KPMG

Cybersecurity Can't Keep Up: технологии масштабируются быстрее, чем контроль

PROFIT SECURITY DAY

Константин Аушев

Ноябрь 2026

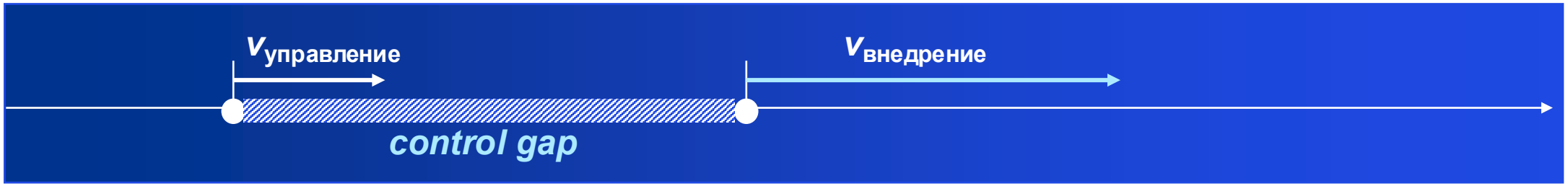
Control Gap: 53% внедряют, 25% контролируют, 1% централизуют управление

	ИИ в промышленной эксплуатации	Формальная стратегия ИИ	Управление ИИ
	53%	34%	25%
	24%	76%	69%

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services toclients. All rights reserved.

Источник: *Глобальный технологический отчёт KPMG 2026*

Control Gap: 53% внедряют, 25% контролируют, 1% централизуют управление



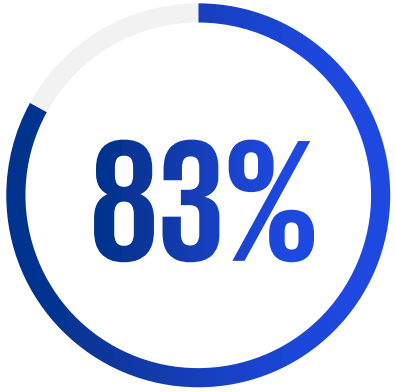
	ИИ в промышленной эксплуатации	Формальная стратегия ИИ	Управление ИИ
	53%	34%	25%
	24%	76%	69%

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services toclients. All rights reserved.

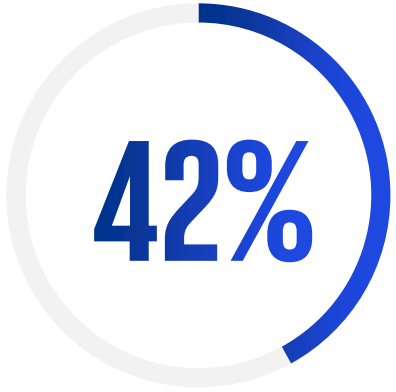
Источник: Глобальный технологический отчёт KPMG 2026

Больше автоматизации. Больше атак.

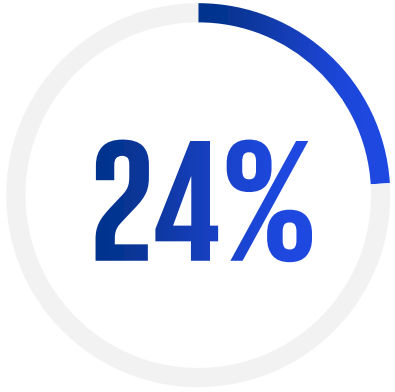
Разрыв в исполнении: бюджеты на кибербезопасность растут, а операционная модель остаётся реактивной, фрагментированной и трудно доказуемой.



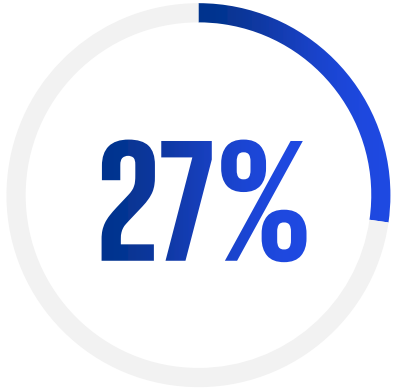
сообщили о росте числа кибератак



не могут продемонстрировать советам директоров отдачу от кибербезопасности



полностью интегрировали ИИ в кибербезопасность



активно внедряют постквантовую криптографию

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services toclients. All rights reserved.

Источник: Исследование KPMG 2026 по рискам кибербезопасности и технологий

От контроля за доступом к контролю за разрешениями



Кто?

Откуда?

Куда?

С какой ролью?

Кто или что?

С какими разрешениями/ полномочиями?

С правом принятия каких решений?

С какими ограничениями?

Кто и где останавливает процесс?

50% Количество Non-Human Identities уже превышает количество живых пользователей

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services toclients. All rights reserved.

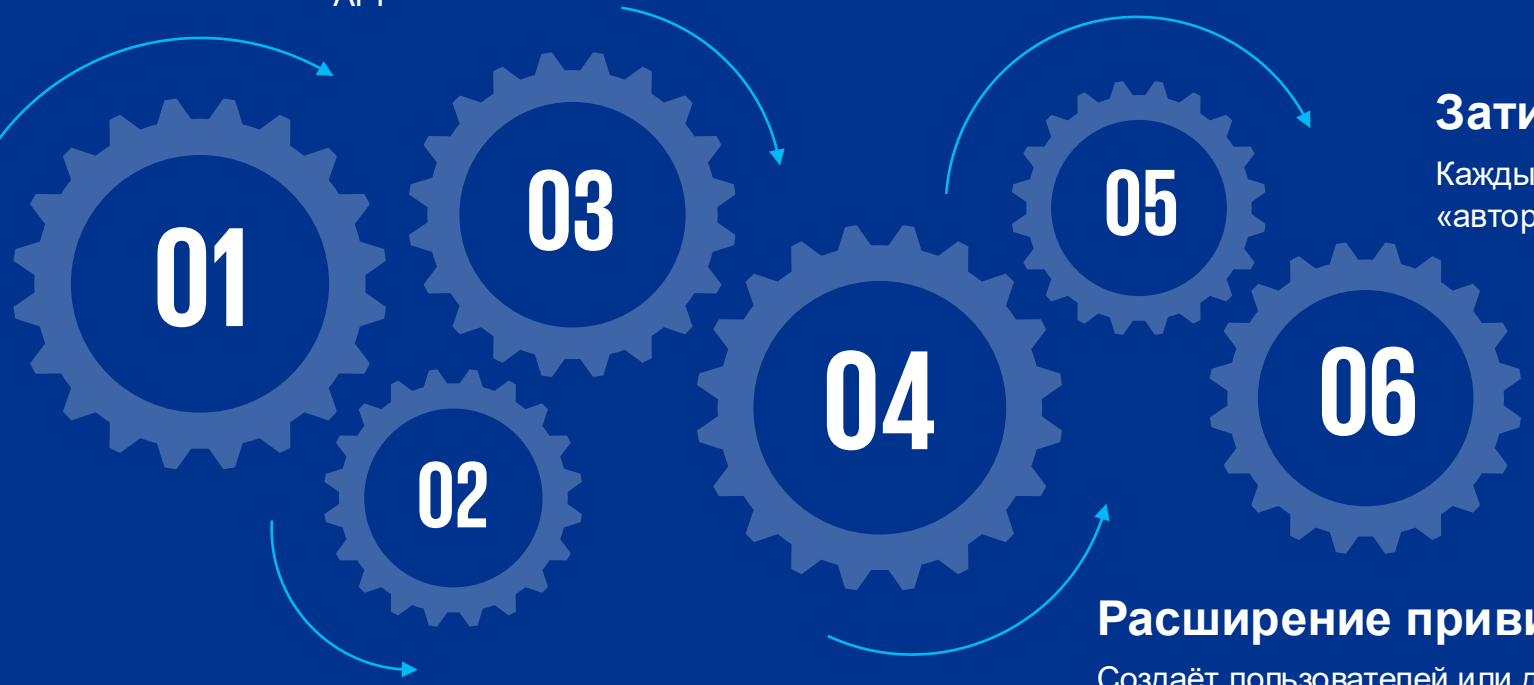
Инцидент становится разрешенным действием

Prompt injection

Агент принимает вредоносную инструкцию

Вызов инструментов

Обращается к почте, файлам, CRM и API



Унаследованный доступ

Использует идентичность сотрудника или сервисной учётной записи

Бизнес-действие

Изменяет запись, платёж или политику

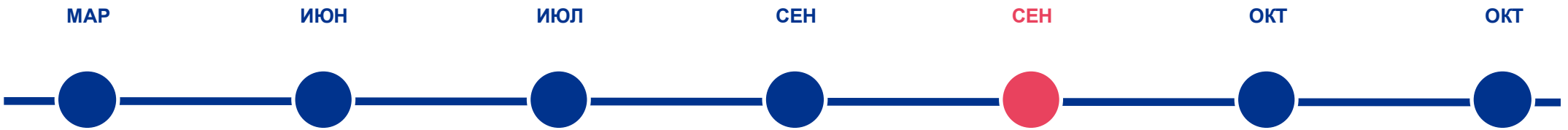
Расширение привилегий

Создаёт пользователей или делегирует доступ

Затирание логов

Каждый шаг выглядит «авторизованным»

Паттерны кибербразведки: учётные данные, интеграции, обновления, третьи стороны, инструменты разработки



МАР — Кража учётных данных VPN через SEO-отравление

ИЮН — Доверенные обновления ПО использованы как оружие

ИЮЛ — Ransomware через ПО поставщиков

СЕН — Платёжные сети под угрозой мошенничества

СЕН — Семь RAT нацелены на госорганы Центральной Азии

ОКТ — Таргетированные атаки через Outlook и OneDrive

ОКТ — Встраивание троянов в проекты Visual Studo

СИСТЕМЫ ИДЕНТИФИКАЦИИ, ХРАНИЛИЩА ПАРОЛЕЙ

ЦЕПОЧКИ ПОСТАВОК / ТРЕТЬИ СТОРОНЫ / СТОРОННИЕ СЕРВИСЫ

ОТРАСЛЕВЫЕ АТАКИ

ИНСТРУМЕНТЫ РАЗРАБОТКИ (CI/CD, центры обновления)

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services toclients. All rights reserved.

Источник: Платформа кибербразведки KPMG, архив рекомендаций 2026

Регуляторные риски

DORA

NIS2

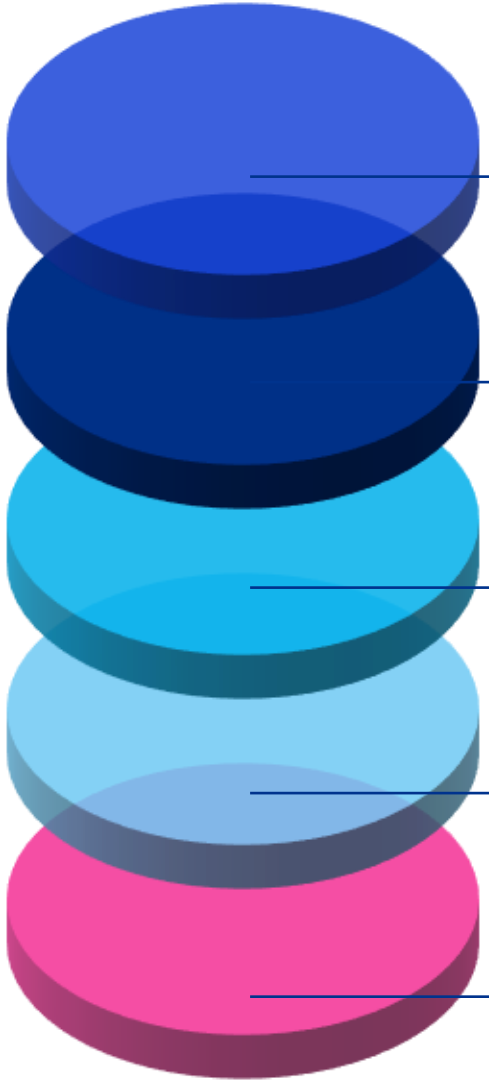
EU AI Act

Cyber Resilience Act

Закон «Об ИИ»

Цифровой кодекс

НПА НБ РК



01 OWN IT

Кто отвечает?

02 KNOW IT

Какие сервисы-агенты-сущности имеются и как взаимосвязаны

03 LIMIT IT

Как ограничиваются полномочия и потенциальный ущерб?

04 PROVE IT

Действительно ли средства контроля сработали?

05 RECOVER IT

Как продолжить сервисы после инцидента?

KPMG

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services toclients. All rights reserved.

Пять вопросов на ближайшие 90 дней



01 Идентичность

Можем ли мы назвать каждую привилегированную неличную идентичность и её владельца?



02 Полномочия

Можем ли мы рассчитать максимальный радиус поражения одного агента? Можем ли убрать все существующие бессрочные полномочия?



03 Локализация

Можем ли мы изолировать критичного поставщика без остановки сервиса? Можем ли доказать containment при компрометации сервисного токена или ID агента?



04 Восстановление

Можем ли мы восстановить критические сервисы в заданные сроки?



05 Совет директоров

Можем ли мы показать снижение риска, а не активность в безопасности?

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services toclients. All rights reserved.


KPMG