласия правообладателя - риск
- ✓ Результат ИИ тоже может нарушать чужие права
- ✓ «Это ИИ сгенерировал» - не защита: алгоритм не снимает охрану исходного объекта
- ✓ Проверяйте права на исходники и результат генерации

Правовая инфраструктура до инцидента



AI Governance

Кто в компании принимает решение о новом ИИ-инструменте, есть ли этический кодекс и ответственные, которые видят Shadow AI раньше ИБ



Оценка рисков (DPIA-подход)

До подключения сервиса: какие данные, на каком основании, генерирует ли он дополнительные данные и где они хранятся



Комплаенс чек-лист

ЛНА по работе с ИИ, проверка объектов ИС, риск дискриминации, человеческий контроль, информирование пользователей

Кейс: увольнение за слив данных в DeepSeek

- ✓ Сотрудница загрузила в DeepSeek лиды по каналам продаж и оперативную панель примерно с 30 финансовыми показателями, выгруженную из защищённого Power BI
- ✓ Уволена не за один эпизод: работодатель объединил разглашение стратегии бренда поставщику, пересылку документов на личную почту и загрузку данных в DeepSeek
- ✓ Суд признал увольнение законным (подп. «в» п. 6 ч. 1 ст. 81 ТК РФ) - режим коммерческой тайны был введён и доведён до работника заранее
- ✓ Скриншоты и логи мониторинга рабочих компьютеров суд принял как допустимые письменные доказательства (ст. 71 ГПК РФ)
- ✓ При этом отдельное взыскание работодатель проиграл - не обосновал соразмерность наказания за отсутствие на рабочем месте

Право и технический контроль работают только вместе

«Юридическое
основание есть -
нужен
технический
контроль, который
его подтверждает»

01

Право без контроля

Правильная политика без контроля
— документ, который никто не
читает и нечем подтвердить.



02

Контроль без права

Контроль без основания и без ЛНА
юридически уязвим при
оспаривании в суде.





Елизавета Воронова

Старший консультант по защите персональных данных ООО «Б152»



elizaveta.voronova@b-152.ru
info@b-152.ru



+7 925 210 87 72
+7 499 372 06 52



АБИСС



ИИ как новый канал утечки данных:

от промпта до утечки: реальные кейсы и технические
меры контроля



Егор Андюков, Старший специалист по информационной безопасности
«Б152»• 24.09.2026

Масштаб проблемы: Shadow AI в цифрах

Масштаб проблемы в цифрах

01

Рост в 30 раз за год

Объём данных, уходящих в публичные нейросети из российских компаний, вырос в 30 раз за 2025 год — по данным анализа трафика 150 компаний (ГК «Солар»).

02

Утечки через ИИ растут

20% компаний, столкнувшихся с утечкой в июле 2026 года, связали её с бесконтрольным использованием ИИ. Год назад таких было около 12% («Информзащита»).

03

Регламентов почти нет

60% компаний до сих пор не имеют регламента по использованию ИИ, а 98% организаций сталкиваются с несанкционированными ИИ-инструментами — от ChatGPT в браузере до агентов с доступом к почте и CRM.

Три реальных кейса из практики

Кейс 1. Samsung: три утечки за три недели



Что произошло

Инженеры Samsung трижды за месяц вставляли в ChatGPT конфиденциальные данные: исходный код полупроводников для проверки ошибок, код для оптимизации оборудования и запись внутреннего совещания для составления протокола.



Масштаб утечки

Каждый промпт мог использоваться OpenAI для дообучения модели. Компания не имела технической возможности отозвать уже отправленные данные — исходный код мог «всплыть» в ответах другим пользователям.



Последствия

Samsung полностью запретила сотрудникам использовать генеративный ИИ на корпоративных устройствах и начала разработку собственного внутреннего ИИ-инструмента — классический сценарий «бан вместо контроля».

Кейс 2. Утечка через корпоративного ИИ-ассистента



Microsoft 365 Copilot

Исследования показывают, что значительная часть компаний столкнулась с тем, что Copilot выдавал сотрудникам данные из документов, к которым у них не было прав доступа — ассистент подключён к общей базе, а не к правам конкретного пользователя.



Sage Copilot

ИИ-ассистент бухгалтерского сервиса Sage в ответах на вопросы одних клиентов приводил фрагменты конфиденциальных данных других клиентов — модель «путала» контексты разных пользователей внутри общей системы.



Общая причина

Утечка происходит не через промпт сотрудника, а через саму архитектуру корпоративного ИИ-инструмента: разграничение прав доступа и изоляция данных между пользователями требуют отдельной, осознанной настройки — по умолчанию это часто не так.

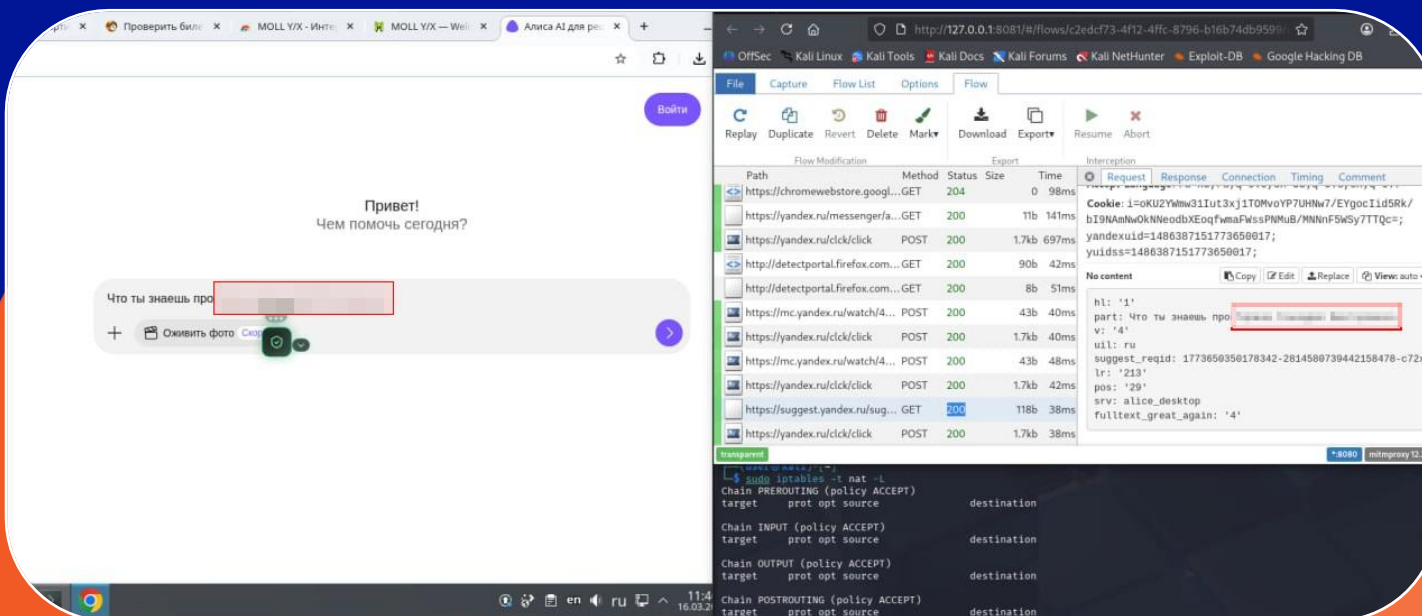
Кейс 3 (наша практика). Риск «черновика»

Что мы обнаружили

В нашей практике перехват трафика показал: черновик запроса к встроенному ИИ-ассистенту (голосовому помощнику) начинает синхронизироваться с сервером ещё в процессе набора текста — фоново, символ за символом.

То есть удаление текста «до отправки» или закрытие приложения не отменяет утечку — часть данных уже ушла на сторону.

Почему это опаснее обычного промпта: стандартные DLP-правила «блокировать по кнопке отправки» здесь не срабатывают — точки контроля просто нет.



Перехват трафика: голосовой ассистент отправляет введенный текст на сервер до нажатия кнопки отправки

Что ещё узнаёт о вас ИИ

Пассивный след: что раскрывает не текст

01

IP-адрес и геолокация запроса

раскрывает офис и адрес инфраструктуры компании даже без единого слова о ней в тексте

02

User-Agent и версия ПО

данные об устройстве и браузере сотрудника — потенциально уязвимой конфигурации

03

Паттерны и частота запросов

по косвенным признакам можно восстановить оргструктуру, штат и интенсивность работы над проектом

04

Метаданные файлов и скриншотов

имя пользователя, путь на диске, версия ПО, а иногда и геометки фотографий

05

Сам факт использования сервиса

известны случаи, когда истории публичных чат-ботов индексировались поисковиками и попадали в открытый доступ



ИИ и пароли: удобно — не значит безопасно

01

Пароли LLM предсказуемы

Модель не использует криптографически стойкий генератор случайных чисел — она предсказывает «наиболее вероятную» комбинацию символов, а не выбирает её случайно.

02

ИИ уже подбирает пароли

По данным Home Security Heroes, инструмент PassGAN взламывает 51% распространённых паролей меньше чем за минуту и 81% — меньше чем за месяц.

03

Вывод

Генерация паролей и ключей — не задача для чат-бота. Секреты должны создаваться только специализированным криптографическим генератором случайных чисел.

Технические варианты контроля

Три уровня технического контроля

01

Полный запрет

Блокировка доступа к публичным ИИ-сервисам на уровне сети. Быстро внедряется, но не устраняет проблему — сотрудники уходят в личные устройства и мобильный интернет («Shadow AI» никуда не девается, просто выпадает из поля зрения ИБ).

02

Корпоративный AI-шлюз

Прокси/DLP-шлюз перед публичными ИИ-сервисами: проверяет промпт на чувствительные данные до отправки, логирует запросы, разрешает работу с одобренными моделями. Требуется внедрения и настройки политик, зато сохраняет продуктивность сотрудников.

03

Локальные российские LLM

Перевод рабочих задач на YandexGPT, GigaChat и другие модели с обработкой данных на российских серверах. Снимает часть вопросов трансграничной передачи ПДн, но требует оценки качества модели под конкретные задачи и своей политики хранения логов.

Дорожная карта на 90 дней



0–30 дней: экстренные меры



31–60 дней: политика и контроль



61–90 дней: технологии и масштаб

- | | | |
|---|--|--|
|  Оценить масштаб Shadow AI: провести аудит трафика к публичным ИИ-сервисам |  Утвердить AI Policy: что можно/нельзя отправлять в публичные нейросети |  Внедрить корпоративный AI-шлюз с DLP-фильтрацией промптов |
|  Ввести временные организационные меры: разослать памятку сотрудникам о рисках |  Добавить пункт про использование ИИ в NDA и трудовые договоры |  Провести пилот на локальных моделях (YandexGPT, GigaChat) для чувствительных задач |
|  Определить ответственного за ИИ-риски (ИБ + юрист + владелец процесса) |  Подготовить IR Plan: порядок действий при обнаружении утечки через ИИ |  Обучить сотрудников и повторно измерить объем Shadow AI-трафика |



Егор Андюков

Старший специалист по информационной безопасности



egor.andyukov@b-152.ru
info@b-152.ru



+7 926 274 23 38
+7 499 372 06 52

Спасибо!