



# Национальная Банковская Премия



Информационная безопасность

Инструмент управления  
зрелостью технологий ИТ и КБ  
«Цифровой фундамент»





Сегодня **любая организация** фактически зависит от своих ИТ-систем и уровня киберзащиты.

Цифровая трансформация развивается стремительно, новые угрозы появляются постоянно, а бизнес всё больше полагается на устойчивость ИТ и безопасность данных.

**Важно не просто внедрять современные решения, а понимать, на каком уровне зрелости мы находимся сейчас, какие сильные стороны уже есть и где существуют пробелы.**

Оценка зрелости перестает быть академическим упражнением.

Она становится **практическим инструментом**, от которого напрямую зависит **устойчивость бизнеса** и его способность адаптироваться.





# «ЦИФРОВОЙ ФУНДАМЕНТ»

Инструмент управления  
зрелостью ключевых  
технологий ИТ и  
кибербезопасности,  
процессов и соответствия  
регуляторным требованиям

## ПРЕДПОСЫЛКИ РАЗРАБОТКИ ИНСТРУМЕНТА

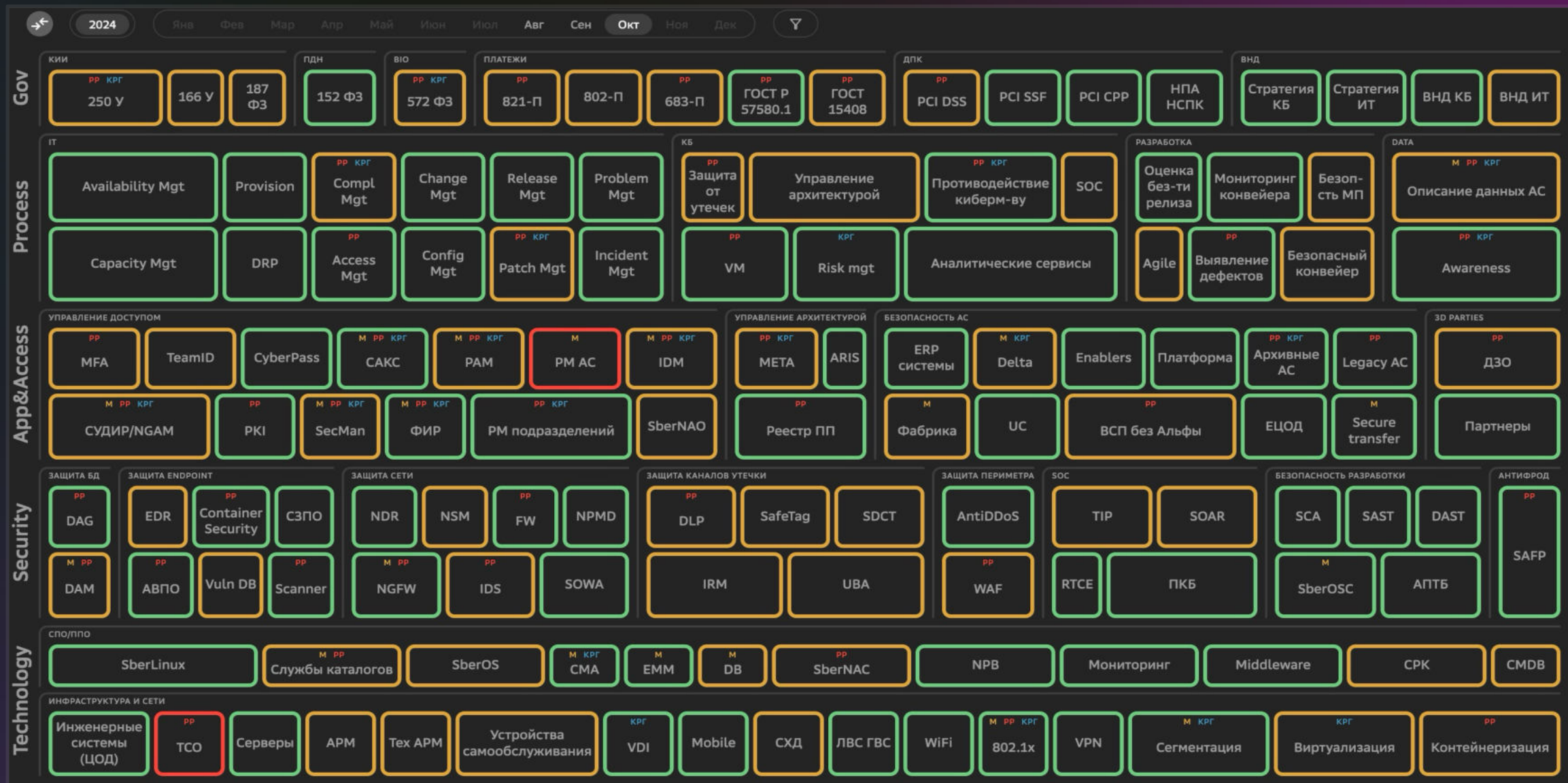
- **Фрагментарность существующих подходов** – ИТ и КБ оцениваются отдельно, что мешает комплексно видеть уровень зрелости технологий и их взаимное влияние
- **Проблема измеримости и сопоставимости** – разные подразделения и эксперты по-разному трактуют уровни зрелости, что снижает объективность и мешает корректному сравнению
- **Разрозненность ведения задач** – задачи распределены между подразделениями, а их результаты остаются локальными, что препятствует прозрачности и согласованной работе
- **Ограниченность практической ценности** – часто готовые модели дают статическую оценку «где мы находимся», но не формируют дорожную карту развития «куда и как двигаться»
- **Потребность в масштабируемости и гибкости** – изменение архитектуры ИТ-ландшафта, появление новых технологий КБ и ИТ должны органично встраиваться в существующий подход
- **Мониторинг динамики** – существующие подходы слабо поддерживают регулярную переоценку и отслеживание прогресса



# «Цифровой фундамент»



\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании



низкий уровень зрелости

0-54%

средний уровень зрелости

55-85%

высокий уровень зрелости

86-100%

# Используемые подходы к оценке уровня зрелости элементов



## Слой Government

- **Соответствие требованиям** – оцениваем процент исполнения требований
- **Условие соответствия** – указываем пороговые значения, достижение которых достаточно для прохождения аудитов

## Слой Process

- **Правила** – оцениваем наличие и актуальность процесса
- **Исполнение** – показываем исполнение целевых показателей и метрик процесса
- **Отчётность** – оцениваем полноту отчётности по метрикам процесса
- **Автоматизация** – оцениваем процент автоматических операций и использование AI технологии

## Слои Technology, Cybersecurity, Apps & Access

- **Правила** – определяем требования КБ и ИТ к оцениваемой технологии, продукту, автоматизированной системе
- **Процессы** – определяем процессы, применимые к конкретному элементу и процессы, в которых реализуются заданные требования. Есть обязательные:
  - ITSM процессы
  - SOC процессы
  - Компетенция команды
- **Технологии** – оцениваем функциональность элемента: проводим сравнение с лидерами отрасли, оцениваем текущее состояние
- **Покрытие** – показываем охват и покрытие технологией инфраструктуры компании

# Кирпичик «Цифрового фундамента»



## Площадки контроля:

- М** Инициатива Метла
- РР** Риск Радар
- КРГ** Комитет по рискам Группы

## Уровни зрелости:

86-100%	Высокий
56-85%	Средний
0-55%	Низкий



**Методика оценки уровня зрелости**



**План достижения целевого уровня зрелости**

# Пример оценки уровня зрелости



\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании

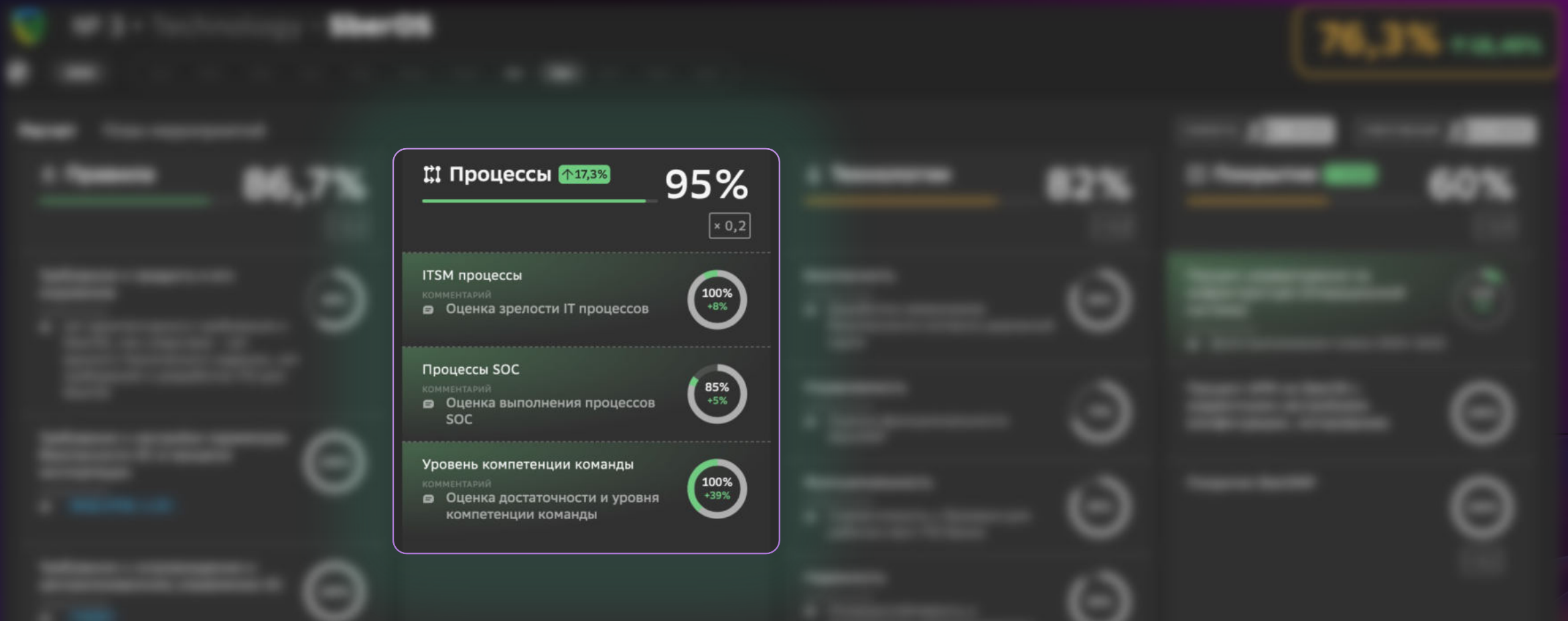
# Пример оценки уровня зрелости



■ Определяем требования КБ и ИТ к оцениваемой технологии, продукту, автоматизированной системе

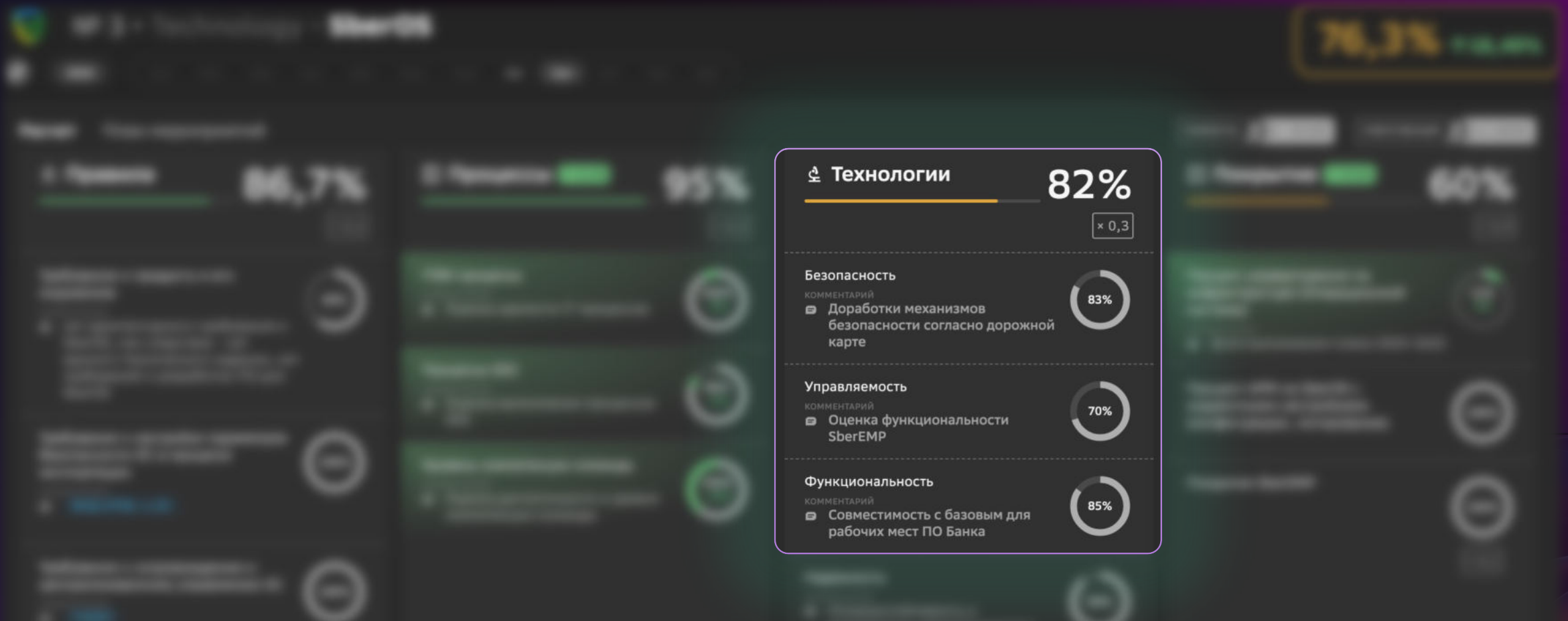
\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании

# Пример оценки уровня зрелости



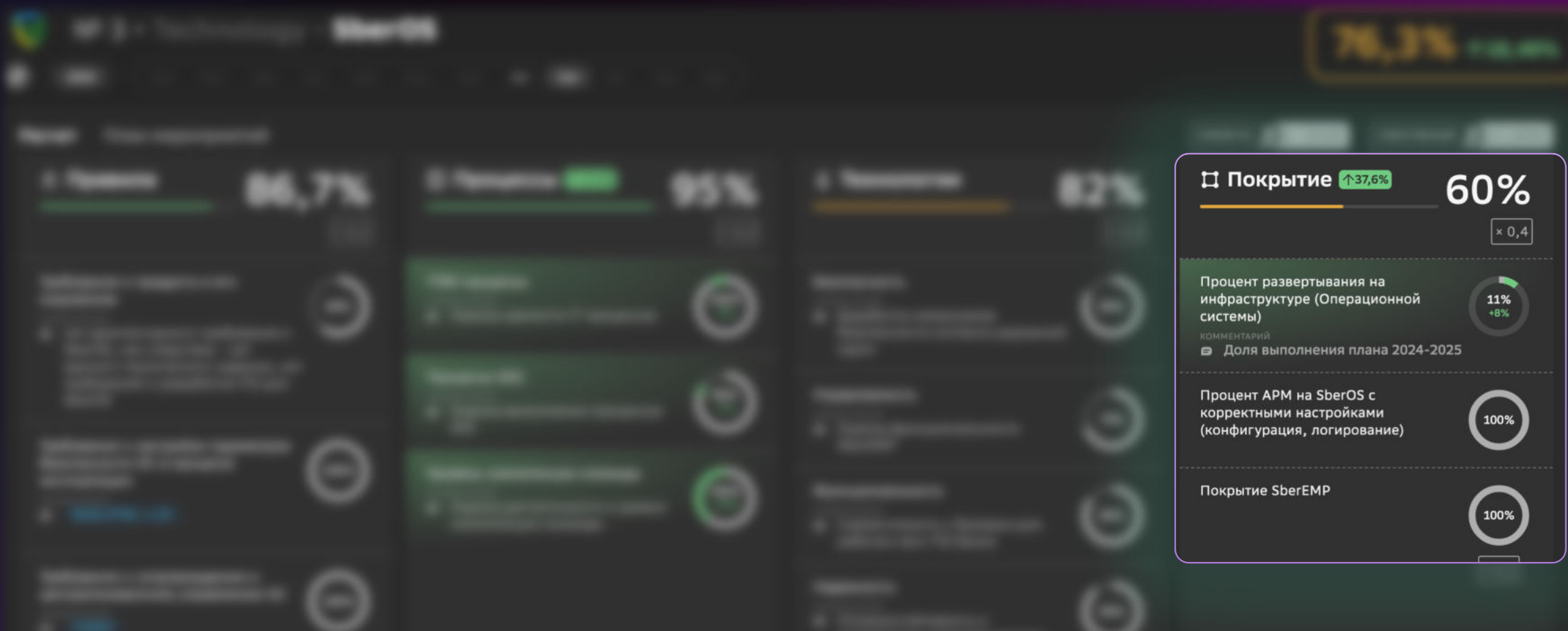
■ Определяем процессы, применимые к конкретному элементу и процессы, в которых реализуются заданные требования

# Пример оценки уровня зрелости



■ Оцениваем функциональность элемента: проводим сравнение с лидерами отрасли, оцениваем текущее состояние

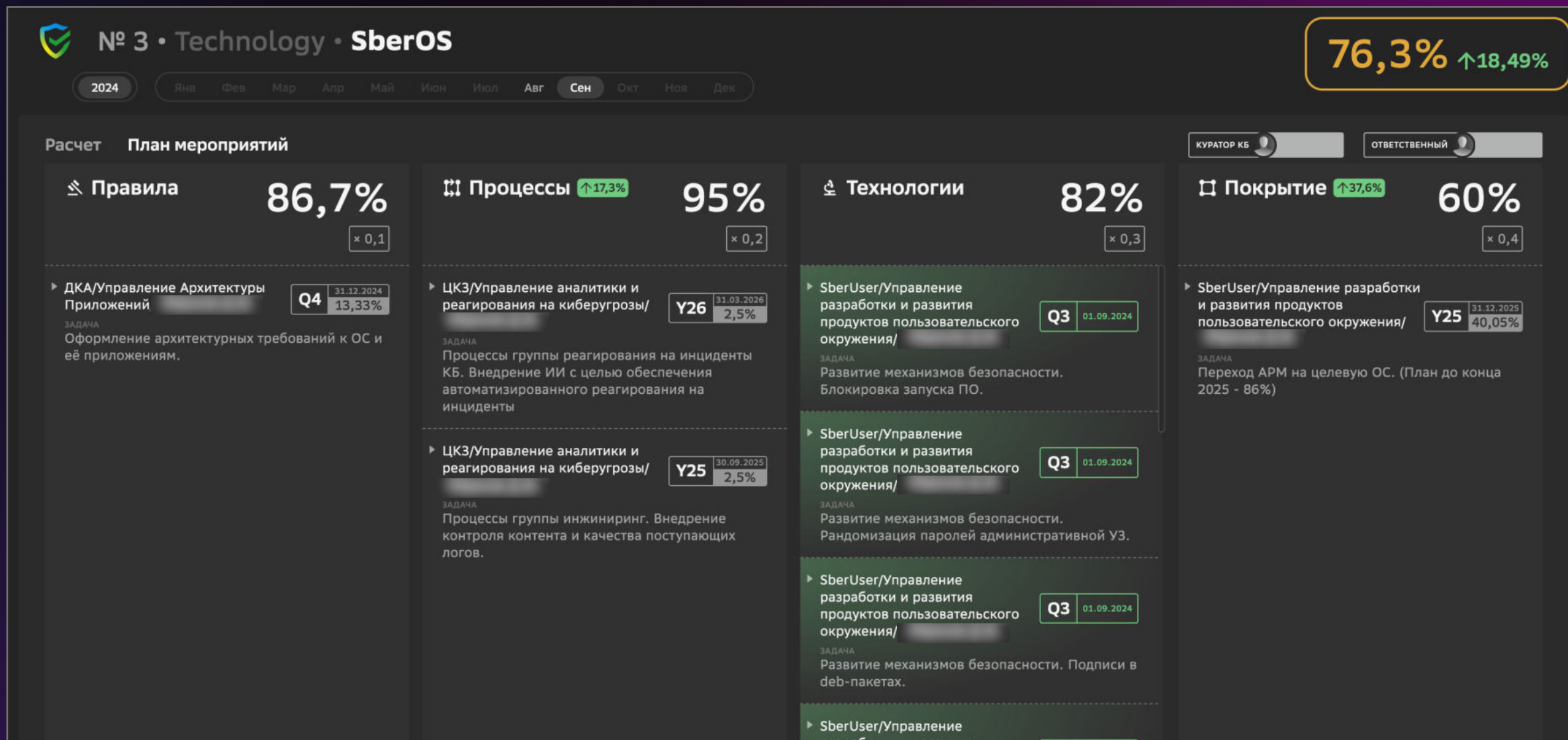
# Пример оценки уровня зрелости



■ Показываем охват и покрытие технологией инфраструктурой Банка

\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании

# План мероприятий по достижению уровня зрелости

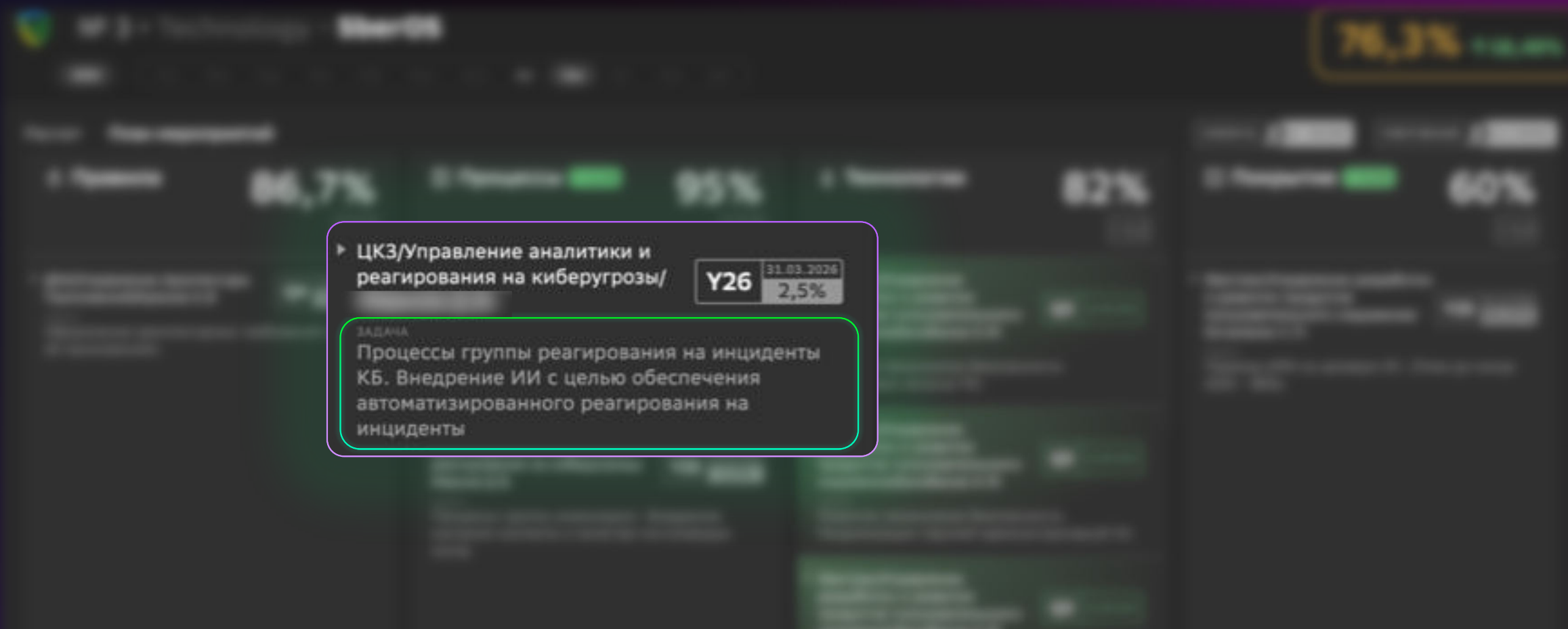


\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании

# План мероприятий по достижению уровня зрелости



\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании

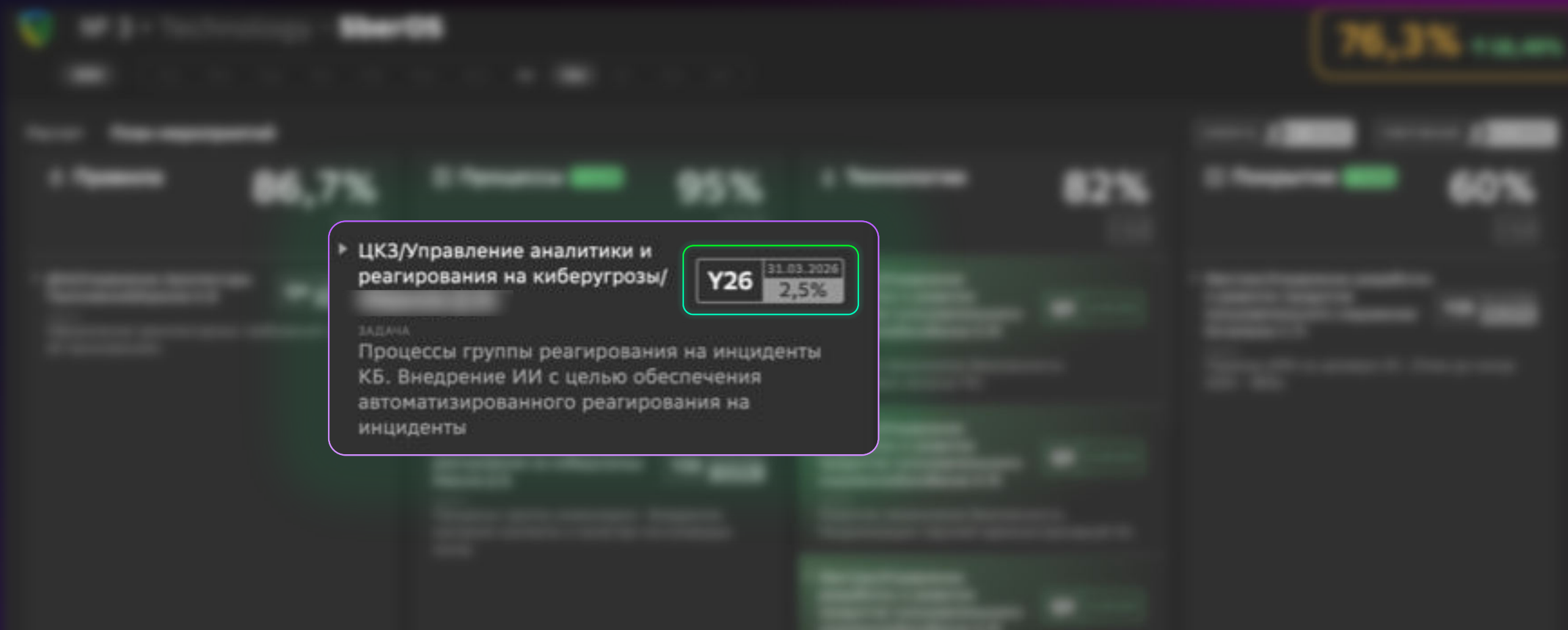


- По всем метрикам в доменах, которые не достигли целевого уровня зрелости, сформированы задачи

# План мероприятий по достижению уровня зрелости



\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании

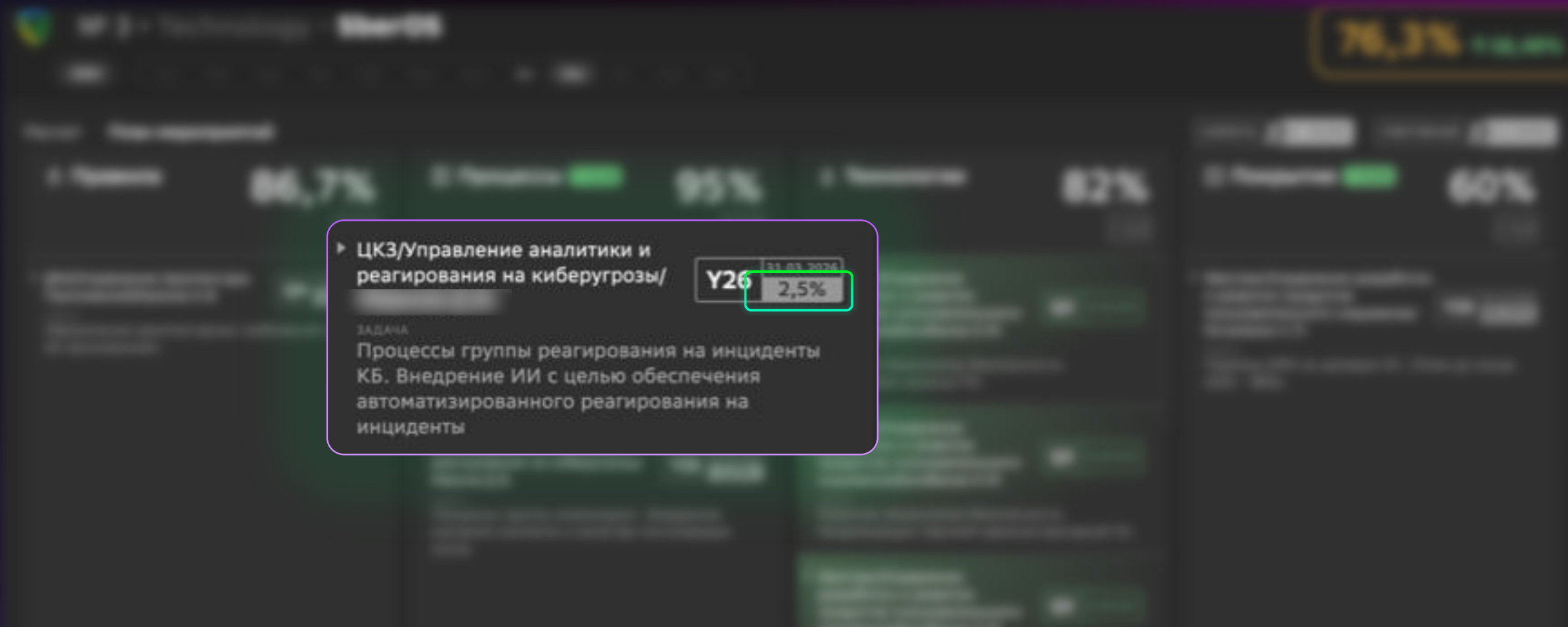


- По каждой задаче назначен ответственный и определен срок её выполнения

# План мероприятий по достижению уровня зрелости



\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании

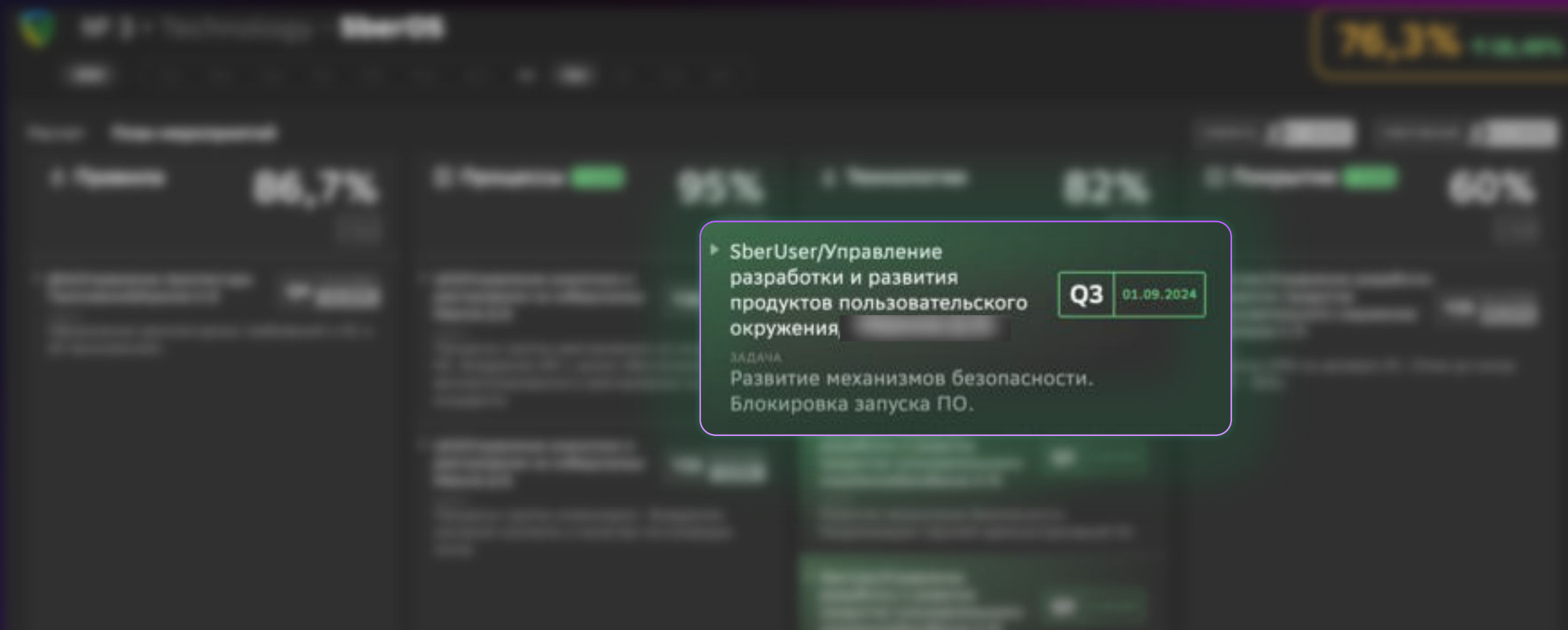


■ Каждая задача имеет свой вес, который повышает зрелость домена при её выполнении

# План мероприятий по достижению уровня зрелости



\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании



■ Фиксируется выполнение, просрочка или перенос сроков по задачам

# Динамика изменения уровня зрелости



\*Данные носят демонстрационный характер и не отражают реальную ситуацию в компании



низкий уровень зрелости

0-54%

средний уровень зрелости

55-85%

высокий уровень зрелости

86-100%

# «ЦИФРОВОЙ ФУНДАМЕНТ» Результаты и эффекты



- Формирование целостной картины зрелости ключевых технологий ИТ и КБ, процессов, нормативных и регуляторных требований.

- Повышение управляемости. Все задачи собраны в едином инструменте, контролируются централизованно и используются для постановки целей.

- Прозрачность статуса инициатив и взаимосвязей задач между смежными подразделениями.

- Снижение рисков кибербезопасности за счёт своевременного выявления проседающих зон.

- Партнерство. Кибербезопасность и ИТ работают как равноправные участники в одном инструменте для достижения совместного результата.

- Вовлечение бизнеса через понятный визуальный язык.

- Возможность использования как best-practice для других компаний.

