



КОНСОРЦИУМ
ИССЛЕДОВАНИЙ
БЕЗОПАСНОСТИ
ТЕХНОЛОГИЙ
ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА

РАБОЧАЯ ГРУППА №3

ПО СОЗДАНИЮ И РАЗВИТИЮ РЕЕСТРА ДОВЕРЕННЫХ
РЕШЕНИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА



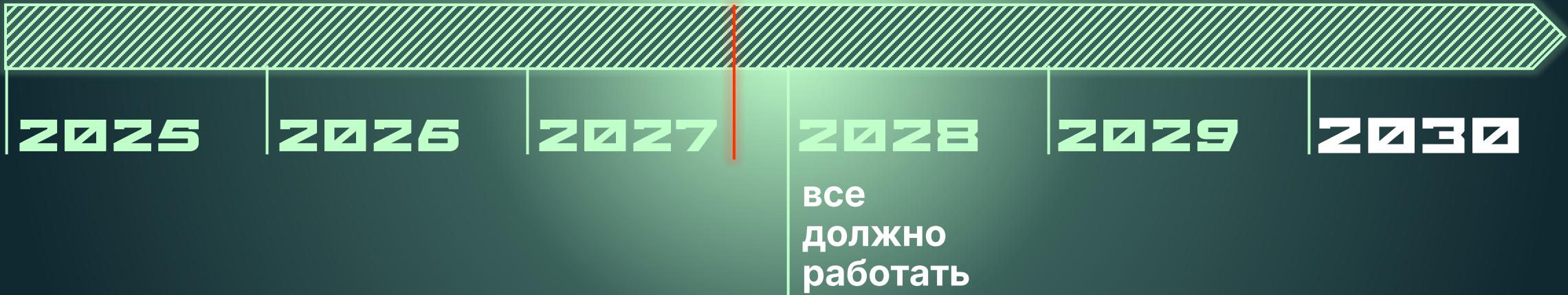


Рабочая группа №3

РЕЕСТР ДОВЕРЕННЫХ ТЕХНОЛОГИЙ ИИ



!





Рабочая группа №3

План работ 2025

- 1.** Апрель 2025:
Разработка концепции реестра доверенных решений искусственного интеллекта
- 2.** Июнь 2025:
Формирование списка функциональных и нефункциональных требований
- 3.** Август 2025:
Разработка проекта технического задания
- 4.** Декабрь 2025:
Проектирование реестра доверенных решений искусственного интеллекта

Реестр доверенных технологий ИИ



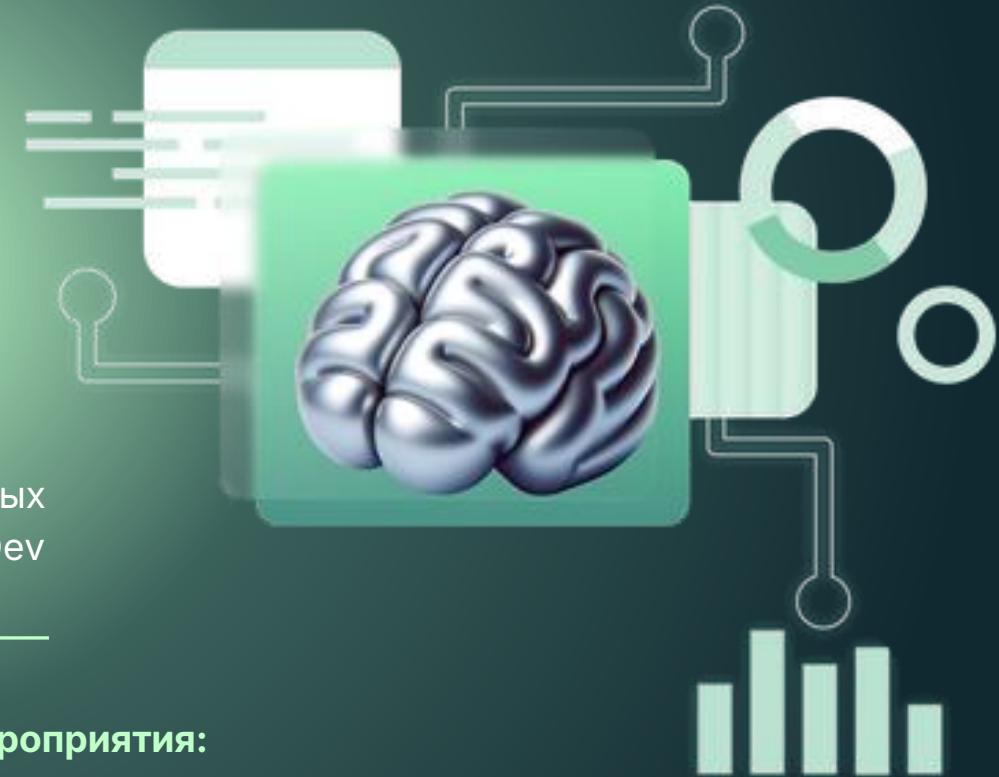
Результаты 1-2 кварталы 2025

4. Разработан драфт архитектуры реестра,
выделены блоки для описания функциональных,
нефункциональных требований

3. Разработан проект **Концепции реестра
доверенных решений ИИ**
Передан в Консорциум на рассмотрение

2. Проведен анализ предложений, сформированных
командами на мероприятиях, проведены CustDev
(проблемные интервью) стейкхолдеров

1. Организованы и проведены мероприятия:
Форсайт и стратегическая сессия для
формирования образа будущего реестра



Реестр доверенных технологий ИИ

ЗАДАЧИ 2-3 кварталы 2025



1. Формирование списка функциональных требований

до 30.06.2025

2. Формирование списка нефункциональных требований

до 30.06.2025

3. Формирование списка требований к безопасности, доступности, масштабируемости, совместимости с существующими системами

до 30.06.2025

4. Описание архитектуры системы

до 30.06.2025

5. Функциональная схема системы (описание потоков)

до 31.07.2025

6. Выбор технологий и инструментов

до 31.08.2025

7. Разработка проекта технического задания

до 31.08.2025

8. Разработка MVP архитектуры реестра

до 30.09.2025



Взаимодействие с РГ

Матрица угроз и продукты ИБ

Матрица угроз безопасности при разработке ПО с применением моделей

Анализ уязвимостей и решения Газинформсервис для различных этапов жизненного цикла разработки

О матрице угроз
Матрица представляет собой структурированный подход к анализу потенциальных угроз безопасности на всех этапах разработки информационной системы или приложения, в которое интегрирован искусственный интеллект. Для каждой угрозы предлагаются соответствующие решения от Газинформсервиса, направленные на минимизацию рисков и обеспечение надежности системы.

Фильтр по этапам разработки

Все этапы Описание бизнес-задачи и разработка ТЗ Сбор данных Предобработка и очистка Разметка Извлечение признаков
Обучение модели Тестирование Разработка ПО Мониторинг, эксплуатация и поддержка модели Вывод из эксплуатации

Всего угроз: **61** Этапов разработки: **10** Доступно решений: **141**

Поиск по названию угрозы или ID...

Сводную по всем продуктам и методикам делаем совместно с консорциумом

Рабочая группа №3

Участники рабочей группы

Руководитель РГ:

к.т.н. Виткова Л. А.

Начальник
аналитического центра
кибербезопасности
Газинформсервис

АНО«НТЦ ЦК»

ООО «Газинформсервис»

Код безопасности

СПб ФИЦ РАН

Swordfish-security

ИТ Бастион

ФОНД ФСРБИТ

РТУ МИРЭА

ФГБУН ИСП РАН

АО «Позитив Текнолоджиз»

GIS ГАЗИНФОРМ
СЕРВИС

