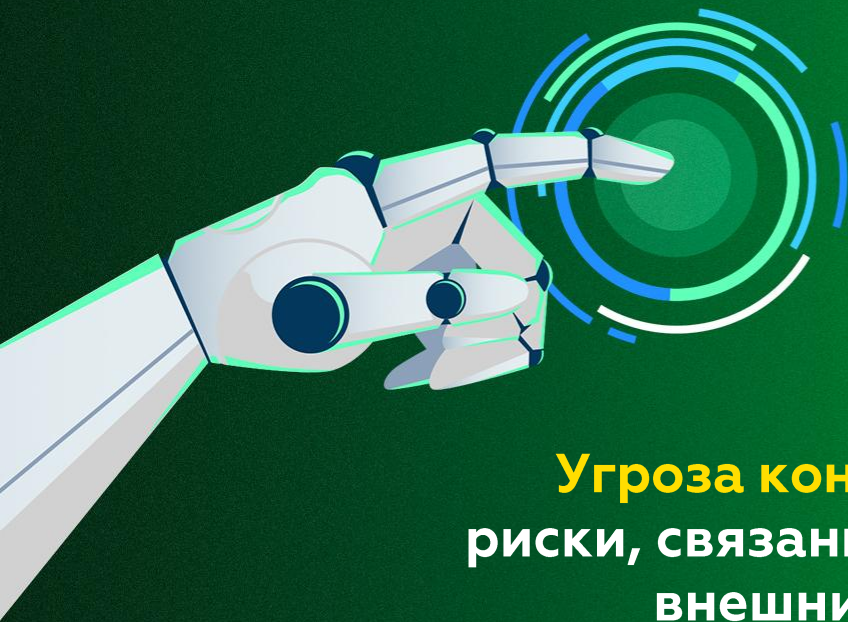
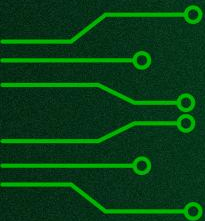


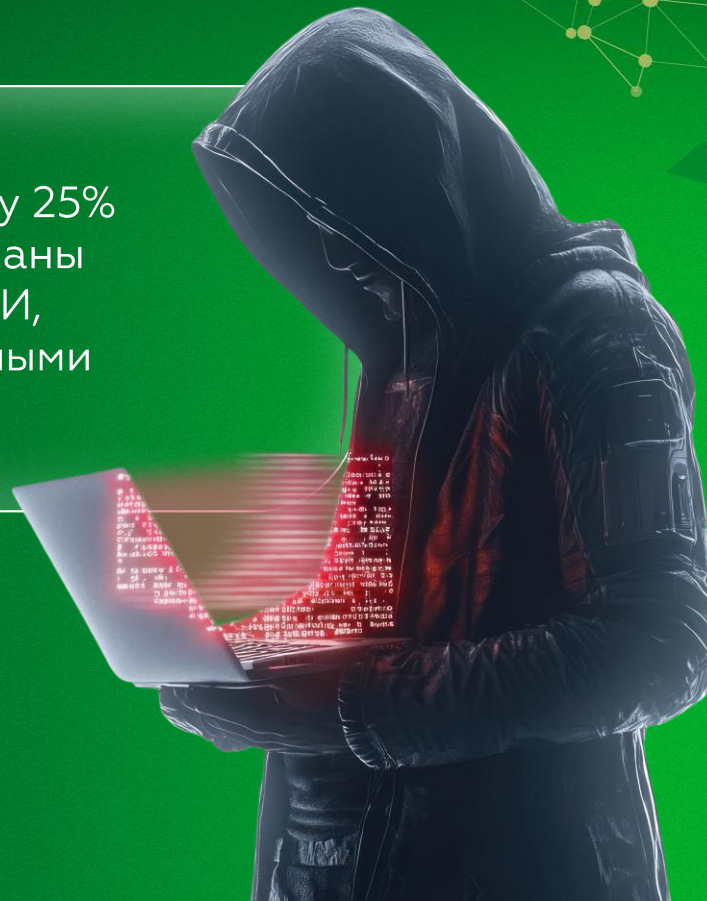
Угроза конфиденциальности:
риски, связанные с использованием
внешних ИИ-сервисов



грузовичкоф

Угроза конфиденциальности: риски, связанные
с использованием внешних ИИ-сервисов

По прогнозам Gartner к 2028 году 25% корпоративных утечек будут связаны со злоупотреблением агентами ИИ, как внешними, так и злонамеренными внутренними субъектами



Угроза конфиденциальности: риски, связанные
с использованием внешних ИИ-сервисов

Как сотрудники «сливают»
данные через промпты —
и что с этим делать?



Угроза конфиденциальности: риски, связанные с использованием внешних ИИ-сервисов

Тихая революция: Растет количество сотрудников использующих внешние AI для повышения своей эффективности. Бизнес этого не внедрил, но использование стало фактом

Угроза материализовалась: В чат с ИИ вводят и конфиденциальные данные — от внутренних отчетов до персональных данных клиентов

Нет официальной политики компании по использованию ИИ — значит, Нет и защиты от этих рисков. Компания теряет контроль над своими данными



Угроза конфиденциальности: риски, связанные с использованием внешних ИИ-сервисов

Типичные промпты, которые ставят под угрозу безопасность данных:

«Перепиши этот договор в более понятной форме» → договор уходит в облако

«Проанализируй список клиентов и выдели топ-10» → ПДн передаются третьему лицу

«Сделай выжимку из внутреннего отчета» → коммерческая тайна становится публичной

Prompt



Угроза конфиденциальности: риски, связанные с использованием внешних ИИ-сервисов



ФЗ-152: Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом



Передача данных ИИ-платформам = передача третьему лицу требуется согласие субъекта ПДн или договор с обеспечением защиты (что невозможно с публичными ИИ)



Угроза конфиденциальности: риски, связанные с использованием внешних ИИ-сервисов

Что делать? Шаг 1 — Блокировка по умолчанию

Запретить доступ к публичным ИИ-сервисам (DeepSeek, Qwen и др.)

Настроить DPI / Proxy / FW с категоризацией трафика

Исключения — только по заявке и под контролем ИБ



Угроза конфиденциальности: риски, связанные с использованием внешних ИИ-сервисов

Шаг 2 — Предложить безопасную альтернативу

Внедрение локальных ИИ-моделей

Корпоративные ИИ-ассистенты без отправки данных наружу



Угроза конфиденциальности: риски, связанные с использованием внешних ИИ-сервисов

Шаг 3 — Обучение и культура

Не запрещать — объяснять

Тренинги: «Почему нельзя вводить ПДн в ChatGPT»

Симуляции фишинга + ИИ-угрозы

Четкая политика в локальных нормативных актах



Угроза конфиденциальности: риски, связанные с использованием внешних ИИ-сервисов

Внешние ИИ — не враг, но и не друг.

Без контроля — это вектор утечки.

С политикой, технологиями и обучением — инструмент в руках, а не риск в облаке

Рекомендация: если не заблокированы — заблокируйте. Если не контролируются — начните сегодня



Угроза конфиденциальности: риски, связанные
с использованием внешних ИИ-сервисов

Спасибо за внимание!



Дмитрий Ляхов

Директор по информационной безопасности
Сервиса «Грузовичкоф»

