



Внедрение Privacy by Design в корпоративные ИИ-системы: управление инновациями через призму конфиденциальности

Выполнил: О.А. Пасечник, аспирант

Научный руководитель: В.М. Ячmeneва, д.э.н., профессор

Введение и актуальность темы

Резкий рост применения корпоративных ИИ-систем.

Риски утечек, ведущие к финансовым и репутационным потерям.

Усиление внимания к защите данных и конфиденциальности.

Необходимость баланса между инновациями и нормативными требованиями.



Цель и задачи исследования

Определить эффективные механизмы внедрения принципа Privacy by Design.

Анализ кейсов (международных и отечественных).

Выявление технологических мер (анонимизация, шифрование, дифференциальная приватность).

Исследование организационных изменений.



Технологические решения и инновации

Анонимизация данных – скрытие личной информации.

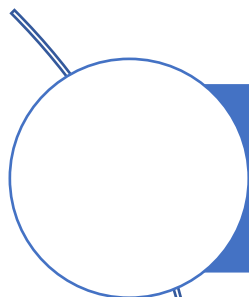
Шифрование и дифференциальная приватность – надежная защита на всех этапах.

Кейсы: Microsoft и Amazon – опыт предотвращения утечек и минимизации рисков.

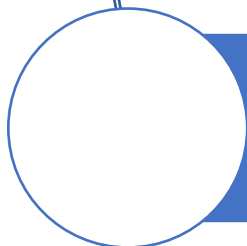
Рекомендуется добавить инфографику для визуализации преимуществ.



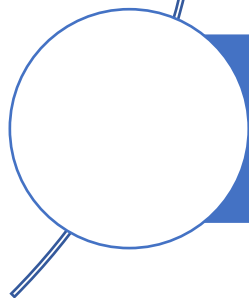
Организационные меры и междисциплинарное сотрудничество



Организационные меры – улучшение управляемости и минимизация регуляторных рисков.



Создание кросс-функциональных команд (разработчики, юристы, эксперты по ИБ).



Пример: система ГИБДД «Паутина» – модернизация с анонимизацией и шифрованием снижает утечки на 80%.



Регуляторный контекст и кейс-стади

Ключевые нормативы: GDPR (ЕС) и ФЗ-152 (Россия).

Своевременное применение Privacy by Design снижает финансовые потери и улучшает репутацию.

Примеры санкций:

- – Microsoft: штрафы и корректирующие меры.
- – Amazon: крупные штрафы за манипуляции с данными.



Выводы и рекомендации

Выводы

Интеграция Privacy by Design обеспечивает устойчивость корпоративных ИИ-систем.

Баланс инноваций и защиты данных создает конкурентные преимущества.

Рекомендации:

– Внедрять Privacy by Design на всех этапах разработки.

– Создавать кросс-функциональные команды.

– Постоянно обновлять технические и организационные меры защиты.

