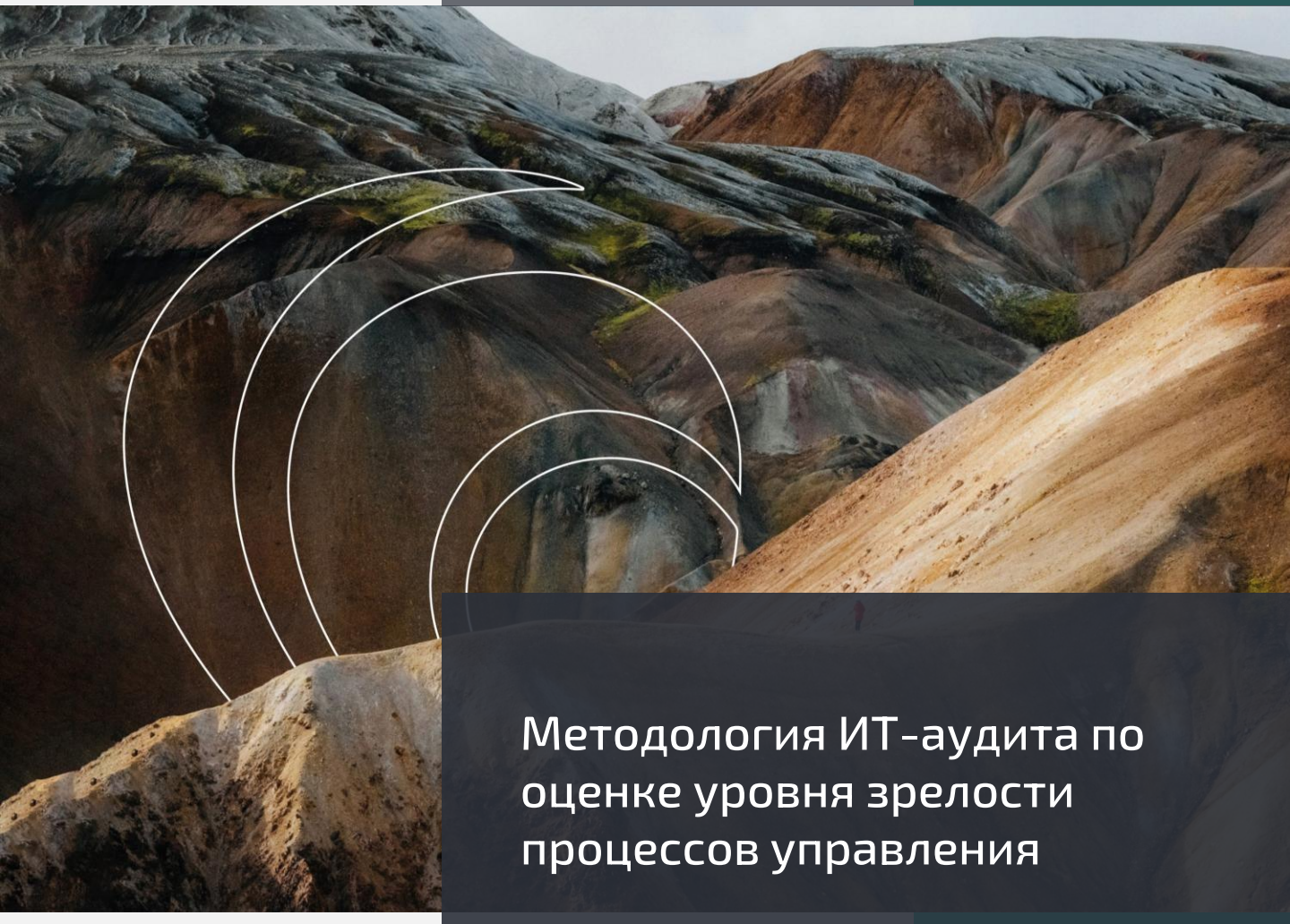
bakertilly

WHITEPAPER



Методология ИТ-аудита по оценке уровня зрелости процессов управления

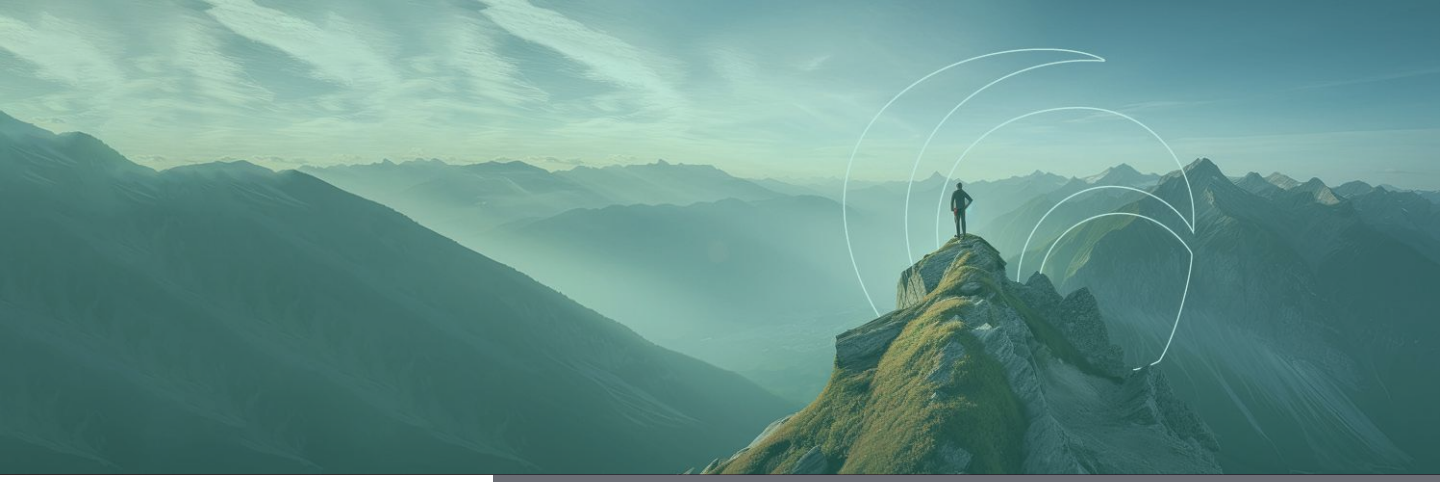
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Новые вызовы, основные отличия от методологии 2017, ключевые подходы трансформации

2025

СОДЕРЖАНИЕ



АНАЛИЗ КЛЮЧЕВЫХ ТРЕНДОВ

Прежняя методология устарела в первую очередь из-за ускоренного развития технологий и угроз, которые вышли за рамки традиционной ИБ. С 2017 по 2025 год ландшафт кибербезопасности претерпел значительные изменения: количество атак на критическую инфраструктуру выросло в разы, а угрозы стали более сложными, включая цепочки поставок и ИИ-генерированные атаки. Например, эволюция от простых нарушений инфраструктуры к управлению восприятием и непрерывным операциям, как отмечается в анализах стратегий кибератак, требует более интегрированного подхода[1]. Регуляторные требования также ужесточились: введение GDPR в 2018 году, NIS2 в ЕС и аналогичных норм в других регионах подчеркнуло необходимость комплексного управления, включая данные и ИИ.

Одним из ключевых факторов устаревания является интеграция ИИ в ИТ и ИБ. К 2025 году ИИ стал неотъемлемой частью[2] как угроз (автономные атаки), так и защит (автономные агенты и этическое управление). Старая модель не учитывала эти аспекты, фокусируясь на реактивных мерах, в то время как современные тренды требуют проактивного подхода, включая модели зрелости для ИИ в кибербезопасности. Кроме того, рост облачных технологий, edge computing и квантовых угроз сделал необходимым расширение на ИТ-управление, где ИБ интегрируется с общим управлением активами и проектами[3]. Наконец, глобальные программы, подобные тайваньской Национальной программе кибербезопасности (2017–2020), продемонстрировали переход к моделям, где квалицированная оценка сочетается с аудитом и стратегическим планированием, что подчёркивает пробелы в старой методологии[4]. Помимо глобальных трендов, в Кыргызстане отмечается активизация Кабинета министров, Агентства по защите персональных данных, Национального банка, которые также обновили требования к ИТ-аудиту и информационной безопасности, демонстрируя стремление к дальнейшему совершенствованию регуляторного воздействия [5, 6, 7, 8].

В целом, прежняя методология стала «старой» не из-за неэффективности, а из-за несоответствия современным реалиям: она была ориентирована на изолированную ИБ, в то время как текущие тренды требуют целостной интеграции ИТ и ИБ для обеспечения устойчивости и соответствия требованиям.

[1] Digital frontlines: What the 12-day war revealed about the evolution of Iran's cyber strategy — https://mei.edu/publications/digital-frontlines-what-12-day-war-revealed-about-evolution-irans-cyber-strategy

[2] The state of AI: How organizations are rewiring to capture value — https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

[3] New cyber security trends for 2025 — https://cds.thalesgroup.com/en/hot-topics/new-cyber-security-trends-2025

[4] National Cyber Security Program of Taiwan https://globaltaiwan.org/2025/07/advancing-cyber-resilience-taiwans-strategic-shift

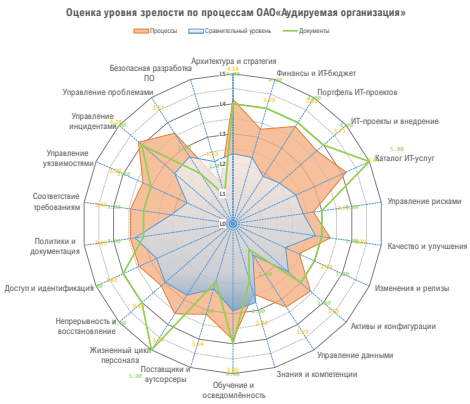
[5] Стратегия защиты киберпространства в Кыргызстане — https://digital.gov.kg/activities/strategiya-zashhity-kiberprostanstva-v-kyrgyzstane/

[6] Итоги деятельности Госагентства по защите персональных данных за 2024 год — https://dpa.gov.kg/ru/post/192

[7] Положение о требованиях по обеспечение информационной безопасности в коммерческих банках КР — https://nbkr.kg/contout.jsp?item=103&lang=RUS&material=106323

[8] Положение о минимальных требованиях к внешнему аудиту банков и других финансово-кредитных организаций — https://nbkr.kg/contout.jsp?item=103&lang=RUS&material=122491

НОВАЯ МЕТОДОЛОГИЯ 2025



Обновлённая методология оценки зрелости процессов ИТ и ИБ, внедрённая Baker Tilly в Центральной Азии в 2025 году для практики проведения ИТ-аудитов, представляет собой эволюционный шаг, расширяющий охват на комплексное управление ИТ, включая стратегические, финансовые и операционные аспекты. Она основана на принципах CMMI, ISO 27001 и COBIT 2019, с интеграцией элементов Zero Trust, DevSecOps и AI governance, что позволяет организациям оценивать не только техническую зрелость, но и её влияние на бизнес-результаты.

Ключевые особенности новой методологии

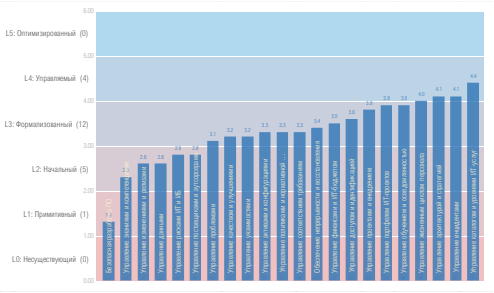
- **Расширение охвата**: включает 22 процесса управления и 70 функциональных подпроцессов, от управления архитектурой и стратегией до безопасной разработки ПО, интегрируя ИБ с ИТ-процессами, такими как управление портфелем проектов и данными.
- **Фокус на стратегии**: подчёркивает вовлеченность руководства, финансовое планирование и непрерывность бизнеса, учитывая современные угрозы, включая квантовые и ИИ-ориентированные. Комплексная оценка процессов по 70 метрикам позволяет руководству организаций принимать взвешенные стратегические решения.
- **Гибкость и масштабируемость**: оценка зрелости проводится по шкале, совместимой с международными стандартами, с акцентом на продолжающееся, постоянное улучшение и адаптацию к регуляционным требованиям.
- **Преимущества**: позволяет организациям лучше адаптироваться к цифровизации, минимизировать риски, инвестировать ресурсы в развитие конкретных областей управления, и повысить эффективность, как подтверждают тренды в глобальных опросах.

Новая модель не заменяет, а дополняет предыдущую, обеспечивая преемственность через специально разработанную математическую модель и трансформационные подходы.

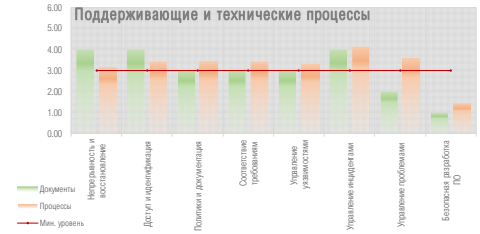
Оценка уровня зрелости по процессам ОАО «Аудируемая организация»

№	Процесс	Сравнительный ур.	Документы	±	Процессы	±
1	Управление архитектурой и стратегией	2.33	4.00	1.67	4.14	1.81
2	Управление финансами и ИТ-бюджетом	2.29	4.00	2.12	3.86	1.98
3	Управление портфелем ИТ-проектов	1.88	4.00	2.69	4.14	1.83
4	Управление проектами и внедрением	2.06	3.00	0.21	3.29	0.50
5	Управление каталогом и уровнями ИТ-услуг	2.31	3.00	1.07	2.43	0.50
6	Управление рисками ИТ и ИБ	2.36	3.00	0.55	3.43	0.98
7	Управление качеством и улучшениями	2.79	1.00	-0.24	3.29	2.04
8	Управление изменениями и релизами	1.93	2.00	-0.73	2.43	-0.30
9	Управление активами и конфигурациями	2.45	4.00	1.09	3.86	0.95
10	Управление данными	1.24	2.00	-0.26	3.14	0.88
11	Управление знаниями и компетенциями	2.73	5.00	2.18	3.57	0.75
12	Управление обучением и осведомленностью	2.91	4.00	1.03	3.14	0.17
13	Управление поставщиками и аутсорсерами	2.26	4.00	1.22	3.43	0.64
14	Управление жизненным циклом персонала	2.82	3.00	-0.29	3.43	0.14
15	Обеспечение непрерывности и восстановления	2.97	3.00	0.93	3.43	1.36
16	Управление доступом и идентификацией	2.78	3.00	1.32	3.29	1.61
17	Управление политиками и нормативной документацией	3.29	4.00	1.45	4.14	1.59
18	Управление соответствием требованиям	2.07	2.00	-0.65	3.57	0.92
19	Управление уязвимостями	1.68	1.00	-1.16	1.43	-0.73
20	Управление инцидентами	2.55				
21	Управление проблемами	2.65				
22	Безопасная разработка ПО	2.16				

ТРАНСФОРМАЦИЯ МЕТОДОВ ОЦЕНКИ 2017 → 2025



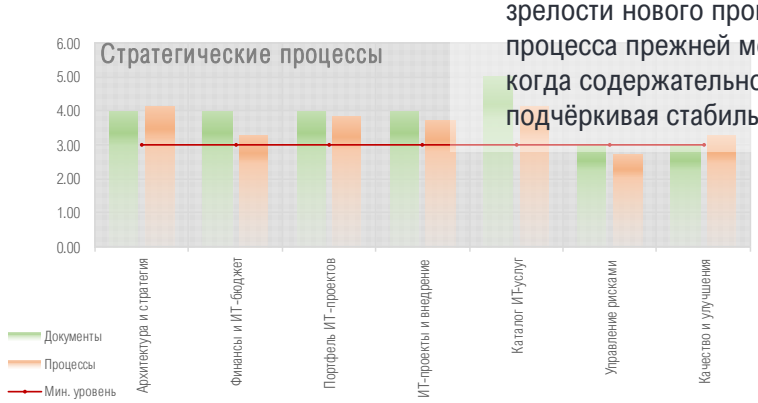
Для обеспечения преемственности исторических данных и сохранения ценности ранее проведенных оценок была разработана трансформационная таблица. Она сопоставляет процессы прежней методологии с процессами новой, определяя правила переноса оценок зрелости на основе анализа их содержательного соответствия и зависимостей. Подход опирается на признанные модели зрелости, такие как CMMI и COBIT, что гарантирует методологическую согласованность и воспроизводимость результатов.



В основе трансформации лежит математическая модель, которая формализует процесс переноса оценок, учитывая разнообразие сценариев сопоставления процессов. Эта модель обоснована принципами многоуровневой зрелости, где оценка нового процесса не может превышать уровень его базовых компонентов из прежней методологии, а потенциальные различия в охвате компенсируются консервативными корректировками. Адекватность модели подтверждается её соответствием подходам в аналогичных фреймворках, где маппинг процессов обеспечивает плавный переход без потери исторической динамики, а применимость — в её универсальности для организаций различного масштаба, позволяющей минимизировать субъективность и облегчить сравнение трендов.

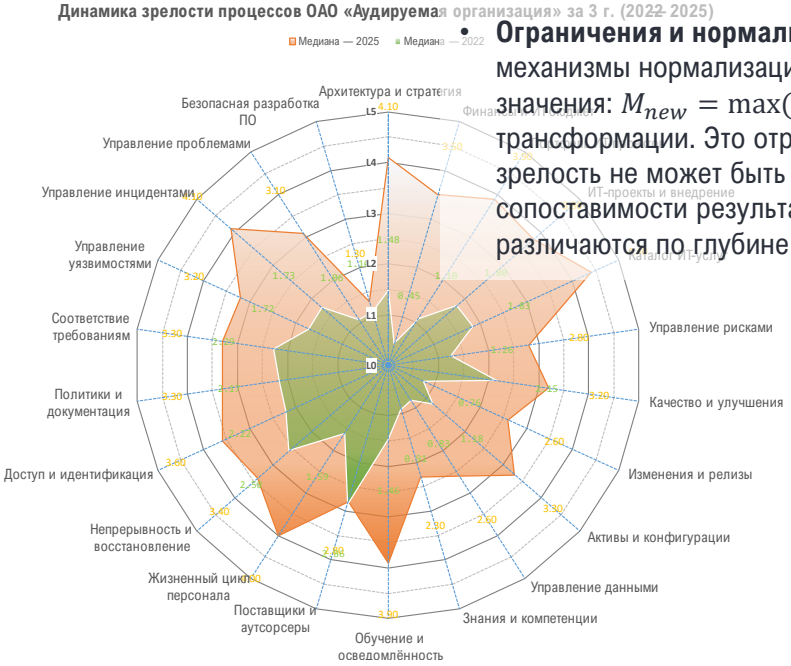
Модель включает несколько категорий трансформации, каждая из которых описана формулами ниже:

- **Прямое наследование**: если процесс новой методологии в значительной степени соответствует процессу прежней, оценка переносится без существенных изменений, отражая полную преемственность. Формула: $M_{new} = M_{old}$, где M_{new} — оценка зрелости нового процесса, M_{old} — оценка зрелости соответствующего процесса прежней методологии. Этот подход применим в случаях, когда содержательное совпадение позволяет избежать искажений, подчёркивая стабильность ключевых практик



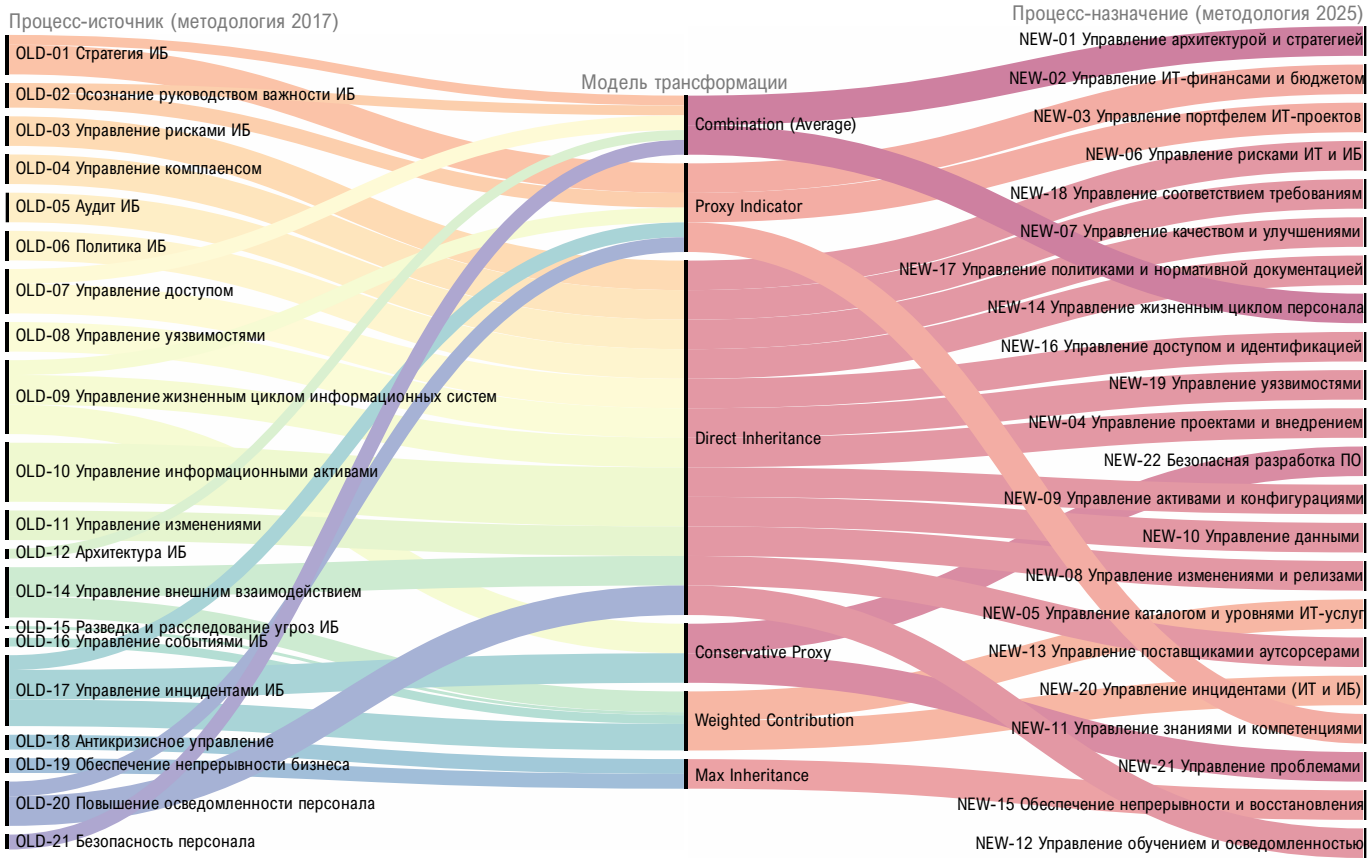
ТРАНСФОРМАЦИЯ МЕТОДОВ ОЦЕНКИ 2017 → 2025

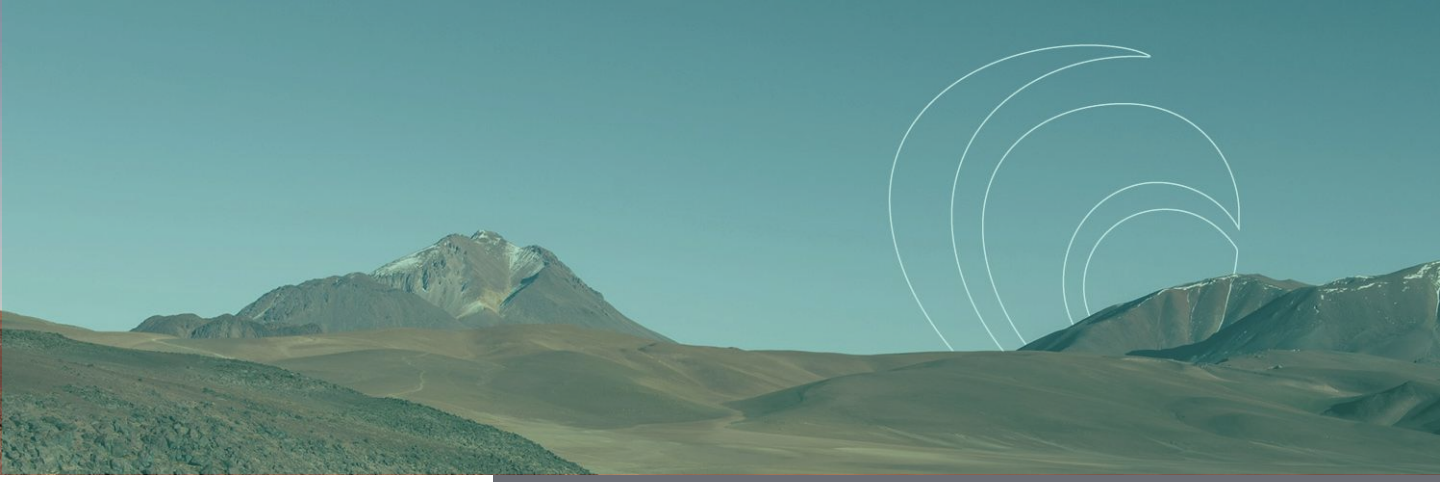
- **Объединение нескольких процессов**: если новый процесс интегрирует аспекты из двух или более процессов прежней методологии, оценка формируется как агрегированная функция, учитывающая вклад каждого компонента. Формула: $M_{new} = f(M_{old_1}, M_{old_2}, \dots, M_{old_n})$, где f — агрегирующая функция, такая как среднее арифметическое или взвешенное среднее. Это обеспечивает баланс, признавая, что объединение может отражать синергию, но требует осторожности в интерпретации, поскольку полное совпадение не всегда гарантировано
- **Прокси-индикаторы** для процессов без прямых аналогов: в ситуациях, когда новый процесс не имеет точного эквивалента, оценка выводится из смежных процессов с применением корректирующей функции, чтобы учесть потенциальные пробелы в формализации. Формула: $M_{new} = g(\min(M_{old_1}, M_{old_2} \dots)) - p$, где g — ограничивающая функция (например, минимум для учёта «слабого звена»), а $p > 0$ — параметр корректировки, вводимый для консервативного снижения оценки. Такой механизм позволяет приблизительно оценить зрелость, избегая завышения и выделяя необходимость дальнейшей верификации на основе актуальных данных.



- **Ограничения и нормализация**: во всех случаях модель включает механизмы нормализации, чтобы предотвратить недопустимые значения: $M_{new} = \max(0, h(M_{old}))$, где h — основная функция трансформации. Это отражает реалистичный подход, учитывая, что зрелость не может быть отрицательной, и способствует сопоставимости результатов, даже если исходные процессы различаются по глубине охвата.

ТРАНСФОРМАЦИЯ МЕТОДОВ ОЦЕНКИ 2017 → 2025





ЗАКЛЮЧЕНИЕ

Разработанная математическая модель и применённые подходы трансформации в новой методологии обеспечивают сохранение ценности ранее проведённых оценок, минимизируя разрывы в данных при переходе. Этот подход способствует планомерному развитию процессов ИТ и ИБ, позволяя организациям эффективно адаптироваться к современным вызовам и требованиям.

По вопросам методологии и проведения ИТ-аудита можно обращаться к партнёру по ИТ-аудиту Бейкер Тилли в Центральной Азии:

Влад Ткачёв

Партнёр по ИТ-аудиту

E: vtkachev@bakertilly.kg
T: 996 (312) 90-05-05
M: 996 (775) 97-74-28

Кыргызская Республика
г. Бишкек, ул. Ибраимова, 103
БЦ «Виктори», 7 этаж
Тел./факс: + 996 312 90 05 05
contact@bakertilly.kg