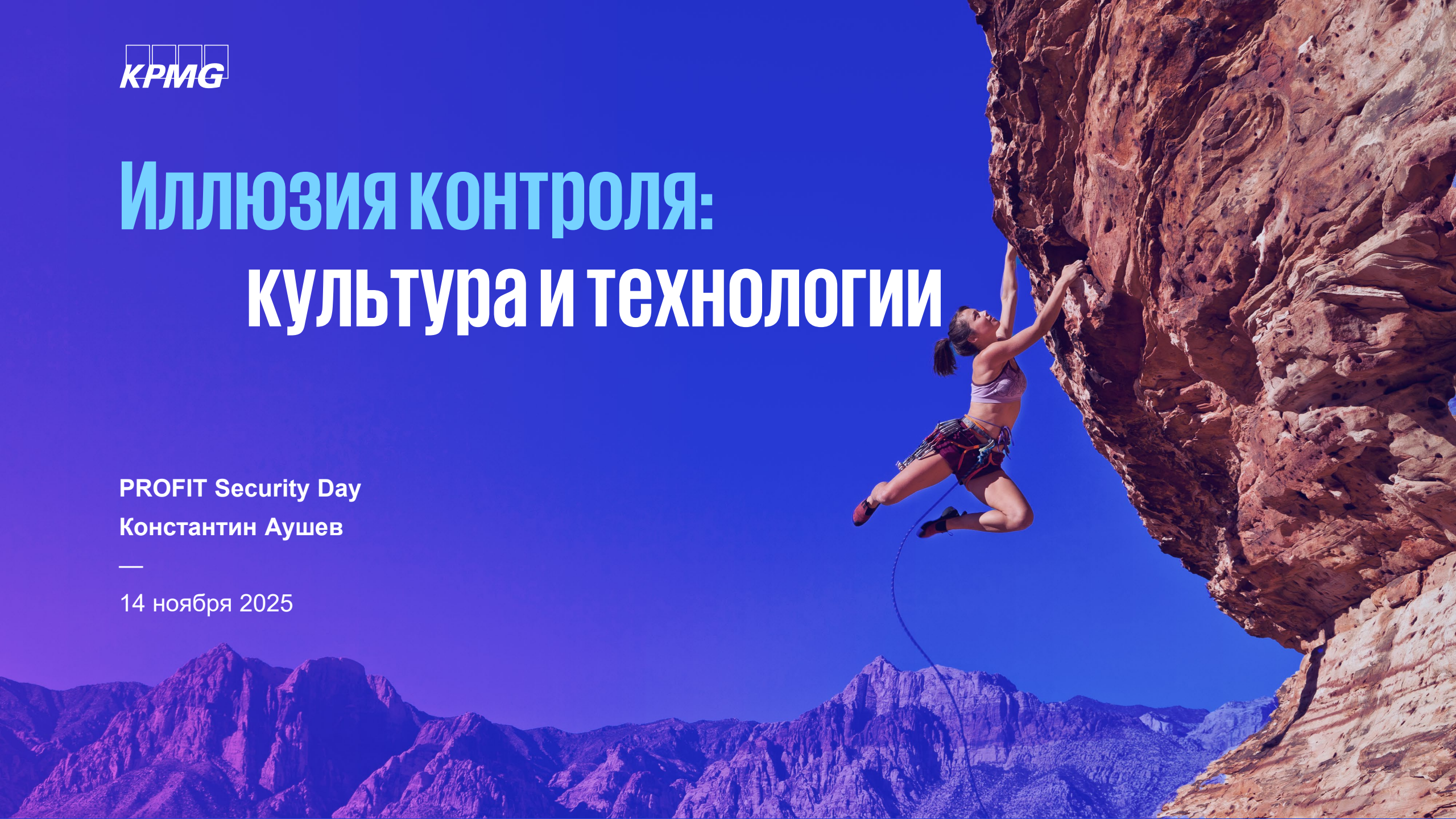
KPMG

Иллюзия контроля: культура и технологии



PROFIT Security Day

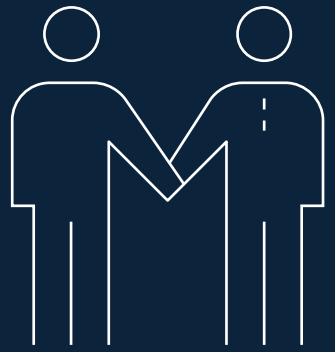
Константин Аушев

—

14 ноября 2025

Роль в организации – главный вопрос для CISO в 2025*

...2020

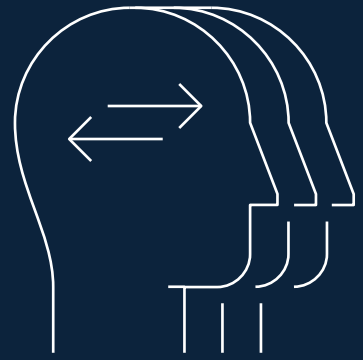


Доверенный партнер и советник

...

…обеспечивающий стратегическое преимущество бизнесу

2025...

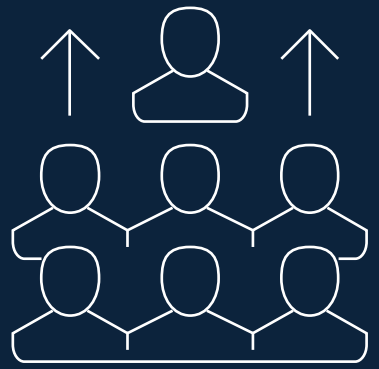


…с постоянно растущей зоной ответственности…

*Согласно KPMG Cybersecurity Considerations, 2025.

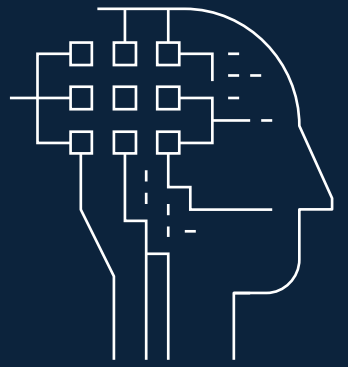
76% ожидают новые успешные виды атак в 2025–2028

Цифровая идентификация



Человеческие возможности

Готовность к восстановлению



Доверие в эпоху ИИ

Киберриски – ТОП 1 беспокойство при внедрении ИИ для 85%

...

chat bots

deep fakes

prompt hoping

prompt injection

conversational fatigue

AI explainability

ethics

...

74%

считают, что исключительно киберкультура определяет безопасность использования ИИ

3 из 5

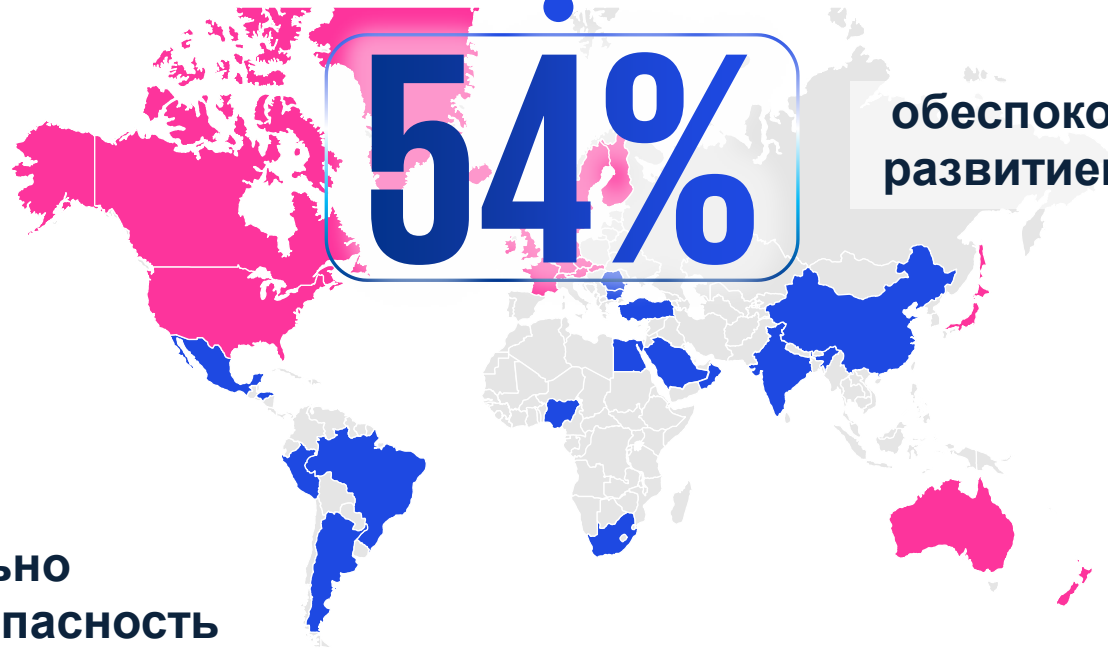
не склонны доверять

склонны доверять

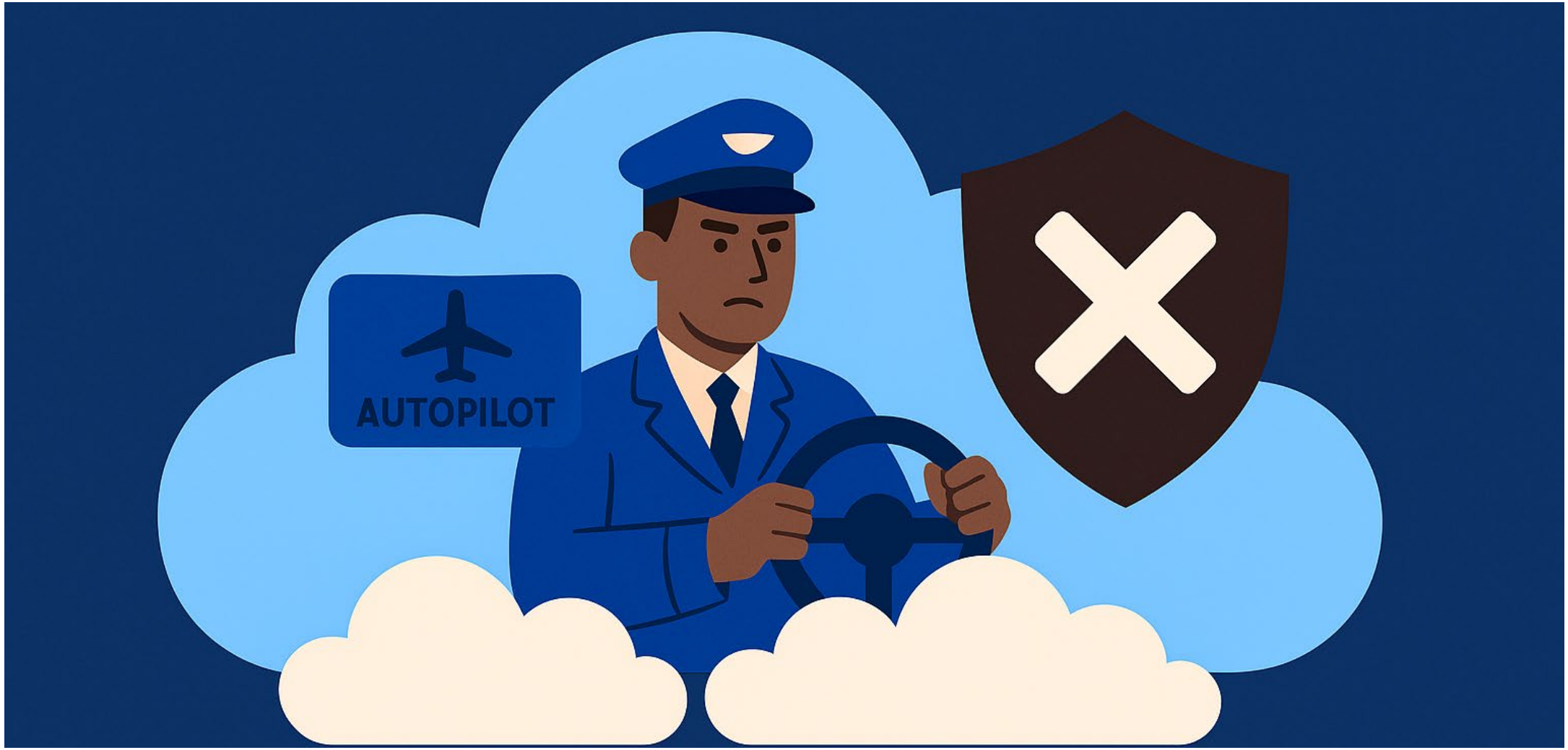
ИИ-системам

54%

обеспокоены развитием ИИ



Zero Trust и облака



«Человеческий фактор» может быть не самым слабым, а самым сильным звеном в системе киберзащиты

Ad-hoc: информационная безопасность – критерий для систем; для сотрудников бывают тренинги

Определенный: менеджмент определил критерии безопасного поведения сотрудников; помимо тренингов, есть дополнительные упражнения

Управляемый: формальный подход к киберкультуре с выделением ответственных и позиционированию тона «сверху»

Развитый: кибербезопасность – приоритет для топ-менеджмента, сотрудники активно вовлекаются в развитие кибербкультуры

Динамичный: все сотрудники не только активно вовлекаются в киберповестку, но и сами проактивно предлагают инициативы, направленные на повышение киберустойчивости

Меньше половины компаний пытаются оценить уровень киберкультуры

78% CISO беспокоятся, что сотрудники используют ИИ как «черный ящик». 78% сотрудников будут больше доверять ИИ, если будут внедрены механизмы контроля его работы.

Честность
Исключение смещенных оценок из-за субъективности отдельных людей или их групп

Прозрачность
Обеспечение возможности указания необходимых раскрытий для понимания стейкхолдерами принципов работы алгоритмов ИИ

Объяснимость
Возможность понять, как и почему решения ИИ сгенерировали те или иные рекомендации

Ответственность
Встроенные механизмы мониторинга на всем цикле работы ИИ для управления рисками и обеспечения регуляторного соответствия

Защита данных
Механизмы защиты от неавторизованного доступа, злоумышленников, подложных данных, повреждения данных и систем

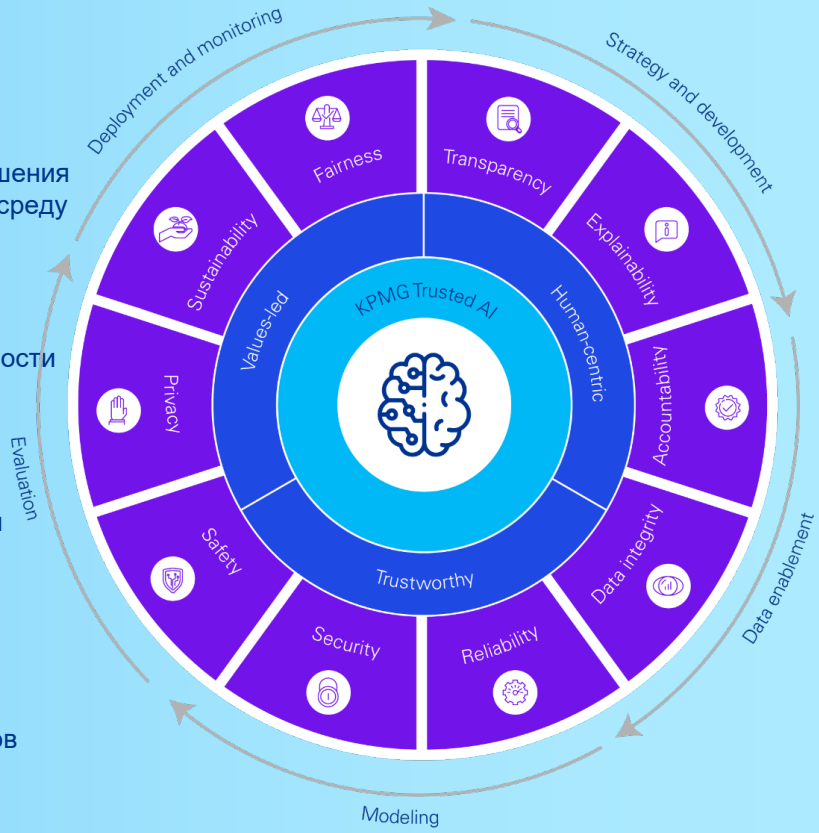
Приватность
Обеспечение соответствия локальному и международному законодательству в области персональных данных

Устойчивость
Оптимизация решений ИИ с целью уменьшения негативного воздействия на окружающую среду

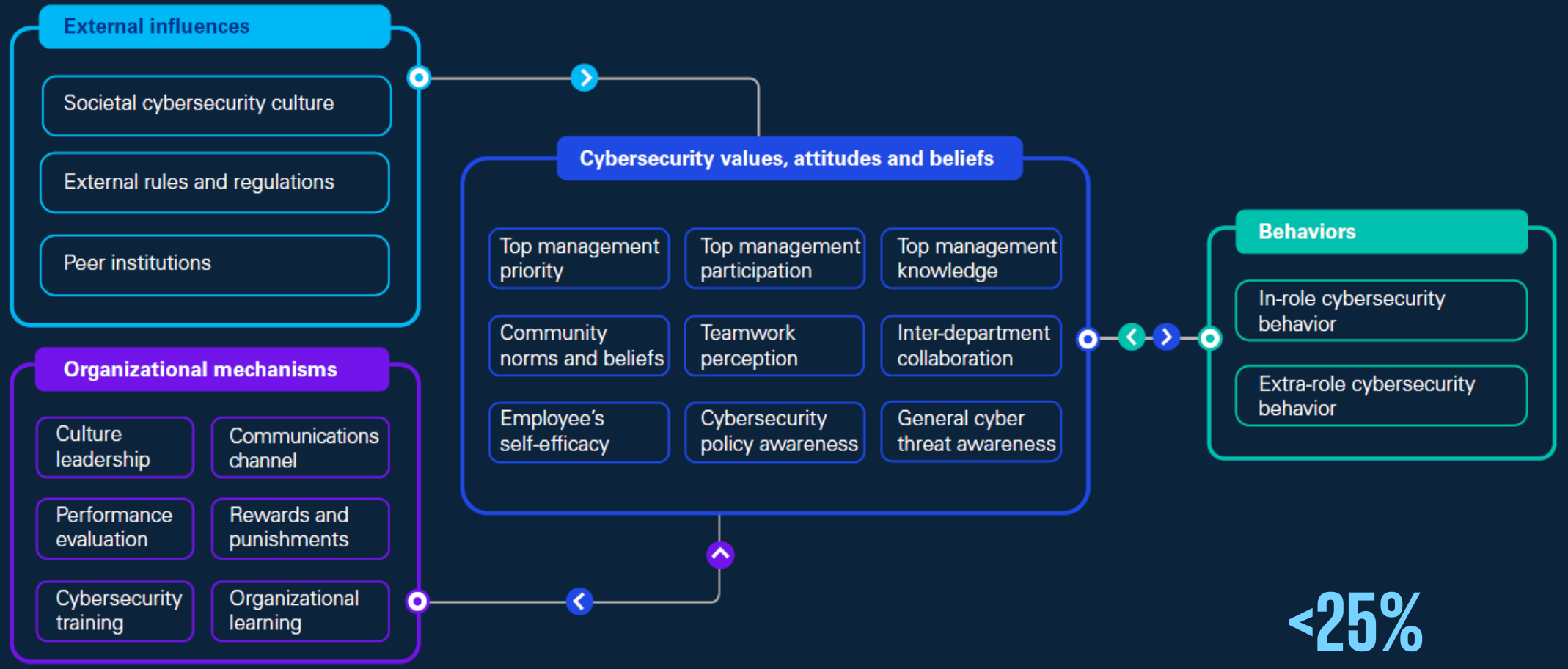
Целостность данных
Обеспечение качества данных, управляемости данных, доверия к данным

Надёжность
Обеспечение заданного уровня точности и консистентности в работе ИИ

Личная безопасность
Механизмы защиты в решениях ИИ от потенциального вреда для людей и активов бизнеса



CAMS Cybersecurity Culture Model



This framework is used with permission of MIT CAMS and Dr. Keri Pearlson.

<25%

CISO не могут выровняться по приоритетам с CEO

ИИ для развития киберкультуры

- **Создание персонализированных тренингов и микросеминаров на темы классификации данных, обнаружения дипфейков, фишинга и т. д.**
- **Автоматизация тестовых фишинговых кампаний**
- **Постоянный анализ поведенческих данных пользователей**
- **Перевод рискованных действий на агентский ИИ**
- **Квантификация «человеческого фактора» на уровне отдельных сотрудников, групп, отделов**
- **Чатботы для консультаций по вопросам кибербезопасности**
- **Геймификация процессов реагирования на киберинциденты**

kpmg.kz

Document Classification: KPMG Public