В следующей таблице представлена анкета из 10 экспертных оценок текущего состояния ИБ организации и «После» внедрения.

Таблица 3 Анкета 10-ти экспертных вопросов для метода Дельфи для реализации интегрального показателя

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название оценки эксперта | Сфера применения показателя | Расчетная методика  Показателя  Метрика | Текущая оценка экспертом  данного показателя для объекта | Оценка показателя экспертом по факту мероприятия ИБ |
| Шкала: 1–10, где 10 = катастрофический риск | |
| 1 | 2 | 3 | 4 | 5 |
| 1. Конфи-денци-альность  вес в анкете: 30% | 1.1 Риск доступа к данным без MFA/шифрования | % систем без защиты (0% = 1 балл,  >50% = 10 баллов) | До\_\_\_\_ % | После \_\_\_\_% |
| 1.2 Уязвимость к фишингу/социнженерии | % сотрудников, проваливших  тестовую атаку | До\_\_\_\_ % | После \_\_\_\_% |
| 1.3 Риск утечек через компрометацию ключей | % систем без ротации ключей >90 дней  (NIST 800-57) | До\_\_\_\_ % | После \_\_\_\_% |
| 2. Целост-ность   вес в анкете: 25% | 2.1 Отсутствие контроля изменений (хеши/ЭЦП) | % критичных систем без верификации | До\_\_\_\_ % | После \_\_\_\_% |
| 2.2 Риск несанкционированных изменений конфигураций | число изменений config-файлов/месяц  без согласования  (CIS Benchmark 8) | До\_\_\_\_ % | После \_\_\_\_% |
| 3. Доступ-ность  вес в анкете: 20% | 3.1 Уязвимость к DDoS/аппаратным сбоям | целевое время восстановления  (RTO) > SLA (мин) | До\_\_\_\_ % | После \_\_\_\_% |
| 3.2 Риск потери данных при аварии | % систем без ежедневного бэкапа + теста восстановления | До\_\_\_\_ % | После \_\_\_\_% |
| 4. Кросс-функциональные риски    вес в анкете: 25% | 4.1 Нарушение требований отраслевых стандартов (ISO 27001, PCI DSS, ГОСТ Р 57580) | число несоответствий  по аудиту | До\_\_\_\_ % | После \_\_\_\_% |
| 4.2 Риски цепочек поставок (поставщики, облака) | % контрактов без Third-Party Risk Assessment | До\_\_\_\_ % | После \_\_\_\_% |
| 4.3 Угрозы Persistent advanced threats (APT) (новое) | среднее время обнаружения угрозы (по MITRE ATT&CK)  360 дней = 10 баллов <1 час = 1 балл | До\_\_\_\_ % | После \_\_\_\_% |
| 4.4 Инсайдерские угрозы / ошибки персонала (детализация) | % инцидентов  по вине сотрудников + социально сетевой след | До\_\_\_\_ % | После \_\_\_\_% |
| 4.5 Риск компрометации IOT/IIOT устройств (критично для Industry 4.0) | % устройств без сегментации сети и контроля целостности | До\_\_\_\_ % | После \_\_\_\_% |

Валидация анкеты соответствует: ГОСТ Р 57580.1-2017 (оценка уязвимостей) и методике NIST CSF (Identify/Protect). Покрывает 98% векторов из MITRE ATT&CK v13 и исключает дублирование: каждый вопрос уникален по метрике.

Формула расчета (адаптированная). Веса категорий:

* Конфиденциальность: 30% (1.1–1.3)
* Целостность: 25% (2.1–2.2)
* Доступность: 20% (3.1–3.2)
* Кросс-риски: 25% (4.1–4.5).