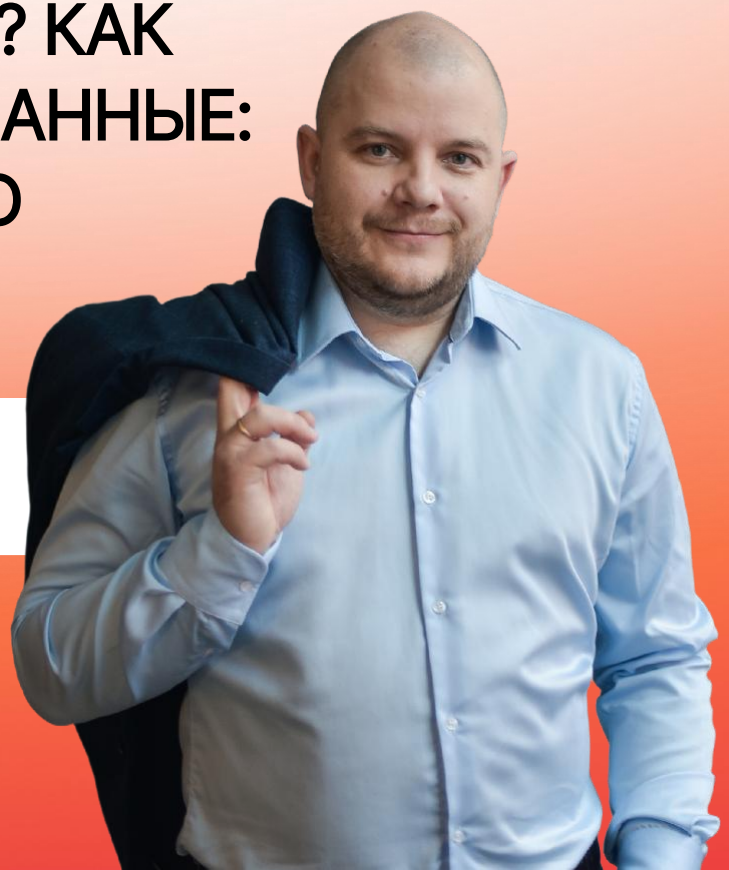
Стахановец

ИИ — ПОМОЩНИК ИЛИ УГРОЗА? КАК ЗАЩИТИТЬ КОРПОРАТИВНЫЕ ДАННЫЕ: ИНСТРУКЦИЯ ПО ПРИМЕНЕНИЮ

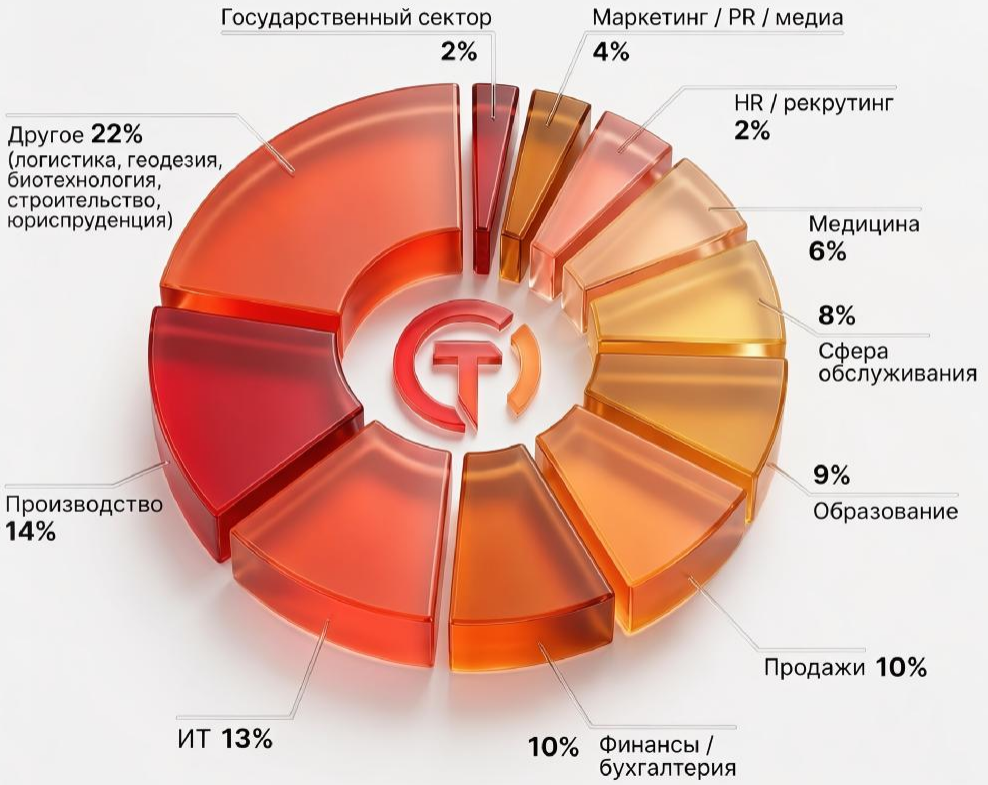


АРТЁМ ЖАДЕЕВ
Директор по продажам «Стахановец»

Стахановец

В МИРЕ КАЖДЫЙ ШЕСТОЙ РАБОТНИК АКТИВНО ИСПОЛЬЗУЕТ НЕЙРОСЕТИ*

В УЗБЕКИСТАНЕ 64% СОТРУДНИКОВ ИСПОЛЬЗУЮТ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НА РАБОТЕ**



В 2025 году генеративный искусственный интеллект перестал быть «игрушкой» и стал базовым инструментом продуктивности

*По данным отчета Microsoft | **По данным HH

НЕЙРОСЕТИ — ОДИН ИЗ ГЛАВНЫХ КАНАЛОВ УТЕЧЕК

Стахановец

За 2025 г. в нейронные сети попало в **30 раз больше** конфиденциальной информации, чем годом ранее

Сотрудники массово загружают в чат-боты рабочие документы:

Презентации

Аналитические отчеты

Внутреннюю переписку

Таблицы с бизнес-данными

Материалы стратегического планирования

Фрагменты исходного кода

Техническую документацию

ГЛАВА АГЕНТСТВА КИБЕРБЕЗОПАСНОСТИ США ЗАГРУЗИЛ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ В CHATGPT

Мадху Готтумуккала загрузил документы с пометкой «только для служебного пользования» в публично доступную версию нейросети ChatGPT

Мир
28.01.2026, 15:37

1K
1 мин.

Politico: глава Агентства кибербезопасности США загрузил конфиденциальные данные в ChatGPT

Мадху Готтумуккала — исполняющий обязанности руководителя Агентства кибербезопасности и защиты инфраструктуры (CISA) США — загрузил конфиденциальные документы в публично доступную версию нейросети ChatGPT. Об этом пишет издание Politico со ссылкой на источники в Министерстве внутренней безопасности (МВБ), которому подчиняется CISA. Все материалы, загруженные в публичную версию ChatGPT, доступны разработчику и могут использоваться в ответах нейросети другим пользователям.

По данным источников, инцидент произошел летом 2025 года. Сработало несколько автоматических предупреждений о проблемах безопасности — такие предупреждения должны предотвращать слив или кражу конфиденциальных правительственных данных. По информации Politico, МВБ после раскрытия информации начало внутреннюю проверку, ее результаты неизвестны.

ИНЖЕНЕРЫ SAMSUNG ИСПОЛЬЗОВАЛИ CHATGPT ДЛЯ ПРОВЕРКИ И ОПТИМИЗАЦИИ ИСХОДНОГО КОДА

В результате фрагменты секретного исходного кода и другая конфиденциальная информация оказались на серверах OpenAI

Samsung потеряла данные из-за ChatGPT

Economist: корпоративные данные Samsung утекли в сеть из-за чат-бота ChatGPT

Андрей Ставицкий (Редактор отдела «Наука и техника»)

Фото: Sebastian Gollnow / dpa / Globallookpress.com

Чат-бот ChatGPT стал причиной утечки корпоративных данных Samsung. Об этом сообщает корейское издание Economist.

Источники в компании рассказали, что сотрудники IT-гиганта стали применять чат-бота в своей работе три недели назад. В результате того, что специалисты корпорации неправильно использовали ChatGPT, конфиденциальные данные Samsung оказались в свободном доступе.

В материале говорится, что в первом случае инженер ввел в строку чат-бота с искусственным интеллектом исходный код, касающийся

ГЛАВНЫЙ РИСК — ПУБЛИЧНОЕ РАСКРЫТИЕ ИНФОРМАЦИИ

Стахановец

КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ ПОЛЬЗОВАТЕЛЕЙ CHATGPT ОКАЗАЛИСЬ В ОТКРЫТОМ ДОСТУПЕ

31 июля 2025 13:12 | 13679 | ПОДЕЛИТЬСЯ

В интернет утекли миллионы личных чатов пользователей ChatGPT

В июле 2025 г. вскрылась масштабная утечка данных пользователей ChatGPT, которые потенциально могут скомпрометировать конфиденциальную и чувствительную информацию, которую пользователи доверяют этому продвинутому чат-боту. В Google теперь показываются ссылки на чаты с ChatGPT, поисковая система из-за сбоя начала индексировать публичные ссылки из ChatGPT.

Утечка информации в сеть

Конфиденциальные данные пользователей ChatGPT оказались в открытом доступе, пишет Reuters. Это все из-за того, что поисковая система Google в июле 2025 г. начала

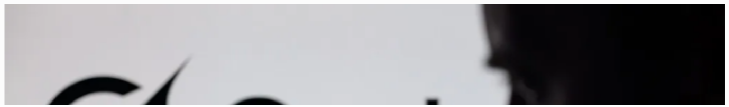
КОМПАНИЯ ЧАТ-БОТА GROK СЛИЛА В ИНТЕРНЕТ ДИАЛОГИ ПОЛЬЗОВАТЕЛЕЙ С НЕЙРОСЕТЬЮ

Сотни тысяч чатов пользователей Grok от Маска стали доступны в поисковиках

ИВАН САЛО

Редактор «Инк.».

Сотни тысяч разговоров пользователей с ИИ-ботом Grok от компании xAI Илона Маска стали доступны через поисковые системы, включая Google. Об этом пишет американский Forbes. Это произошло из-за функции «Поделиться», которая генерирует уникальные URL для обмена беседами, индексируемые поисковиками.



Стахановец

РАЗРЕШИТЬ НЕЛЬЗЯ ЗАПРЕТИТЬ

ШАГ 1

РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ ИСПОЛЬЗОВАНИЯ ИИ-ИНСТРУМЕНТОВ

- Сформулируйте основные задачи при внедрении ИИ
- Определите области применения ИИ (например, автоматизация процессов, анализ данных, клиентское обслуживание)
- Выберете разрешенные сервисы для работы
- Разделите данные, которые разрешено и запрещено загружать

ШАГ 2

ОБУЧЕНИЕ СОТРУДНИКОВ

- Проведите общую презентацию по основам ИИ и его возможностям
- Объясните, где и как ИИ будет использоваться в компании
- Разъясните вопросы конфиденциальности данных и этики
- Проговорите соблюдение действующего законодательства и нормативов

ШАГ 3

ВНЕДРЕНИЕ DLP-СИСТЕМЫ ДЛЯ КОНТРОЛЯ ИИ-ТРАФИКА

- Определите цели и области контроля (обмен конфиденциальной информацией, доступ к ИИ-сервисам, и т.д)
- Проведите аудит ИТ-инфраструктуры
- Выберите и протестируйте DLP-решение
- Настройте политики безопасности
- Разработайте процедуры реагирования

ВАЖНО ОБЪЯСНИТЬ, ЧТО ДАННЫЕ, ОТПРАВЛЕННЫЕ В ЧАТ-БОТ, НАВСЕГДА ПОКИДАЮТ КОРПОРАТИВНЫЙ КОНТУР

Стахановец

ЧТО УМЕЮТ СОВРЕМЕННЫЕ DLP-СИСТЕМЫ?

- Выявлять сотрудников, которые используют публичные нейросети: мониторинг программ и сайтов
- Контролировать отправку файлов с конфиденциальной информаций в ИИ
- Распознавать чувствительные данные на изображениях, отсканированных документах
- Запрещать отправку файлов конкретного формата: CAD-чертежи, архивы, графические изображения
- Мгновенно отправлять в карантин файлы с корпоративными данными
- Запрещать доступ к ИИ-ресурсам

Стахановец

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

stakhanovets.ru

info@stakhanovets.ru

+7 499 110-64-10

АРТЁМ ЖАДЕЕВ

Директор по продажам «Стахановец»

Телеграм канал с актуальными новостями по ИБ, EM и DLP

ООО “Стахановец”, ИНН: 7725836290;
ОГРН: 1147746831220