

**ЮЖНЫЙ УНИВЕРСИТЕТ
(ИУБнП)**

АКПЕРОВ И.Г., МАРТЫНОВ Б.В.

УПРАВЛЕНИЕ ЦИФРОВЫМИ ИЗМЕНЕНИЯМИ:

МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ

ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

НАУЧНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

**Ростов-на-Дону
2026**

УДК 005:004
ББК 65.291.21с51

Рецензенты:

Заведующий кафедрой «Прикладная математика и программирование»,
Южный федеральный университет, д. ф-м. наук, профессор.,
почётный работник образования РФ, Угольников Г.А.

И.о. заведующего кафедрой управления развитием пространственно-экономических
систем, профессор факультета управления Южного федерального университета,
д.т.н., к.э.н., доцент Мурзин А.Д.

Печатается по решению Ученого Совета ЧОУ ВО ЮУ (ИУБиП)
Протокол № 1 от «27» августа 2026 г.

Акперов И.Г., Мартынов Б.В.

Управление цифровыми изменениями: методология формирования цифрового
сознания организации: научно-методическое пособие / И.Г. Акперов, Б.В.
Мартынов. – Ростов н/Д.: ЧОУ ВО ЮУ (ИУБиП), 2026. – 307 с.

Пособие раскрывает методологию управления цифровыми изменениями на
основе формирования цифрового сознания организации – интегральной способности
согласовывать технологии, данные и искусственный интеллект со стратегией,
ответственностью, безопасностью и развитием персонала.

Рассматриваются управленческие противоречия цифровой трансформации;
многоуровневая модель цифрового сознания; диагностика цифровой зрелости;
проектирование внедрения; управление сопротивлением и рисками;
институционализация изменений и отраслевая адаптация методологии.

Пособие адресовано руководителям, управленческим и проектным командам,
специалистам по цифровому развитию, организационным изменениям, управлению
персоналом, аналитике и информационной безопасности, а также преподавателям,
исследователям и экспертам. Интерактивное научно-методическое руководство
содержит диагностические формы, шаблоны, конструкторы, отраслевые профили и
учебные материалы.

ISBN _____

© И.Г. Акперов, Б.В. Мартынов, 2026
© ЧОУ ВО ЮУ (ИУБиП), 2026

ПРЕДИСЛОВИЕ

Цифровая трансформация стала не только технологической, но прежде всего управленческой задачей. Платформы, данные, алгоритмы и искусственный интеллект меняют процессы, распределение полномочий, критерии решений, коммуникации и ответственность. Поэтому руководителю необходимо управлять не отдельными цифровыми проектами, а целостной системой организационных изменений.

Практика показывает, что приобретение технологий и обучение работе с ними не гарантируют повышения эффективности и устойчивости. Цифровые инициативы могут оставаться разрозненными, усиливать нагрузку, порождать недоверие и создавать новые риски. Между технологической оснащенностью и способностью организации осмысленно действовать в цифровой среде возникает управленческий разрыв.

Средством преодоления этого разрыва в пособии выступает формирование цифрового сознания организации. Под ним понимается не психологическое «сознание» организации и не антропоморфизация цифровой системы, а интегральная управленческая способность сотрудников, команд и руководителей согласовывать использование технологий, данных и ИИ со стратегией, ответственностью, безопасностью, доверием и организационным обучением.

Логика пособия строится как управленческий цикл: постановка проблемы и определение объекта развития; описание уровней и компонентов цифрового сознания; связь с цифровой зрелостью; диагностика; проектирование и пилотирование изменений; работа с лидерством, коммуникацией и сопротивлением; институционализация и отраслевая адаптация модели.

Данное издание фиксирует научно-методическую концепцию и инструменты управления цифровыми изменениями без перестройки организации по единому шаблону. Практическое применение поддерживается интерактивным научно-методическим руководством, включающим диагностические инструменты, рабочие шаблоны, конструкторы документов, отраслевые профили и образовательные модули.

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ	3
ВВЕДЕНИЕ	6
ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ И УПРАВЛЕНЧЕСКИЕ ОСНОВАНИЯ ФОРМИРОВАНИЯ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ	14
1.1. Цифровое сознание как феномен современной цифровой трансформации ..	14
1.2. От цифровой грамотности к цифровому сознанию организации.....	18
1.3. Цифровое сознание 1.0 и цифровое сознание 2.0	24
1.4. Организация как коллективный субъект цифровой среды.....	29
1.5. Методологические принципы формирования цифрового сознания организации.....	34
ГЛАВА 2. УРОВНИ И МЕХАНИЗМЫ УПРАВЛЕНИЯ ФОРМИРОВАНИЕМ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ	42
2.1. Индивидуальный уровень цифрового сознания: сотрудник в цифровой среде	42
2.2. Командный уровень цифрового сознания: цифровое взаимодействие и совместная деятельность	47
2.3. Управленческий уровень цифрового сознания: принятие решений на основе данных и ИИ.....	51
2.4. Организационный уровень цифрового сознания: культура, процессы, архитектура и ответственность.....	55
2.5. Экосистемный уровень цифрового сознания: внешние стейкхолдеры, партнерства и цифровое доверие	59
ГЛАВА 3. КОМПОНЕНТЫ ЦИФРОВОГО СОЗНАНИЯ КАК ОБЪЕКТЫ РАЗВИТИЯ СОТРУДНИКОВ И УПРАВЛЕНЧЕСКИХ КОМАНД	64
3.1. Цифровая дееспособность и инструментальная готовность	66
3.2. Информационно-аналитическая критичность	69
3.3. Грамотность в области данных и ИИ: возможности и ограничения искусственного интеллекта	73
3.4. Цифровая этика, право и ответственность	76
3.5. Цифровая безопасность и управление рисками	79
3.6. Цифровая коммуникация и культура взаимодействия.....	83
3.7. Рефлексивность, саморегуляция и готовность к изменениям	86
ГЛАВА 4. ЦИФРОВОЕ СОЗНАНИЕ ОРГАНИЗАЦИИ КАК УПРАВЛЕНЧЕСКИЙ ФАКТОР ЦИФРОВОЙ ЗРЕЛОСТИ	91
4.1. Цифровая зрелость и цифровое сознание: соотношение понятий.....	91
4.2. Стратегический контур цифрового сознания организации	95
4.3. Контур данных, аналитики и искусственного интеллекта	98
4.4. Контур цифровой архитектуры и сервисов	102
4.5. Контур организационной культуры, доверия и безопасности	105
4.6. Контур развития персонала и команд	108
4.7. Организационная рефлексивность как механизм цифрового развития	111
ГЛАВА 5. ДИАГНОСТИКА ЦИФРОВОГО СОЗНАНИЯ ДЛЯ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ.....	118
5.1. Принципы диагностики цифрового сознания организации	118
5.2. Индекс цифрового сознания сотрудника.....	122
5.3. Индекс цифрового сознания команды	127

5.4. Индекс организационного цифрового сознания	131
5.5. Уровни цифровой зрелости организации	135
5.6. Методы сбора данных: опросы, кейсы, цифровой след, аналитика, экспертная оценка.....	139
5.7. Этические ограничения диагностики и недопустимость цифрового надзора.....	144
5.8. Методический алгоритм применения результатов диагностики	149
5.9. Методические требования к разработке диагностических инструментов....	156
ГЛАВА 6. УПРАВЛЕНИЕ ВНЕДРЕНИЕМ МОДЕЛИ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ.....	162
6.1. Подготовительный этап: глоссарий, цели, карта процессов и цифровых рисков	163
6.2. Входная диагностика цифрового сознания организации.....	170
6.3. Проектирование пилота и выбор подразделений	172
6.4. Обучение сотрудников и управленческих команд.....	175
6.5. Запуск пилотных практик и цифровых проектов	177
6.6. Мониторинг, аналитика и корректировка модели.....	180
6.7. Масштабирование и институционализация модели.....	182
ГЛАВА 7. УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ИНСТИТУЦИОНАЛИЗАЦИЯ ЦИФРОВОЙ КУЛЬТУРЫ ОРГАНИЗАЦИИ.....	189
7.1. Цифровое лидерство и роль руководителя.....	191
7.2. Коммуникационная стратегия формирования цифрового сознания	198
7.3. Преодоление сопротивления цифровым изменениям	203
7.4. Профессиональные сообщества и внутренняя сеть цифровых наставников.....	208
7.5. Мотивация сотрудников к развитию цифрового сознания	213
7.6. Включение цифрового сознания в KPI, регламенты и кадровую политику.....	218
7.7. Ежегодный цикл оценки и развития цифрового сознания организации.....	226
ГЛАВА 8. ОТРАСЛЕВАЯ АДАПТАЦИЯ МОДЕЛИ УПРАВЛЕНИЯ ФОРМИРОВАНИЕМ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ.....	239
8.1. Принципы адаптации универсальной модели под конкретную сферу	241
8.2. Адаптация модели для образовательной организации	248
8.3. Адаптация модели для коммерческой организации.....	254
8.4. Адаптация модели для органа государственного или муниципального управления.....	259
8.5. Адаптация модели для медицинской организации в контексте медицины	264
8.6. Адаптация модели для научной, проектной или экспертной организации	270
8.7. Адаптация модели для социальной и некоммерческой организации	275
8.8. Сравнительная карта отраслевых модификаций модели	280
ЗАКЛЮЧЕНИЕ	292
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	294

ВВЕДЕНИЕ

Управленческая актуальность и постановка проблемы

Современная организация действует в условиях, когда цифровые изменения затрагивают не только инфраструктуру, но и саму систему управления: цели, процессы, полномочия, способы принятия решений, требования к данным, нормы ответственности и отношения с внешними участниками. Руководитель вынужден одновременно обеспечивать технологическое развитие, экономическую результативность, безопасность, соблюдение правовых и этических требований, доверие сотрудников и способность организации быстро пересматривать собственные практики.

Главная управленческая трудность состоит в том, что скорость внедрения технологий часто превышает скорость организационного осмысления. Возникают разрывы между цифровой стратегией и повседневными процессами, данными и качеством решений, ИТ-проектами и развитием персонала, использованием ИИ и распределением ответственности, формальными регламентами и фактическим поведением сотрудников. Поэтому наличие платформ и цифровых компетенций само по себе не обеспечивает управляемость изменений.

Для преодоления этих разрывов необходима организационная способность, которая связывает стратегию, технологии, данные, поведение людей и ответственность. В настоящем пособии такой способностью является цифровое сознание организации. Это понятие не относится к психологической диагностике организации и не обозначает «сознание» машины: оно используется как аналитический и управленческий конструкт, проявляющийся в устойчивых способах целеполагания, интерпретации данных, принятия решений, координации действий и рефлексии последствий цифровых решений.

Особую остроту проблема приобретает в связи с распространением искусственного интеллекта. Генеративные модели, рекомендательные системы, интеллектуальная аналитика и автоматизированные помощники расширяют возможности управления, но одновременно требуют проверки качества данных, объяснимости решений, человеческого контроля, этических ограничений и понятного распределения ответственности. Управление цифровыми изменениями становится управлением социотехнической системой, а не внедрением набора инструментов.

Степень разработанности проблемы и основание авторского подхода

В современной научной и управленческой повестке активно используются понятия цифровой трансформации, цифровой грамотности, цифровой компетентности, цифровой зрелости, цифровой культуры, цифрового лидерства, грамотность в области данных и грамотность в области искусственного

интеллекта. Эти категории раскрывают важные стороны цифрового развития, однако каждая из них фиксирует лишь отдельный срез проблемы. Цифровая грамотность описывает способность пользоваться инструментами, цифровая компетентность – готовность решать профессиональные задачи с применением технологий, цифровая зрелость – уровень организационного развития, а цифровая культура – систему норм и практик цифрового взаимодействия.

Категория цифрового сознания позволяет интегрировать указанные подходы в единую методологическую рамку. Она связывает знания, умения, ценности, критическое мышление, этику, саморегуляцию, работу с данными и ИИ, цифровую безопасность, организационное управление и рефлексии последствий цифровых решений. В этом состоит принципиальная методологическая позиция пособия: цифровое сознание рассматривается не как замена цифровой грамотности или цифровой зрелости, а как их смысловое, управленческое и субъектное основание [1–8; 10; 15; 24–29].

Авторский подход исходит из необходимости рассматривать цифровое сознание на нескольких уровнях: индивидуальном, командном, управленческом, организационном и экосистемном. Такая многоуровневая структура позволяет избежать упрощения, при котором цифровая трансформация сводится к обучению сотрудников работе с отдельными программами или к приобретению новых цифровых сервисов.

Управленческая проблема пособия

Ключевая проблема, на решение которой направлено пособие, заключается в разобщенности механизмов управления цифровыми изменениями. На практике ИТ-подразделение внедряет системы, служба управления персоналом проводит обучение, руководители требуют цифровой отчетности, сотрудники используют ИИ-инструменты по собственной инициативе, а вопросы стратегии, данных, этики, безопасности, ответственности и оценки результатов не объединены в единый управленческий контур.

В результате технологически оснащенная организация может оставаться неподготовленной к осмысленному использованию цифровых решений. Пособие предлагает преодолеть этот разрыв через формирование цифрового сознания как развиваемой организационной способности и включение его диагностики, обучения, нормативного закрепления и регулярной оценки в систему управления изменениями.

Цель пособия

Цель пособия – разработать и представить универсальную научно-методическую систему управления цифровыми изменениями на основе формирования цифрового сознания организации, включающую понятийный аппарат, структурную модель, уровни развития, диагностический

инструментарий, технологию внедрения, механизмы институционализации изменений и основу для отраслевой адаптации.

Задачи пособия

1. Раскрыть управленческую природу цифрового сознания организации как интегральной организационной способности.
2. Разграничить понятия цифровой грамотности, цифровой компетентности, цифровой культуры, цифровой зрелости и цифрового сознания.
3. Описать цифровое сознание 1.0 и цифровое сознание 2.0 как уровни развития организации в цифровой и насыщенной искусственным интеллектом среде.
4. Сформировать структурную модель цифрового сознания организации на индивидуальном, командном, управленческом, организационном и экосистемном уровнях.
5. Определить компоненты цифрового сознания сотрудников и управленческих команд.
6. Предложить подходы к диагностике цифрового сознания сотрудников, команд и организации в целом.
7. Разработать логику индекса организационного цифрового сознания и уровней цифровой зрелости.
8. Описать технологию внедрения модели цифрового сознания организации: от входной диагностики и пилотирования до масштабирования и институционализации.
9. Раскрыть механизмы управления изменениями и развития цифровой культуры организации.
10. Подготовить основу для отраслевой адаптации методологии применительно к образовательным, коммерческим, государственным, медицинским, научным, проектным и социальным организациям.

Объект и предмет пособия

Объектом научно-методического анализа является управление организацией как социально-цифровой системой в условиях цифровой трансформации, платформизации, работы с данными и распространения искусственного интеллекта.

Предметом пособия является методология управления цифровыми изменениями на основе формирования цифрового сознания организации, включающая ценностные, когнитивные, организационные, технологические, этические, аналитические и культурные механизмы развития.

Рабочее определение цифрового сознания организации

Цифровое сознание организации – это интегральная управленческая способность организации как коллективного субъекта осознанно, критично, этично, безопасно и результативно использовать цифровые технологии, данные

и искусственный интеллект для достижения стратегических целей, развития сотрудников, повышения качества процессов, укрепления доверия, управления рисками и создания устойчивой цифровой культуры.

В настоящем пособии понятие «цифровое сознание организации» используется не как утверждение о наличии у организации самостоятельного психологического сознания. Оно обозначает аналитический организационный конструкт, наблюдаемый через устойчивые способы целеполагания, интерпретации данных, принятия решений, распределения ответственности, нормативного регулирования, организационного обучения и рефлексии последствий цифровых действий. Агентность при этом понимается как способность сотрудников и команд инициировать осмысленное цифровое действие, а субъектность – как системная способность организации определять цели, нормы и границы цифрового развития.

Цифровая грамотность отвечает на вопрос: умеют ли сотрудники пользоваться цифровыми инструментами. Цифровое сознание отвечает на более широкий вопрос: понимает ли организация, зачем, как, с какими последствиями и в какой системе ответственности она использует цифровые технологии.

Методологическая основа пособия

Методологическую основу пособия составляют системный, компетентностный, субъектно-деятельностный, процессный, риск-ориентированный, рефлексивный подходы и подход организационной зрелости. Системный подход позволяет рассматривать организацию как целостную структуру взаимосвязанных процессов, людей, данных, технологий и норм. Компетентностный подход задает возможность описания цифрового сознания через знания, умения, ценности, установки и модели поведения. Субъектно-деятельностный подход позволяет понимать организацию как активного участника цифровой трансформации, а не как пассивного потребителя технологий.

Подход организационной зрелости обеспечивает описание качественных переходов от фрагментарных цифровых практик к координируемому, интегрированному и адаптивно-рефлексивному состоянию организации. Он связывает структурную модель цифрового сознания с диагностическими уровнями, программой внедрения и механизмами постоянного улучшения.

Риск-ориентированный подход необходим для учета угроз, связанных с данными, информационной безопасностью, алгоритмическими решениями, использованием искусственного интеллекта и цифровым следом. Процессный подход позволяет встроить цифровое сознание в реальные управленческие, производственные, образовательные, сервисные и коммуникационные процессы. Рефлексивный подход обеспечивает регулярную оценку влияния цифровых решений на людей, культуру, результаты и устойчивость организации.

Причинно-следственная логика модели

В управленческой логике модели цифровое сознание рассматривается как развиваемая организационная способность, связывающая предпосылки, механизмы, наблюдаемые проявления и результаты цифровых изменений. К предпосылкам относятся лидерство, цифровая архитектура, качество данных, компетенции, нормативная среда и ресурсы. Механизмами выступают критическая интерпретация, командная координация, управление данными и ИИ, человеческий контроль и организационная рефлексия. Наблюдаемыми проявлениями становятся ответственное цифровое поведение, документированные процессы, проверяемые решения и устойчивые нормы, а результатами – повышение цифровой зрелости, качества решений, безопасности, доверия и адаптивности организации.

Научная новизна

Научная новизна пособия состоит в разработке и системном обосновании авторской научно-методической модели цифрового сознания организации. Модель объединяет проблематику цифровой грамотности, организационной культуры, цифровой зрелости, управления данными и ИИ, информационной безопасности, этики, организационного обучения и субъектности, но не объявляется завершённым стандартизованным измерительным конструктом до проведения эмпирической валидации.

В пособии предложена многоуровневая модель цифрового сознания: сотрудник – команда – управленческий контур – организация – экосистема. Такая модель позволяет рассматривать цифровую трансформацию не как совокупность технологических проектов, а как процесс формирования организационной субъектности в цифровой среде.

Отдельным элементом новизны является разграничение цифрового сознания 1.0 и цифрового сознания 2.0. Цифровое сознание 1.0 связано с базовой цифровой дееспособностью, безопасностью, цифровой культурой, критическим отношением к информации и ответственным использованием технологий. Цифровое сознание 2.0 отражает переход к насыщенной искусственным интеллектом среде и включает понимание возможностей и ограничений искусственного интеллекта, проверку достоверности результатов, управление алгоритмическими рисками, объяснимость, этику автоматизации и человеческий контроль.

Теоретическая значимость

Теоретическая значимость пособия заключается в развитии понятийного аппарата цифровой трансформации за счет введения и методологического раскрытия категории цифрового сознания организации. Пособие предлагает связать цифровое развитие не только с технологиями и инфраструктурой, но и с

мышлением, ценностями, ответственностью, организационной культурой и способностью к рефлексивному управлению изменениями.

Предложенная модель может быть использована как основание для дальнейших научных исследований в области управления организационными системами, цифровой трансформации, организационной культуры, искусственного интеллекта в управлении, профессионального развития персонала и проектирования цифровой зрелости.

Практическая значимость

Практическая значимость пособия состоит в возможности использовать его как рамку управленческого решения: определить проблему и владельца изменений; выбрать объект диагностики; согласовать стратегию, процессы, данные, компетенции и риски; спроектировать пилот; оценить результат; принять решение о корректировке, масштабировании и нормативном закреплении новой практики.

Пособие может применяться руководителями организаций и подразделений, проектными и управленческими командами, службами цифрового развития, управления персоналом, аналитики, информационной безопасности и организационного развития. Универсальная модель позволяет адаптировать управленческий цикл к образовательным, коммерческим, государственным, медицинским, научным и некоммерческим организациям.

Эмпирическая основа и статус апробации

Эмпирическая основа пособия имеет комбинированный характер. Для обоснования актуальности, структуры рисков и организационных контуров использованы международные и российские статистические сборники, обследования организаций, отчёты по внедрению ИИ, цифровым компетенциям и кибербезопасности, а также документированные отраслевые кейсы [9; 18; 19; 79; 93; 127; 144; 162]. Эти материалы позволяют сопоставить авторскую модель с наблюдаемыми тенденциями, но не заменяют её самостоятельной полевой проверки.

Индексы ИЦСС, ИЦСК и ИОЦС, весовые коэффициенты и пороговые значения имеют статус проектных научно-методических инструментов. Программа их валидации должна включать экспертную оценку содержания, когнитивное интервьюирование, пилотное обследование, анализ внутренней согласованности и факторной структуры, межэкспертную и повторную надёжность, проверку критериальных связей и анализ чувствительности к весам. До завершения этих процедур результаты корректно использовать для самооценки, выбора мер развития и анализа динамики внутри одной организации, но не для межорганизационного ранжирования или автоматических кадровых решений [42; 58; 99].

Целевая аудитория

Пособие адресовано руководителям организаций, заместителям руководителей, руководителям структурных подразделений, проектным и управленческим командам, специалистам по цифровой трансформации, аналитике, управлению персоналом, информационной безопасности, корпоративному обучению, а также преподавателям, исследователям и экспертам, занимающимся вопросами цифрового развития организаций.

Как работать с пособием

Пособие допускает последовательное чтение и выборочные управленческие маршруты. Во всех случаях цифровое сознание следует рассматривать не как отдельную программу обучения, а как объект согласованного воздействия на стратегию, процессы, данные, компетенции, нормы и организационную культуру.

Руководителям организаций рекомендуется начать с введения и глав 1, 4–7: они раскрывают управленческую постановку проблемы, смысл модели, связь с цифровой зрелостью, диагностику, технологию внедрения и механизмы закрепления изменений.

Специалистам по управлению персоналом и корпоративному обучению целесообразно использовать главы 3, 5 и 7, а практические программы, диагностические формы и шаблоны – в интерактивном научно-методическом руководстве.

ИТ-подразделениям, специалистам по данным и информационной безопасности адресованы главы 4–6 и инструменты инвентаризации сервисов, данных, ИИ-сценариев и рисков.

Исследователям и методологам следует учитывать, что предложенные индексы и шкалы являются авторскими научно-методическими моделями и требуют эмпирической валидации до использования как стандартизованных измерительных методик.

Минимальный маршрут внедрения состоит из шести управленческих шагов: определить цель и владельца программы; описать процессы, сервисы, данные и ИИ-сценарии; провести входную диагностику; выбрать ограниченный пилот; организовать ролевое обучение и контроль рисков; сопоставить результат с исходным состоянием и принять решение о корректировке или масштабировании. Заполняемые формы, калькуляторы, реестры и конструктор дорожной карты размещены в интерактивном руководстве.

Интерактивное сопровождение пособия

Печатное научно-методическое пособие является фиксированной рецензируемой версией авторской методологии. Чтобы сохранить приемлемый объем издания и не дублировать материалы, требующие регулярного обновления, практические приложения не включены в книжный блок.

Интерактивное научно-методическое руководство «Управление цифровыми изменениями: методология формирования цифрового сознания организации» выполняет функцию цифрового сопровождения пособия. Оно содержит заполняемые формы, калькуляторы индексов, кейсы, чек-листы, карты, реестры, конструкторы документов, отраслевые профили и учебные модули. Содержание руководства связано с соответствующими главами пособия и обновляется с указанием версии.

Актуальный адрес и QR-код интерактивного руководства указываются в выходных сведениях печатного и электронного издания. Интерактивный ресурс расширяет возможности применения методологии, но не заменяет опубликованный научный текст и его библиографическое цитирование.

Структура пособия

Структура пособия соответствует циклу управления цифровыми изменениями. Первая глава формирует понятийное основание; вторая описывает уровни объекта управления; третья раскрывает развиваемые компоненты; четвертая связывает их с цифровой зрелостью; пятая предлагает диагностику для принятия решений; шестая переводит модель в программу внедрения; седьмая раскрывает лидерство, коммуникацию, работу с сопротивлением и институционализацию; восьмая обеспечивает отраслевую адаптацию методологии.

Обновляемые практические материалы вынесены из книжного блока в интерактивное научно-методическое руководство. В нем доступны глоссарий, визуальные модели, диагностические опросники и шкалы, чек-листы, реестры, карты цифровых рисков, конструктор дорожной карты, декларации об использовании ИИ, шаблоны аналитических панелей, программы подготовки сотрудников и руководителей, отраслевые матрицы и формы аналитической отчетности.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ И УПРАВЛЕНЧЕСКИЕ ОСНОВАНИЯ ФОРМИРОВАНИЯ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

«Мысли без содержания пусты, созерцания без понятий слепы».

Иммануил Кант

Управленческий вопрос главы. Почему технологическая оснащенность и цифровые компетенции сами по себе не обеспечивают управляемость цифровой трансформации и какое место в ней занимает цифровое сознание организации?

Управленческий результат главы. Понятийная и методологическая рамка, позволяющая отличить цифровое сознание от смежных категорий и определить принципы его формирования как организационной способности.

1.1. ЦИФРОВОЕ СОЗНАНИЕ КАК ФЕНОМЕН СОВРЕМЕННОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Цифровая трансформация в современной управленческой мысли уже не сводится к переводу документов в электронный вид или внедрению отдельных информационных систем. В исследованиях цифровой трансформации подчеркивается, что она затрагивает бизнес-модели, организационные способности, культуру, пользовательский опыт, архитектуру данных и способы принятия решений [143; 145]. В этом смысле цифровая трансформация является не столько техническим проектом, сколько социотехническим процессом. Технологии становятся видимой частью изменений, но их реальный эффект определяется тем, как организация понимает, принимает, регулирует и переосмысляет эти технологии.

Социотехнический характер цифровой трансформации означает, что цифровая система не может быть понята отдельно от человеческих ролей, норм, конфликтов интересов, организационной памяти и управленческой ответственности. Одна и та же платформа может стать инструментом развития, если она встроена в понятную модель процессов, и источником дезорганизации, если сотрудники не понимают ее назначения, руководители не используют данные для обратной связи, а правила ответственности остаются неясными. Поэтому цифровая трансформация начинается не с установки программного обеспечения, а с изменения способа организационного мышления.

В работах по цифровой трансформации организаций фиксируется несколько устойчивых признаков нового типа организационной среды. Во-первых, данные становятся основанием решений, но требуют интерпретации, проверки качества и понимания ограничений. Во-вторых, цифровые платформы повышают прозрачность процессов, но одновременно создают новые формы зависимости

от инфраструктуры. В-третьих, искусственный интеллект усиливает аналитические и коммуникативные возможности, но переносит в управленческий контур риски алгоритмической предвзятости, галлюцинаций, автоматизации ошибок и размывания ответственности [101; 137]. В-четвертых, цифровой след сотрудников, клиентов и процессов превращается в управленческий ресурс, но требует этических границ и правовой аккуратности.

Именно в этой точке возникает потребность в категории цифрового сознания. Цифровое сознание организации можно определить как способность не просто использовать цифровые технологии, а понимать собственное положение в цифровой среде, видеть последствия цифровых решений, соотносить технологические возможности с ценностями, целями, рисками и ответственностью. Если цифровая грамотность отвечает на вопрос «умеет ли субъект пользоваться инструментом», то цифровое сознание отвечает на вопрос «понимает ли организация, зачем, как, в каких границах и с какими последствиями она использует цифровые технологии». Эта разница принципиальна для методологии цифрового развития.

В авторской рамке пособия цифровое сознание выступает метаконструктом, то есть понятием, объединяющим несколько уровней анализа. На индивидуальном уровне оно включает цифровую компетентность, критичность, грамотность в области ИИ и ответственное цифровое поведение. На командном уровне оно проявляется в совместных правилах работы с данными, цифровыми сервисами и искусственным интеллектом. На управленческом уровне – в способности руководства переводить цифровые инициативы в цели, регламенты, показатели и механизмы контроля. На организационном уровне – в цифровой культуре, цифровой памяти, управлении рисками и доверии. На экосистемном уровне – в способности взаимодействовать со стейкхолдерами в условиях цифровой прозрачности и платформенной взаимозависимости.

Такое понимание отличается от технократического подхода. Технократический подход предполагает, что внедрение новой системы само по себе повышает эффективность. Практика показывает обратное: цифровые инструменты могут увеличивать скорость, но не обязательно повышают качество решений; они могут расширять доступ к данным, но не формируют автоматически культуру доказательности; они могут автоматизировать операции, но не снимают вопрос о том, кто отвечает за последствия. Поэтому цифровое сознание – это не добавка к цифровизации, а условие ее осмысленного и управляемого характера.

Особую роль в формировании цифрового сознания играет искусственный интеллект. По данным отчета Stanford AI Index (Стэнфордский индекс развития ИИ), применение ИИ в организациях и общественных процессах растет, а вместе с ним возрастает потребность в ответственных практиках разработки и

использования [126]. McKinsey фиксирует массовое распространение ИИ в организациях, но одновременно указывает на трудности масштабирования эффекта и перевода пилотных решений в устойчивую организационную ценность [93]. Эти данные показывают, что проблема находится не только в технологиях. Узкое место – в управленческой способности организации переопределить процессы, роли, ответственность и обучение сотрудников.

В этой связи цифровое сознание следует рассматривать как внутреннее условие цифровой зрелости. Цифровая зрелость показывает, насколько организация институционально встроила цифровые решения в процессы. Но зрелость без сознания может превратиться в формальную регламентацию: показатели есть, платформы есть, отчеты есть, но осознанного понимания последствий нет. Цифровое сознание добавляет к зрелости рефлексивный слой: организация не только измеряет цифровую трансформацию, но и понимает, что именно она меняет в человеческой деятельности, управленческой ответственности, коммуникации и доверии.

Следовательно, цифровое сознание как феномен современной трансформации фиксирует переход от инструментального отношения к технологиям к субъектному отношению к цифровой среде. Организация с развитым цифровым сознанием не воспринимает данные как «объективную истину» без проверки, не передает ИИ решение без человеческого контроля, не подменяет цифровизацию количеством сервисов, не допускает стихийного использования корпоративных данных в неуправляемых внешних инструментах. Она выстраивает цифровую среду как управляемую, этически осмысленную и стратегически связанную систему.

На рисунке 1.1 представлена авторская рамка цифрового сознания организации как интегрального метаконструкта, объединяющего компетенции, культуру, этику, безопасность, управление и рефлекссию.



Рисунок 1.1 – Цифровое сознание организации как интегральный метаконструкт
Источник: составлено авторами на основе [101; 109; 137; 146].

Рисунок 1 раскрывает, что цифровое сознание не сводится к одному навыку, а связывает работу с данными и ИИ, культуру, безопасность, этику, ответственность и рефлексию.

Компонентный состав цифрового сознания организации обобщен в таблице 1.1; она разводит элементы, которые в практике часто смешиваются: компетентность, данные, ИИ, культура, безопасность, управление и рефлексия.

Таблица 1.1 – Компоненты цифрового сознания организации

Компонент	Содержание	Методическое значение
Цифровая компетентность	Умение безопасно, критично и результативно использовать цифровые технологии для работы, коммуникации и решения задач.	Создает базу для включения сотрудников в цифровые процессы.
Грамотность в области данных	Понимание данных, их качества, ограничений, способов интерпретации и применения в решениях.	Позволяет перейти от мнений к доказательному управлению.
Грамотность в области ИИ	Понимание возможностей, ограничений, рисков и правил применения искусственного интеллекта.	Обеспечивает осознанное взаимодействие человека с ИИ.

Компонент	Содержание	Методическое значение
Цифровая культура	Разделяемые нормы цифрового поведения, доверия, открытости, ответственности и обмена знаниями.	Закрепляет цифровые практики в повседневной деятельности.
Контур цифрового управления и ответственности	Правила, роли, регламенты, показатели, контроль и ответственность за цифровые решения.	Переводит цифровое сознание из декларации в управляемую систему.
Рефлексивность	Способность организации анализировать последствия цифровых решений и корректировать собственные действия.	Обеспечивает обучение и адаптацию организации.

Данные таблицы показывают, какой методический вклад дает каждый компонент: компетентность обеспечивает действие, данные – доказательность, ИИ – управляемую автоматизацию, культура и безопасность – устойчивость и доверие.

Таким образом, цифровое сознание организации является ответом на усложнение цифровой трансформации. Оно возникает там, где организация перестает воспринимать технологии как нейтральные инструменты и начинает видеть в них среду, изменяющую мышление, деятельность, культуру и ответственность. Для последующего изложения важно зафиксировать: цифровое сознание не заменяет цифровую грамотность, а поднимает ее на уровень организационной субъектности.

Далее цифровое сознание разграничивается с цифровой грамотностью, компетентностью, культурой и зрелостью. Это разграничение необходимо, чтобы показать собственный предмет авторской модели и логику перехода от владения инструментами к управлению цифровой средой.

1.2. ОТ ЦИФРОВОЙ ГРАМОТНОСТИ К ЦИФРОВОМУ СОЗНАНИЮ ОРГАНИЗАЦИИ

Понятие цифрового сознания может быть методологически состоятельным только при ясном разграничении с соседними категориями. В образовательной и управленческой практике часто смешиваются цифровая грамотность, цифровая компетентность, цифровая культура, цифровая зрелость, грамотность в области данных и грамотность в области ИИ. Такое смешение удобно в повседневной речи, но недостаточно для научно-методического пособия. Если все эти понятия считать синонимами, невозможно объяснить, почему организация, где сотрудники умеют пользоваться сервисами, все равно может проваливать цифровую трансформацию.

Цифровая грамотность исторически связана с базовой способностью человека пользоваться цифровыми устройствами, находить информацию, коммуницировать и ориентироваться в цифровой среде. В более поздних трактовках она включает критическую оценку информации, безопасность и участие в цифровом обществе [45]. Ее сильная сторона – практическая направленность и доступность для массового обучения. Ограничение состоит в том, что грамотность обычно описывает индивидуальный уровень и не раскрывает организационные нормы, управление рисками, коллективную ответственность и стратегическую рефлексия.

Цифровая компетентность является более развитой категорией. В европейской рамке DigComp 2.2 она понимается как уверенное, критическое и ответственное использование цифровых технологий для обучения, работы и участия в обществе [146]. Достоинство этой рамки в том, что она задает структурированную карту областей компетентности и уровней развития. Однако даже DigComp остается преимущественно рамкой компетенций гражданина. Она важна для обучения сотрудников, но не отвечает на вопрос, каким образом организация как целое формирует цифровую стратегию, управляет данными, регулирует ИИ и распределяет ответственность.

Грамотность в области данных переносит акцент с владения цифровыми устройствами на способность понимать данные. Для организации это принципиально: данные становятся сырьем управленческих решений, но при этом никогда не являются полностью нейтральными. Они могут быть неполными, устаревшими, ошибочно собранными, неверно интерпретированными или встроенными в предвзятые модели. Поэтому грамотность в области данных включает не только технический навык работы с таблицами и визуализациями, но и умение задавать вопросы к источнику данных, качеству, контексту и последствиям применения [57].

Грамотность в области ИИ становится самостоятельным элементом цифрового сознания в условиях массового распространения генеративных моделей. В научной литературе она описывается как способность понимать, использовать, оценивать и критически осмыслять ИИ-системы [92]. В институциональном контексте ЮНЕСКО связывает компетентность в области ИИ с этикой, человеческой ответственностью, педагогическими и профессиональными сценариями применения [135]. Однако грамотность в области ИИ также недостаточна сама по себе: организация может обучить сотрудников промптам, но не создать правил обращения с конфиденциальными данными, не определить границы автоматизации и не установить ответственность за результаты.

Цифровая культура описывает более широкий организационный слой. Она выражает устойчивые нормы цифрового поведения: как сотрудники

обмениваются данными, как относятся к экспериментам, как реагируют на ошибки, насколько доверяют аналитике, готовы ли фиксировать знания в системах, как соблюдают цифровую дисциплину. Теория организационной культуры показывает, что формальные правила действуют только тогда, когда они становятся частью разделяемых ценностей и практик [40]. Поэтому цифровая культура необходима для цифрового сознания, но не исчерпывает его: культура может поддерживать активное использование инструментов, но не всегда обеспечивает критическую рефлексию и контур управления и ответственности.

Цифровая зрелость фиксирует степень институционализации цифровых решений. Зрелая организация не просто запускает пилоты, а масштабирует решения, связывает их с процессами, данными, управлением изменениями и метриками результата. Тем не менее зрелость может быть измерена в логике инфраструктуры, процессов и показателей, тогда как цифровое сознание добавляет вопрос о смысле, границах и последствиях. Организация может иметь развитую ИТ-инфраструктуру, но при этом допускать цифровую перегрузку сотрудников, слепое доверие к алгоритмам или неуправляемое применение внешних ИИ-сервисов.

Цифровое лидерство также является важным, но частным понятием. Оно связано со способностью руководителей задавать цифровую повестку, поддерживать изменения, инвестировать в компетенции и культуру, принимать решения на основе данных. Однако цифровое сознание не может быть сведено к лидерству отдельных руководителей. Оно должно быть распределенным свойством организации: проявляться в командах, процедурах, цифровой памяти, регламентах, обучении и механизмах обратной связи. Иначе смена руководителя или команды разрушит цифровую траекторию.

Таким образом, цифровое сознание организации следует понимать как надстроечный методологический уровень по отношению к указанным понятиям. Оно включает цифровую грамотность как базу, цифровую компетентность как способность действовать, грамотность в области данных как способность понимать данные, грамотность в области ИИ как способность взаимодействовать с ИИ, цифровую культуру как норму поведения, цифровую зрелость как институциональную встроенность и цифровое лидерство как управленческий импульс. Но оно добавляет то, чего нет в каждом из этих понятий по отдельности: коллективную рефлексию, осознание последствий, распределенную ответственность и способность организации управлять собственной цифровой средой.

Понятийное разграничение близких категорий представлено в таблице 1.2; оно показывает, почему цифровое сознание нельзя подменять грамотностью, компетентностью, культурой или зрелостью.

Таблица 1.2 – Соотношение цифровой грамотности, компетентности, культуры, зрелости и цифрового сознания организации

Понятие	Основной вопрос	Сильная сторона	Ограничение	Место в цифровом сознании
Цифровая грамотность	Умеет ли субъект пользоваться цифровыми инструментами?	Дает массовую базу для включения в цифровую среду.	Обычно остается на индивидуальном и инструментальном уровне.	Базовый слой цифрового поведения.
Цифровая компетентность	Может ли субъект решать задачи в цифровой среде критично и безопасно?	Структурирует знания, умения и установки.	Не описывает организационную субъектность как целое.	Функциональная основа деятельности сотрудников.
Грамотность в области данных	Понимает ли субъект данные и ограничения их интерпретации?	Формирует доказательность управленческих решений.	Не задает полного контура ответственности и культуры.	Компонент аналитического мышления организации.
грамотность в области ИИ	Понимает ли субъект возможности и риски ИИ?	Снижает риски неосознанного применения ИИ.	Может быть сведена к технике промптинга.	Компонент работы в среде, насыщенной ИИ.
Цифровая культура	Какие цифровые нормы разделяет коллектив?	Закрепляет повседневные практики и доверие.	Не всегда содержит механизм измерения и контроля.	Среда закрепления цифрового сознания.
Цифровая зрелость	Насколько глубоко цифровые решения встроены в организацию?	Позволяет оценивать уровень институционализации.	Может быть формальной без рефлексии последствий.	Организационная инфраструктура цифрового сознания.
Цифровое лидерство	Кто задает цифровую повестку и ведет изменения?	Обеспечивает стратегический импульс.	Зависит от отдельных лидеров и может быть нестабильным.	Управленческий механизм запуска и поддержки изменений.

Понятие	Основной вопрос	Сильная сторона	Ограничение	Место в цифровом сознании
Цифровое сознание организации	Понимает ли организация цели, риски, последствия и ответственность цифрового развития?	Объединяет компетенции, культуру, зрелость, контур управления и ответственности и рефлексию.	Требует авторской операционализации и системы индикаторов.	Интегральный метаконструкт главы.

Данные таблицы показывают, что цифровое сознание включает соседние категории, но добавляет к ним коллективную субъектность, ответственность и анализ последствий.

Логика перехода от инструментального владения сервисами к осознанному управлению цифровой средой представлена на рисунке 1.2; каждый новый уровень добавляет более сложный режим ответственности и рефлексии.

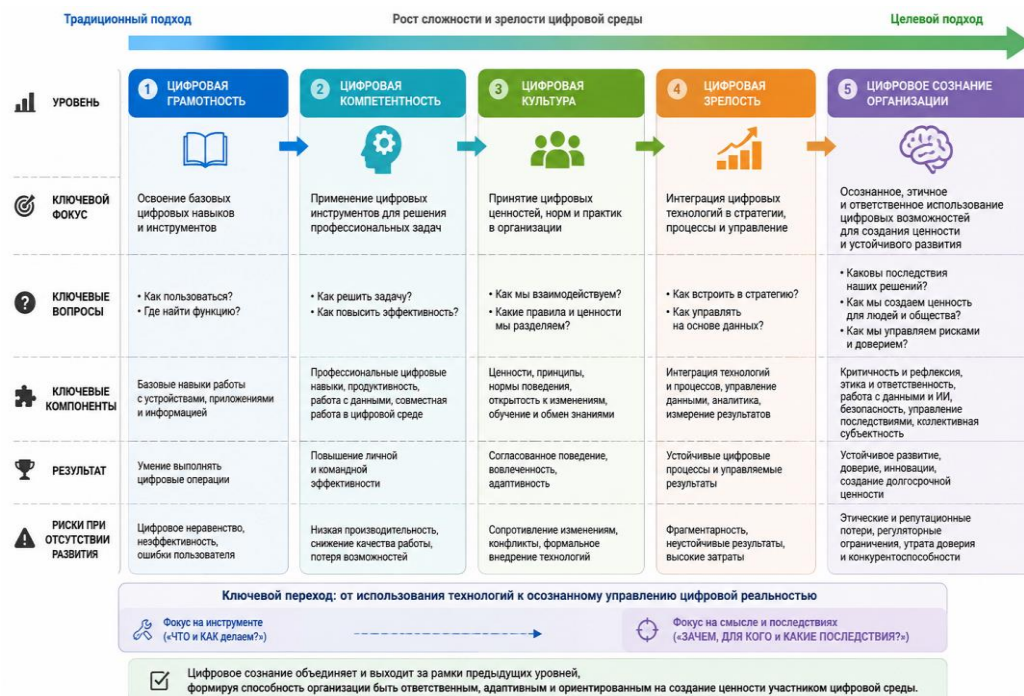


Рисунок 1.2 – Переход от цифровой грамотности к цифровому сознанию организации

Источник: составлено авторами.

Представленная схема фиксирует движение от пользовательских навыков к компетентному действию, цифровой культуре, зрелости и цифровому сознанию как уровню осознания целей, рисков и последствий.

Переход от цифровой грамотности к цифровому сознанию можно представить как движение от индивидуального навыка к коллективной субъектности. На первом уровне человек осваивает инструмент. На втором уровне он применяет цифровую компетентность для решения профессиональных задач. На третьем уровне он учится работать с данными и ИИ, то есть выходит за пределы обычного пользовательского поведения. На четвертом уровне коллектив закрепляет нормы цифровой культуры. На пятом уровне организация достигает цифровой зрелости и масштабирует цифровые процессы. На шестом уровне появляется цифровое сознание: способность не только действовать, но и осознавать последствия цифровых решений.

В образовательной организации этот переход особенно важен. Можно обучить преподавателя пользоваться системой дистанционного обучения, но это не означает, что он понимает, как цифровая среда меняет педагогическое взаимодействие, академическую честность, оценивание, обратную связь и самостоятельность студента. Можно научить сотрудника применять генеративный ИИ для подготовки текста, но это не означает, что он умеет проверять факты, отделять допустимое использование от недопустимого, учитывать персональные данные, авторское право и ответственность за итоговый документ. Поэтому обучение инструментам должно быть встроено в более широкую программу формирования цифрового сознания.

Управленческие ошибки при отсутствии цифрового сознания имеют типовую структуру. Первая ошибка – формальная цифровизация, когда цифровой сервис внедряется ради отчетности, но не меняет процесс. Вторая – цифровая перегрузка, когда количество платформ, каналов и уведомлений увеличивает шум, но не повышает качество управления. Третья – слепая вера в данные, когда показатели воспринимаются как истина без анализа качества и контекста. Четвертая – неуправляемое использование ИИ, когда сотрудники самостоятельно применяют внешние сервисы к рабочим данным. Пятая – размывание ответственности, когда результат алгоритма используется в решении, но никто не отвечает за его проверку.

Данные индекса трудовых тенденций Microsoft Work Trend Index показывают, что массовое использование генеративного ИИ сотрудниками часто опережает готовность организаций к выработке правил: значительная доля работников использует собственные инструменты ИИ на работе [95]. IBM связывает отсутствие управления ИИ и распространение теневого использования ИИ с ростом рисков информационной безопасности и стоимости инцидентов [79]. Эти факты подтверждают: обучение цифровым инструментам без контура управления, распределённой ответственности и культуры проверки не формирует цифровое сознание, а иногда усиливает уязвимость организации.

Методически важно не противопоставлять грамотность и сознание, а выстроить их как уровни одной траектории. Низкий уровень цифровой грамотности делает невозможным цифровое сознание: сотрудник не может критически оценивать то, чем не умеет пользоваться. Но высокая цифровая грамотность также не гарантирует сознания: человек может хорошо владеть инструментом и одновременно использовать его неэтично, небезопасно или вне стратегических целей организации. Следовательно, цифровое сознание начинается там, где навык соединяется с критичностью, нормой, ответственностью и пониманием системного эффекта.

В практическом плане это означает необходимость проектировать образовательные и управленческие программы не по логике «изучим сервисы», а по логике «сформируем способность осмысленно действовать в цифровой среде». Такая программа должна включать не только перечень инструментов, но и сценарии применения, критерии качества результата, правила обращения с данными, требования к проверке ИИ-ответов, этические дилеммы, алгоритм фиксации ошибок и механизм пересмотра цифровых практик. Тогда цифровая грамотность становится входом, а цифровое сознание – управленческим результатом.

Таким образом, цифровое сознание организации не отменяет цифровую грамотность, цифровую компетентность, грамотность в области данных, грамотность в области ИИ, цифровую культуру и цифровую зрелость. Оно интегрирует их и выводит на уровень коллективной рефлексии и ответственности. Поэтому формирование цифрового сознания нельзя свести к курсам по цифровым сервисам; оно требует изменения норм, процессов, управленческих решений и культуры работы с данными и ИИ.

Развитие цифровой среды требует различать базовую цифровую дееспособность и действие в условиях генеративного и агентного ИИ. Этому различию посвящена модель цифрового сознания 1.0 и 2.0.

1.3. ЦИФРОВОЕ СОЗНАНИЕ 1.0 И ЦИФРОВОЕ СОЗНАНИЕ 2.0

Разграничение цифрового сознания 1.0 и цифрового сознания 2.0 является авторским аналитическим приемом. Оно позволяет описать не две независимые категории, а две волны развития организационной способности жить и действовать в цифровой среде. Первая волна связана с освоением цифровых платформ, сервисов, кибергигиены и базовой цифровой культуры. Вторая волна связана с ИИ-насыщенной средой, где алгоритмы начинают участвовать не только в обработке информации, но и в генерации текстов, рекомендаций, прогнозов, решений и управленческих сценариев.

Цифровое сознание 1.0 можно определить как уровень базовой цифровой дееспособности организации. Организация на этом уровне умеет использовать

цифровые инструменты, поддерживать цифровую дисциплину, соблюдать базовые правила безопасности, работать с информацией, понимать значение цифрового следа и включать сотрудников в платформенное взаимодействие. Этот уровень не является примитивным: без него невозможны дистанционная работа, электронный документооборот, цифровые образовательные среды, аналитические панели, электронные коммуникации и базовое управление данными.

Однако цифровое сознание 1.0 имеет ограничение. Оно ориентировано преимущественно на инструментальную и дисциплинарную сторону цифровизации. Главный вопрос здесь: «как правильно использовать цифровой инструмент?». В условиях генеративного ИИ этого вопроса уже недостаточно. Сотрудник может пользоваться ИИ-инструментом технически корректно, но получить ложный ответ, нарушить режим конфиденциальности, воспроизвести предвзятость, подменить профессиональное суждение машинной генерацией или выдать результат ИИ за собственную экспертизу. Поэтому необходим уровень 2.0.

Цифровое сознание 2.0 можно определить как уровень рефлексивного и регулируемого действия в организационной среде, насыщенной ИИ. Он включает грамотность в области ИИ, грамотность в области данных, понимание ограничений генеративных моделей, проверку достоверности результатов, управление алгоритмическими рисками, объяснимость и прозрачность ИИ, принцип «человек в контуре принятия решения» (human-in-the-loop – участие человека в проверке и утверждении результата), этику автоматизации, регламентацию применения ИИ и сохранение ответственности человека за решения, принятые с использованием алгоритмов [92; 101; 135; 137].

Ключевое отличие между уровнями состоит в изменении самой природы цифровой среды. В цифровом сознании 1.0 технология обычно выступает инструментом: платформа хранит документы, система передает сообщения, сервис помогает организовать процесс. В цифровом сознании 2.0 технология становится соучастником интеллектуального действия: ИИ предлагает формулировки, интерпретации, прогнозы, решения, обучающие сценарии и управленческие гипотезы. Поэтому организация должна не только использовать инструмент, но и устанавливать границы делегирования.

Вторая волна цифрового сознания требует нового контура цифрового управления и ответственности. Рамка управления рисками ИИ NIST AI RMF (система управления рисками искусственного интеллекта Национального института стандартов и технологий США) описывает управление рисками ИИ как системную практику, включающую управление, картирование, измерение и контроль рисков [101]. Стандарт ISO/IEC 42001:2023 закрепляет логику системы менеджмента искусственного интеллекта для организаций, разрабатывающих,

предоставляющих или использующих ИИ-системы [83]. Эти рамки важны для пособия потому, что они переводят обсуждение ИИ из уровня энтузиазма или запретов в уровень управляемой организационной архитектуры.

Цифровое сознание 2.0 также требует переосмысления ответственности. В кейсе Air Canada, связанном с неверной информацией чат-бота, организация столкнулась с вопросом: может ли компания снять с себя ответственность за сообщение алгоритмического агента? С точки зрения цифрового сознания ответ очевиден: цифровой агент является частью организационной среды, а значит, информация, генерируемая им во взаимодействии с клиентом, должна быть включена в контур контроля и ответственности [98]. Этот пример показывает, почему цифровое сознание 2.0 не может быть сведено к пользовательской грамотности.

Другой типовой пример – неуправляемая автоматизация в публичном секторе. Австралийский кейс Robodebt показал, что автоматизированная система взыскания задолженностей может привести к масштабным социальным и правовым последствиям, если данные, алгоритмы и управленческая ответственность не соотнесены с правами граждан и человеческой проверкой [120]. Для организации любой сферы это предупреждение: цифровая эффективность без цифрового сознания может обернуться автоматизацией несправедливости.

В бизнес-среде проблема проявляется иначе. По данным McKinsey, организации активно внедряют ИИ, но не всегда достигают масштабируемого эффекта [93]. Это связано не только с качеством моделей. Часто не перестроены процессы, не определены роли, не подготовлены данные, не разработаны правила проверки, не согласованы показатели результата. Цифровое сознание 2.0 здесь выступает как условие перехода от пилотов к устойчивым изменениям: организация должна понимать не только «что может ИИ», но и «какую часть процесса мы готовы ему доверить и как будем контролировать последствия».

Содержательный переход от цифрового сознания 1.0 к цифровому сознанию 2.0 представлен на рисунке 1.3; схема показывает смену фокуса от цифровой дисциплины к ответственному включению ИИ в процессы организации.

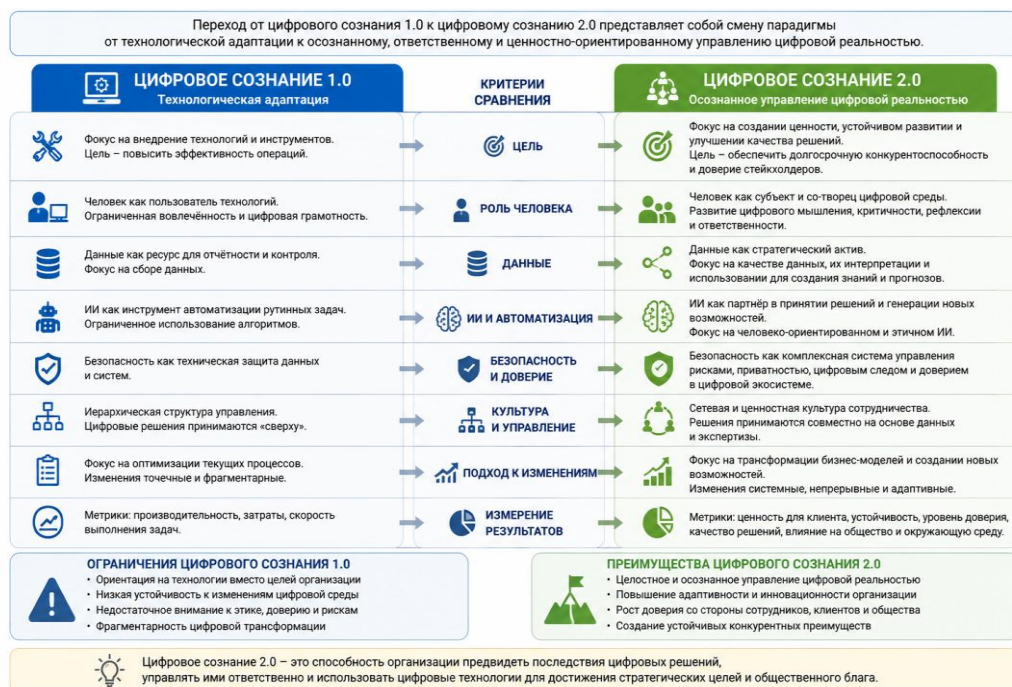


Рисунок 1.3 – Переход от цифрового сознания 1.0 к цифровому сознанию 2.0

Источник: составлено авторами на основе [92; 101; 135; 137].

На рисунке 3 левая часть отражает базовую цифровую дееспособность, правая – среду, насыщенную ИИ, где необходимы проверка результатов, управление рисками и человеческая ответственность.

Сравнение цифрового сознания 1.0 и цифрового сознания 2.0 представлено в таблице 1.3; она сопоставляет содержание уровней, риски, управленческие задачи и индикаторы.

Таблица 1.3 – Цифровое сознание 1.0 и 2.0: содержание, риски, управленческие задачи и индикаторы

Параметр	Цифровое сознание 1.0	Цифровое сознание 2.0
Базовая среда	Цифровые сервисы, платформы, электронные документы, коммуникационные системы.	Генеративный ИИ, агентные системы, автоматизированная аналитика, человеко-алгоритмические контуры.
Главная задача	Освоить инструменты и обеспечить цифровую дисциплину.	Сохранить управляемость, ответственность и критичность при применении ИИ.
Ключевые компетенции	Работа с информацией, цифровая коммуникация, кибергигиена, безопасное	грамотность в области ИИ, грамотность в области данных, проверка ИИ-результатов,

Параметр	Цифровое сознание 1.0	Цифровое сознание 2.0
	поведение.	управление алгоритмическими рисками.
Основные риски	Цифровой разрыв, низкая дисциплина, утечки из-за слабой кибергигиены, формальная цифровизация.	теневое использование ИИ, галлюцинации, предвзятость, нарушение конфиденциальности, размывание ответственности.
Контур управления и ответственности	Правила доступа, регламенты платформ, политика информационной безопасности.	политика применения ИИ, риск-оценка ИИ-сценариев, человек в контуре принятия решения, журналирование применения ИИ.
Индикаторы	Доля сотрудников, прошедших обучение; соблюдение цифровых регламентов; уровень использования платформ.	Наличие политики ИИ; доля проверяемых ИИ-результатов; карта рисков ИИ; ответственные за управление ИИ.
Методический результат	Организация становится цифрово дееспособной.	Организация становится способной к ответственному человеко-алгоритмическому управлению.

Таблица 3 фиксирует различие между цифровой дееспособностью уровня 1.0 и ответственным человеко-алгоритмическим управлением уровня 2.0.

Содержательно переход от 1.0 к 2.0 должен быть организован как управленческая программа. На первом этапе необходимо описать реальные сценарии использования ИИ сотрудниками, включая неформальные практики. На втором – классифицировать сценарии по уровню риска: низкий риск, умеренный риск, высокий риск, недопустимые практики. На третьем – разработать правила применения ИИ в зависимости от типа данных, функции, роли сотрудника и значимости решения. На четвертом – включить обучение грамотности в области ИИ и грамотности в области данных. На пятом – создать механизм мониторинга и корректировки практик.

Особое значение имеет принцип «человек в контуре принятия решения». Его часто трактуют формально: человек просто «присутствует» при решении. Для цифрового сознания 2.0 этого недостаточно. Человек должен иметь компетентность, время, право и обязанность проверить результат ИИ, оспорить его, запросить альтернативу, зафиксировать ошибку и принять окончательное решение. Иначе принцип «человек в контуре принятия решения» превращается в формальное участие человека при фактической передаче решения алгоритму.

В образовательной организации цифровое сознание 2.0 проявляется в нескольких практиках. Преподаватель понимает, когда ИИ может быть помощником при проектировании заданий, а когда его применение разрушает цель обучения. Руководитель образовательной программы понимает, какие

данные студентов допустимо анализировать, а какие требуют отдельного правового и этического режима. Административный сотрудник понимает, что генерация служебного текста ИИ не снимает с него ответственности за факты и формулировки. Студент понимает разницу между допустимой поддержкой мышления и подменой собственной работы.

В управленческом контуре цифровое сознание 2.0 меняет критерий эффективности. В цифровом сознании 1.0 эффективность часто оценивается количеством внедренных систем, скоростью документооборота или долей электронных операций. В цифровом сознании 2.0 к этим показателям добавляются качество данных, объяснимость решений, защищенность цифрового следа, доверие пользователей, снижение рисков, проверяемость ИИ-результатов и способность организации обучаться на ошибках. То есть эффективность становится не только операционной, но и рефлексивной.

Таким образом, цифровое сознание 1.0 обеспечивает цифровую дееспособность организации, но цифровое сознание 2.0 необходимо для насыщенной ИИ среды, где ИИ участвует в генерации знания, решений и управленческих действий. Переход к уровню 2.0 требует не только обучения сотрудников, но и создания системы управления ИИ, правил делегирования, механизмов проверки и сохранения человеческой ответственности.

Цифровое сознание не сводится к сумме индивидуальных компетенций. Далее организация рассматривается как коллективный субъект, который определяет цели цифрового развития, распределяет ответственность, управляет цифровой памятью и корректирует собственную стратегию.

1.4. ОРГАНИЗАЦИЯ КАК КОЛЛЕКТИВНЫЙ СУБЪЕКТ ЦИФРОВОЙ СРЕДЫ

Рассмотрение организации как коллективного субъекта является необходимым условием теоретического обоснования цифрового сознания. Если организация понимается только как сумма работников, то цифровое сознание распадается на набор индивидуальных навыков. Но цифровая трансформация показывает обратное: цифровые решения принимаются, реализуются и оцениваются через распределенные структуры – руководителей, команды, регламенты, данные, платформы, алгоритмы, внешних партнеров и пользователей. Поэтому субъектность организации в цифровой среде имеет коллективный и социотехнический характер.

Классическая субъектно-деятельностная логика подчеркивает, что сознание связано с деятельностью, целями, мотивами и предметным преобразованием мира [11; 22; 36]. Для организации это означает: цифровое сознание проявляется не в декларации о важности технологий, а в том, как организация действует в цифровой среде, какие цели ставит, какие решения принимает, какие

последствия отслеживает и какие нормы закрепляет. Организация осознает цифровую среду через практику: через проектирование процессов, работу с данными, обучение сотрудников и исправление ошибок.

Теория совместной деятельности и коллективной субъектности позволяет дополнить эту рамку. Коллективный субъект возникает не тогда, когда люди находятся в одной структуре, а тогда, когда они имеют общую цель, координацию действий, разделяемые нормы, взаимную ответственность и способность к совместной рефлексии [17]. В цифровой организации эти признаки усложняются: координация осуществляется через платформы, ответственность распределяется между людьми и алгоритмами, а обратная связь поступает в виде данных, метрик, цифровых следов и пользовательских реакций.

Организационное обучение также является важной теоретической опорой. П. Сенге описывает обучающуюся организацию как систему, способную развивать коллективное видение, командное обучение и системное мышление [123]. И. Нонака и Х. Такеучи показывают, что организационное знание создается через взаимодействие явного и неявного знания [104]. В цифровой среде этот процесс получает новую форму: знания фиксируются в цифровых платформах, аналитических панелях, базах данных, чат-ботах, цифровых следах и моделях ИИ. Поэтому цифровое сознание включает способность управлять цифровой памятью организации.

Под цифровой памятью организации в данной главе понимается совокупность данных, документов, цифровых следов, решений, регламентов, моделей, аналитических отчетов и накопленных сценариев, которые позволяют организации помнить, объяснять и корректировать собственную деятельность. Цифровая память не равна архиву. Архив хранит документы, а цифровая память должна поддерживать обучение, диагностику, управленческую рефлексию и передачу опыта. Если цифровая память фрагментирована, организация теряет способность учиться на собственных цифровых действиях.

Организация как коллективный субъект цифровой среды обладает несколькими ключевыми способностями. Первая – способность формулировать цели цифрового развития и связывать их со стратегией. Вторая – способность задавать правила цифрового поведения. Третья – способность управлять данными и цифровым следом. Четвертая – способность распределять ответственность за цифровые решения. Пятая – способность оценивать риски ИИ и автоматизации. Шестая – способность корректировать цифровую стратегию на основе обратной связи. Седьмая – способность поддерживать доверие внешних стейкхолдеров.

Цифровой след играет в этой модели двойственную роль. С одной стороны, он является ресурсом управления: позволяет видеть активность, качество процессов, нагрузку, траектории обучения, клиентский опыт и эффективность

коммуникаций. С другой стороны, цифровой след может стать источником цифрового надзора, недоверия и этических конфликтов. Ш. Зубофф показала, что цифровые данные о поведении человека могут превращаться в объект экономического извлечения и управления поведением [152]. Для организации это означает необходимость различать аналитику развития и практики контроля, подрывающие доверие.

Искусственный интеллект усиливает коллективную субъектность, но одновременно усложняет ее. ИИ может помогать организации видеть закономерности, готовить аналитические материалы, поддерживать обучение и ускорять принятие решений. Однако он может встраивать в организацию непрозрачные критерии, воспроизводить ошибки данных, создавать иллюзию объективности и снижать ответственность человека. Поэтому организация как коллективный субъект должна не просто внедрять ИИ, а понимать, какие решения можно поддерживать алгоритмом, какие требуют экспертного суждения, а какие не должны автоматизироваться.

Важным элементом коллективной субъектности является организационное осмысление событий. К. Вейк показывает, что организации действуют не только на основе объективной информации, но и через процессы интерпретации, придания смысла и коллективного объяснения происходящего [147]. В цифровой среде организационное осмысление становится критически важным: данные сами по себе не говорят, что происходит; ИИ-выводы сами по себе не объясняют, почему следует действовать именно так. Организация должна уметь превращать цифровые сигналы в осмысленные управленческие решения.

Динамические способности организации также помогают раскрыть цифровое сознание. Д. Тис связывает устойчивое развитие организации со способностью распознавать изменения, использовать возможности и трансформировать ресурсы [130]. Цифровое сознание можно рассматривать как когнитивно-культурное условие этих динамических способностей. Без него организация может видеть технологии, но не понимать их стратегического значения; может покупать решения, но не перестраивать процессы; может собирать данные, но не превращать их в организационное знание.

Модель организации как коллективного субъекта цифровой среды представлена на рисунке 1.4; она показывает связь целей, людей, данных, платформ, ИИ, решений, норм и доверия.

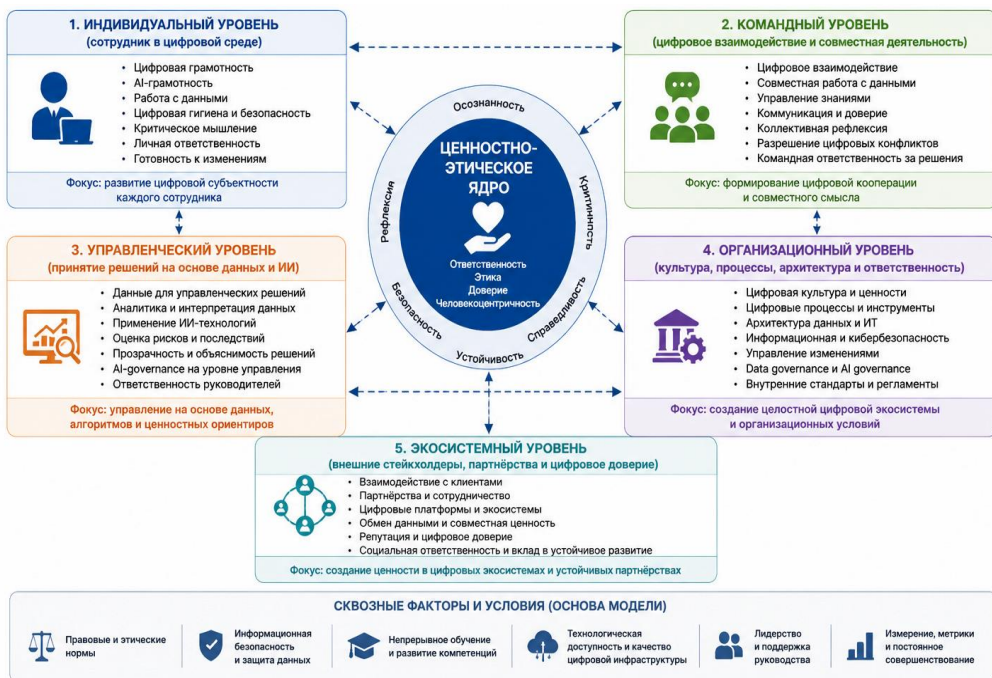


Рисунок 1.4 – Модель цифрового сознания организации

Источник: составлено авторами на основе [17; 123; 130; 147].

Представленная схема показывает, что цифровое сознание формируется не в отдельном подразделении, а в архитектуре совместного действия организации.

Аналитическая модель организации как коллективного субъекта цифровой среды раскрыта в таблице 1.4; она конкретизирует элементы, через которые организация управляет цифровым развитием.

Таблица 1.4 – Аналитическая модель организации как коллективного субъекта цифровой среды

Элемент модели	Содержание	Проявление цифрового сознания
Ценности и цели	Стратегические ориентиры цифрового развития, связь цифровизации с миссией и результатами.	Организация понимает, ради чего использует технологии.
Люди и команды	Сотрудники, руководители, проектные группы, эксперты, пользователи.	Компетенции соединяются с координацией и совместной ответственностью.
Данные и цифровой след	Данные процессов, действий, решений, обучения, коммуникаций, клиентского опыта.	Данные используются критично, этично и с пониманием ограничений.

Элемент модели	Содержание	Проявление цифрового сознания
Платформы и сервисы	Цифровая инфраструктура, системы управления, коммуникации, образовательные и аналитические платформы.	Платформы не навязывают хаос, а поддерживают осмысленные процессы.
ИИ и алгоритмы	Генеративные модели, аналитические алгоритмы, рекомендательные системы, чат-боты.	ИИ включается в контур решения при наличии проверки и ответственности.
Управленческие решения	Выбор, планирование, контроль, оценка, корректировка действий.	Решения принимаются с учетом данных, целей, рисков и последствий.
Нормы и регламенты	Политики, инструкции, права доступа, правила применения ИИ, этические нормы.	Ответственность становится институционально закрепленной.
Рефлексия и корректировка	Анализ результатов, ошибок, обратной связи и непредвиденных последствий.	Организация учится на цифровом опыте.
Стейкхолдеры и доверие	Клиенты, студенты, партнеры, регуляторы, общество.	Цифровое развитие соотносится с доверием и легитимностью.

Данные таблицы показывают, что диагностика цифрового сознания должна охватывать не только компетенции сотрудников, но и управленческую архитектуру организации.

В образовательной организации коллективная субъектность имеет особую специфику. Здесь цифровая среда затрагивает не только административные процессы, но и содержание образования, методику преподавания, оценивание, академическую честность, индивидуальные траектории и воспитательную работу. Поэтому цифровое сознание университета должно объединять педагогическую, управленческую, этическую и технологическую составляющие. Недостаточно внедрить систему управления обучением (LMS – электронная платформа управления обучением), цифровое портфолио или ИИ-ассистента; необходимо понимать, как эти инструменты меняют образовательное взаимодействие и ответственность участников.

Организация как коллективный субъект цифровой среды должна иметь способность к самоограничению. Это важный, но часто недооцененный аспект цифрового сознания. Цифровая возможность не всегда должна превращаться в цифровое действие. Если можно собрать больше данных, это не значит, что их следует собирать. Если можно автоматизировать решение, это не значит, что его

следует автоматизировать. Если можно заменить часть общения чат-ботом, это не значит, что такое решение сохранит доверие. Цифровое сознание проявляется не только в способности внедрять, но и в способности устанавливать границы.

Таким образом, цифровое сознание организации раскрывается полноценно только при рассмотрении организации как коллективного субъекта цифровой среды. Такой субъект действует через людей, данные, платформы, алгоритмы, нормы и обратную связь. Его ключевое качество – способность связывать цифровые решения с целями, ответственностью, доверием и обучением. Поэтому формирование цифрового сознания должно быть направлено не на отдельных пользователей, а на организацию как социотехническую систему.

Теоретическую модель завершает система принципов, определяющих правила проектирования, обучения, управления, оценки и корректировки цифрового развития организации.

1.5. МЕТОДОЛОГИЧЕСКИЕ ПРИНЦИПЫ ФОРМИРОВАНИЯ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

Формирование цифрового сознания организации требует принципиальной рамки. Принципы необходимы для того, чтобы цифровое сознание не превратилось в красивую декларацию или набор лозунгов о цифровизации. Они задают методологические ограничения: что считать допустимым, что считать результативным, что подлежит измерению, как распределяется ответственность и каким образом организация должна учиться на цифровом опыте (рисунок 1.5).

Первым является принцип системности. Цифровое сознание невозможно сформировать через разрозненные мероприятия: один курс по ИИ, одну инструкцию по безопасности или один цифровой сервис. Системность означает, что технологии, данные, люди, процессы, культура и контур управления и ответственности должны рассматриваться во взаимосвязи. Если меняется цифровой инструмент, должны быть пересмотрены роли, регламенты, обучение, показатели и риски. Иначе цифровая трансформация останется фрагментарной.

Второй принцип – человекоцентричность. Он означает, что цифровые технологии должны усиливать человека и организацию, а не подменять человеческое суждение там, где оно необходимо. ЮНЕСКО и ОЭСР связывают ответственное применение ИИ с человеческими правами, достоинством, справедливостью, прозрачностью и подотчетностью [109; 137]. Для цифрового сознания это означает: человек не является помехой для цифровизации, а остается смысловым центром, субъектом ответственности и источником профессионального суждения [12; 20; 109; 124; 137].



Рисунок 1.5 – Методологические принципы формирования цифрового сознания организации

Источник: составлено авторами.

Третий принцип – субъектность. Организация должна быть не объектом технологического давления, а субъектом цифрового развития. Это означает способность самостоятельно определять цели, выбирать цифровые решения, задавать границы автоматизации, оценивать риски и корректировать траекторию. Субъектность противоположна состоянию, при котором организация просто следует моде, копирует чужие практики или внедряет платформы без понимания собственных задач.

Четвертый принцип – этичность. Цифровая среда неизбежно затрагивает персональные данные, цифровой след, справедливость алгоритмов, доступность, прозрачность и доверие. Поэтому любые цифровые решения должны оцениваться не только по эффективности, но и по последствиям для человека и коллективов. Этичность в цифровом сознании означает наличие вопросов: кого затрагивает решение, какие данные используются, кто может пострадать, как предотвращается дискриминация, как обеспечивается право на объяснение и пересмотр.

Пятый принцип – безопасность. Он включает кибергигиену, защиту данных, управление доступами, предотвращение утечек, контроль внешних сервисов и устойчивость цифровой инфраструктуры. ISO/IEC 27001 задает международную логику системы менеджмента информационной безопасности [81]. В контексте цифрового сознания безопасность должна пониматься не как функция ИТ-отдела, а как повседневная ответственность всей организации.

Шестой принцип – критичность. Цифровое сознание невозможно без способности ставить вопросы к данным, алгоритмам и интерфейсам. Критичность не означает недоверие ко всему цифровому. Она означает профессиональную проверку: откуда данные, как они собраны, что не учитывают, какие предположения встроены в модель, насколько результат ИИ проверяем, какие альтернативные объяснения возможны. Без критичности цифровая организация становится уязвимой к иллюзии объективности.

Седьмой принцип – доказательность. Управление на основе данных не должно быть лозунгом. Доказательность требует, чтобы решения опирались на надежные данные, проверяемые показатели, прозрачную интерпретацию и сопоставление с целями. При этом доказательность не равна механическому следованию метрикам. Показатель должен быть объяснен, соотнесен с контекстом и дополнен профессиональным суждением. В противном случае организация рискует управлять не реальностью, а цифровыми суррогатами реальности.

Восьмой принцип – управляемость. Цифровая среда должна быть включена в систему ролей, полномочий, регламентов, показателей и обратной связи. Управляемость особенно важна для ИИ, поскольку неформальное использование внешних инструментов может возникнуть быстрее, чем официальные правила. Поэтому организация должна не только запрещать рискованные практики, но и предлагать легитимные сценарии, обучать сотрудников и создавать понятные каналы консультации.

Девятый принцип – прозрачность и объяснимость. Пользователи, сотрудники и руководители должны понимать, какие цифровые решения используются, какие данные обрабатываются, где применяется ИИ, какие критерии влияют на результат, и кто отвечает за итоговое решение. Рамка управления рисками ИИ NIST AI RMF связывает доверенность ИИ с управлением рисками, измеримостью и объяснимостью на протяжении жизненного цикла системы [101]. Для организации это означает необходимость переводить сложные технологические решения в понятный управленческий язык.

Десятый принцип – риск-ориентированность. Не все цифровые сценарии одинаковы по последствиям. Подготовка информационного текста, анализ обезличенных данных и автоматизированная рекомендация, влияющая на права

человека, требуют разных режимов контроля. Поэтому цифровое сознание предполагает классификацию цифровых и ИИ-сценариев по уровню риска, а не единый запрет или единое разрешение для всех случаев.

Одиннадцатый принцип – адаптивность. Цифровая среда меняется быстрее, чем традиционные регламенты. Поэтому формирование цифрового сознания должно включать регулярный пересмотр правил, обновление образовательных программ, анализ новых инструментов и корректировку практик. Жесткая инструкция без механизма обновления быстро устареет и начинает стимулировать неформальные обходные практики.

Двенадцатый принцип – рефлексивность. Организация должна уметь анализировать собственные цифровые действия: что получилось, что не сработало, какие ошибки возникли, какие риски проявились, как изменилась нагрузка сотрудников, повысилось ли доверие. Рефлексивность превращает цифровой опыт в организационное обучение. Без нее цифровая трансформация превращается в цепочку проектов без накопления понимания.

Тринадцатый принцип – баланс автоматизации и человеческой ответственности. Он особенно важен для цифрового сознания 2.0. Автоматизация должна освобождать человека от рутинных операций и усиливать качество решения, но не уничтожать ответственность. Человек должен сохранять право и обязанность проверки, особенно там, где решение затрагивает права, развитие, оценку, безопасность или репутацию людей.

Четырнадцатый принцип – организационное обучение. Цифровое сознание не формируется одновременно. Оно требует образовательных программ, практических кейсов, обмена опытом, внутренних методических материалов, анализа инцидентов и поддержки руководителей. Организационное обучение должно связывать индивидуальные компетенции с командными и управленческими практиками.

Пятнадцатый принцип – отраслевая адаптируемость. Университет, банк, медицинская организация, промышленное предприятие и орган государственной власти используют данные и ИИ в разных режимах риска. Поэтому методология цифрового сознания должна иметь общий каркас, но адаптироваться к отрасли, типам данных, правовому режиму, профессиональной этике и характеру решений. Универсальная рамка без отраслевой адаптации будет слишком общей, а узкая инструкция без общей рамки – несистемной.

Система методологических принципов формирования цифрового сознания организации представлена в таблице 1.5; она переводит теоретическую рамку в управленческие ориентиры, индикаторы и риски.

Таблица 1.5 – Методологические принципы формирования цифрового сознания организации

Принцип	Краткое содержание	Практический индикатор	Риск нарушения
Системность	Связь технологий, данных, людей, процессов, культуры и контур управления и ответственности.	Наличие единой программы цифрового развития.	Фрагментарная цифровизация и дублирование сервисов.
Человекоцентричность	Приоритет развития человека и сохранения профессионального суждения.	Оценка влияния цифровых решений на сотрудников и пользователей.	Технологическое давление и снижение доверия.
Субъектность	Способность организации самостоятельно задавать цели и границы цифровизации.	Цифровая стратегия, согласованная с миссией и процессами.	Следование моде без управленческого смысла.
Этичность	Учет справедливости, прав, доверия, цифрового следа и последствий.	Этическая экспертиза высокорисковых цифровых сценариев.	Дискриминация, репутационные потери, недоверие.
Безопасность	Кибергигиена, защита данных, контроль доступа и внешних сервисов.	Регламент работы с данными и ИИ, обучение сотрудников.	Утечки, теневое использование ИИ, нарушение конфиденциальности.
Критичность	Проверка данных, алгоритмов, ИИ-ответов и цифровых метрик.	Чек-листы проверки ИИ-результатов и источников данных.	Слепая вера в алгоритмы и автоматизация ошибок.
Доказательность	Опора на качественные данные и проверяемые показатели.	Показатели связаны с целями и имеют владельцев.	Управление цифровыми суррогатами вместо реальности.
Управляемость	Роли, полномочия, регламенты, контроль и обратная связь.	Назначены ответственные за цифровые и ИИ-сценарии.	Неуправляемые практики и размывание ответственности.
Прозрачность и объяснимость	Понимание логики цифровых решений и	Пользователи знают, где и как	Недоверие, невозможность

Принцип	Краткое содержание	Практический индикатор	Риск нарушения
	применения ИИ.	применяется ИИ.	оспорить результат.
Риск-ориентированность	Разные режимы контроля для разных уровней риска.	Карта рисков цифровых и ИИ-сценариев.	Единые правила для неравных по последствиям ситуаций.
Адаптивность	Регулярное обновление правил и программ обучения.	Периодический пересмотр цифровых регламентов.	Устаревание правил и уход в неформальные практики.
Рефлексивность	Анализ последствий, ошибок, нагрузки и доверия.	Постпроектный анализ цифровых инициатив.	Повторение ошибок и отсутствие организационного обучения.
Баланс автоматизации и ответственности	ИИ поддерживает, но не снимает человеческое решение.	Определены зоны обязательной человеческой проверки.	Формальный человек в контуре принятия решения и потеря ответственности.
Организационное обучение	Связь индивидуальных компетенций с командными практиками.	Внутренние курсы, кейсы, методические материалы.	Разрыв между обучением и реальной практикой.
Отраслевая адаптируемость	Учет специфики отрасли, данных, правового режима и этики.	Отраслевые сценарии и матрицы допустимого применения.	Слишком общие или неприменимые правила.

Данные таблицы показывают, что каждый принцип имеет практический индикатор и риск нарушения, поэтому может использоваться для диагностики, обучения и регламентации.

Практическая реализация этих принципов предполагает поэтапный алгоритм. На первом этапе проводится диагностика текущего состояния: цифровые сервисы, данные, ИИ-практики, компетенции сотрудников, цифровая культура, риски и регламенты. На втором этапе формируется карта целевого цифрового сознания: какие компетенции, нормы, роли и механизмы ответственности должны быть достигнуты. На третьем этапе разрабатываются образовательные и управленческие инструменты: программы обучения, инструкции, матрицы рисков, чек-листы проверки, регламенты применения ИИ.

На четвертом этапе запускаются пилотные практики. На пятом – проводится оценка результата и корректировка.

Для университета такая методология особенно значима, поскольку цифровое сознание должно формироваться не только у административных сотрудников, но и у преподавателей, студентов, руководителей образовательных программ и проектных команд. При этом уровни должны различаться. Студенту необходима грамотность ответственного использования ИИ в обучении. Преподавателю – методика включения цифровых сервисов и ИИ в образовательную деятельность. Руководителю – способность управлять данными, процессами, рисками и качеством. Организации в целом – культура доказательности, доверия, безопасности и рефлексии.

Важно, что принципы не являются абстрактными декларациями. Каждый из них должен иметь индикаторы. Например, принцип критичности может проявляться в наличии чек-листа проверки ИИ-ответа; принцип безопасности – в запрете загрузки персональных данных в неутвержденные сервисы; принцип прозрачности – в маркировке материалов, подготовленных с использованием ИИ; принцип организационного обучения – в регулярном разборе кейсов удачного и неудачного применения цифровых инструментов; принцип риск-ориентированности – в матрице допустимых сценариев использования ИИ.

Таким образом, формирование цифрового сознания организации должно строиться на системе принципов, соединяющих системность, человекоцентричность, субъектность, этичность, безопасность, критичность, доказательность, управляемость, прозрачность, риск-ориентированность, адаптивность, рефлексивность, баланс автоматизации и ответственности, организационное обучение и отраслевую адаптируемость. Только такая система позволяет перевести цифровое сознание из концепта в управленческую и образовательную практику.

ИТОГИ ГЛАВЫ

В главе цифровое сознание организации обосновано как самостоятельный аналитический и управленческий конструкт, который интегрирует цифровую грамотность, компетентность, культуру и зрелость, но не сводится к ним. Разграничение цифрового сознания 1.0 и 2.0 показывает переход от базовой цифровой дееспособности к ответственному действию в среде, насыщенной ИИ.

Управленческий переход к главе 2: сформированные принципы становятся критериями проектирования цифровых изменений и задают требования к ответственности, безопасности и контролю. Далее они переводятся в уровни объекта управления, для каждого из которых определяются субъекты, проявления, риски и механизмы развития.

Интерактивное сопровождение. В цифровом руководстве размещены глоссарий, сравнительная карта смежных понятий, визуальная модель цифрового сознания 1.0 и 2.0 и чек-лист методологических принципов.

ГЛАВА 2. УРОВНИ И МЕХАНИЗМЫ УПРАВЛЕНИЯ ФОРМИРОВАНИЕМ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

«По существу, все модели неверны, но некоторые полезны».

Джордж Бокс

Управленческий вопрос главы. На каких уровнях формируется цифровое сознание и как индивидуальные действия превращаются в командные практики, управленческие решения и организационные нормы?

Управленческий результат главы. Уровневая карта субъектов, наблюдаемых проявлений, рисков дефицита и механизмов развития на индивидуальном, командном, управленческом, организационном и экосистемном уровнях.

2.1. ИНДИВИДУАЛЬНЫЙ УРОВЕНЬ ЦИФРОВОГО СОЗНАНИЯ: СОТРУДНИК В ЦИФРОВОЙ СРЕДЕ

Индивидуальный уровень является исходным, но не самодостаточным уровнем цифрового сознания организации. На нем цифровое сознание проявляется как способность конкретного сотрудника действовать в цифровой среде не только технически грамотно, но и осмысленно: понимать назначение инструмента, качество исходных данных, ограничения цифрового сервиса, риски распространения информации, правовые и этические последствия собственных действий. В этом смысле сотрудник перестает быть только пользователем цифровых систем и становится субъектом цифровой среды. Он не просто нажимает кнопки и выполняет инструкции, а соотносит цифровое действие с профессиональной задачей, нормами организации и ответственностью перед другими участниками процесса [59; 146].

В научно-методическом плане индивидуальный уровень целесообразно раскрывать через сочетание четырех групп характеристик. Первая группа – инструментальная: владение устройствами, приложениями, корпоративными платформами, системами документооборота, аналитическими панелями и средствами коммуникации. Вторая группа – информационно-аналитическая: умение искать, оценивать, структурировать, интерпретировать и использовать данные. Третья группа – критико-рефлексивная: способность выявлять ошибки, проверять выводы ИИ, задавать уточняющие вопросы и понимать последствия цифрового действия. Четвертая группа – этико-правовая: соблюдение правил работы с персональными и конфиденциальными данными, учет прав участников процессов, кибергигиена и ответственность за результат.

Европейская рамка DigComp 3.0 задает полезную основу для такого описания, поскольку цифровая компетентность в ней понимается не только как набор навыков, но как сочетание знаний, умений и установок. Важно, что компетентность в области ИИ в DigComp 3.0 встроена во все компетенции, а не

выделена в отдельный технологический блок. Для многоуровневой логики формирования цифрового сознания это принципиально: грамотность в области ИИ не должна пониматься как навык работы с одним чат-ботом или сервисом генерации текста. Она должна рассматриваться как часть профессионального суждения сотрудника, включающего понимание возможностей, ограничений, рисков и зоны человеческой ответственности [59].

Индивидуальный уровень цифрового сознания особенно значим для любой организации, где сотрудник регулярно взаимодействует с цифровыми системами, данными, автоматизированной аналитикой, сервисами генерации текстов, корпоративными платформами и внешними цифровыми каналами. Сотрудник сталкивается не только с интерфейсом инструмента, но и с данными клиентов, контрагентов, коллег, производственных или управленческих процессов. Поэтому цифровое сознание сотрудника включает профессиональную, правовую, этическую и управленческую ответственность: нельзя использовать ИИ для ускорения работы, не понимая, как проверить результат, как не нарушить режим данных, как не подменить экспертное суждение автоматической рекомендацией и как объяснить принятое решение [67; 101; 137].

На практике индивидуальный уровень часто подменяется краткосрочным обучением работе с отдельным инструментом. Такая подмена создает иллюзию цифровой готовности. Сотрудник может уметь сформировать запрос к генеративной модели, но не понимать, почему полученный результат требует проверки; может пользоваться аналитической панелью, но не видеть, что показатель построен на неполных данных; может работать в облачном сервисе, но не различать открытые, служебные и персональные данные. Поэтому методическое проектирование обучения должно строиться не по логике «освоить сервис», а по логике «сформировать ответственное цифровое действие» [79; 88].

Структура индивидуального уровня представлена на рисунке 2.1. Схема объединяет компетентность, работу с данными, грамотность в области ИИ, критичность, кибергигиену и этику в единый профиль ответственного цифрового действия.



Рисунок 2.1 – Профиль сотрудника в цифровой среде
Источник: составлено авторами на основе [59; 88; 133; 146].

Представленная схема фиксирует ключевую методическую идею: сотрудник должен быть не пассивным пользователем, а ответственным участником цифрового действия. Каждая составляющая профиля связана с практическими индикаторами: умением проверять данные, оценивать результаты ИИ, соблюдать кибергигиену, учитывать этические последствия и сохранять профессиональное суждение.

Для диагностики индивидуального уровня недостаточно спрашивать, владеет ли сотрудник тем или иным сервисом. Более продуктивно использовать индикаторы, показывающие качество цифрового поведения: умеет ли сотрудник описать цель применения инструмента; проверяет ли результат ИИ по независимым источникам; знает ли правила работы с персональными и конфиденциальными данными; понимает ли, какие решения нельзя полностью передавать алгоритму; способен ли объяснить клиенту, коллеге, партнеру или руководителю основания цифрового решения. Такой подход требует сочетать самооценку, проверку практических действий, анализ инцидентов, обратную связь руководителя и командную рефлекссию [59; 88; 93].

Особое место занимает грамотность в области данных. В организации данные редко бывают нейтральными: они собираются в конкретных процессах, зависят от качества ввода, имеют владельцев, контекст возникновения, ограничения использования и правовой режим. Сотрудник с развитым цифровым сознанием понимает, что показатель не равен реальности, а является моделью реальности. Поэтому он задает вопросы: кто собрал данные, как они очищались, какие категории не попали в выборку, какие выводы допустимы, какие решения могут быть ошибочными. Такое отношение к данным формирует основу доказательного управления, но одновременно защищает организацию от ложной уверенности в формальной аналитике [18; 93].

Грамотность в области ИИ также должна включать не только знакомство с генеративными сервисами, но и понимание алгоритмических рисков. К ним относятся недостоверные ответы, воспроизведение предвзятости данных, нарушение авторских прав, подмена экспертного суждения статистической вероятностью, несанкционированная передача информации во внешние сервисы, снижение самостоятельности мышления. Поэтому индивидуальный уровень цифрового сознания требует закрепления простого правила: ИИ может быть помощником, аналитическим инструментом и средством ускорения рутинных операций, но не может быть безответственным заместителем профессионального решения [46; 93; 137].

В организационной практике индивидуальный уровень целесообразно формировать через короткие модульные программы, разбор реальных кейсов, инструкции по допустимому применению ИИ, чек-листы верификации результатов, наставничество и регулярное обновление компетенций. Результатом должна быть не только способность работать с сервисом, но и способность принимать обоснованные цифровые решения в пределах своей роли и зоны ответственности.

Методическая детализация индивидуального уровня дана в таблице 2.1. Таблица связывает компоненты индивидуального цифрового сознания с наблюдаемыми индикаторами и типовыми управленческими действиями.

Таблица 2.1 – Компоненты индивидуального уровня цифрового сознания

Компонент	Содержание	Наблюдаемые индикаторы	Методические средства формирования
Цифровая компетентность	Уверенное применение цифровых инструментов для профессиональных задач	Выполняет операции без постоянной помощи; выбирает инструмент под задачу; соблюдает правила работы в системе	Практикумы, инструкции, наставничество, внутренние курсы

Компонент	Содержание	Наблюдаемые индикаторы	Методические средства формирования
Грамотность в области данных	Понимание источников, качества, ограничений и интерпретации данных	Проверяет источник данных; различает факт, оценку и прогноз; умеет объяснить показатель	Обучение работе с показателями, карта источников данных, разбор ошибок аналитики
Грамотность в области ИИ	Понимание возможностей и ограничений ИИ-сервисов	Проверяет выводы ИИ; не передает конфиденциальные сведения; знает допустимые сценарии применения	Регламент ИИ, чек-лист запросов, библиотека проверенных сценариев
Критичность и рефлексия	Способность оценивать последствия цифрового действия	Выявляет сомнительные результаты; задает уточняющие вопросы; фиксирует ошибки	Кейс-семинары, разбор инцидентов, рефлексивные отчеты
Кибергигиена и ответственность	Безопасное поведение в цифровой среде	Использует надежную аутентификацию; соблюдает режим доступа; распознает риски фишинга	Инструктаж, тестирование, имитационные проверки, персональная ответственность

Источник: составлено авторами на основе [59; 88; 93; 133; 146].

Данные таблицы показывают, что индивидуальный уровень может быть операционализирован через конкретные индикаторы поведения. Это важно для последующей диагностики: цифровое сознание сотрудника должно проявляться не в декларации уверенности, а в проверяемых действиях.

Таким образом, индивидуальный уровень является базовым условием цифрового сознания организации, но не исчерпывает его. Сотрудник в цифровой среде должен обладать не только навыками работы с инструментами, но и способностью критически интерпретировать данные, проверять результаты ИИ, соблюдать нормы безопасности и понимать последствия цифровых решений. Переход к следующему уровню связан с тем, что индивидуальные компетенции должны стать командной практикой, иначе организация получает набор разрозненных пользователей, а не коллективного субъекта цифровой среды.

2.2. КОМАНДНЫЙ УРОВЕНЬ ЦИФРОВОГО СОЗНАНИЯ: ЦИФРОВОЕ ВЗАИМОДЕЙСТВИЕ И СОВМЕСТНАЯ ДЕЯТЕЛЬНОСТЬ

Командный уровень показывает, как индивидуальные цифровые способности превращаются в согласованные практики совместной деятельности. На этом уровне цифровое сознание проявляется в том, что группа людей формирует общее понимание задачи, данных, допустимых инструментов, правил коммуникации и зоны ответственности. Если индивидуальный уровень отвечает на вопрос, способен ли сотрудник действовать осознанно, то командный уровень отвечает на вопрос, способна ли группа людей выработать единое понимание цифровой ситуации и согласованно действовать в ней [43; 145].

Команда в цифровой среде работает не только с людьми, но и с цифровыми посредниками: корпоративными порталами, системами управления проектами, корпоративными мессенджерами, аналитическими панелями, хранилищами документов, сервисами ИИ, системами контроля исполнения. Эти посредники меняют характер взаимодействия: часть знаний переносится в документы и базы данных, часть решений фиксируется в системах, часть коммуникации становится цифровым следом, а часть управленческого контроля реализуется через платформенные показатели. Поэтому командное цифровое сознание должно включать правила совместной работы с такими посредниками.

Ключевая проблема командного уровня – разрыв интерпретаций. Разные участники одной команды могут по-разному понимать показатели, по-разному оценивать риски ИИ, по-разному относиться к цифровым регламентам. Один сотрудник воспринимает аналитику как точное отражение реальности, другой – как вспомогательный сигнал; один использует ИИ для черновиков документов, другой считает это нарушением профессиональных норм; один хранит материалы в утвержденной системе, другой – в личном облаке. При отсутствии согласования такие различия порождают не цифровую зрелость, а скрытую фрагментацию практик.

Цифровое сознание команды формируется через общие ментальные модели. Это означает, что участники должны одинаково понимать цели цифрового действия, качество используемых данных, границы автоматизации, порядок проверки результатов и критерии приемлемого риска. В теории организационного обучения такой переход можно описать как превращение индивидуального опыта в коллективное знание, а в логике управления знаниями – как преобразование личных навыков и наблюдений в разделяемую практику команды [43; 101].

В организации командный уровень проявляется в работе проектных групп, функциональных подразделений, межфункциональных команд, рабочих групп

по внедрению ИИ, команд сопровождения цифровых продуктов и операционных процессов. Например, цифровое сознание подразделения выражается не в том, что отдельные сотрудники умеют пользоваться корпоративной системой, а в том, что команда имеет общие требования к данным, единые правила подготовки цифровых материалов, согласованный порядок применения ИИ, понятные процедуры работы с цифровым следом и общую ответственность за качество результата.

На рисунке 2.2 командный уровень представлен как замкнутый контур взаимодействия: от общей задачи и единых данных к правилам применения ИИ, командному решению, рефлексии и обновлению практик.

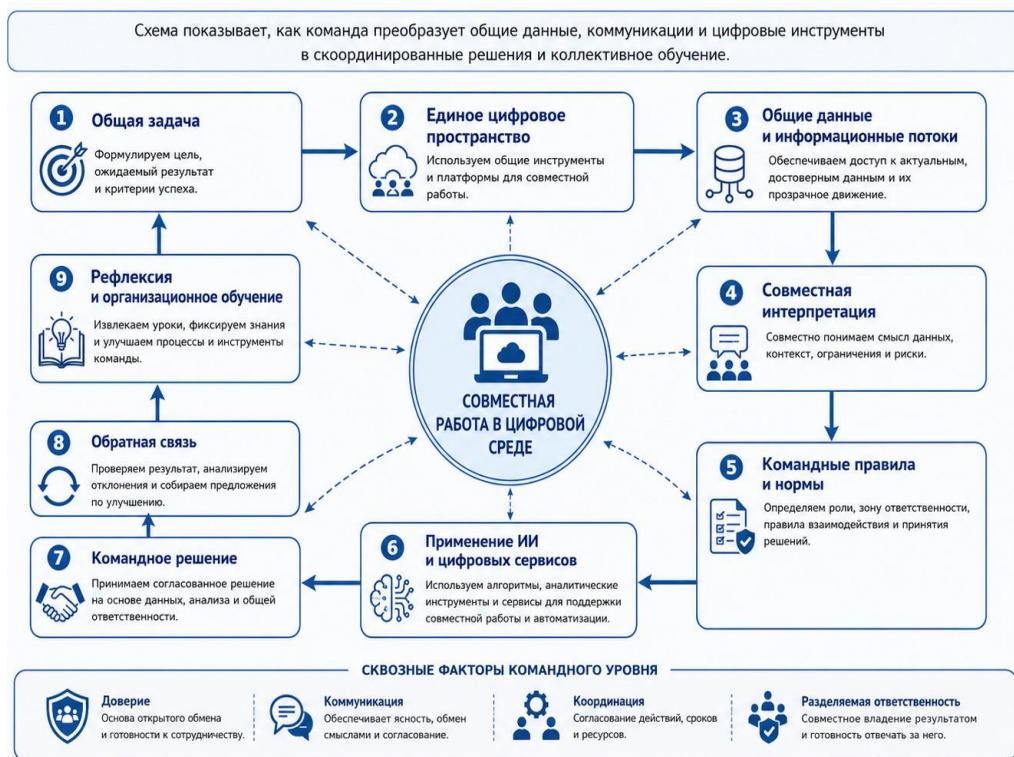


Рисунок 2.2 – Командный контур цифрового взаимодействия

Источник: составлено авторами на основе [43; 88; 101; 145].

Представленная схема показывает, что командное цифровое сознание возникает не в момент использования общего цифрового сервиса, а в момент согласования смыслов, правил и ответственности. Важным элементом является рефлексия: команда должна возвращаться к результату, анализировать ошибки и уточнять цифровые практики.

Командный уровень требует особого внимания к цифровой коммуникации. Быстрая коммуникация через мессенджеры и платформы повышает

оперативность, но может снижать качество обсуждения, размывать ответственность и создавать информационную перегрузку. Для цифрового сознания команды важно различать каналы: где обсуждается идея, где фиксируется решение, где хранится документ, где назначается ответственное лицо, где отражается риск. Без такого разграничения цифровая среда становится источником хаоса, а не управляемости.

Другой компонент командного уровня – совместная работа с данными. Команда должна иметь единые правила чтения показателей. Если показатели производительности, качества, вовлеченности, финансовой устойчивости или проектной активности интерпретируются без контекста, они легко превращаются в источник ошибочных решений. Поэтому командная аналитическая культура предполагает регулярное обсуждение не только самих цифр, но и того, как они получены, что они не показывают, какие управленческие действия допустимы на их основе [18; 93].

Особую роль играет командное применение ИИ. На практике генеративные модели часто начинают использоваться снизу: сотрудники пробуют сервисы для подготовки служебных писем, аналитических записок, отчетов, презентаций, программного кода и сценариев коммуникации. Без командных правил это приводит к скрытому применению ИИ, различию качества материалов, рискам утечки информации и конфликтам вокруг авторства. Поэтому команда должна договориться о допустимых сценариях: где ИИ используется как инструмент черновой подготовки, где требуется обязательная экспертная проверка, где применение ИИ запрещено, где нужен след проверки результата [79; 88].

Командное цифровое сознание формируется через регулярные практики: короткие сессии обмена цифровыми находками, совместный разбор ошибок ИИ, коллективное описание удачных запросов и шаблонов, единое хранилище проверенных материалов, назначение ответственных за данные, горизонтальную взаимопомощь, обсуждение этических ситуаций. Такие практики переводят цифровое развитие из режима индивидуальных экспериментов в режим коллективного обучения.

При этом командный уровень не должен превращаться в чрезмерную регламентацию. Его задача – не подавить инициативу сотрудников, а создать безопасный контур совместной деятельности. Команда должна иметь пространство для цифровых экспериментов, но эксперименты должны быть прозрачными, обсуждаемыми и соотнесенными с целями организации. Именно в этом балансе инициативы и ответственности проявляется зрелость командного цифрового сознания.

Диагностические признаки командного уровня систематизированы в таблице 2.2. Она показывает, какие элементы совместной деятельности должны быть проверены при оценке цифрового сознания команды.

Таблица 2.2 – Диагностика командного уровня цифрового сознания

Элемент	Содержание	Индикатор наличия	Риск дефицита
Общая цель цифрового действия	Команда понимает, для чего используется цифровой инструмент или ИИ	Участники одинаково формулируют цель, ожидаемый результат и ограничения	Инструменты используются ради формы, а не ради задачи
Единая интерпретация данных	Команда согласует источники, показатели и правила чтения данных	Показатели обсуждаются с учетом контекста, ограничений и качества данных	Разные сотрудники принимают несовместимые решения на основе одних данных
Правила применения ИИ	Участники знают допустимые и недопустимые сценарии	Есть общий протокол проверки, хранения и маркировки материалов, подготовленных с ИИ	Скрытое применение ИИ, нарушение конфиденциальности, падение качества
Цифровая коммуникация	Каналы общения и фиксации решений разведены	Решения фиксируются в утвержденных системах; ответственные видимы	Потеря решений в переписке, информационная перегрузка
Командная рефлексия	Команда анализирует последствия цифровых действий	Проводятся разборы кейсов, ошибок, успешных практик	Ошибки повторяются, знания не закрепляются

Источник: составлено авторами на основе [43; 88; 101; 145].

Данные таблицы показывают, что командное цифровое сознание можно оценивать по согласованности целей, данных, правил применения ИИ, коммуникации и рефлексии. Эти признаки позволяют отличить команду, которая просто использует цифровые сервисы, от команды, которая осознанно управляет цифровым взаимодействием.

Таким образом, командный уровень переводит индивидуальные цифровые компетенции в коллективную практику. Его ядро составляет согласование целей, данных, правил цифровой коммуникации, допустимых сценариев применения ИИ и процедур совместной ответственности. Без командного уровня цифровое сознание остается личным качеством отдельных сотрудников и

не становится свойством организации. Следующий уровень показывает, как эти командные практики включаются в управленческие решения.

2.3. УПРАВЛЕНЧЕСКИЙ УРОВЕНЬ ЦИФРОВОГО СОЗНАНИЯ: ПРИНЯТИЕ РЕШЕНИЙ НА ОСНОВЕ ДАННЫХ И ИИ

Управленческий уровень является переходом от коллективных практик к целенаправленному управлению организацией. На этом уровне цифровое сознание проявляется в способности руководителей использовать данные, цифровые следы, аналитические модели и ИИ не как декоративное сопровождение, а как доказательную основу управленческих решений. Однако такая основа должна быть критически осмысленной: данные требуют интерпретации, алгоритмы требуют проверки, а окончательная ответственность за решение остается за человеком и организацией [93; 101].

В условиях цифровой трансформации управленческое решение меняет структуру. Раньше руководитель часто опирался преимущественно на опыт, экспертное мнение и отчетность. В цифровой среде к этим основаниям добавляются массивы данных, автоматизированные показатели, прогнозные модели, рекомендации ИИ, цифровые сигналы поведения сотрудников, клиентов, пользователей или партнеров. Это расширяет возможности управления, но одновременно создает риск ложной объективности. Цифровое сознание руководителя состоит в том, чтобы видеть не только показатель, но и способ его производства; не только рекомендацию ИИ, но и границы ее применимости; не только скорость решения, но и последствия его автоматизации [18; 93].

Управленческий уровень связан с понятием управления ИИ (AI governance, система правил, ролей и процедур ответственного применения ИИ). В дальнейшем в главе используется русская формулировка «управление ИИ». Управление ИИ включает определение допустимых сценариев, распределение ответственности, требования к качеству данных, процедуры оценки рисков, документирование решений, контроль доступа, журналирование действий и механизмы пересмотра результатов. Без этого ИИ в управлении превращается в неформальный источник рекомендаций, за которые никто реально не отвечает [67; 83; 93].

Для организации особенно опасна подмена управленческого решения алгоритмической рекомендацией. Алгоритм может предложить вариант, но не несет ответственности за социальные, этические, правовые и стратегические последствия. Поэтому развитое цифровое сознание предполагает сохранение человека в контуре принятия решений (human-in-the-loop, обязательное участие человека в контроле значимого цифрового решения). Далее используется русская формулировка «человек в контуре решения». Этот принцип особенно

важен в управлении персоналом, финансах, медицине, клиентских сервисах, промышленной безопасности и государственных сервисах, где цифровые решения влияют на права, безопасность и жизненные траектории людей [67; 101; 137].

Управленческий уровень требует от руководителя нового набора вопросов. Не только «какой показатель изменился?», но и «почему он изменился?», «какие данные не попали в анализ?», «какая модель построила прогноз?», «кто проверил вывод ИИ?», «какие группы могут пострадать от решения?», «как будет зафиксирована ответственность?», «как мы узнаем, что решение привело к нужному результату?». Эти вопросы переводят цифровизацию из режима технической автоматизации в режим ответственного управления.

Управленческий цикл решения на основе данных и ИИ представлен на рисунке 2.3. Схема показывает, что данные и ИИ являются элементами управленческого цикла, но не отменяют человеческое решение, журналирование, обратную связь и оценку рисков.



Рисунок 2.3 – Управленческий цикл решения на основе данных и ИИ

Источник: составлено авторами на основе [67; 83; 93; 101].

Рисунок 2.3 раскрывает управленческий уровень как цикл: данные проходят аналитическую обработку, ИИ формирует рекомендацию, человек принимает решение, организация внедряет действие, после чего результат возвращается в контур обратной связи. Схема подчеркивает, что цифровое сознание

руководителя проявляется в умении управлять всем циклом, а не только пользоваться итоговой рекомендацией.

На управленческом уровне особое значение приобретает качество данных. Некачественные данные порождают качественно оформленные, но содержательно ошибочные решения. Например, если система аналитики процесса не учитывает сезонность, пропуски данных, технические сбои, различия в методиках учета или контекст подразделения, управленческий вывод может быть несправедливым или неэффективным. Поэтому руководитель должен понимать, что цифровая аналитика требует не только технологической платформы, но и методологии сбора, верификации, очистки, интерпретации и правомерного использования данных [13; 18].

Второй компонент управленческого уровня – риск-ориентированность. NIST AI RMF переводит тему надежного ИИ в управленческий язык: необходимо не только декларировать этичность и прозрачность, но и описывать риски, измерять их, управлять ими и контролировать последствия на протяжении жизненного цикла системы. ISO/IEC 42001:2023 усиливает эту логику, поскольку требует рассматривать ИИ как объект системы менеджмента: с политиками, целями, ролями, документированной информацией, оценкой результативности и постоянным улучшением [83; 93].

Третий компонент – прозрачность управленческого решения. Прозрачность не означает раскрытие всех технических деталей алгоритма каждому участнику процесса. Она означает, что организация способна объяснить, какие данные использовались, кто принимал решение, как была проверена рекомендация, какой порядок обжалования или пересмотра предусмотрен, какие риски были учтены. Это особенно важно при использовании аналитики для управления персоналом, клиентским опытом, распределением ресурсов, оценкой эффективности процессов, прогнозированием рисков и административными решениями.

Четвертый компонент – управленческая рефлексия. Руководитель должен оценивать не только достижение показателя, но и побочные эффекты цифрового решения. Автоматизация может ускорить процесс и одновременно снизить доверие; аналитика может выявить проблему и одновременно создать ощущение цифрового надзора; ИИ может повысить скорость подготовки документов и одновременно стандартизировать мышление. Цифровое сознание управленца проявляется в способности видеть эти эффекты заранее и корректировать управленческую практику после получения обратной связи [137; 145].

Практическое формирование управленческого уровня требует обучения руководителей не только инструментам аналитики, но и логике цифровой ответственности. Руководитель должен понимать основы жизненного цикла данных, принципы работы ИИ, правила информационной безопасности, этику

автоматизации, требования к документированию решений, способы оценки цифровой нагрузки на сотрудников. Это делает управленческое звено не потребителем готовых панелей, а активным субъектом цифрового развития организации.

В таблице 2.3 представлена карта управленческих задач, которые необходимо закрепить для формирования цифрового сознания на уровне принятия решений.

Таблица 2.3 – Управленческие задачи цифрового сознания при принятии решений

Задача	Содержание	Инструмент закрепления	Риск при отсутствии
Целеполагание	Связать цифровую инициативу со стратегическими целями	Паспорт цифровой инициативы, ожидаемый эффект, критерии успеха	Формальная цифровизация без результата
Качество данных	Проверить источники, полноту, актуальность и правовой режим данных	Реестр данных, владелец данных, правила обновления	Ошибочные выводы, недоверие к аналитике
Проверка ИИ-рекомендации	Оценить достоверность, ограничения и риски результата ИИ	Чек-лист верификации, экспертная проверка, журнал запроса и ответа	Слепое доверие алгоритму, неуправляемая ошибка
Человеческий контроль	Сохранить ответственность руководителя за значимое решение	Фиксация ответственного лица, порядок пересмотра решения	Подмена ответственности ссылкой на систему
Оценка последствий	Проверить влияние решения на людей, процессы и доверие	Мониторинг результата, обратная связь, разбор инцидентов	Скрытые социальные и репутационные потери

Источник: составлено авторами на основе [67; 83; 93; 101; 137].

Данные таблицы показывают, что управленческий уровень требует не только аналитических инструментов, но и процедур ответственности. Каждая задача должна быть закреплена в управленческом регламенте, иначе данные и ИИ остаются внешним дополнением к решению, а не частью зрелой системы управления.

Таким образом, управленческий уровень цифрового сознания раскрывает способность руководителей принимать решения на основе данных и ИИ без

утраты человеческой ответственности. Его ядро составляют качество данных, критическая интерпретация, риск-ориентированность, прозрачность, человек в контуре решения и анализ последствий. Следующий параграф показывает, как эти управленческие практики закрепляются в культуре, процессах, архитектуре и регламентах организации.

2.4. ОРГАНИЗАЦИОННЫЙ УРОВЕНЬ ЦИФРОВОГО СОЗНАНИЯ: КУЛЬТУРА, ПРОЦЕССЫ, АРХИТЕКТУРА И ОТВЕТСТВЕННОСТЬ

Организационный уровень является ядром формирования цифрового сознания организации. Именно здесь цифровое сознание перестает быть качеством отдельных сотрудников, команд или руководителей и становится свойством организации как коллективного субъекта. На этом уровне оно выражается в культуре, процессах, архитектуре данных, цифровых платформах, регламентах, ролях, системе безопасности, механизмах контроля и постоянного улучшения. Иначе говоря, организация не просто поощряет цифровую активность, а институционализирует осознанное цифровое поведение [83; 109].

Цифровая культура организации задает ценностную основу. Она отвечает на вопросы: как организация относится к данным, ошибкам, экспериментам, прозрачности, безопасности, ИИ, цифровому следу, правам сотрудников и клиентов. В зрелой цифровой культуре использование технологий не отделяется от ответственности. Сотрудники понимают, что цифровой инструмент – не нейтральная внешняя вещь, а часть организационной практики, влияющая на качество решений, доверие, справедливость и устойчивость. Поэтому цифровая культура должна соединять инновационность с этичностью, а эффективность – с человеческой ориентированностью [109; 137] [21; 49].

Процессный компонент организационного уровня означает, что цифровое сознание должно быть встроено в регулярные операции. Если работа с данными, проверка ИИ, защита информации и оценка рисков существуют только как разовые кампании, организация не становится в цифровом плане осознанной. Необходимы устойчивые процессы: назначение владельцев данных, управление доступом, порядок применения ИИ, согласование цифровых инициатив, аудит цифровых сервисов, реагирование на инциденты, обновление регламентов, обучение сотрудников, измерение цифровой нагрузки и качества цифровых решений [13; 83].

Архитектура данных и цифровых сервисов является материальной основой организационного цифрового сознания. Организация должна понимать, где находятся данные, кто ими владеет, как они обновляются, кто имеет доступ, какие цифровые следы формируются, какие системы связаны между собой, какие решения зависят от внешних платформ. Без такой архитектуры

невозможно управлять ни безопасностью, ни качеством аналитики, ни ответственным применением ИИ. В этом смысле цифровое сознание требует не только культуры, но и прозрачной цифровой инфраструктуры [13; 18; 83].

Особое значение имеет управление данными (data governance, распределение правил владения, качества, доступа и ответственности за данные). Далее используется формулировка «управление данными». Управление данными переводит информационные ресурсы из состояния разрозненных файлов и отчетов в состояние управляемого актива. Для организации это означает описание источников кадровых, финансовых, клиентских, операционных, проектных, производственных и исследовательских данных, определение ответственных лиц, правил доступа, сроков хранения, процедур обновления и оснований для аналитического использования.

Организационная архитектура цифрового сознания представлена на рисунке 2.4. Схема показывает, что организационный уровень нельзя свести к одному регламенту или одной платформе: он включает стратегию, культуру, процессы, данные, сервисы, безопасность и контроль.

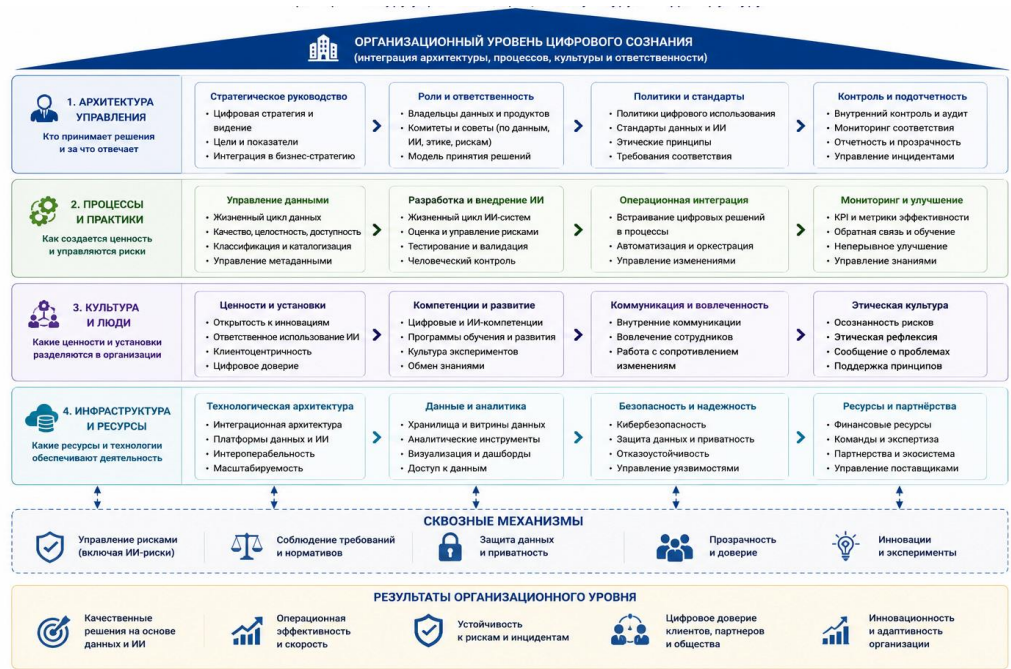


Рисунок 2.4 – Организационная архитектура цифрового сознания

Источник: составлено авторами на основе [13; 83; 109; 126; 143].

Представленная схема показывает, что цифровое сознание организации закрепляется через архитектуру. Центральная цифровая экосистема соединяет стратегию, процессы, данные, платформы, культуру с безопасностью. Если хотя

бы один элемент выпадает, цифровая трансформация становится фрагментарной.

На организационном уровне необходимо различать цифровые правила и цифровую бюрократию. Цифровые правила создают ясность: что можно делать, кто отвечает, где хранить данные, как проверять результат, когда обращаться за согласованием. Цифровая бюрократия, напротив, накапливает документы без реального изменения практики. Поэтому регламенты цифрового сознания должны быть короткими, применимыми, проверяемыми и связанными с реальными сценариями. Особенно важно, чтобы они не блокировали инициативу, а задавали безопасные границы для эксперимента.

Система менеджмента ИИ по стандарту ISO/IEC 42001:2023 дает организации полезный управленческий язык. Она ориентирует не на разовые инструкции, а на систему: контекст организации, лидерство, планирование, поддержку, операции, оценку результативности и улучшение. Для главы это важно методически: цифровое сознание на организационном уровне можно описывать как способность строить и поддерживать систему, в которой ИИ и цифровые технологии применяются не стихийно, а управляемо, документированно и с учетом рисков [83].

Не менее важна информационная безопасность. Стандарт ISO/IEC 27001 связывает защиту информации с системой менеджмента, оценкой рисков и постоянным улучшением. В контексте цифрового сознания безопасность не должна рассматриваться как техническая функция ИТ-подразделения. Она является элементом организационной культуры и ответственности: каждый сотрудник работает с доступом, данными, документами, цифровым следом, коммуникацией. Поэтому безопасность должна быть включена в обучение, процессы, должностные роли и управленческие решения [13].

Организационный уровень также требует механизма постоянного обучения. Технологии меняются быстрее, чем локальные документы. Поэтому цифровое сознание не может быть сформировано один раз. Организация должна иметь цикл обновления: мониторинг новых технологий и рисков, пересмотр регламентов, обучение сотрудников, оценка цифровых практик, разбор ошибок, адаптация архитектуры. Этот цикл соединяет теорию организационного обучения и современные требования к управлению цифровой средой [43; 126].

В организации организационный уровень может быть закреплён через комплекс документов и практик: положение о применении ИИ, паспорт данных цифровых сервисов, матрицу доступа, регламент работы с цифровым следом клиентов, сотрудников и партнеров, порядок экспертизы цифровых инициатив, правила маркировки материалов, созданных с использованием ИИ, программу развития компетенций сотрудников, комитет или рабочую группу по

ответственному цифровому развитию, регулярную отчетность по цифровым рискам и эффектам.

Таблица 2.4 раскрывает организационный уровень через элементы архитектуры, которые должны быть описаны и закреплены в управлении.

Таблица 2.4 – Организационные элементы цифрового сознания

Элемент	Содержание	Форма закрепления	Риск дефицита
Стратегия цифрового развития	Цели, приоритеты, ожидаемые эффекты, связь с миссией организации	Цифровая стратегия или раздел стратегии, паспорт инициатив	Технологии внедряются без связи с целями
Культура и нормы	Ценности ответственного цифрового поведения, отношение к данным, ИИ, ошибкам и безопасности	Кодекс цифрового поведения, этические принципы, регулярные обсуждения	Цинизм, формализм, сопротивление изменениям
Процессы и роли	Распределение ответственности за данные, сервисы, риски и решения	Матрица ролей, владельцы данных, ответственные за ИИ-сценарии	Никто не отвечает за последствия цифровых решений
Архитектура данных	Источники, потоки, качество, доступ, хранение и правовой режим данных	Реестр данных, карта потоков, матрица доступа	Потеря данных, ошибки аналитики, правовые нарушения
Безопасность и контроль	Управление рисками, доступом, инцидентами, аудитом и улучшением	Политики безопасности, журналирование, план реагирования	Утечки, несанкционированное использование, репутационные потери
Организационное обучение	Обновление компетенций, разбор кейсов, распространение лучших практик	Программа обучения, база знаний, регулярные рефлексивные сессии	Отставание практик от технологий

Источник: составлено авторами на основе [13; 43; 83; 109; 126].

Данные таблицы показывают, что организационный уровень требует не отдельной цифровой инициативы, а целостной архитектуры. В ней стратегия, культура, данные, процессы, безопасность и обучение должны работать как взаимосвязанные элементы.

Таким образом, организационный уровень делает цифровое сознание устойчивым свойством организации. Он закрепляет индивидуальные, командные и управленческие практики в культуре, процессах, архитектуре

данных, системах безопасности, регламентах и механизмах обучения. Следующий параграф расширяет модель за пределы организации и показывает, что цифровое сознание зависит от взаимодействия с внешними стейкхолдерами, партнерами, регуляторами и цифровыми платформами.

2.5. ЭКОСИСТЕМНЫЙ УРОВЕНЬ ЦИФРОВОГО СОЗНАНИЯ: ВНЕШНИЕ СТЕЙКХОЛДЕРЫ, ПАРТНЕРСТВА И ЦИФРОВОЕ ДОВЕРИЕ

Экосистемный уровень завершает структурную модель, поскольку ни одна организация не действует в цифровой среде изолированно. Ее цифровые решения связаны с государственным регулированием, отраслевыми стандартами, платформенными поставщиками, партнерами, клиентами, пользователями, сотрудниками, профессиональными сообществами, общественными ожиданиями и медийной репутацией. Поэтому цифровое сознание организации должно включать способность видеть не только внутренние процессы, но и внешние последствия цифровых действий [104; 137].

Экосистемный уровень особенно важен для любой организации, чьи цифровые решения затрагивают внешних участников и зависят от цифровой инфраструктуры партнеров. Организация является не только внутренней административной системой, но и участником технологической, отраслевой, социальной и региональной экосистемы. Она работает с клиентами, пользователями, сотрудниками, подрядчиками, государственными органами, поставщиками цифровых платформ, профессиональными ассоциациями и отраслевыми партнерами. Любое цифровое решение – корпоративная платформа, цифровой профиль клиента, применение ИИ в процессе, аналитика поведения пользователей, цифровой сервис или цифровой след сотрудника – влияет на доверие этих участников.

Цифровое доверие можно определить как готовность внешних и внутренних участников признавать цифровые решения организации правомерными, понятными, безопасными, этически приемлемыми и полезными. Доверие формируется не только качеством платформы, но и ясностью правил: какие данные собираются, зачем они используются, кто имеет доступ, как применяются результаты ИИ, как можно оспорить решение, кто несет ответственность. Если организация не объясняет эти правила, цифровая трансформация может восприниматься как надзор, формализация или технологическое давление [137].

Международные рамки ответственного ИИ подчеркивают, что цифровое развитие должно учитывать права человека, справедливость, прозрачность, безопасность, устойчивость и подотчетность. Рекомендация ЮНЕСКО по этике искусственного интеллекта связывает ИИ с человеческим достоинством,

правами и общественным благом. Принципы Организации экономического сотрудничества и развития (ОЭСР) акцентируют человекоцентричность, прозрачность, надежность и подотчетность. Закон Европейского союза об искусственном интеллекте усиливает риск-ориентированный подход и требования к грамотности, прозрачности и человеческому надзору [67; 104; 137].

В российском контексте экосистемный уровень связан с национальной повесткой экономики данных и цифровой трансформации государства. Указ Президента Российской Федерации от 7 мая 2024 года № 309 закрепляет цифровую трансформацию государственного и муниципального управления, экономики и социальной сферы как одну из национальных целей развития до 2030 года и на перспективу до 2036 года. Национальная стратегия развития искусственного интеллекта до 2030 года задает долгосрочный контур развития ИИ, кадров, инфраструктуры и регулирования. Для организаций это означает, что цифровое сознание становится частью более широкой институциональной среды [30; 31].

Экосистемный контур цифрового доверия представлен на рисунке 2.5. Схема показывает, что организация включена в сеть отношений с регуляторами, партнерами, клиентами, платформами, обществом и профессиональными сообществами.



Рисунок 2.5 – Экосистемный контур цифрового доверия

Источник: составлено авторами на основе [30; 31; 67; 104; 137; 148].

Рисунок 2.5 подчеркивает, что цифровое доверие является результатом взаимодействия внутренней ответственности организации и внешних ожиданий цифровой среды. Организация должна не только соблюдать требования, но и объяснять свои цифровые практики тем, на кого они влияют.

Экосистемный уровень включает партнерскую совместимость. Если организация использует внешние платформы, цифровые сервисы, облачные решения, системы ИИ или специализированные цифровые решения, она должна понимать условия хранения данных, порядок доступа, правовой режим, зависимость от поставщика, возможность переноса данных, риски прекращения сервиса, требования к информационной безопасности. Цифровое сознание здесь проявляется в способности не только выбрать удобный инструмент, но и оценить последствия платформенной зависимости.

Другой аспект экосистемного уровня – взаимодействие с регуляторикой. Регуляторная среда в области данных, персональной информации, ИИ, информационной безопасности и цифровых платформ развивается быстро. Организация должна иметь механизм мониторинга изменений, обновления локальных актов и обучения сотрудников. Если такой механизм отсутствует, даже добросовестные цифровые практики могут быстро устареть и стать источником правовых рисков.

Экосистемное цифровое сознание связано и с репутацией. Ошибка цифрового сервиса, утечка данных, некорректное применение ИИ, непрозрачное решение на основе аналитики или несправедливый алгоритмический результат становятся не только внутренним инцидентом, но и публичным событием. Поэтому цифровая ответственность организации должна включать коммуникационный контур: как объяснять цифровые решения, как реагировать на вопросы, как признавать ошибки, как демонстрировать исправление практик [79; 137].

Для организации экосистемный уровень может быть усилен через партнерские правила ответственного цифрового развития. Например, при совместных проектах, интеграции цифровых сервисов, обмене данными с подрядчиками, внедрении ИИ-систем, создании клиентских или корпоративных цифровых профилей необходимо заранее описывать права сторон, режим данных, допустимые сценарии ИИ, требования к безопасности, порядок использования результатов и принципы прозрачности для затронутых участников.

Экосистемный уровень возвращает структурную модель к ее исходной методологической идее: цифровое сознание организации – это не внутреннее самоописание, а способность ответственно действовать в цифровой среде, где

каждое решение имеет внешние последствия. Поэтому зрелость организации определяется не только тем, насколько эффективно она использует технологии внутри, но и тем, насколько она сохраняет доверие, справедливость, безопасность и ценность для участников своей цифровой экосистемы.

Таблица 2.5 систематизирует ключевые направления экосистемного уровня. Она может использоваться как практический чек-лист для оценки цифрового доверия организации.

Таблица 2.5 – Направления экосистемного уровня цифрового сознания

Направление	Содержание	Практический индикатор	Риск дефицита
Регуляторы	Соответствие требованиям законодательства, стандартов и отраслевых норм	Мониторинг требований, ответственный за соответствие, обновление локальных актов	Правовые санкции, запреты, предписания
Партнеры и поставщики	Безопасное и понятное взаимодействие с внешними цифровыми сервисами	Оценка поставщика, договорные условия, требования к данным и безопасности	Платформенная зависимость, утечки, потеря контроля
Клиенты, пользователи, сотрудники	Понимание того, как используются данные и цифровые решения	Уведомления, правила, согласия, каналы обратной связи	Недоверие, сопротивление, конфликты
Профессиональные сообщества	Обмен практиками и участие в формировании норм	Методические сети, экспертные группы, публикации, совместные проекты	Изоляция, отставание от практик отрасли
Общество и публичная среда	Репутационная устойчивость цифровых решений	Прозрачная коммуникация, разбор ошибок, публичная отчетность	Репутационные потери, медийные кризисы

Источник: составлено авторами на основе [30; 31; 67; 104; 137; 148].

Данные таблицы показывают, что экосистемный уровень требует системной работы с внешними ожиданиями. Цифровое доверие возникает тогда, когда организация может объяснить свои цифровые решения, подтвердить их безопасность и показать, что они создают ценность для участников экосистемы.

Таким образом, экосистемный уровень раскрывает цифровое сознание организации как способность действовать ответственно не только внутри собственных процессов, но и в отношениях с внешней средой. Внешние стейкхолдеры, регуляторы, партнеры, платформы и общество задают требования

к прозрачности, безопасности, объяснимости и доверию. Поэтому цифровое сознание организации завершается не технологической эффективностью, а устойчивым цифровым доверием.

ИТОГИ ГЛАВЫ

Цифровое сознание организации формируется на пяти взаимосвязанных уровнях: индивидуальном, командном, управленческом, организационном и экосистемном. Каждый уровень имеет собственный предмет диагностики, но устойчивый результат возникает только при их согласованности.

Управленческий переход к главе 3: уровневая модель показывает, где и кем формируется цифровое сознание. Далее раскрываются его компоненты как конкретные объекты развития, диагностики и управленческого воздействия.

***Интерактивное сопровождение.** В цифровом руководстве размещены профили сотрудника, команды и управленческого контура, карта распределения ролей и чек-листы оценки уровней цифрового сознания.*

ГЛАВА 3. КОМПОНЕНТЫ ЦИФРОВОГО СОЗНАНИЯ КАК ОБЪЕКТЫ РАЗВИТИЯ СОТРУДНИКОВ И УПРАВЛЕНЧЕСКИХ КОМАНД

«Система – это сеть взаимозависимых компонентов, которые совместно работают, стремясь достичь цели системы».

Уильям Эдвардс Деминг

«Новая экономика для промышленности, государственного управления и образования», с. 50. Перевод авторов.

Управленческий вопрос главы. Какие способности сотрудников и управленческих команд определяют качество, безопасность и ответственность цифровых решений?

Управленческий результат главы. Семикомпонентная модель цифрового сознания, связывающая дееспособность, критичность, грамотность в области данных и ИИ, этику, безопасность, коммуникацию и рефлексивность с индикаторами, рисками и средствами развития (рисунок 3.1).



Рисунок 3.1 – Семь компонентов цифрового сознания сотрудников и управленческих команд

Источник: составлено авторами на основе [67; 83; 101; 102; 109; 137; 146].

Представленная схема показывает, что цифровое сознание сотрудников и управленческих команд складывается из взаимосвязанных компонентов. Центральным является не владение отдельным сервисом, а способность действовать в цифровой среде критично, безопасно, этично и ответственно.

Содержательная структура этих компонентов обобщена в таблице 3.1. Таблица задаёт методическую рамку всей главы: она показывает, какой вопрос решает каждый компонент, как он проявляется у сотрудника и какую управленческую задачу ставит перед руководителями.

Таблица 3.1 – Компонентная карта цифрового сознания сотрудников и управленческих команд

Компонент	Ключевой вопрос	Индивидуальное проявление	Управленческая задача
Цифровая дееспособность и инструментальная готовность	Может ли сотрудник самостоятельно и результативно действовать в цифровой среде?	Осознанный выбор инструмента, соблюдение цифровой дисциплины, корректное сохранение результата.	Создать условия для самостоятельной работы без хаоса сервисов и версий.
Информационно-аналитическая критичность	Способен ли участник процесса отличать данные, интерпретации и предположения?	Проверка источников, понимание ограничений показателей, вопросы к методике.	Закрепить стандарт доказательности и качество управленческой аналитики.
Грамотность в области данных и ИИ	Понимает ли субъект возможности и ограничения данных и ИИ?	Проверка ИИ-результатов, недопущение передачи чувствительных данных, понимание предвзятости и ошибок.	Ввести правила применения ИИ, контур проверки и распределение ответственности.
Цифровая этика, право и ответственность	Где проходят допустимые границы цифрового действия?	Учет персональных данных, авторского права, справедливости, конфиденциальности и последствий.	Институционализировать этико-правовую экспертизу и ответственность.
Цифровая безопасность и управление рисками	Как не превратить цифровизацию в источник ущерба?	Кибергигиена, защита доступов, предупреждение фишинга, сообщение об инцидентах.	Связать безопасность с обучением, ролями, процессами и риск-менеджментом.
Цифровая коммуникация и культура взаимодействия	Как цифровые каналы поддерживают совместную деятельность и доверие?	Ясная коммуникация, фиксация решений, работа с общими знаниями, соблюдение норм каналов.	Снизить цифровой шум и закрепить правила совместной работы.
Рефлексивность, саморегуляция и готовность к	Способна ли команда учиться на цифровом	Анализ последствий, цифровой нагрузки, ошибок и	Создать цикл организационного обучения и обновления

Компонент	Ключевой вопрос	Индивидуальное проявление	Управленческая задача
изменениям	опыте и корректировать практики?	результатов.	цифровых правил.

Источник: составлено авторами на основе [43; 67; 83; 101; 102; 109; 123; 137; 146].

Данные таблицы показывают, что каждый компонент цифрового сознания имеет индивидуальное и управленческое измерение. Поэтому развитие цифрового сознания требует не только обучения сотрудников, но и изменения правил, процессов и управленческих практик.

3.1. ЦИФРОВАЯ ДЕЕСПОСОБНОСТЬ И ИНСТРУМЕНТАЛЬНАЯ ГОТОВНОСТЬ

Цифровая дееспособность является базовым компонентом цифрового сознания. Она означает способность сотрудника самостоятельно, осознанно и результативно использовать цифровые инструменты для решения профессиональных задач без постоянной внешней технической опеки. Однако в контексте настоящего пособия этот компонент не сводится к бытовому владению устройствами или интерфейсами. Цифровая дееспособность включает понимание того, какой инструмент соответствует задаче, где проходит граница собственной компетентности, какие данные можно вводить в систему, где должен быть сохранен результат, кто отвечает за последующее использование цифрового артефакта.

Исторически цифровая грамотность формировалась как способность человека ориентироваться в цифровой среде, находить информацию, использовать цифровые устройства и коммуникационные каналы [45]. Современная рамка DigComp 2.2 существенно расширяет это понимание: цифровая компетентность включает информационную грамотность, коммуникацию и сотрудничество, создание цифрового контента, безопасность и решение проблем [146]. Следовательно, базовая инструментальная готовность должна рассматриваться не как отдельный набор операций, а как вход в более широкую систему цифрового действия.

Для организации инструментальная готовность имеет практическое значение. Если сотрудники не умеют самостоятельно выбирать цифровые средства, корректно работать с корпоративными платформами, соблюдать версию документов, использовать утвержденные каналы и фиксировать результаты, то даже качественная цифровая инфраструктура начинает порождать хаос. Появляются дублирующие файлы, неофициальные хранилища, разрывы коммуникации, зависимость от отдельных «продвинутых»

пользователей, рост нагрузки на техническую поддержку и снижение доверия к цифровым решениям.

При этом дееспособность не означает требование полной автономности. Напротив, зрелый сотрудник понимает, когда нужно запросить помощь, уточнить правило, обратиться к владельцу данных или остановить действие из-за риска. В этой точке цифровая дееспособность соединяется с ответственностью. Человек не должен решать любую проблему в одиночку, но он должен понимать цифровую ситуацию настолько, чтобы не создавать новый риск своими действиями.

На рисунке 3.2 представлена схема инструментальной готовности. Она показывает, что цифровая дееспособность включает полный цикл: от понимания задачи до выбора средства, выполнения действия, проверки результата, фиксации итогов и обновления практики.

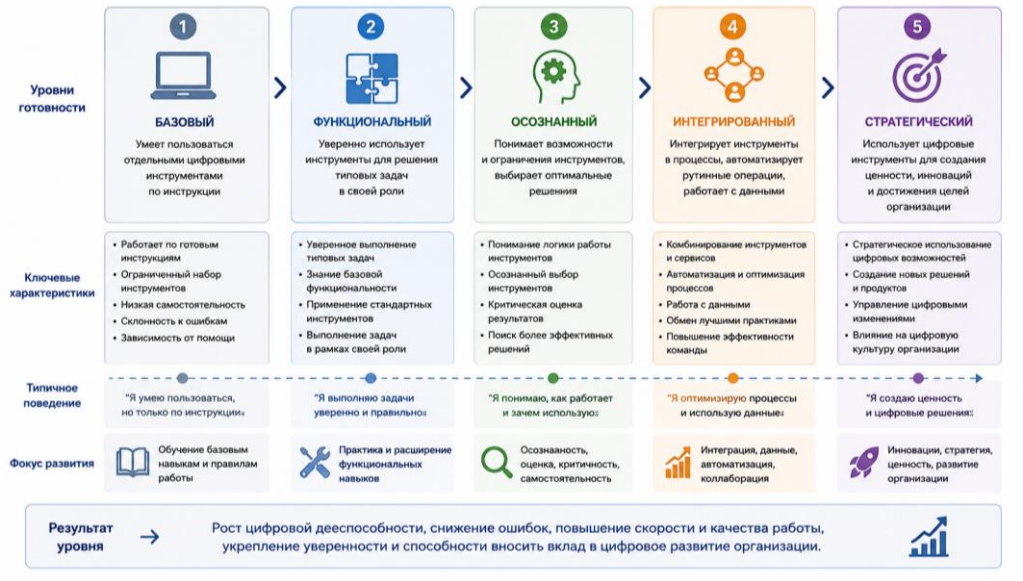


Рисунок 3.2 – Уровни инструментальной готовности сотрудников и управленческих команд

Источник: составлено авторами на основе [45; 82; 146].

Представленная схема показывает, что инструментальная готовность не ограничивается нажатием кнопок. Она включает осмысленный выбор цифрового средства, контроль результата, соблюдение правил хранения и способность корректировать собственную цифровую практику.

В управленческой практике цифровая дееспособность развивается через ролевое обучение, наставничество, короткие инструкции по типовым сценариям, библиотеку допустимых инструментов, внутренние консультации и регулярное обновление цифровых правил. Особенно важно избегать двух крайностей.

Первая крайность – чрезмерная техническая детализация, когда сотрудника перегружают инструкциями, но не формируют понимания смысла действия. Вторая крайность – неопределенная свобода, когда сотруднику предлагают «использовать любые удобные сервисы», не описывая границ данных, безопасности и ответственности.

Для управленческих команд цифровая дееспособность означает способность отличать техническую проблему от организационной. Если сотрудники не используют платформу, причина может заключаться не в низкой цифровой грамотности, а в плохом процессе, избыточной сложности, отсутствии владельца данных или конфликте между формальными регламентами и реальной деятельностью. Руководитель с развитым цифровым сознанием не обвиняет пользователей автоматически, а анализирует, почему цифровое действие не стало устойчивой практикой.

Методически этот компонент следует диагностировать через наблюдаемое поведение. Недостаточно спрашивать сотрудника, «уверенно ли он пользуется цифровыми сервисами». Необходимо проверять, способен ли он выбрать инструмент под задачу, правильно классифицировать данные, не создавать хаос версий, оформить результат в утвержденном пространстве, объяснить ограничение своей компетентности и вовремя запросить поддержку. Такая диагностика должна иметь развивающий, а не карательный характер.

Таблица 3.2 переводит цифровую дееспособность из абстрактного понятия в набор наблюдаемых признаков. Это позволяет использовать компонент при диагностике, обучении и проектировании цифровых регламентов.

Таблица 3.2 – Индикаторы цифровой дееспособности и инструментальной готовности

Аспект	Содержание	Наблюдаемый индикатор	Методическое действие
Выбор инструмента	Сотрудник выбирает цифровое средство в зависимости от задачи, а не по привычке или личному удобству.	Может объяснить, почему использует конкретную систему или канал.	Разработать карту утвержденных сервисов и типовых сценариев.
Цифровая дисциплина	Соблюдаются правила хранения, именования, версий, доступа и передачи документов.	Результаты сохраняются в утвержденной среде, решения не теряются в переписке.	Ввести простые правила versionности и хранения рабочих артефактов.
Самостоятельность	Сотрудник способен выполнять базовые	Снижается число повторяющихся	Создать микрокурсы, инструкции и

Аспект	Содержание	Наблюдаемый индикатор	Методическое действие
	операции без постоянной помощи.	запросов технической поддержки по типовым действиям.	систему наставничества.
Границы компетентности	Сотрудник понимает, когда цифровое действие требует консультации специалиста или руководителя.	Опасные действия останавливаются до инцидента; вопросы эскалируются вовремя.	Определить каналы консультации по данным, ИИ, праву и безопасности.
Цифровая нагрузка	Использование инструментов не приводит к перегрузке и дублированию действий.	Сотрудники понимают, какой канал для чего используется.	Регулярно пересматривать цифровой ландшафт и устранять дублирование сервисов.

Источник: составлено авторами на основе [45; 82; 146].

Таким образом, цифровая дееспособность является нижним операционным слоем цифрового сознания. Без нее невозможно ни ответственное применение данных и ИИ, ни цифровая безопасность, ни командная работа. Однако сама по себе инструментальная готовность недостаточна: сотрудник может уверенно использовать сервисы и одновременно некритично воспринимать данные. Поэтому следующий компонент связан с информационно-аналитической критичностью.

3.2. ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ КРИТИЧНОСТЬ

Информационно-аналитическая критичность является компонентом цифрового сознания, который защищает организацию от цифрового шума, поверхностных выводов, псевдоаналитики и ложной уверенности в числовых показателях. В цифровой среде данные становятся одним из главных оснований решений, однако данные не тождественны реальности. Они собираются в конкретных процессах, зависят от методики, качества ввода, полноты охвата, контекста и способа визуализации. Поэтому цифровое сознание требует способности задавать вопросы не только к выводам, но и к самим основаниям выводов.

В управлении давно сформировалась идея конкуренции на аналитике: организации получают преимущества тогда, когда умеют превращать данные в управленческие решения [57]. Но для современной организации этого тезиса уже недостаточно. Наличие аналитической панели, набора показателей или автоматизированного отчета не гарантирует качества управленческого вывода.

Показатель может быть корректным технически, но неправильно понятым управленчески. Поэтому информационно-аналитическая критичность выступает промежуточным звеном между данными и ответственным решением.

Сотрудник с развитой критичностью умеет отличать факт от интерпретации, источник от пересказа, показатель от вывода, корреляцию от причинности, репрезентативные данные от случайного наблюдения. Он проверяет источник, уточняет период, задает вопросы к методике, понимает, что визуализация может усиливать или скрывать определенные смыслы. Управленческая команда с развитой критичностью не принимает решение только на основании красивой диаграммы; она требует пояснения методики, ограничений и альтернативных трактовок.

Отдельная проблема возникает при работе с цифровым следом. Системы фиксируют большое количество действий: посещения, клики, запросы, время активности, документы, коммуникации, этапы процессов. Эти данные могут быть полезны для улучшения процессов, но могут породить ошибочное впечатление полной прозрачности деятельности. Цифровой след показывает только то, что было зафиксировано системой, но не раскрывает мотивы, контекст, качество мышления, скрытую нагрузку и социальные условия действия. Поэтому использовать цифровой след как единственное основание оценки человека или команды методологически опасно.

На рисунке 3.3 показана логика перехода от данных к ответственному решению. Схема подчеркивает, что каждый переход требует критического вопроса: кто собрал данные, что исключено, как измерено, можно ли интерпретировать иначе, кого затронет решение.

Представленная схема показывает, что данные проходят несколько смысловых преобразований: становятся информацией, затем интерпретацией, знанием, решением и ответственным действием. На каждом этапе возможны ошибки, поэтому критичность является обязательным компонентом цифрового сознания.



Рисунок 3.3 – Структура информационно-аналитической критичности

Источник: составлено авторами на основе [57; 130; 146].

Информационно-аналитическая критичность особенно важна в условиях генеративного ИИ. Системы ИИ могут быстро формировать текстовые объяснения, выводы, резюме и аналитические обзоры, но убедительная форма ответа не гарантирует его достоверности. Исследования больших языковых моделей показывают, что они способны воспроизводить предвзятости обучающих данных, создавать правдоподобные, но неверные утверждения и усиливать иллюзию компетентности пользователя [46]. Поэтому критичность должна распространяться не только на статистические данные, но и на машинно сгенерированные интерпретации.

В организации этот компонент формируется через культуру доказательности. Она предполагает, что участники процессов ссылаются на источники, различают первичные данные и вторичную интерпретацию, фиксируют допущения, проверяют выводы, не используют единичные показатели как универсальный аргумент и умеют признавать неопределенность. Для управленческих команд критичность должна стать нормой совещаний и аналитических записок: каждый значимый вывод должен сопровождаться вопросом о качестве данных и ограничениях интерпретации.

Методически информационно-аналитическую критичность целесообразно развивать не через лекции о статистике, а через разбор кейсов. Сотрудникам и руководителям можно предлагать реальные или моделируемые ситуации:

неполные данные, противоречивые показатели, неверная визуализация, корреляция без причинности, ИИ-ответ с ошибкой, отчет без методики. Задача обучения – сформировать привычку не отвергать данные, а работать с ними профессионально.

Данные таблицы 3.3 показывают, что критичность должна быть встроена в работу с источниками, методиками, показателями и результатами ИИ. Без этого данные перестают быть ресурсом управления и становятся источником цифрового самообмана.

Таблица 3.3 – Информационно-аналитическая критичность: признаки и риски дефицита

Аспект критичности	Ключевой вопрос	Практический индикатор	Риск дефицита
Проверка источника	Кто создал данные или сообщение, каков уровень надежности источника?	Сотрудник указывает первоисточник и не ограничивается пересказом.	Решения на основе слухов, фейков и вторичной информации.
Проверка методики	Как собраны данные, какие категории учтены, какие исключены?	В аналитических материалах указывается период, способ сбора и ограничения.	Ошибочная экстраполяция и ложные управленческие выводы.
Различение факта и вывода	Что является наблюдаемым фактом, а что интерпретацией?	В документах разделяются данные, оценка и рекомендация.	Подмена анализа мнением или авторитетом.
Понимание ограничений показателей	Что показатель не измеряет и где его нельзя применять?	При обсуждении метрик фиксируются исключения и риски неправильного чтения.	Управление цифровыми суррогатами вместо реальных процессов.
Критика ИИ-выводов	Может ли ответ ИИ содержать ошибку, предвзятость или неполноту?	Результаты ИИ проверяются по источникам и экспертному суждению.	Слепое доверие машинной интерпретации.

Источник: составлено авторами на основе [46; 57; 130].

Таким образом, информационно-аналитическая критичность является условием доказательного цифрового поведения. Она не отрицает ценность данных, а задает правила их ответственного использования. Переход к следующему компоненту связан с тем, что данные все чаще используются вместе с системами ИИ; следовательно, организация должна развивать специальную грамотность в области данных и искусственного интеллекта.

3.3. ГРАМОТНОСТЬ В ОБЛАСТИ ДАННЫХ И ИИ И ПОНИМАНИЕ ОГРАНИЧЕНИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Грамотность в области данных и ИИ – способность понимать, оценивать и ответственно использовать данные и системы искусственного интеллекта – является центральным компонентом цифрового сознания 2.0. Она отражает переход от обычного использования цифровых сервисов к работе в среде, где алгоритмы участвуют в подготовке текстов, аналитике, прогнозировании, классификации, коммуникации и поддержке управленческих решений. В этой среде сотрудник и руководитель должны понимать не только возможности ИИ, но и его ограничения [125].

В научной литературе грамотность в области ИИ описывается как способность понимать, использовать, оценивать и критически осмысливать системы искусственного интеллекта [92]. Для организации этого определения недостаточно, если оно остается на уровне индивидуального пользователя. Необходимо добавить управленческий слой: какие сценарии ИИ допустимы, какие данные можно использовать, кто проверяет результат, когда требуется человек в контуре решения, как фиксируется ответственность, какие риски считаются неприемлемыми.

Данные являются исходным материалом для аналитики и ИИ, но они всегда имеют происхождение, качество, владельца, режим доступа и контекст. Система ИИ может усиливать ошибки, уже содержащиеся в данных; может воспроизводить предвзятость; может создавать уверенные, но неверные ответы; может формировать текст, не имеющий достаточной доказательной базы; может скрывать неопределенность за гладкой формулировкой. Поэтому цифровое сознание требует не восхищения ИИ и не запрета ИИ, а грамотного режима его включения в деятельность.

NIST рассматривает управление рисками ИИ как процесс, направленный на учет доверенности ИИ при проектировании, разработке, использовании и оценке систем [101]. Профиль NIST для генеративного ИИ отдельно подчеркивает специфические риски, возникающие при использовании моделей, создающих текст, изображения, код и другие результаты [101]. ISO/IEC 42001 переводит эту проблематику в язык системы менеджмента ИИ: политика, роли, цели, процедуры, оценка результативности и постоянное улучшение [83]. Эти рамки подтверждают, что грамотность в области ИИ должна быть связана с управлением, а не только с навыками составления запросов.

На рисунке 3.4 представлен контур ответственного использования ИИ. Он показывает, что применение ИИ начинается не с запроса к модели, а с профессиональной задачи и проверки данных, а завершается человеческим решением и фиксацией ответственности.



Рисунок 3.4 – Контур ответственного использования ИИ
Источник: составлено авторами на основе [67; 83; 92; 101].

Представленная схема показывает, что ИИ должен использоваться в управляемом цикле: задача, данные, запрос, результат, проверка человеком, решение и ответственность. Центральный смысл модели состоит в сохранении человеческого контроля и организационной подотчетности.

В практической деятельности сотрудник должен владеть несколькими базовыми правилами. Во-первых, нельзя вводить в внешние ИИ-сервисы персональные, конфиденциальные, коммерчески чувствительные или служебные сведения без разрешения и правового основания. Во-вторых, результат ИИ всегда требует проверки, особенно если он используется в документе, управленческом решении, коммуникации с клиентом, проектном выводе или правовом контексте. В-третьих, ИИ-результат должен быть маркирован или раскрыт в тех случаях, когда это требуется внутренними правилами или характером работы. В-четвертых, ИИ не должен использоваться для решений, затрагивающих права, безопасность и существенные интересы людей, без установленного режима проверки.

Для управленческой команды грамотность в области данных и ИИ означает способность проектировать безопасные и полезные сценарии. Руководитель должен знать, где ИИ действительно повышает качество или скорость работы, а где создает только видимость эффективности. Управленческая команда должна вести реестр сценариев применения ИИ, классифицировать их по рискам, назначать владельцев, описывать порядок проверки результатов и регулярно оценивать фактический эффект. Это соответствует риск-ориентированной

логике Закона Европейского союза об ИИ и международным подходам к ответственному ИИ [67; 109; 137].

Отдельное значение имеет понимание ограничений генеративного ИИ. Генеративная модель не является базой знаний в обычном смысле; она формирует вероятностно правдоподобный ответ на основе закономерностей в данных. Поэтому ответ может быть стилистически убедительным и одновременно фактически ошибочным. В организациях это создает риск автоматизации не только рутинных операций, но и ошибок мышления. Цифровое сознание требует, чтобы сотрудник видел ИИ как помощника, а не как автономный источник истины.

Формирование этого компонента требует сочетания обучения и регламентации. Одного запрета недостаточно: сотрудники будут искать удобные инструменты, если организация не предлагает легитимных сценариев. Одного обучения также недостаточно: без правил и инфраструктуры сотрудники не будут понимать, где проходит граница допустимого. Поэтому в организации должны быть одновременно учебные модули, список разрешенных инструментов, карта запрещенных данных, чек-листы проверки результатов, порядок маркировки ИИ-использования и канал консультации по спорным случаям.

Данные таблицы 3.4 показывают, что грамотность в области данных и ИИ включает не только навык обращения с ИИ-сервисом, но и понимание качества данных, ограничений модели, правил запроса, человеческой проверки и управления сценариями применения.

Таблица 3.4 – Грамотность в области данных и ИИ: содержание, риски и инструменты развития

Аспект	Содержание	Риск дефицита	Инструмент развития
Качество данных	Сотрудник понимает происхождение, полноту, актуальность и правовой режим данных.	Использование недостоверных или недопустимых данных в аналитике и ИИ.	Карта источников данных, владельцы данных, правила классификации.
Ограничения ИИ	Понимание вероятностного характера ответа, возможности ошибок и предвзятости.	Убедительные, но неверные выводы, автоматизация ошибок.	Кейс-семинары по ошибкам ИИ, чек-лист верификации.
Безопасный запрос	Запрос к ИИ не содержит чувствительных сведений и	Утечка персональных или конфиденциальных данных.	Политика допустимых запросов, перечень запрещенных

Аспект	Содержание	Риск дефицита	Инструмент развития
	соответствует задаче.		данных.
Человек в контуре решения	Значимый результат проверяется компетентным человеком.	Формальная передача решения алгоритму, размывание ответственности.	Протокол проверки, ответственный эксперт, журнал результата.
Управление сценариями ИИ	Организация знает, где, кем и для чего используется ИИ.	Теневое применение ИИ, несогласованность практик, репутационные риски.	Реестр ИИ-сценариев, оценка риска, правила допуска и мониторинга.

Источник: составлено авторами на основе [67; 83; 92; 101].

Таким образом, грамотность в области данных и ИИ является ключевым компонентом цифрового сознания в ИИ-насыщенной среде. Она требует соединения знаний о данных, понимания ограничений ИИ, навыка проверки результатов и управленческого контура ответственности. Следующий компонент задает нормативные границы применения цифровых технологий: этику, право и ответственность.

3.4. ЦИФРОВАЯ ЭТИКА, ПРАВО И ОТВЕТСТВЕННОСТЬ

Цифровая этика, право и ответственность задают границы допустимого цифрового действия. Этот компонент отвечает на вопрос не только «можем ли мы сделать это технически», но и «имеем ли мы право, должны ли мы делать это, кого затронет решение, и кто отвечает за последствия». В условиях цифровой трансформации именно эти вопросы становятся ключевыми: данные могут быть собраны, профиль может быть построен, решение может быть автоматизировано, коммуникация может быть ускорена, но не всякая техническая возможность является этически и правово допустимой.

UNESCO связывает ответственное применение ИИ с правами человека, человеческим достоинством, прозрачностью, справедливостью, человеческим надзором, приватностью, подотчетностью и грамотностью [137]. OECD подчеркивает надежность, безопасность, прозрачность, объяснимость и ответственность на протяжении жизненного цикла ИИ [109]. Эти принципы важны для цифрового сознания потому, что они расширяют рамку цифровой деятельности: организация должна оценивать не только эффект и скорость, но и влияние на человека, доверие и общественную легитимность.

В российской правовой среде особое значение имеет соблюдение законодательства о персональных данных. Федеральный закон «О персональных данных» закрепляет требования к обработке персональных данных и задает правовой контур, в котором организации должны работать с информацией о

людях [32]. Для цифрового сознания это означает, что сотрудник и управленческая команда должны понимать различие между открытыми, служебными, конфиденциальными и персональными данными, а также недопустимость загрузки таких данных в неутвержденные цифровые и ИИ-сервисы.

Этика не сводится к формальному соблюдению закона. Закон определяет минимально обязательные рамки, а этика заставляет задавать вопрос о последствиях и справедливости. Например, цифровая аналитика может быть правомерной, но восприниматься сотрудниками как скрытый надзор. ИИ-рекомендация может быть удобной, но усиливать предвзятость. Автоматизация может сокращать время обработки заявок, но снижать возможность человеческого объяснения и пересмотра. Поэтому цифровое сознание предполагает этическую рефлексию до запуска цифрового решения, а не только после инцидента.

На рисунке 3.5 представлен контур цифровой ответственности. Он показывает, что ответственность распределяется между сотрудником, командой, руководителем, организацией и внешними стейкхолдерами. Однако распределенность не означает размывание: в каждом цифровом сценарии должно быть понятно, кто действует, кто проверяет, кто утверждает и кто отвечает за последствия.



Рисунок 3.5 – Контур цифровой ответственности

Источник: составлено авторами на основе [32; 61; 67; 88; 109; 137].

Представленная схема показывает, что цифровая ответственность должна быть распределена по ролям и закреплена в правилах. Участники цифрового действия несут разные виды ответственности, но итоговое решение не может быть списано на алгоритм или платформу.

Для сотрудника цифровая этика проявляется в повседневных действиях: не передавать данные без основания, не использовать чужой контент без учета

авторства, не выдавать машинно сгенерированный результат за проверенную экспертизу, не создавать цифровую коммуникацию, унижающую достоинство другого человека, не использовать данные вне заявленной цели. Для управленческой команды этика проявляется в создании правил, процедур согласования, механизмов пересмотра и каналов обращения в случае цифрового конфликта.

Особое внимание требуется к авторству и интеллектуальной собственности. Генеративные ИИ-системы облегчают создание текстов, изображений, презентаций и программного кода, но одновременно усложняют вопрос авторства, заимствования, проверки фактов и ответственности за результат. Организация должна заранее определить, где использование ИИ допустимо, как оно раскрывается, кто отвечает за проверку результата и какие материалы не могут создаваться без участия компетентного специалиста.

В управленческом контуре цифровая ответственность должна быть институционализована. Это означает наличие политики цифрового поведения, правил применения ИИ, порядка обработки персональных данных, этической экспертизы высокорисковых сценариев, требований к объяснению цифровых решений, процедур обжалования и пересмотра. Без таких механизмов этика остается декларацией, а право воспринимается как внешнее ограничение, а не как часть цифровой культуры.

Методически этот компонент целесообразно развивать через анализ этических дилемм. Участникам можно предлагать ситуации, где технически возможное действие конфликтует с доверием, приватностью, справедливостью или правом: анализ цифрового следа работников, применение ИИ при оценке эффективности, использование внешнего сервиса для конфиденциального текста, автоматическая сортировка обращений клиентов, генерация публичного сообщения от имени организации. Разбор таких ситуаций формирует не только знание правил, но и практику ответственного суждения.

Данные таблицы 3.5 показывают, что этико-правовой компонент должен быть выражен через понятные правила работы с данными, контентом, ИИ-результатами и процедурами пересмотра цифровых решений.

Таблица 3.5 – Цифровая этика, право и ответственность: практическая операционализация

Аспект	Содержание	Риск дефицита	Механизм закрепления
Персональные данные	Данные о людях обрабатываются только на законном основании, с соблюдением цели и режима доступа.	Нарушение прав, санкции, утрата доверия.	Регламент обработки данных, классификация данных, обучение ролей.

Аспект	Содержание	Риск дефицита	Механизм закрепления
Конфиденциальность	Служебная и чувствительная информация не передается в неутвержденные сервисы.	Утечки, репутационный ущерб, нарушение договорных обязательств.	Перечень запрещенных данных, контроль доступа, инструкции по ИИ.
Авторство и контент	Использование цифрового и ИИ-контента сопровождается проверкой, корректным оформлением и ответственностью.	Плагиат, нарушение прав, недостоверные материалы.	Правила маркировки ИИ-использования, проверка источников, редакторский контроль.
Справедливость	Цифровые решения не должны воспроизводить дискриминацию или непропорционально влиять на группы людей.	Предвзятые решения, конфликт, снижение легитимности.	Этическая экспертиза, анализ воздействия, возможность пересмотра.
Объяснимость и пересмотр	Участники понимают, как принято значимое цифровое решение и как его можно оспорить.	Недоверие, невозможность защиты интересов, формальная автоматизация.	Порядок объяснения, ответственный владелец решения, журнал оснований.

Источник: составлено авторами на основе [32; 61; 67; 88; 109; 137].

Таким образом, цифровая этика, право и ответственность задают границы допустимого цифрового действия. Без этого компонента цифровая компетентность может привести к быстрому, но неправомерному или несправедливому результату. Следующий компонент раскрывает риск-ориентированную сторону цифрового сознания: безопасность и управление цифровыми рисками.

3.5. ЦИФРОВАЯ БЕЗОПАСНОСТЬ И УПРАВЛЕНИЕ РИСКАМИ

Цифровая безопасность и управление рисками образуют компонент цифрового сознания, который связывает повседневное поведение сотрудников с устойчивостью организации. В цифровой среде безопасность не может оставаться исключительной функцией технического подразделения. Каждый сотрудник работает с доступами, файлами, ссылками, цифровыми сообщениями, данными, ИИ-сервисами и внешними платформами. Поэтому цифровая

безопасность становится организационной культурой повседневной осматрительности.

Стандарты ISO/IEC 27001 и ISO/IEC 27002 рассматривают информационную безопасность как систему управления, включающую риски, политики, роли, доступы, инциденты, обучение и постоянное улучшение [81]. Рамка NIST по кибербезопасности 2.0 подчеркивает, что управление киберрисками должно быть связано с управлением организацией в целом, а не только с техническими мерами защиты [102]. Это соответствует логике цифрового сознания: безопасность является не внешним запретом, а условием доверенного цифрового действия [68].

Актуальность компонента подтверждается данными Verizon Data Breach Investigations Report 2026. В анализируемом массиве эксплуатация уязвимостей стала начальным вектором 31 % утечек, а программы-вымогатели присутствовали в 48 % подтверждённых утечек. Одновременно в массиве наблюдений по предотвращению потерь данных 45 % сотрудников были отнесены к регулярным пользователям ИИ на корпоративных устройствах, причём 67 % пользователей обращались к ИИ-сервисам через некорпоративные учётные записи; теневое использование ИИ стало третьим по распространённости видом непреднамеренного внутреннего нарушения [144]. IBM также фиксирует дефицит политик управления ИИ и контроля доступа в организациях, столкнувшихся с ИИ-инцидентами [79]. Эти данные показывают, что кибербезопасность, управление ИИ и цифровая грамотность персонала должны развиваться как единый контур.

Для сотрудника безопасность начинается с базовых действий: надежная аутентификация, осторожность к ссылкам и вложениям, проверка адресата, соблюдение режима доступа, отказ от передачи паролей, использование утвержденных хранилищ, своевременное сообщение об инцидентах. Однако цифровое сознание требует большего: сотрудник должен понимать, почему эти правила важны для организации, какие последствия может иметь нарушение, и почему сообщение о подозрительном событии является не признаком вины, а частью культуры безопасности.

Для управленческой команды безопасность означает создание условий, при которых безопасное поведение становится нормальным и удобным. Если утвержденные сервисы неудобны, а правила непонятны, сотрудники будут искать обходные пути. Поэтому управление рисками должно включать не только запреты, но и дизайн процессов: понятные инструменты, обучение, классификацию данных, доступные консультации, быстрые реакции на инциденты и культуру, в которой сообщение о проблеме не наказывается автоматически. На рисунке 3.6 представлена карта цифровых рисков, с которыми сталкиваются сотрудники и управленческие команды.

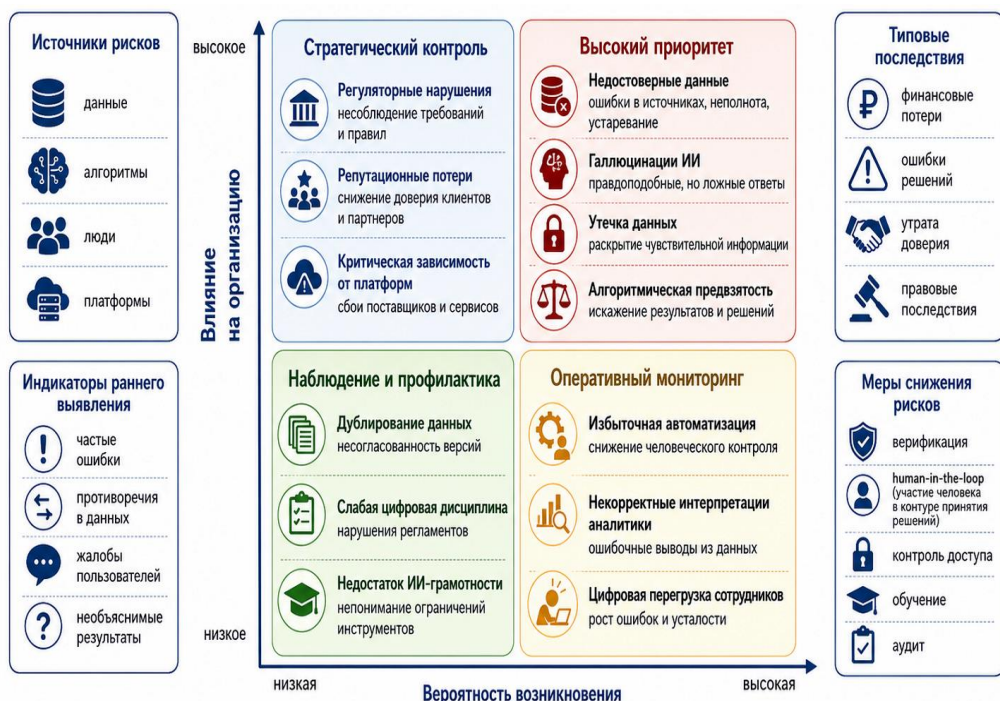


Рисунок 3.6 – Карта цифровых рисков сотрудника и управленческой команды
 Источник: составлено авторами на основе [79; 81; 102; 144].

Рисунок 3.6 систематизирует, что цифровые риски возникают в разных зонах: данные, доступы, ИИ, коммуникация, репутация и цифровая перегрузка. Следовательно, управление рисками должно быть межфункциональным и включать обучение, регламенты и постоянное улучшение.

Особое место занимает теневое использование ИИ. Под ним понимается применение сотрудниками неутвержденных ИИ-инструментов для рабочих задач без уведомления организации, оценки рисков, контроля доступа и правил хранения данных. Теневое использование ИИ часто возникает не из злого умысла, а из дефицита организационного дизайна: сотрудник хочет ускорить работу, но не имеет понятного легального инструмента. Поэтому управленческий ответ должен сочетать ограничения и поддержку: запрет на чувствительные данные, разрешенные сценарии, корпоративные инструменты, обучение и мониторинг рисков.

Цифровая безопасность должна быть встроена в компонентную модель цифрового сознания, а не вынесена в отдельный технический раздел. Безопасность связана с дееспособностью, потому что пользователь должен понимать инструмент; с критичностью, потому что нужно распознавать подозрительные сообщения; с ИИ-грамотностью, потому что ИИ может усиливать атаки и создавать утечки; с этикой и правом, потому что защита

данных является обязательством перед людьми; с коммуникацией, потому что многие инциденты начинаются с социальной инженерии; с рефлексивностью, потому что организация должна учиться на инцидентах.

Методически безопасность развивается через регулярные практики: короткие тренировки кибергигиены, имитационные проверки фишинга, обучение классификации данных, разбор инцидентов без обвинительной культуры, матрицы доступа, контроль внешних сервисов, обновление паролей и многофакторной аутентификации, сценарии реагирования на утечки и инциденты ИИ. Важно, чтобы такие практики не воспринимались как формальные тесты, а были связаны с реальными цифровыми рисками организации (таблица 3.6).

Таблица 3.6 – Цифровая безопасность и управление рисками: компоненты поведения и управления

Направление	Содержание	Риск дефицита	Механизм развития
Доступы и аутентификация	Управление правами, многофакторная аутентификация, отказ от передачи учетных данных.	Компрометация аккаунтов, несанкционированный доступ.	Матрица доступа, регулярный пересмотр ролей, обучение пользователей.
Фишинг и социальная инженерия	Распознавание подозрительных сообщений, ссылок, звонков и запросов.	Кража учетных данных, заражение, финансовый ущерб.	Имитационные тренировки, правила проверки, канал сообщения о подозрении.
Работа с данными	Классификация данных, безопасное хранение, соблюдение правового режима.	Утечки, неверное распространение, нарушение закона.	Политика данных, утвержденные хранилища, запрет личных облаков для служебных данных.
ИИ-риски	Контроль теневого использования ИИ, защита запросов и результатов.	Передача чувствительных данных, ошибочные ИИ-выводы, репутационный ущерб.	Список допустимых ИИ-сценариев, проверка результатов, журналирование.
Инциденты и обучение	Своевременное сообщение о проблемах, разбор причин и корректировка правил.	Соккрытие ошибок, повторение инцидентов, рост ущерба.	План реагирования, культура без обвинения, регулярные разборы.

Источник: составлено авторами на основе [79; 81; 102; 144].

Данные таблицы показывают, что цифровая безопасность проявляется одновременно в личной дисциплине сотрудника и в управленческих механизмах организации. Один без другого не обеспечивает устойчивости.

Таким образом, цифровая безопасность и управление рисками являются поведенческим и управленческим компонентом цифрового сознания. Они требуют не только технических средств защиты, но и культуры осмотрительности, понятных правил, межфункционального взаимодействия и регулярного обучения. Следующий компонент показывает, как цифровое сознание проявляется в коммуникации и культуре взаимодействия.

3.6. ЦИФРОВАЯ КОММУНИКАЦИЯ И КУЛЬТУРА ВЗАИМОДЕЙСТВИЯ

Цифровая коммуникация и культура взаимодействия отвечают за превращение цифровой инфраструктуры в среду совместной деятельности. Организация может иметь платформы, мессенджеры, электронный документооборот, базы знаний, системы задач и аналитические панели, но без культуры коммуникации эти средства не обеспечивают согласованного действия. Напротив, они могут создавать цифровой шум, перегрузку, потерю решений, конфликт каналов и размывание ответственности.

Организационная культура, по Э. Шейну, проявляется в разделяемых базовых предположениях, ценностях и практиках [121]. В цифровой среде эти предположения выражаются в том, как сотрудники пишут сообщения, где фиксируют решения, как обращаются с общими документами, как ведут совещания, как делятся знаниями, как реагируют на ошибки и насколько готовы к открытой обратной связи. Поэтому цифровая коммуникация является не «мягким» дополнением к технологиям, а самостоятельным компонентом цифрового сознания.

Цифровая коммуникация имеет несколько уровней. Первый уровень – канал: где обсуждается идея, где фиксируется задача, где хранится документ, где принимается решение. Второй уровень – норма: как формулируются сообщения, кто является адресатом, какой срок ответа ожидается, как соблюдается уважение и конфиденциальность. Третий уровень – знание: как информация превращается в общий организационный ресурс, а не остается в личной переписке. Четвертый уровень – доверие: участники понимают, что цифровая коммуникация не будет использована как скрытый инструмент давления или манипуляции.

Управление знаниями показывает, что организация создает ценность тогда, когда личный опыт становится коллективным знанием [104]. В цифровой среде этот процесс зависит от качества коммуникационных практик. Если решения остаются в переписке, документы хранятся в личных папках, договоренности не

фиксируются, а успешные цифровые сценарии не описываются, организация теряет цифровую память. Следовательно, цифровое сознание требует не только культуры общения, но и архитектуры совместного знания.

На рисунке 3.7 представлена архитектура цифровой коммуникации и культуры взаимодействия. Она показывает, что коммуникация становится управляемой при согласовании каналов, норм, знаний, доверия и результата.



Рисунок 3.7 – Архитектура цифровой коммуникации и культуры взаимодействия

Источник: составлено авторами на основе [95; 104; 121; 123].

Представленная схема показывает, что цифровая коммуникация должна быть спроектирована как система: каналы, нормы, знания, доверие и результат. Иначе цифровые средства начинают создавать перегрузку вместо координации.

Для сотрудника цифровая коммуникация проявляется в ясности сообщений, уважительном тоне, умении выбирать канал, краткости, фиксации договоренностей, соблюдении режима информации и понимании адресата. Для команды – в правилах совместного редактирования, протоколировании решений, единых хранилищах, регулярных синхронизациях и способности обсуждать цифровые ошибки без взаимных обвинений. Для управленческой команды – в проектировании коммуникационной среды: какие каналы обязательны, какие избыточны, где хранится решение, кто владелец информации, как предотвращается перегрузка.

Особое значение имеет цифровая перегрузка. Большое количество уведомлений, параллельных каналов, срочных сообщений и дублирующих совещаний снижает качество мышления, увеличивает усталость и

сопротивление цифровым изменениям. Microsoft Work Trend Index 2024 указывал на массовый рост использования ИИ на работе и необходимость управленческой настройки новых практик [95]. Это означает, что организация должна заботиться не только о внедрении инструментов, но и о цифровой гигиене коммуникации: какие каналы использовать, когда не писать, как фиксировать решение и как не превращать цифровую среду в постоянный поток отвлечений.

Цифровая коммуникация также связана с внешним образом организации. Публичные сообщения, ответы клиентам, цифровые сервисы, чат-боты, автоматические уведомления, страницы в сетевых средах и документы формируют цифровую репутацию. Сотрудник и управленческая команда должны понимать, что цифровая коммуникация организации воспринимается как действие институционального субъекта. Ошибка в цифровом ответе или некорректная автоматическая коммуникация может повлиять на доверие не меньше, чем управленческое решение.

Методически развитие этого компонента требует создания коммуникационного кодекса цифровой среды. Такой кодекс не должен быть длинным документом. Он должен отвечать на практические вопросы: какой канал для какой цели используется; где фиксируются решения; как называются документы; какие сроки ответа приемлемы; какие темы нельзя обсуждать в незащищенных каналах; как маркировать материалы, созданные с использованием ИИ; как проводить цифровое совещание; как сохранять знания после проекта (таблица 3.7).

Таблица 3.7 – Цифровая коммуникация и культура взаимодействия: нормы и индикаторы

Направление	Содержание	Индикатор	Риск дефицита
Каналы коммуникации	Разведение каналов для обсуждения, задач, решений, документов и экстренных сообщений.	Сотрудники знают, где обсуждать, где фиксировать, где хранить.	Хаос переписки, потеря решений, дублирование действий.
Фиксация договоренностей	Решения, сроки, ответственные и основания сохраняются в утвержденной системе.	После совещания есть протокол или карточка задачи.	Размытая ответственность и конфликт памяти.
Культура сообщений	Сообщения ясны, адресны, уважительны и не создают лишнего шума.	Снижается число уточнений, пересылок и конфликтов.	Перегрузка, раздражение, снижение доверия.
Работа со	Опыт, шаблоны,	Есть база знаний,	Потеря опыта при

Направление	Содержание	Индикатор	Риск дефицита
знаниями	инструкции и удачные цифровые решения становятся общим ресурсом.	регулярно обновляемые шаблоны и практики.	смене сотрудников или команд.
Цифровая репутация	Внешняя коммуникация организации понятна, корректна, проверена и ответственна.	Публичные материалы проходят проверку; автоматические ответы контролируются.	Репутационные сбои и снижение доверия стейкхолдеров.

Источник: составлено авторами на основе [95; 104; 121; 123].

Данные таблицы показывают, что цифровая коммуникация включает не только вежливость в каналах, но и управление знаниями, фиксацию решений, предотвращение перегрузки и защиту цифровой репутации организации.

Таким образом, цифровая коммуникация превращает цифровую инфраструктуру в среду сотрудничества. Без коммуникационных норм цифровые сервисы порождают шум, перегрузку и потерю ответственности. Следующий компонент раскрывает способность сотрудников и управленческих команд анализировать собственный цифровой опыт, корректировать поведение и адаптироваться к изменениям.

3.7. РЕФЛЕКСИВНОСТЬ, САМОРЕГУЛЯЦИЯ И ГОТОВНОСТЬ К ИЗМЕНЕНИЯМ

Рефлексивность, саморегуляция и готовность к изменениям являются завершающим и одновременно сквозным компонентом цифрового сознания. Если предыдущие компоненты описывают способность действовать, проверять данные, использовать ИИ, соблюдать этику, обеспечивать безопасность и коммуницировать, то рефлексивность отвечает за обновление этих способностей. Цифровая среда меняется быстрее, чем инструкции и учебные программы; поэтому цифровое сознание не может быть сформировано один раз. Оно должно постоянно корректироваться.

Теории организационного обучения показывают, что организация развивается тогда, когда способна обнаруживать ошибки, переосмысливать правила действия и изменять практики [43]. П. Сенге описывает обучающуюся организацию как систему, развивающую способность к коллективному видению, системному мышлению и командному обучению [123]. В контексте цифрового сознания эти идеи означают: организация должна учиться на цифровом опыте, а не только внедрять новые сервисы. Она должна анализировать, какие цифровые решения повысили качество, какие усилили перегрузку, какие риски проявились, какие правила оказались неработающими.

На индивидуальном уровне рефлексивность проявляется в способности сотрудника замечать собственные цифровые привычки, оценивать нагрузку, признавать ошибки, пересматривать способы работы и учиться новым инструментам. Саморегуляция означает, что человек способен не только использовать цифровую среду, но и управлять своей вовлеченностью в нее: не поддаваться постоянному потоку уведомлений, не передавать ответственность ИИ, не использовать сервисы автоматически, не заменять собственное мышление машинной подсказкой.

На управленческом уровне рефлексивность проявляется в способности руководителей проводить постпроектный анализ цифровых инициатив, собирать обратную связь, корректировать регламенты, пересматривать цифровую архитектуру, обновлять программы обучения и не рассматривать сопротивление сотрудников как простую неготовность. Сопротивление может указывать на реальную перегрузку, плохой дизайн процесса, неясность целей или конфликт между цифровым инструментом и профессиональной логикой деятельности.

На рисунке 3.8 представлен цикл цифровой рефлексии и организационного обучения. Он показывает, что цифровое действие должно завершаться не только результатом, но и анализом цифрового следа, оценкой последствий, выводом, корректировкой и закреплении новой практики.



Рисунок 3.8 – Цикл цифровой рефлексии и организационного обучения

Источник: составлено авторами на основе [43; 123; 130].

Представленная схема показывает, что рефлексивность превращает цифровой опыт в обучение. Без такого цикла организация повторяет ошибки, а цифровые регламенты быстро устаревают.

Готовность к изменениям не означает безусловное согласие со всеми цифровыми инициативами. Напротив, зрелая готовность включает способность отличать необходимое изменение от технологической моды, продуктивный эксперимент от необоснованного риска, полезную автоматизацию от потери ответственности. Сотрудник с развитым цифровым сознанием не сопротивляется новому из-за страха, но и не принимает новое без критической оценки. Управленческая команда с развитым цифровым сознанием не требует мгновенного принятия любой цифровой новации, а объясняет смысл, риски, ожидаемый результат и поддержку.

Динамические способности организации связаны с умением распознавать изменения, использовать возможности и трансформировать ресурсы [130]. Рефлексивность можно рассматривать как когнитивно-культурное условие таких способностей. Если организация не анализирует цифровые последствия, она не видит, когда инструмент перестает работать, когда данные искажают реальность, когда ИИ-сценарий создает риск, когда сотрудники перегружены, когда внешние ожидания меняются. Поэтому рефлексивность является не психологическим дополнением, а управленческим механизмом цифровой адаптации.

Для диагностики этого компонента можно использовать самооценку цифровой нагрузки, анализ участия в обучении, качество постпроектных разборов, наличие обновленных регламентов, частоту пересмотра ИИ-сценариев, количество улучшений, инициированных сотрудниками, и наличие культуры обсуждения цифровых ошибок. При этом диагностика должна быть этически ограниченной: данные цифрового следа не должны превращаться в скрытый надзор за сотрудниками. Они могут использоваться агрегированно и развивающе, с понятными правилами и запретом на автоматические персональные санкции.

Методически рефлексивность развивается через регулярные сессии анализа цифровых практик, разбор инцидентов, внутренние сообщества практиков, наставничество, дневники цифровых наблюдений, короткие циклы улучшения, ежегодное обновление цифровых правил и включение сотрудников в проектирование изменений (таблица 3.8). Главный результат – формирование организации, которая не только реагирует на цифровую среду, но и осознанно корректирует свое поведение в ней.

Таблица 3.8 – Рефлексивность, саморегуляция и готовность к изменениям: уровни проявления

Уровень	Содержание	Индикатор	Риск дефицита
Индивидуальная рефлексия	Сотрудник оценивает свои	Самооценка, запрос на обучение,	Автоматизм, выгорание,

Уровень	Содержание	Индикатор	Риск дефицита
	цифровые привычки, ошибки, нагрузку и необходимость обучения.	корректировка способа работы.	повторение ошибок.
Командная рефлексия	Команда обсуждает цифровые решения, ошибки, ИИ-результаты и улучшения.	Регулярные разборы кейсов, обновление командных правил.	Фрагментация практик, скрытые конфликты, потеря знаний.
Управленческая рефлексия	Руководители анализируют последствия цифровых решений и корректируют процессы.	Постпроектные отчеты, пересмотр регламентов, обратная связь.	Формальная цифровизация и управленческая слепота.
Организационное обучение	Цифровой опыт превращается в новые программы, правила и архитектурные решения.	База знаний, обновленные регламенты, программы повышения квалификации.	Устаревание правил и отставание от технологий.
Адаптивность	Организация умеет корректировать цифровую стратегию при изменении технологий и рисков.	Периодический пересмотр ИИ-сценариев и цифровой архитектуры.	Зависимость от старых решений и рост теневых практик.

Источник: составлено авторами на основе [43; 123; 130].

Данные таблицы показывают, что рефлексивность проявляется на индивидуальном, командном, управленческом и организационном уровнях. Она обеспечивает обновление всех остальных компонентов цифрового сознания.

Таким образом, рефлексивность, саморегуляция и готовность к изменениям выступают метакомпонентом цифрового сознания. Они связывают опыт, ошибки, цифровой след, обучение и корректировку практик. Без рефлексивности цифровое сознание быстро превращается в набор устаревающих инструкций.

ИТОГИ ГЛАВЫ

Компонентная модель объединяет цифровую дееспособность, критичность, грамотность в области данных и ИИ, этику и ответственность, безопасность, коммуникацию и рефлексивность. Эти компоненты проявляются одновременно в поведении сотрудников, совместной работе команд и управленческих решениях.

Управленческий переход к главе 4: компоненты цифрового сознания связываются с контурами цифровой зрелости, чтобы определить организационные результаты и зоны ответственности руководства.

***Интерактивное сопровождение.** В цифровом руководстве размещены диагностические опросники, кейсы, карты компонентов, чек-листы проверки ИИ-результатов и модульные программы обучения.*

ГЛАВА 4. ЦИФРОВОЕ СОЗНАНИЕ ОРГАНИЗАЦИИ КАК УПРАВЛЕНЧЕСКИЙ ФАКТОР ЦИФРОВОЙ ЗРЕЛОСТИ

*«Системное мышление – это дисциплина, позволяющая видеть
целое».*

Питер Сенге

Управленческий вопрос главы. Как связать формирование цифрового сознания со стратегией и цифровой зрелостью, не сводя развитие организации к внедрению технологий?

Управленческий результат главы. Система из шести контуров управления: стратегия; данные, аналитика и ИИ; архитектура и сервисы; культура, доверие и безопасность; развитие персонала и команд; организационная рефлексивность.

4.1. ЦИФРОВАЯ ЗРЕЛОСТЬ И ЦИФРОВОЕ СОЗНАНИЕ: СООТНОШЕНИЕ ПОНЯТИЙ

Понятие цифровой зрелости широко используется в управленческой и аналитической литературе для описания уровня развития организации в условиях цифровой трансформации. В разных моделях акцент делается на цифровой стратегии, лидерстве, процессах, клиентском опыте, данных, архитектуре, технологиях, инновациях, безопасности, компетенциях и культуре. Подход MIT Sloan Management Review и Deloitte подчеркивает, что цифровую трансформацию определяет не технология сама по себе, а стратегия, организационная готовность и лидерство [89]. В работах Westerman, Bonnet и McAfee цифровая зрелость связывается с сочетанием цифровых возможностей и управленческих способностей [148]. Исследования Vial и Verhoef с соавторами показывают, что цифровая трансформация является многомерным процессом изменения бизнес-моделей, организационных структур, процессов и пользовательского опыта [143; 145] [14; 34; 35; 38; 39].

Следовательно, цифровая зрелость описывает не только технологическое оснащение, а степень согласованности цифровых решений с организационными целями. Однако даже развитые модели зрелости чаще отвечают на вопрос о состоянии: что внедрено, какие процессы оцифрованы, какие данные используются, какие компетенции сформированы, какие показатели достигнуты. Они полезны для диагностики, сравнения и планирования развития, но сами по себе не всегда раскрывают внутренний механизм осознания, оценки и корректировки цифрового развития.

Именно здесь необходима категория цифрового сознания организации. В пособии цифровое сознание понимается как способность организации как коллективного субъекта осознанно, критично, этично, безопасно и результативно использовать цифровые технологии, данные и ИИ для

достижения стратегических целей, развития сотрудников, повышения качества процессов, укрепления доверия, управления рисками и создания устойчивой цифровой культуры. Если цифровая зрелость показывает, на каком уровне находится организация, то цифровое сознание показывает, как организация осмысляет, управляет, оценивает и корректирует свое цифровое развитие.

Методологически важно не противопоставлять эти понятия. Цифровая зрелость без цифрового сознания рискует стать формальным индексом: организация отмечает наличие платформ, регламентов и аналитических панелей, но не анализирует их влияние на качество решений, доверие, безопасность и человеческую ответственность. Цифровое сознание без зрелости также остается неполным: организация может декларировать этичность и критичность, но не иметь архитектуры данных, регламентов ИИ, системы обучения, ответственных ролей и показателей результата. Поэтому связь между ними должна пониматься как связь состояния и механизма развития.

В практической работе с организацией цифровая зрелость может быть диагностическим языком, а цифровое сознание – языком методологического проектирования изменений. Первая показывает разрыв между текущим и целевым состоянием. Второе объясняет, какие управленческие и культурные действия необходимы, чтобы этот разрыв не был закрыт только формально. На рисунке 4.1 показано соотношение этих двух понятий: цифровая зрелость фиксирует уровень развития, а цифровое сознание выступает смысловой основой, связывающей стратегию, данные, архитектуру, культуру, безопасность, персонал и рефлекссию.

Представленная схема показывает, что цифровая зрелость и цифровое сознание не являются конкурирующими понятиями: зрелость фиксирует достигнутый уровень, а цифровое сознание задает смысл, управление, ответственность и рефлексивный механизм достижения этого уровня

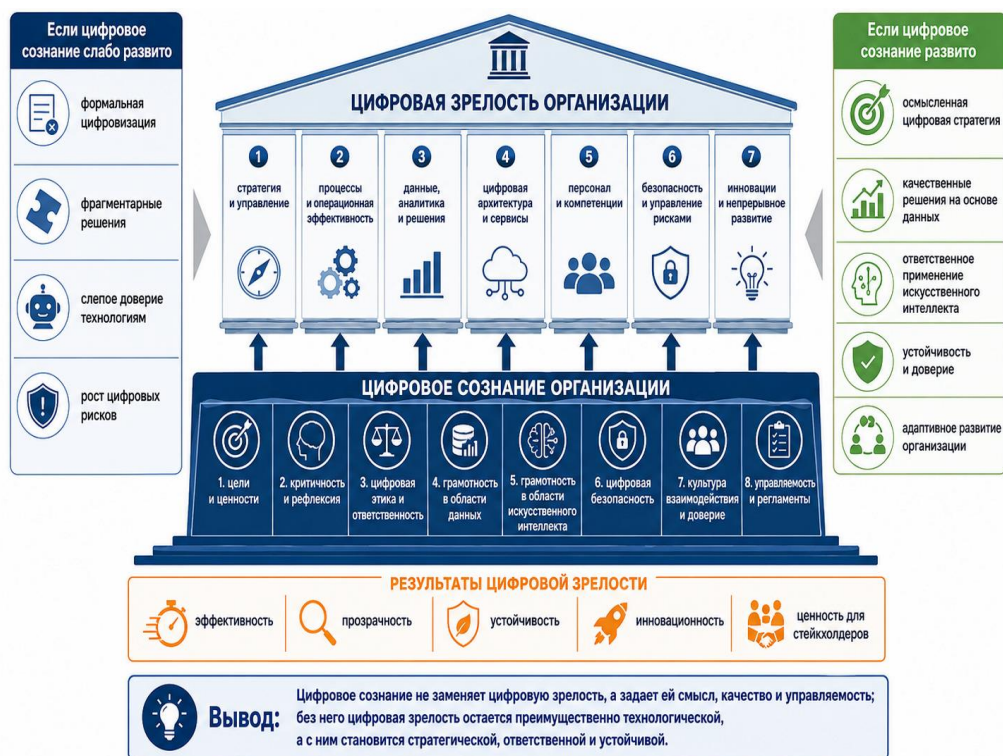


Рисунок 4.1 – Цифровое сознание как смысловая основа цифровой зрелости

Источник: составлено авторами на основе [83; 89; 101; 143; 145; 148].

Сравнение цифровой зрелости и цифрового сознания организации систематизировано в таблице 4.1. Таблица необходима для дальнейшего текста главы, поскольку все последующие контуры раскрывают не отдельные блоки цифровизации, а механизмы превращения цифрового сознания в цифровую зрелость.

Таблица 4.1 – Цифровая зрелость и цифровое сознание организации: соотношение понятий

Критерий	Цифровая зрелость	Цифровое сознание	Связь между понятиями
Что фиксирует	Состояние цифрового развития: процессы, платформы, данные, компетенции, культура, безопасность.	Способность организации осмысливать, управлять, оценивать и корректировать это развитие.	Зрелость описывает уровень, сознание объясняет механизм достижения и удержания уровня.
Главный вопрос	На каком уровне находится организация?	Зачем, как, с какими последствиями и в какой системе ответственности	Вместе вопросы дают управленческую картину развития.

Критерий	Цифровая зрелость	Цифровое сознание	Связь между понятиями
		организация использует цифровые технологии?	
Тип результата	Индикаторы, уровни, домены, баллы, сравнительная оценка.	Смысл, нормы, ответственность, рефлексия, контуры управления.	Цифровая зрелость становится не формальной метрикой, а управляемым состоянием.
Риск дефицита	Формальный рост показателей без устойчивой ценности.	Осознанность без организационного закрепления может остаться декларацией.	Необходима связка: измерение зрелости плюс управление цифровым сознанием.
Значение для управления	Позволяет видеть разрывы и планировать развитие.	Позволяет объяснять причины разрывов и проектировать изменения.	Создает основу диагностики, обучения и корректировки цифровой стратегии.

Источник: составлено авторами.

Данные таблицы показывают, что цифровая зрелость отвечает за оценку состояния, а цифровое сознание – за управленческое осмысление и корректировку развития. В методическом плане они должны использоваться совместно: зрелость задает шкалу, цифровое сознание – механизм формирования.

Наиболее слабым местом многих программ цифровой зрелости является риск подмены зрелости инфраструктурной насыщенностью. Количество сервисов, платформ, цифровых рабочих мест и аналитических панелей еще не гарантирует, что организация принимает более качественные решения. Для этого необходимы владельцы данных, понятные процедуры проверки, критическая интерпретация показателей, обучение руководителей и сотрудников, а также контур рефлексии. Поэтому цифровое сознание позволяет уточнить зрелость: зрелой является не та организация, которая имеет больше цифровых инструментов, а та, которая умеет ответственно использовать их для создания ценности.

Таким образом, цифровая зрелость организации может быть определена как уровень институциональной встроенности цифровых технологий, данных, ИИ, цифровой архитектуры, компетенций, культуры и безопасности в стратегию, процессы и систему управления организации. Цифровое сознание организации является основанием этой зрелости, потому что связывает технические

возможности с целями, нормами, рисками, доверием и обучением. Последующие параграфы раскрывают эту связь через шесть контуров.

Таким образом, цифровая зрелость показывает уровень цифрового развития организации, а цифровое сознание задает смысловой и управленческий механизм его формирования. Для научно-методического пособия принципиально важно рассматривать зрелость не как сумму технологий, а как результат согласованной работы стратегии, данных, ИИ, архитектуры, культуры, безопасности, персонала и рефлексии.

4.2. СТРАТЕГИЧЕСКИЙ КОНТУР ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

Стратегический контур является исходным для формирования цифровой зрелости, потому что он отвечает на вопрос, зачем организация использует цифровые технологии, данные и ИИ. Без стратегического контура цифровизация превращается в набор отдельных проектов: внедряется документооборот, запускается аналитическая панель, создается чат-бот, закупается платформа, но не формируется единая логика ценности. Такая цифровизация может быть активной, но незрелой, поскольку она не связана с миссией, приоритетами, ресурсами и ответственностью.

В исследованиях цифровой трансформации неоднократно подчеркивается, что стратегия, а не технология, определяет зрелость цифрового развития [89]. Динамические способности организации позволяют ей распознавать технологические возможности, соотносить их со стратегическими задачами и перестраивать ресурсы [130]. Поэтому стратегический контур цифрового сознания должен включать не только планы внедрения, но и способность руководства формулировать смысл цифровых изменений: какую ценность они создают для клиентов, пользователей, партнеров, сотрудников и самой организации.

Первым элементом стратегического контура является цифровая миссия. Она не заменяет общую миссию организации, а показывает, как цифровые технологии усиливают ее реализацию. Для коммерческой организации это может быть повышение качества клиентского опыта, скорости процессов и инновационности продукта. Для органа публичного управления – доступность, прозрачность и удобство сервисов. Для научной или проектной организации – ускорение работы со знаниями, данными и экспертными продуктами. В универсальной модели пособия важен не отраслевой пример, а общий принцип: цифровая миссия должна связывать технологию с ценностью, а не с модой.

Второй элемент – портфель цифровых инициатив. Организация с развитым цифровым сознанием не запускает цифровые проекты изолированно. Она описывает их цели, ожидаемый эффект, ресурсы, риски, владельцев и

показатели результата. Портфельный подход позволяет сравнивать инициативы не только по стоимости и срокам, но и по стратегической значимости, влиянию на процессы, рискам данных, требованиям к компетенциям и эффекту для доверия. Это особенно важно в условиях дефицита ресурсов и высокой скорости технологических изменений.

Третий элемент – управленческая ответственность. Цифровая зрелость невозможна, если цифровые решения рассматриваются как зона только технических специалистов. Руководители должны отвечать не только за запуск систем, но и за организационный эффект: изменение процессов, качество данных, обучение сотрудников, принятие рисков и объяснение результатов. Стандарт ISO/IEC 38500 (международный стандарт управления ИТ в организации) подчеркивает связь цифровых решений с организационным управлением и ответственностью руководящих органов [82].

На рисунке 4.2 стратегический контур представлен как система связи целей, цифровой стратегии, портфеля инициатив, ресурсов, рисков, показателей и обратной связи. Этот рисунок используется как методическая рамка для проектирования цифровой стратегии организации.

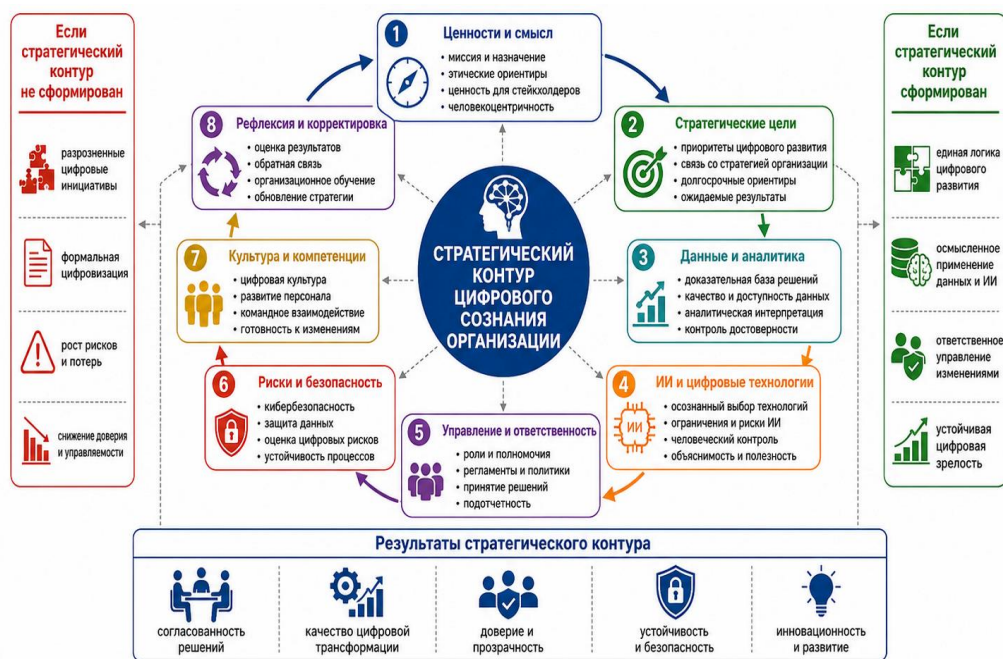


Рисунок 4.2 – Стратегический контур цифрового сознания организации

Источник: составлено авторами на основе [82; 89; 130; 148].

Представленная схема показывает, что цифровая стратегия не является отдельным документом об ИТ. Она связывает цели организации, портфель

инициатив, ресурсы, риски, ответственность, показатели результата и механизм корректировки.

Содержательные элементы стратегического контура, управленческие вопросы и индикаторы представлены в таблице 4.2. Таблица может использоваться как предварительная карта самооценки цифровой стратегии организации.

Таблица 4.2 – Стратегический контур цифрового сознания: элементы, управленческие вопросы и индикаторы

Элемент	Управленческий вопрос	Практический индикатор	Риск дефицита
Цифровая миссия	Как цифровые технологии связаны с назначением организации?	Формулировка цифровой миссии в стратегии или программе развития	Технологии внедряются без управленческого смысла
Портфель инициатив	Какие цифровые проекты создают наибольшую ценность?	Реестр инициатив с приоритетами, ответственными и ожидаемым эффектом	Ресурсы распыляются между несвязанными проектами
Ответственность	Кто принимает решения и кто отвечает за последствия?	Матрица ролей руководителей, владельцев данных и цифровых продуктов	Размывание ответственности и конфликт полномочий
Ресурсы	Какие компетенции, бюджет и инфраструктура необходимы?	Ресурсный план и дорожная карта внедрения	Недофинансирование сопровождения и обучения
Показатели	Как доказать результативность цифровой инициативы?	Набор показателей ценности, качества, риска и доверия	Отчетность ради отчетности
Корректировка	Как цифровая стратегия меняется по данным и обратной связи?	Регулярный пересмотр портфеля и постпроектный анализ	Сохранение устаревших или неэффективных решений

Источник: составлено авторами.

Таблица 4.2 переводит стратегический контур в управленческие вопросы. Она показывает, что цифровая зрелость начинается не с закупки решений, а с осмысленного ответа на вопросы о миссии, ценности, ресурсах, ответственности, рисках и результате.

Важным признаком стратегического цифрового сознания является способность организации различать эффективность и ценность. Эффективность

показывает, насколько быстрее или дешевле выполняется операция. Ценность показывает, улучшает ли цифровое решение качество результата, доверие, доступность, устойчивость, инновационность и способность организации развиваться. Если цифровая инициатива оценивается только по экономии времени, она может не учитывать риски безопасности, перегрузку сотрудников, потерю качества коммуникации или снижение доверия внешних участников.

Стратегический контур также требует механизма остановки и пересмотра инициатив. Цифровое сознание проявляется не только в готовности внедрять, но и в способности отказаться от решений, которые перестали создавать ценность, усиливают технический долг или противоречат принципам безопасности и человекоцентричности. Поэтому зрелая цифровая стратегия должна иметь не только дорожную карту запуска, но и правила пересмотра портфеля.

Таким образом, стратегический контур цифрового сознания связывает цифровые технологии, данные и ИИ с миссией, целями, портфелем инициатив, ресурсами, рисками, показателями и управленческой ответственностью. Без этого контура цифровая зрелость остается фрагментарной: технологии есть, но их ценность, границы и последствия не управляются.

4.3. КОНТУР ДАННЫХ, АНАЛИТИКИ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Контур данных, аналитики и ИИ является центральным элементом современной цифровой зрелости. Данные становятся основой решений, аналитические панели формируют управленческую видимость процессов, а ИИ начинает участвовать в подготовке текстов, прогнозов, рекомендаций, классификаций и сценариев действий. Однако именно здесь особенно заметен разрыв между цифровизацией и цифровым сознанием. Сбор данных и внедрение ИИ не гарантируют зрелости, если организация не управляет качеством данных, правовым режимом, доступом, интерпретацией, рисками, проверкой результатов и ответственностью [56; 57; 83; 101].

Управление данными является первым условием этого контура. DAMA-DMBOK рассматривает управление данными как центральную область, связывающую архитектуру, качество, безопасность, метаданные, интеграцию, хранилища, аналитику и жизненный цикл данных [56]. Для цифрового сознания организации это означает: данные должны быть не случайным побочным продуктом процессов, а управляемым активом. У каждого критичного набора данных должны быть владелец, описание, режим доступа, правила обновления, методика использования и ограничения интерпретации.

Второе условие – аналитическая интерпретация. Управление на основе данных не означает автоматическое следование показателям. Показатель является моделью реальности, построенной на определенной методике.

Руководитель и команда должны понимать, что включено в показатель, что исключено, каковы ограничения данных, какие искажения возможны, в каких случаях показатель нельзя использовать для индивидуальных выводов или санкций. Без такого понимания цифровая аналитика превращается в цифровой самообман: организация получает точные числа, но делает неверные управленческие выводы.

Третье условие – управление ИИ. NIST AI RMF (рамка управления рисками искусственного интеллекта Национального института стандартов и технологий США) описывает управление ИИ как работу с рисками для людей, организаций и общества на протяжении жизненного цикла ИИ-систем [101]. ISO/IEC 42001 (международный стандарт системы менеджмента ИИ) закрепляет необходимость устанавливать политики, цели, процессы, оценку результативности и постоянное улучшение в отношении ответственного применения ИИ [83]. Эти документы переводят ИИ из режима экспериментов в режим организационного управления [113].

Четвертое условие – сохранение человеческой ответственности. Человек в контуре решения (human-in-the-loop – участие человека в проверке и утверждении значимого цифрового результата) не должен быть формальной фигурой. Он должен иметь компетентность, полномочия, доступ к данным, время на проверку и право остановить применение результата ИИ. Иначе организация только имитирует контроль, а фактически передает ответственность непрозрачному алгоритмическому процессу.

На рисунке 4.3 контур данных, аналитики и ИИ представлен как управляемый цикл: источники данных, управление данными, аналитика, сценарии ИИ, человеческая проверка и мониторинг последствий. Такой цикл позволяет отличить зрелое применение ИИ от стихийного использования цифровых сервисов.

Представленная схема показывает, что данные и ИИ должны быть включены в единый контур управляемости: качество данных, владельцы, аналитика, реестр сценариев ИИ, проверка человеком и мониторинг последствий.



Рисунок 4.3 – Контур данных, аналитики и ИИ в цифровом сознании организации

Источник: составлено авторами на основе [56; 57; 83; 101].

Операционализация контура данных и ИИ представлена в таблице 4.3. Таблица показывает, какие элементы управления должны быть закреплены в локальных документах и какие риски возникают при их отсутствии.

Таблица 4.3 – Управление данными и ИИ как элемент организационного цифрового сознания

Элемент управления	Управленческое назначение	Возможный локальный документ	Риск при отсутствии	Индикатор зрелости
Реестр данных	Понимание источников, владельцев, качества и правового режима данных	Положение об управлении данными; каталог данных	Хаос источников, некачественная аналитика, конфликт владельцев	Доля критичных наборов данных с владельцем и описанием
Качество данных	Проверка полноты, актуальности, точности и сопоставимости данных	Регламент качества данных; правила очистки и обновления	Ошибочные решения на формально красивых показателях	Число выявленных и исправленных дефектов данных

Элемент управления	Управленческое назначение	Возможный локальный документ	Риск при отсутствии	Индикатор зрелости
Аналитические панели	Перевод данных в управленческие показатели и интерпретации	Методика расчета показателей; паспорт панели	Слепая вера в показатели без контекста	Наличие методики и ответственного за показатель
Реестр ИИ-сценариев	Учет применяемых ИИ-решений и сценариев использования	Положение о применении ИИ; реестр сценариев	Теневое использование ИИ и отсутствие контроля	Доля сценариев ИИ, прошедших классификацию риска
Проверка результатов ИИ	Сохранение человеческой проверки значимых результатов	Чек-лист проверки; журнал использования ИИ	Автоматизация ошибок, галлюцинаций и предвзятости	Доля значимых ИИ-результатов с подтвержденной проверкой
Мониторинг последствий	Оценка влияния решений, принятых с использованием данных и ИИ	Постпроектный анализ; отчет по рискам ИИ	Накопление скрытых социальных и репутационных эффектов	Регулярность пересмотра сценариев и мер контроля

Источник: составлено авторами.

Данные таблицы показывают, что работа с данными и ИИ требует не только технических решений, но и владельцев, правил, проверок, регламентов и показателей зрелости. Это делает контур данных и ИИ частью организационного цифрового сознания.

Эмпирические данные подтверждают актуальность этого контура. McKinsey в глобальном опросе 2025 года фиксирует, что 88 % респондентов сообщили о регулярном использовании ИИ хотя бы в одной функции организации, но большинство организаций остаются на стадии экспериментов или пилотов, а масштабирование ИИ остается сложной задачей [93]. IBM в отчете о стоимости утечки данных 2025 года указывает на разрыв между быстрым внедрением ИИ и управлением безопасностью: 63 % организаций не имели политик управления ИИ для предотвращения теневого ИИ, а 97 % организаций, сообщивших об ИИ-инцидентах безопасности, не имели надлежащего контроля доступа к ИИ [79]. Эти данные прямо подтверждают тезис главы: цифровая зрелость невозможна без управления данными, ИИ и человеческой ответственностью.

Для организации практическая реализация контура может начинаться с инвентаризации данных и ИИ-сценариев. Необходимо выявить, какие данные используются в управлении, где они хранятся, кто отвечает за качество, какие внешние сервисы применяются, какие решения поддерживаются ИИ, какие

сценарии затрагивают права, безопасность, финансы, персонал, клиентов или репутацию. После этого сценарии следует классифицировать по уровню риска и закрепить для них разные режимы проверки.

Таким образом, контур данных, аналитики и ИИ является центральным для цифровой зрелости, но становится зрелым только при наличии управления данными, качества данных, реестра ИИ-сценариев, риск-классификации, человеческой проверки, прозрачности и мониторинга последствий. Без этого цифровая организация накапливает не зрелость, а неконтролируемую алгоритмическую зависимость.

4.4. КОНТУР ЦИФРОВОЙ АРХИТЕКТУРЫ И СЕРВИСОВ

Архитектурно-сервисный контур является инфраструктурно-процессной основой цифровой зрелости. Он отвечает на вопрос, как цифровая среда организации устроена и насколько она поддерживает стратегию, процессы, данные, безопасность и удобство работы. Организация с низким уровнем архитектурного цифрового сознания может иметь много сервисов, но они плохо интегрированы, дублируют функции, создают ручные операции, повышают нагрузку и не дают единой картины данных. Такая ситуация часто воспринимается как цифровизация, хотя фактически она усиливает фрагментацию.

Корпоративная архитектура позволяет рассматривать организацию не как набор систем, а как согласованную совокупность бизнес-процессов, данных, приложений, технологий и управленческих решений. Подход TOGAF (методология корпоративной архитектуры The Open Group) предлагает описывать архитектуру через взаимосвязь бизнес-, информационной, прикладной и технологической архитектур [131]. Для методологии цифрового сознания это важно: цифровые сервисы должны проектироваться не сами по себе, а как часть целевой архитектуры организации.

Сервисная логика означает, что цифровые решения должны быть понятными, полезными и доступными для пользователей. Пользователями выступают не только клиенты или граждане, но и сотрудники, руководители, проектные команды, партнеры. Если внутренний сервис неудобен, требует двойного ввода данных, не связан с процессом или создает избыточные уведомления, организация получает цифровую перегрузку. Поэтому зрелая цифровая архитектура должна учитывать пользовательский опыт, цифровую нагрузку и реальные сценарии работы.

Архитектурный контур также связан с управлением техническим долгом. Технический долг возникает, когда организация быстро внедряет решения без достаточной интеграции, документации, безопасности, поддержки и обновления. В краткосрочном периоде это может ускорить запуск проекта, но в

долгосрочном снижает управляемость, усложняет изменения, повышает стоимость сопровождения и создает уязвимости. Цифровое сознание организации проявляется в способности видеть эти отложенные последствия.

На рисунке 4.4 показан архитектурно-сервисный контур цифрового сознания. Он раскрывает, как стратегия и процессы должны быть связаны с целевой архитектурой, платформами, данными, интеграциями, безопасностью и опытом пользователя.

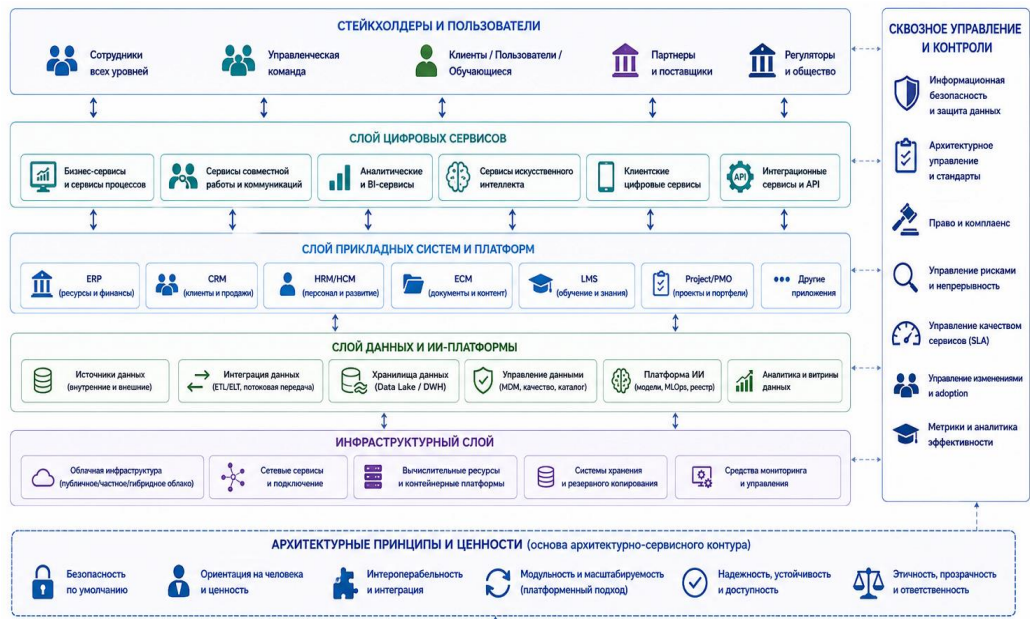


Рисунок 4.4 – Архитектурно-сервисный контур цифрового сознания организации

Источник: составлено авторами на основе [82; 83; 131].

Представленная схема показывает, что цифровая архитектура должна связывать стратегию, процессы, платформы, данные, интеграции, безопасность и пользовательский опыт. Зрелость достигается не количеством сервисов, а их согласованностью и управляемостью.

Основные элементы архитектурно-сервисного контура, риски и управленческие механизмы представлены в таблице 4.4. Таблица может использоваться при инвентаризации цифровой среды организации.

Таблица 4.4 – Цифровая архитектура и сервисы: элементы зрелости, риски и управленческие механизмы

Элемент	Содержание зрелости	Управленческий механизм	Риск дефицита
Целевая	Согласованное описание	Архитектурный	Фрагментация

Элемент	Содержание зрелости	Управленческий механизм	Риск дефицита
архитектура	процессов, данных, систем и сервисов	комитет, карта целевой архитектуры	сервисов и дублирование функций
Интеграция систем	Связь платформ, обмен данными, совместимость интерфейсов	Интеграционная шина, правила обмена, API-паспорта	Ручной перенос данных и ошибки согласования
Сервисная логика	Проектирование цифровых решений как удобных сервисов для пользователей	Карта пользовательских сценариев, сервисный каталог	Сервисы существуют, но не поддерживают реальную деятельность
Управление жизненным циклом	Планирование разработки, эксплуатации, обновления и вывода систем	Паспорт цифрового продукта, регламент сопровождения	Рост технического долга и устаревание решений
Безопасность по замыслу	Встраивание требований защиты данных и устойчивости на этапе проектирования	Экспертиза безопасности до запуска сервиса	Дорогие исправления после инцидентов
Опыт пользователя	Оценка доступности, понятности и цифровой нагрузки	Исследование пользовательского опыта, обратная связь	Соппротивление, обходные практики, снижение доверия

Источник: составлено авторами.

Данные таблицы показывают, что архитектурная зрелость предполагает целевую архитектуру, интеграцию, сервисную логику, управление жизненным циклом, безопасность по замыслу и учет пользовательского опыта.

В практической плоскости архитектурно-сервисный контур должен начинаться с карты цифровых сервисов и процессов. Организация описывает, какие сервисы используются, какие задачи они поддерживают, какие данные формируют, с какими системами интегрированы, кто владеет сервисом, как обеспечиваются доступность, безопасность и поддержка. Такая карта позволяет увидеть не только наличие сервисов, но и их вклад в цифровую зрелость.

Важным принципом является безопасность по замыслу. Это означает, что требования защиты данных, контроля доступа, журналирования, резервирования и устойчивости должны учитываться до запуска цифрового решения, а не после инцидента. Связь архитектуры и безопасности особенно важна в условиях применения ИИ, поскольку ИИ-сервисы работают с запросами, данными, результатами, внешними моделями и новыми типами уязвимостей [83; 101; 102].

Таким образом, архитектурно-сервисный контур переводит цифровое сознание в устройство цифровой среды. Зрелая организация создает не набор разрозненных инструментов, а согласованную архитектуру, поддерживающую стратегию, процессы, данные, безопасность, пользовательский опыт и развитие.

4.5. КОНТУР ОРГАНИЗАЦИОННОЙ КУЛЬТУРЫ, ДОВЕРИЯ И БЕЗОПАСНОСТИ

Культурно-безопасностный контур является гуманитарно-управленческим ядром цифровой зрелости. Если стратегический контур задает направление, данные и ИИ дают доказательную основу, а архитектура обеспечивает инфраструктуру, то культура, доверие и безопасность определяют, будет ли цифровая среда принята организацией и внешними участниками. Без доверия цифровая зрелость становится формальной: сотрудники соблюдают правила только из-за контроля, пользователи сомневаются в цифровых решениях, а руководство получает искаженную картину практик.

Организационная культура, по Э. Шейну, включает базовые предположения, ценности и нормы, которые определяют поведение людей в организации [121]. В цифровой среде культура проявляется в том, как сотрудники относятся к данным, ошибкам, цифровому следу, ИИ, безопасности, прозрачности и обмену знаниями. Если культура поддерживает скрытие ошибок, формальное выполнение требований и индивидуальные обходные практики, никакая цифровая архитектура не обеспечит зрелость. Если культура поддерживает доверие, ответственное сообщение о рисках и совместное обучение, цифровые решения получают устойчивую основу.

Доверие имеет несколько уровней. Внутреннее доверие означает, что сотрудники понимают цели цифровых изменений и не воспринимают аналитику как скрытый надзор. Внешнее доверие означает, что клиенты, пользователи, партнеры и общество признают цифровые решения организации понятными, безопасными и справедливыми. Технологическое доверие означает, что цифровые системы работают надежно, а решения, основанные на данных и ИИ, можно объяснить и при необходимости пересмотреть. Все эти уровни связаны между собой.

Информационная безопасность является необходимым условием доверия. ISO/IEC 27001 (международный стандарт системы менеджмента информационной безопасности) рассматривает безопасность как систему управления рисками, включающую людей, политики и технологии [81]. NIST CSF 2.0 (рамка кибербезопасности Национального института стандартов и технологий США) связывает кибербезопасность с управлением рисками на уровне организации [102]. Следовательно, безопасность не должна быть

изолированной функцией ИТ-подразделения; она является частью цифрового поведения каждого сотрудника и управленческого решения.

На рисунке 4.5 показана взаимосвязь культуры, доверия и безопасности. Схема подчеркивает, что зрелая цифровая организация не может выбрать только один из этих элементов: культура без безопасности уязвима, безопасность без доверия превращается в систему запретов, доверие без прозрачных правил становится нестабильным.



Рисунок 4.5 – Культура, доверие и безопасность как контур цифровой зрелости
Источник: составлено авторами на основе [61; 70; 81; 102; 121; 137].

Представленная схема показывает три взаимосвязанных основания культурно-безопасностного контура: цифровую культуру, цифровое доверие и информационную безопасность. Их согласованность формирует устойчивость цифровой зрелости.

Культурно-безопасностный контур систематизирован в таблице 4.5. Она показывает, какие элементы должны быть закреплены не только в документах, но и в повседневных нормах цифрового поведения.

Таблица 4.5 – Культурно-безопасностный контур цифровой зрелости организации

Элемент	Содержание	Механизм закрепления	Риск дефицита
Цифровые	Разделяемые правила	Кодекс цифрового	Формальные

Элемент	Содержание	Механизм закрепления	Риск дефицита
нормы	работы с данными, сервисами, ИИ и цифровым следом	поведения; внутренние коммуникации	регламенты без повседневного следования
Доверие сотрудников	Понимание целей цифровых изменений и отсутствие ощущения скрытого надзора	Прозрачные правила мониторинга и обратной связи	Сопротивление, цифровая тревожность, скрытые обходные практики
Доверие внешних участников	Понятность цифровых сервисов, правил данных и ответственности организации	Публичные правила, согласия, каналы обращения	Репутационные потери и снижение лояльности
Информационная безопасность	Культура кибергигиены, доступа, защиты данных и реагирования на инциденты	Система менеджмента информационной безопасности, обучение	Утечки, простои, финансовые и правовые последствия
Этика и инклюзивность	Учет справедливости, доступности и недискриминации при цифровых решениях	Этическая экспертиза высокорисковых сценариев	Алгоритмическая несправедливость и недоверие
Культура сообщения о рисках	Готовность сотрудников сообщать о проблемах без страха наказания	Канал сообщений, разбор инцидентов без поиска виноватого	Скрытые риски обнаруживаются слишком поздно

Источник: составлено авторами.

Данные таблицы показывают, что доверие и безопасность требуют не только технических мер, но и норм цифрового поведения, прозрачных правил мониторинга, этической экспертизы и культуры сообщения о рисках.

Особое внимание необходимо уделить границе между аналитикой развития и цифровым надзором. Организация может использовать цифровой след для улучшения процессов, снижения нагрузки, выявления проблем и поддержки обучения. Однако тот же цифровой след может стать инструментом микроконтроля, санкций и недоверия. Цифровое сознание требует прозрачного ответа на вопросы: какие данные собираются, зачем они используются, кто имеет доступ, как долго они хранятся, какие выводы допустимы и какие решения нельзя принимать только на основе цифрового следа.

Этическая составляющая культурно-безопасностного контура усиливается в условиях ИИ. Рекомендация ЮНЕСКО по этике ИИ подчеркивает права человека, человеческое достоинство, прозрачность, подотчетность и

недискриминацию [137]. Принципы ОЭСР по ИИ также акцентируют надежность, безопасность, прозрачность и ответственность [109]. Для организации это означает необходимость этической экспертизы высокорисковых цифровых сценариев, особенно если они затрагивают права людей, оценку деятельности, доступ к услугам, безопасность или репутацию.

Таким образом, культура, доверие и безопасность являются не мягким дополнением к цифровой зрелости, а ее устойчивым основанием. Без них цифровая зрелость остается формальной и хрупкой: технологии внедрены, но сотрудники и внешние участники не доверяют их целям, правилам и последствиям.

4.6. КОНТУР РАЗВИТИЯ ПЕРСОНАЛА И КОМАНД

Контур развития персонала и команд переводит цифровое сознание из концепции в устойчивую организационную практику. Цифровая зрелость невозможна, если организация развивает только инфраструктуру, но не развивает людей, которые должны работать с данными, цифровыми сервисами, ИИ, рисками и последствиями решений. Технологии меняются быстрее, чем должностные инструкции; поэтому организация должна иметь постоянный механизм обновления компетенций сотрудников, руководителей и проектных команд.

В европейской рамке DigComp 3.0 (рамка цифровой компетентности граждан) цифровая компетентность определяется как уверенное, критическое и ответственное использование цифровых технологий, включающее знания, умения и установки [59]. Важно, что ИИ-компетентность в DigComp 3.0 встроена во все области, а не выделена как отдельный технический модуль. Это соответствует логике настоящего пособия: грамотность в области ИИ должна развиваться не как навык работы с одним сервисом, а как способность понимать возможности, ограничения, права, ответственность и риски ИИ в профессиональной деятельности.

Отчет World Economic Forum о будущем рабочих мест 2025 года показывает, что технологические изменения, ИИ, большие данные и кибербезопасность становятся ключевыми факторами трансформации навыков к 2030 году [151]. Для организации это означает, что обучение должно перестать быть разовой реакцией на внедрение новой системы. Оно должно стать частью стратегии цифровой зрелости: регулярная диагностика, модульные программы, ролевые траектории, цифровые наставники, профессиональные сообщества, связь обучения с реальными проектами и оценка эффекта [72].

Особую роль в этом контуре играет управленческая команда. Руководители не могут ограничиваться общими заявлениями о важности цифровизации. Они должны понимать жизненный цикл данных, логику ИИ, риски информационной

безопасности, цифровую нагрузку сотрудников, требования прозрачности и способы оценки эффекта. Если руководители не обладают цифровым сознанием, обучение сотрудников остается несвязанным с реальными управленческими решениями.

На рисунке 4.6 контур развития персонала и команд представлен как цикл: диагностика компетенций, обучение сотрудников, обучение руководителей, цифровые наставники, командное обучение, профессиональные сообщества, связь с проектами и оценка эффекта. Такой цикл позволяет организации переходить от отдельных курсов к устойчивой системе развития.



Рисунок 4.6 – Контур развития персонала и команд в системе цифрового сознания организации

Источник: составлено авторами на основе [59; 123; 146; 151].

Представленная схема показывает, что развитие персонала и команд должно быть циклическим: диагностика, обучение, наставничество, командная практика, проектное применение и оценка эффекта. Только такой цикл превращает цифровое сознание в устойчивое поведение.

Инструменты формирования цифрового сознания персонала и команд представлены в таблице 4.6. Таблица показывает, что разные группы участников требуют разных форматов развития и разных ожидаемых результатов.

Таблица 4.6 – Развитие персонала и команд: инструменты формирования цифрового сознания

Инструмент	Целевая группа	Развиваемый компонент	Формат	Управленческий результат
Диагностика компетенций	Все сотрудники и руководители	Цифровая компетентность, грамотность в области данных и ИИ	Самооценка, кейсы, практические задания	Профиль дефицитов и программа развития
Модульное обучение	Сотрудники функциональных подразделений	Цифровая дееспособность, кибергигиена, работа с данными	Короткие модули и практикумы	Рост качества повседневного цифрового поведения
Обучение руководителей	Управленческая команда	Стратегия, управление данными и ИИ, риск-ориентированность	Семинары, управленческие кейсы, разбор решений	Доказательное и ответственное управление
Цифровые наставники	Команды и подразделения	Командная поддержка, обмен практиками, снижение сопротивления	Наставничество, консультации, внутренние сообщества	Ускорение адаптации и снижение цифрового стресса
Профессиональные сообщества	Эксперты и проектные команды	Обмен знаниями, рефлексия, лучшие практики	Регулярные встречи, база знаний, демонстрации кейсов	Организационное обучение и распространение опыта
Связь обучения с проектами	Все участники цифровых инициатив	Применение компетенций в реальных процессах	Проектное обучение, пилоты, постпроектный анализ	Переход от курсов к изменению практики

Источник: составлено авторами.

Данные таблицы показывают, что развитие цифрового сознания должно включать диагностику, обучение, наставничество, сообщества и связь с реальными проектами. Отдельные курсы без управленческого применения не формируют цифровую зрелость.

Для практического внедрения важно различать обучение инструментам и развитие цифрового сознания. Обучение инструментам отвечает на вопрос, как пользоваться сервисом. Развитие цифрового сознания отвечает на вопрос, как

выбрать инструмент, какие данные допустимо использовать, как проверить результат ИИ, как не нарушить безопасность, как оценить последствия и как улучшить практику. Поэтому программы подготовки должны включать кейсы, этические дилеммы, анализ инцидентов, работу с чек-листами, практику проверки ИИ-результатов и обсуждение реальных процессов организации.

Командный аспект развития не менее важен. Если сотрудник прошел обучение, но команда продолжает работать по старым нормам, компетенция не закрепляется. Поэтому цифровое обучение должно включать командные практики: совместное описание сценариев, правила каналов коммуникации, общие шаблоны документов, библиотеку проверенных ИИ-запросов, разбор ошибок и обмен лучшими практиками. Так индивидуальные компетенции становятся коллективным ресурсом.

Таким образом, контур развития персонала и команд является механизмом воспроизводства цифрового сознания. Он обеспечивает переход от знаний отдельных сотрудников к коллективным практикам и управленческой зрелости. Без него цифровая зрелость быстро устаревает, потому что технологии, риски и требования к компетенциям постоянно меняются.

4.7. ОРГАНИЗАЦИОННАЯ РЕФЛЕКСИВНОСТЬ КАК МЕХАНИЗМ ЦИФРОВОГО РАЗВИТИЯ

Организационная рефлексивность является завершающим и одновременно сквозным контуром цифрового сознания. Она означает способность организации регулярно оценивать последствия цифровых решений, анализировать ошибки, корректировать стратегию, обновлять процессы, пересматривать регламенты, развивать компетенции и удерживать баланс между технологической эффективностью и человеческой ответственностью. Без рефлексивности цифровая трансформация превращается в последовательность внедрений без накопления понимания.

Классическая теория организационного обучения показывает, что организации учатся не только через накопление информации, но и через пересмотр собственных предпосылок действия. Argyris и Schön описывают различие между одноцикловым и двухцикловым обучением: в первом случае исправляются действия, во втором пересматриваются нормы и основания решений [43]. Для цифрового сознания это принципиально. Организация должна не только исправлять сбои цифровых сервисов, но и задавать вопрос, почему эти сбои возникли, какие предпосылки были неверны, какие правила устарели, какие цифровые эффекты оказались незамеченными.

Организационная рефлексивность включает несколько практик: регулярную оценку цифровых инициатив, анализ последствий внедрения сервисов, обратную связь от сотрудников и пользователей, мониторинг цифровой

нагрузки, аудит данных и ИИ-сценариев, пересмотр регламентов, анализ инцидентов, корректировку цифровой стратегии, обновление программ обучения и развитие организационной памяти. Все эти практики должны быть связаны в цикл, а не существовать как разовые мероприятия.

Цифровая рефлексия особенно важна в условиях ИИ. Генеративные и агентные системы могут давать неожиданные эффекты: изменение качества текстов, рост зависимости от шаблонов, снижение самостоятельной проверки, новые риски утечки данных, конфликт авторства, неясность ответственности за рекомендации. Поэтому организация должна анализировать не только производительность ИИ, но и его влияние на мышление, культуру, компетенции, доверие и распределение ответственности.

На рисунке 4.7 представлен цикл организационной цифровой рефлексии. Он начинается с цифрового действия или проекта, затем включает данные и цифровой след, мониторинг результатов, анализ эффектов и рисков, обсуждение с участниками, управленческий вывод, корректировку стратегии, процессов, регламентов и обучения, после чего цикл повторяется.



Рисунок 4.7 – Цикл организационной цифровой рефлексии

Источник: составлено авторами на основе [43; 104; 123; 147].

Представленная схема показывает, что цифровая рефлексия должна быть циклом постоянного улучшения: действие, данные, мониторинг, анализ, обсуждение, вывод, корректировка и повторная оценка. Именно этот цикл делает цифровую зрелость адаптивной.

Механизмы организационной рефлексивности, вопросы и индикаторы представлены в таблице 4.7. Таблица может использоваться как практическая основа для постпроектного анализа цифровых инициатив.

Таблица 4.7 – Организационная рефлексивность: механизмы, вопросы и индикаторы

Механизм	Рефлексивный вопрос	Практическое содержание	Индикатор
Постпроектный анализ	Что изменилось после цифровой инициативы?	Обсуждение целей, результатов, побочных эффектов и ошибок	Доля проектов с проведенным анализом
Мониторинг цифровой нагрузки	Не создает ли цифровая среда перегрузку?	Опросы, анализ каналов коммуникации, обратная связь команд	Снижение лишних платформ, уведомлений и дублирующих отчетов
Аудит данных и ИИ	Какие данные и ИИ-сценарии требуют пересмотра?	Проверка качества данных, рисков, правового режима и человеческого контроля	Доля критичных сценариев, прошедших аудит
Анализ инцидентов	Какие ошибки повторяются и почему?	Разбор киберинцидентов, ошибок ИИ, сбоев сервисов, конфликтов доверия	Сокращение повторяющихся причин инцидентов
Корректировка регламентов	Какие правила устарели или не работают?	Пересмотр локальных актов, инструкций, чек-листов и матриц рисков	Регулярность обновления документов
Обновление обучения	Какие новые компетенции нужны?	Актуализация программ обучения на основе цифровых изменений	Доля программ, обновленных по итогам анализа

Источник: составлено авторами.

Данные таблицы показывают, что рефлексивность может быть операционализирована через конкретные механизмы: постпроектный анализ, мониторинг нагрузки, аудит данных и ИИ, анализ инцидентов, корректировку регламентов и обновление обучения.

Рефлексивный контур позволяет организации отличить устойчивую цифровую зрелость от разового достижения показателей. Если организация не возвращается к уже внедренным цифровым решениям, она не видит накопления технического долга, не замечает изменения цифровой нагрузки, не фиксирует новые способы обхода правил и не обновляет обучение. Поэтому зрелость должна пониматься как динамическое состояние, которое постоянно подтверждается практикой анализа и корректировки.

На основе предыдущих параграфов можно собрать интегральную модель организационного цифрового сознания как основы цифровой зрелости. Она включает шесть контуров: стратегический; данные, аналитика и ИИ; архитектура и сервисы; культура, доверие и безопасность; персонал и команды; организационная рефлексивность. Содержательная связь контуров показана на рисунке 4.8, а их управленческое содержание систематизировано в таблице 4.8.

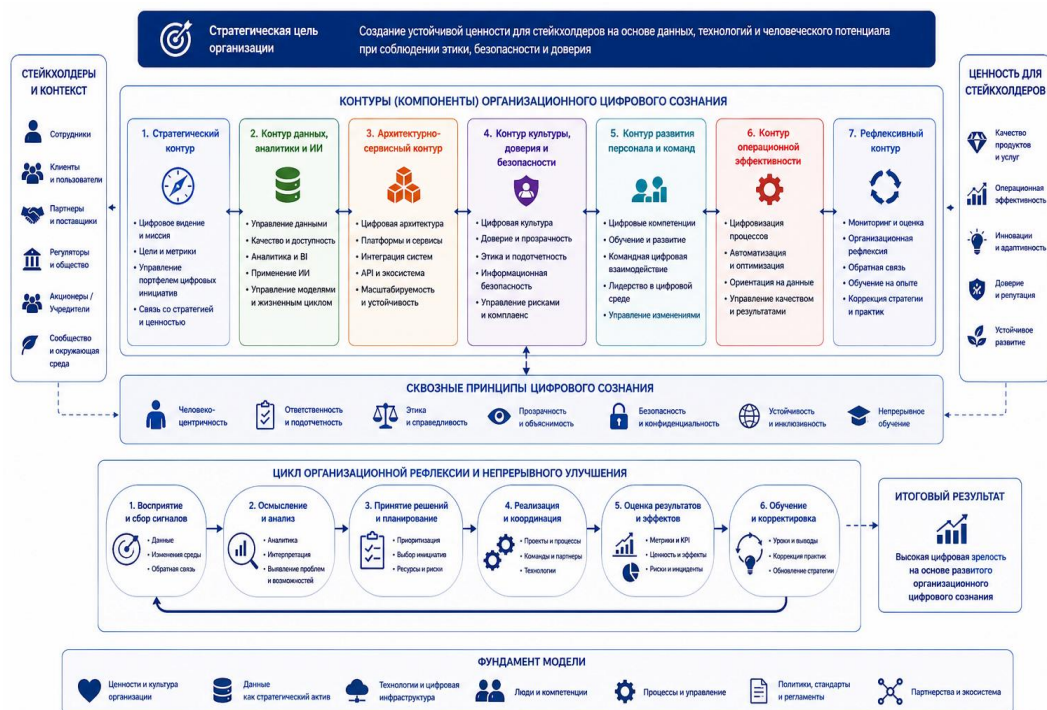


Рисунок 4.8 – Модель организационного цифрового сознания как основы цифровой зрелости

Источник: составлено авторами на основе [83; 89; 101; 102; 123; 130].

Рисунок 4.8 обобщает, что цифровая зрелость формируется не линейно, а через согласованность шести контуров цифрового сознания. Дефицит любого контура снижает устойчивость всей модели.

Таблица 4.8 обобщает шесть контуров организационного цифрового сознания как основание цифровой зрелости. Она выполняет функцию итоговой методической карты главы.

Таблица 4.8 – Контуров организационного цифрового сознания как основа цифровой зрелости

Контур	Назначение	Управленческие механизмы	Риски дефицита	Связь с цифровой зрелостью
Стратегический контур	Связывает цифровые решения с миссией, целями и ценностью	Цифровая стратегия, портфель инициатив, показатели результата	Формальная цифровизация без эффекта	Задаёт направление всем остальным контурам
Данные, аналитика и ИИ	Превращает данные и ИИ в управляемую доказательную основу решений	Каталог данных, реестр ИИ-сценариев, проверка качества, риск-классификация	Ошибочные решения, теневой ИИ, потеря доверия	Питаёт стратегию, управление, архитектуру и рефлексию
Архитектура и сервисы	Обеспечивает согласованную цифровую среду	Целевая архитектура, сервисный каталог, интеграции, управление жизненным циклом	Фрагментарность, технический долг, цифровая перегрузка	Создаёт инфраструктурные условия зрелости
Культура, доверие и безопасность	Формирует нормы ответственности о поведении и устойчивость цифровой среды	Кодекс, политики безопасности, этическая экспертиза, каналы сообщений	Недоверие, утечки, репутационные потери	Закрепляет зрелость в повседневной культуре
Персонал и команды	Развивает компетенции и командные практики цифрового действия	Диагностика, обучение, наставники, сообщества, проектная практика	Разрыв между технологиями и готовностью людей	Переводит модель в поведение сотрудников и руководителей
Рефлексивность	Обеспечивает регулярную оценку последствий и	Постпроектный анализ, аудит, обратная связь, обновление	Повторение ошибок, негибкость трансформации	Делает зрелость адаптивной и самообновляющейся

Контур	Назначение	Управленческие механизмы	Риски дефицита	Связь с цифровой зрелостью
	корректировка развития	регламентов		

Источник: составлено авторами.

Данные таблицы показывают, что цифровая зрелость возникает не из одного домена, а из согласованности стратегии, данных и ИИ, архитектуры, культуры и безопасности, персонала и рефлексивности. Она может использоваться как каркас для последующей диагностики.

Для обоснования актуальности связи цифрового сознания и цифровой зрелости в таблице 4.9 приведены эмпирические аргументы. Они показывают, что организации сталкиваются одновременно с массовым распространением ИИ, дефицитом управления, рисками безопасности и необходимостью развития компетенций.

Таблица 4.9 – Эмпирические аргументы связи цифрового сознания и цифровой зрелости

Показатель	Значение / факт	Год	Источник	Значение для главы
Распространение ИИ в организациях	88 % респондентов McKinsey сообщили о регулярном использовании ИИ хотя бы в одной функции организации	2025	McKinsey & Company [93]	Показывает, что ИИ стал массовой управленческой реальностью, но требует зрелого контура управления
Переход от пилотов к масштабу	Большинство организаций остаются на стадии экспериментов или пилотов; около трети сообщили о масштабировании ИИ	2025	McKinsey & Company [93]	Подтверждает необходимость стратегического и рефлексивного контура
Дефицит управления ИИ	63 % организаций, по данным IBM, не имели политик управления ИИ для предотвращения теневого использования ИИ	2025	IBM [79]	Обосновывает контур данных, ИИ и безопасности
Риски ИИ-инцидентов	97 % организаций с ИИ-инцидентами безопасности не имели надлежащего контроля доступа к ИИ	2025	IBM [79]	Показывает связь зрелости ИИ с информационной безопасностью

Показатель	Значение / факт	Год	Источник	Значение для главы
Рост требований к компетенциям	Отчет WEF описывает технологические изменения, ИИ, большие данные и кибербезопасность как ключевые факторы трансформации навыков к 2030 году	2025	World Economic Forum [151]	Обосновывает контур развития персонала и команд
Развитие ответственного ИИ	AI Index фиксирует рост внедрения ИИ и одновременную неравномерность практик ответственного ИИ	2026	Stanford HAI [127]	Подчеркивает необходимость зрелой рефлексии и управления рисками

Источник: составлено авторами.

Данные таблицы показывают, что цифровая зрелость требует не только внедрения ИИ и цифровых сервисов, но и управления рисками, данными, компетенциями, безопасностью и ответственным масштабированием цифровых решений.

Таким образом, организационная рефлексивность является механизмом самообновления цифровой зрелости. Она позволяет организации видеть последствия цифровых решений, пересматривать правила, обновлять компетенции, корректировать стратегию и предотвращать повторение ошибок. Без рефлексии цифровая зрелость быстро превращается в статичную отчетность.

ИТОГИ ГЛАВЫ

Цифровая зрелость характеризует достигнутое состояние организации, а цифровое сознание определяет смысловой и управленческий механизм его формирования. Устойчивость зрелости обеспечивается согласованностью стратегии, данных и ИИ, архитектуры, культуры и безопасности, развития персонала и организационной рефлексии.

Управленческий переход к главе 5: шесть контуров переводятся в диагностическую модель, необходимую для выбора приоритетов и принятия управленческих решений.

Интерактивное сопровождение. В цифровом руководстве размещены матрица самооценки контуров зрелости, карты цифровых сервисов и данных, реестр ИИ-сценариев и шаблон архитектурного аудита.

ГЛАВА 5. ДИАГНОСТИКА ЦИФРОВОГО СОЗНАНИЯ ДЛЯ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

*«Когда вы можете измерить то, о чём говорите, и выразить
это в числах, вы кое-что об этом знаете».*

Уильям Томсон, лорд Кельвин

Управленческий вопрос главы. Какие данные позволяют руководству отличить реальное развитие цифрового сознания от формального освоения инструментов и принять обоснованное решение?

Управленческий результат главы. Диагностическая рамка, включающая модели ИЦСС, ИЦСК и ИОЦС, уровни зрелости, триангуляцию методов и этические ограничения. Индексы требуют эмпирической валидации до стандартизованного применения.

5.1. ПРИНЦИПЫ ДИАГНОСТИКИ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

Диагностика цифрового сознания организации начинается с методологического выбора: что именно считать объектом оценки. Если объектом объявить только уровень владения цифровыми сервисами, то диагностика сведется к проверке пользовательских навыков. Если же объектом считать способность организации как коллективного субъекта осознанно управлять цифровыми технологиями, данными и ИИ, то диагностика должна охватывать компетентность, критичность, этику, безопасность, командную координацию, управленческую ответственность, организационную культуру и контуры управления.

Поэтому диагностика цифрового сознания строится как многоуровневая процедура. На уровне сотрудника оцениваются знания, установки, поведенческие практики, критическое отношение к информации, кибергигиена и готовность к обучению. На уровне команды оценивается не сумма индивидуальных баллов, а качество совместной цифровой деятельности: согласованность данных, правил коммуникации, распределение ролей, коллективная ответственность и способность к совместной рефлексии. На уровне организации оцениваются стратегия, архитектура, управление данными и ИИ, цифровая культура, безопасность, доверие и рефлексивность.

Важным методологическим основанием выступает доказательный менеджмент. Его логика предполагает, что управленческие выводы должны опираться не на один показатель, а на сочетание научных данных, локальных организационных данных, профессионального суждения и контекста конкретной организации [44]. Для диагностики цифрового сознания это означает обязательное сочетание самооценки, кейсовых заданий, экспертной оценки,

анализа документов, цифровых артефактов, интервью, аналитики процессов и анализа инцидентов.

На рисунке 5.1 представлена логика диагностики цифрового сознания организации как развивающего управленческого цикла. Рисунок важен для всей главы, поскольку показывает: оценка не завершается расчетом индекса, а должна приводить к планам развития, корректировке регламентов, уточнению цифровой стратегии и повторной оценке.



Рисунок 5.1 – Диагностика цифрового сознания как развивающий управленческий цикл

Источник: составлено авторами на основе [42; 44; 86; 101; 102].

Представленная схема показывает последовательность диагностики: цель, индикаторы, сбор данных, триангуляция, расчет индексов, интерпретация, управленческие решения и повторная оценка. Диагностика рассматривается как цикл развития, а не как разовая проверка.

Принципы диагностики выполняют роль методического фильтра. Они позволяют отличить научно-методическую оценку от произвольного анкетирования, формального аудита или скрытого мониторинга активности сотрудников. Если нарушаются валидность, прозрачность, конфиденциальность или развивающая направленность, результаты становятся не только методически сомнительными, но и опасными для доверия внутри организации.

В таблице 5.1 представлены базовые принципы диагностики цифрового сознания организации. Каждый принцип связан с практическим проявлением, диагностической процедурой и риском нарушения.

Таблица 5.1 – Принципы диагностики цифрового сознания организации

Принцип	Содержание	Практическое проявление	Риск нарушения	Диагностическая процедура
Комплексность	Оценка не одного навыка, а системы взаимосвязанных доменов: компетенции, данные, ИИ, этика, безопасность, коммуникация, культура и управление.	Матрица доменов по трем уровням: сотрудник, команда, организация.	Редукция диагностики к узкому тесту цифровой грамотности.	Проверка полноты диагностической модели.
Многоуровневость	Разделение индивидуального, командного и организационного уровней оценки.	Отдельные индексы ИЦСС, ИЦСК и ИОЦС.	Ложный вывод, что высокий индивидуальный балл равен зрелой организации.	Раздельные шкалы, источники данных и интерпретация.
Валидность	Инструмент должен измерять заявленный конструкт, а не общую удовлетворенность цифровыми сервисами.	Экспертная ревизия вопросов, пилотирование, содержательная валидация.	Измерение комфортности вместо цифрового сознания.	Экспертная оценка соответствия пункта домену.
Надежность	Результаты должны быть устойчивыми и воспроизводимыми при повторном применении.	Проверка внутренней согласованности и межэкспертной согласованности.	Случайные колебания баллов и невозможность мониторинга динамики.	Расчет коэффициентов надежности после пилотирования.
Доказательность	Выводы строятся на нескольких типах данных.	Сопоставление самооценки, кейса, артефактов и экспертной	Произвольные решения по одному источнику.	Правило подтверждения значимого вывода минимум двумя

Принцип	Содержание	Практическое проявление	Риск нарушения	Диагностическая процедура
		оценки.		источниками.
Прозрачность	Участникам заранее известны цели, критерии, методы и порядок использования результатов.	Положение о диагностике, информационная памятка, доступ к критериям.	Недоверие, сопротивление, искажение ответов.	Открытая программа диагностики и порядок обратной связи.
Этичность	Диагностика не должна причинять неоправданный вред участникам и организации.	Этическая экспертиза методов, запрет скрытого контроля.	Стигматизация, давление, превращение диагностики в надзор.	Этический чек-лист диагностического инструмента.
Конфиденциальность	Персональные результаты защищены, доступ к ним ограничен ролями.	Псевдонимизация, агрегирование, ограничение сроков хранения.	Утечки, репутационный и психологический ущерб.	Ролевая модель доступа и журнал обращения к данным.
Развивающая направленность	Результат используется для обучения, поддержки и улучшения практик.	Индивидуальные и командные планы развития.	Манипуляция ответами, страх оценки и формализм.	Отчет обратной связи и траектория развития.
Риск-ориентированность	Более глубокая оценка проводится в зонах высоких цифровых, этических и ИИ-рисков.	Взвешивание доменов по профилю риска организации.	Недооценка критичных областей: данных, ИИ и безопасности.	Карта цифровых и алгоритмических рисков.
Недопустимость цифрового надзора	Диагностика не превращается в скрытое отслеживание поведения.	Запрет скрытых трекеров, непрозрачных рейтингов и автоматических санкций.	Потеря доверия и правовые риски.	Этический фильтр использования цифрового следа.

Источник: составлено авторами на основе [42; 44; 86; 99; 101; 102].

Таблица 5.1 задает нормативный каркас главы. Она показывает, что диагностика должна быть комплексной, валидной, надежной, прозрачной, этической и развивающей.

Таким образом, диагностика цифрового сознания организации должна быть встроена в управленческий цикл развития. Она не может быть разовой проверкой сотрудников или способом ранжирования подразделений. Ее назначение состоит в выявлении дефицитов, проектировании обучения, корректировке регламентов, усилении управления данными и ИИ, снижении цифровых рисков и поддержке организационного обучения.

5.2. ИНДЕКС ЦИФРОВОГО СОЗНАНИЯ СОТРУДНИКА

Индекс цифрового сознания сотрудника (ИЦСС) отражает индивидуальный уровень цифрового сознания. Он показывает, насколько сотрудник способен самостоятельно и ответственно действовать в цифровой среде, критически оценивать данные и результаты ИИ, соблюдать правила безопасности, учитывать правовые и этические ограничения, поддерживать качественную цифровую коммуникацию и корректировать собственные практики.

ИЦСС не является оценкой «цифровой пригодности» человека. Его корректная интерпретация должна быть развивающей: результат показывает не статус сотрудника, а профиль его сильных сторон, дефицитов, рисков и потребностей в обучении. Особенно важно исключить автоматическое использование индивидуального индекса как основания для кадровых санкций. Такой запрет соответствует человекоцентричной и этической логике диагностики.

Расчет индекса предполагает компонентную модель. Каждый компонент оценивается по шкале от 0 до 5, затем результат переводится в интегральную шкалу от 0 до 100. Веса компонентов могут быть равными, экспертно-взвешенными или риск-ориентированными. Если организация работает с чувствительными данными, критической инфраструктурой, высокорисковыми ИИ-сценариями или значимыми правовыми решениями, домены безопасности, этики, данных и ИИ должны иметь повышенный вес.

$$\text{ИЦСС} = (\sum w_i \times C_i / \sum w_i \times C_{\max}) \times 100$$

где C_i – балл по компоненту цифрового сознания сотрудника; w_i – вес компонента; $C_{\max}$ – максимальный балл по компоненту; $\sum$ – сумма по всем компонентам. При равновесной модели веса компонентов одинаковы. При риск-ориентированной модели веса задаются экспертно и подтверждаются организацией.

На рисунке 5.2 показана структура ИЦСС: формула расчета, семь компонентов и шкала интерпретации. Рисунок служит методической схемой для

разработки опросника, кейсовых заданий и индивидуального отчета обратной связи.

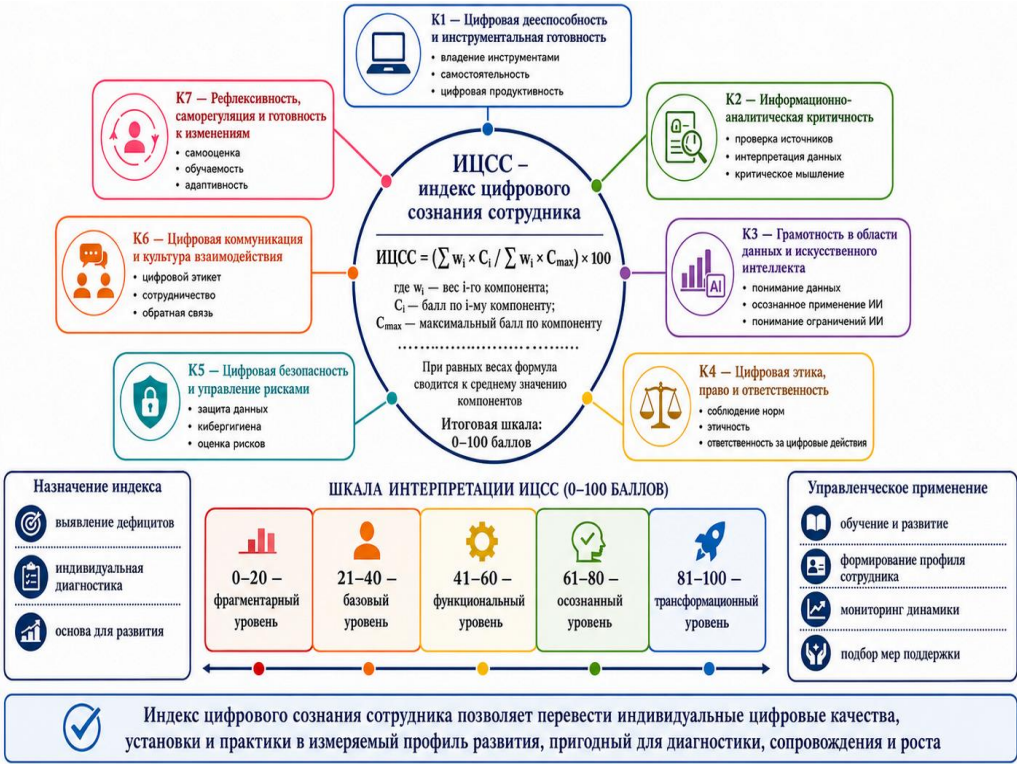


Рисунок 5.2 – Индекс цифрового сознания сотрудника

Источник: составлено авторами на основе [59; 83; 101; 135; 137; 146].

Представленная схема показывает, что индивидуальный индекс включает семь компонентов и интерпретируется по шкале 0–100. Расчет индекса должен сопровождаться пояснением профиля сотрудника и рекомендациями развития.

В таблице 5.2 представлена диагностическая спецификация индивидуального индекса. Она задает связь между компонентом, содержанием, индикаторами, возможными заданиями и способами верификации.

Таблица 5.2 – Структура индекса цифрового сознания сотрудника

Компонент	Содержание	Диагностическ ие индикаторы	Кейсовое задание	Способ верификации
Цифровая дееспособность	Уместное и самостоятельное использование цифровых сервисов в	Выбор инструмента под задачу; соблюдение правил общей цифровой	Выбрать набор инструментов для типового процесса и обосновать выбор.	Практическое задание, аудит цифровых артефактов.

Компонент	Содержание	Диагностические индикаторы	Кейсовое задание	Способ верификации
	рабочем контексте.	среды; устойчивость к изменению интерфейса.		
Информационно-аналитическая критичность	Поиск, проверка и интерпретация информации и данных.	Проверка источников; выявление манипуляций; различение факта, мнения и прогноза.	Разобрать спорный график, найти ошибку вывода и указать недостающие данные.	Кейс на проверку данных, экспертная оценка вывода.
Грамотность в области данных и ИИ	Понимание принципов работы данных и ИИ, ограничений, рисков и областей применения.	Понимание качества данных, предвзятости, галлюцинаций ИИ, необходимости человеческой проверки.	Оценить ответ ИИ и указать, что требует перепроверки.	Ситуационный тест, разбор запроса и результата.
Цифровая этика, право и ответственность	Осознание правовых и этических границ цифрового действия.	Понимание режима данных, согласия, авторства, объяснимости, недискриминации.	Кейс об использовании персональных или конфиденциальных данных.	Экспертный разбор кейса.
Цифровая безопасность и кибергигиена	Соблюдение правил безопасного поведения в цифровой среде.	Многофакторная аутентификация, безопасный обмен файлами, распознавание фишинга, сообщение об инцидентах.	Распознать подозрительное сообщение и выбрать безопасный канал обмена.	Имитационная проверка, короткие практические задания.
Цифровая коммуникация и культура взаимодействия	Корректное и результативное цифровое взаимодействие с коллегами и партнерами.	Выбор канала, ясность сообщений, фиксация договоренностей, уважение цифровых границ.	Отреагировать на конфликтную коммуникационную ситуацию.	Взаимная оценка, анализ коммуникационных артефактов.

Компонент	Содержание	Диагностические индикаторы	Кейсовое задание	Способ верификации
Рефлексивность и готовность к изменениям	Осмысление собственных цифровых практик и их корректировка.	Готовность учиться, замечать ошибки, менять паттерны поведения, снижать цифровую перегрузку.	Предложить изменение собственного процесса после цифрового сбоя.	Интервью, обратная связь руководителя, план развития.

Источник: составлено авторами на основе [59; 92; 101; 135; 137; 146].

Данные таблицы показывают, что ИЦСС измеряет не уверенность пользователя, а наблюдаемое цифровое поведение, включая критичность, безопасность, этику, работу с данными и ИИ.

Для практического применения требуется единая рубрика оценивания. В таблице 5.3 представлена шкала 0–5, которая может использоваться при оценке каждого компонента ИЦСС.

Таблица 5.3 – Рубрика компонентной оценки ИЦСС

Балл	Уровень	Поведенческая характеристика	Методическое действие
0	Признак отсутствует	Сотрудник не демонстрирует требуемого поведения или не понимает соответствующую норму.	Нужна первичная подготовка и разъяснение базовых правил.
1	Фрагментарный уровень	Поведение проявляется случайно, зависит от подсказок, инструкций или внешнего контроля.	Необходима поддержка, практические задания и наставничество.
2	Базовый уровень	Основные действия выполняются по инструкции, но перенос в новые ситуации ограничен.	Требуется закрепление навыка на рабочих кейсах.
3	Устойчивый функциональный уровень	Сотрудник уверенно применяет компонент в типовых ситуациях и понимает ограничения.	Возможен переход к более сложным задачам и взаимной поддержке коллег.
4	Осознанный и переносимый уровень	Сотрудник адаптирует практику к новым задачам, объясняет основания действий и риски.	Может быть включен в роль цифрового наставника.
5	Рефлексивный и развивающий	Сотрудник анализирует последствия, улучшает	Может участвовать в разработке правил,

Балл	Уровень	Поведенческая характеристика	Методическое действие
	уровень	практики и помогает другим участникам.	кейсов и программ обучения.

Источник: составлено авторами на основе [42; 58; 99].

Таблица 5.3 обеспечивает единое понимание уровней оценки и делает результаты сопоставимыми между подразделениями и периодами диагностики.

После компонентной оценки результат переводится в шкалу 0–100. Интерпретация ИЦСС представлена в таблице 5.4; она задает развивающий, а не карательный смысл индивидуального результата.

Таблица 5.4 – Шкала интерпретации индекса цифрового сознания сотрудника

Значение ИЦСС	Уровень	Диагностический смысл	Рекомендуемое управленческое действие
0–20	Фрагментарный	Сотрудник действует ситуативно, не видит рисков и нуждается в базовой поддержке.	Первичное обучение, индивидуальный план развития, сопровождение наставника.
21–40	Базовый	Базовые действия выполняются, но критичность, безопасность и работа с ИИ нестабильны.	Модульное обучение, практические кейсы, проверка применения в работе.
41–60	Функциональный	Сотрудник способен выполнять большинство цифровых действий, но не всегда переносит их в новые ситуации.	Развитие критичности, грамотности в области данных и ИИ, повышение самостоятельности.
61–80	Осознанный	Цифровое поведение устойчиво, сотрудник понимает риски и может объяснить действия.	Включение в командные практики, наставничество, участие в улучшении регламентов.
81–100	Развивающий	Сотрудник способен к рефлексии, развитию практик и поддержке других.	Роль цифрового наставника, участие в проектировании обучения и пилотных практик.

Источник: составлено авторами.

Данные таблицы показывают, как числовой результат связывается с управленческой поддержкой: обучением, наставничеством, вовлечением в командные практики и развитием роли цифрового наставника.

Таким образом, ИЦСС целесообразно использовать как профиль развития сотрудника. Сила индекса не в том, что он дает одно число, а в том, что позволяет увидеть структуру цифрового сознания: где сотруднику нужна поддержка, где он готов к самостоятельному действию, а где может выступать носителем практик для команды.

5.3. ИНДЕКС ЦИФРОВОГО СОЗНАНИЯ КОМАНДЫ

Командный индекс цифрового сознания (ИЦСК) предназначен для оценки качества совместной цифровой деятельности. Его нельзя рассчитывать как простое среднее арифметическое индивидуальных индексов сотрудников. Команда может состоять из цифрово сильных участников и при этом иметь низкое цифровое сознание, если в ней отсутствуют общие правила, единые данные, прозрачность решений, взаимная проверка, распределенные роли и коллективная ответственность.

ИЦСК фиксирует согласованность командной практики. Он показывает, как команда распределяет цифровые задачи, работает с документами и данными, фиксирует решения, применяет ИИ, управляет цифровой памятью проекта, соблюдает безопасность и учится на ошибках. Поэтому диагностическим объектом является не «сумма людей», а контур совместного действия.

Базовая формула ИЦСК может быть задана в равновесной или взвешенной форме. В равновесной версии все домены командного цифрового сознания имеют одинаковое значение. В риск-ориентированной версии повышенный вес получают домены проверки данных и ИИ, цифровой безопасности, распределения ролей и коллективной ответственности.

$$\text{ИЦСК} = (\sum D_j / D_{\max}) \times 100$$

где D_j – балл по домену командного цифрового сознания; $D_{\max}$ – максимально возможная сумма баллов по всем доменам. При необходимости формула может быть расширена: $\text{ИЦСК} = (\sum w_j \times D_j / \sum w_j \times D_{\max}) \times 100$, где w_j – вес домена.

На рисунке 5.3 представлена структура командного индекса. Схема подчеркивает, что командное цифровое сознание проявляется в координации, прозрачности, цифровой дисциплине, управлении знаниями, проверке данных и ИИ, цифровой памяти и обучении команды.



Рисунок 5.3 – Командный индекс цифрового сознания
 Источник: составлено авторами на основе [44; 85; 123; 147].

Представленная схема показывает двенадцать доменов командной оценки и сквозные факторы командного уровня: доверие, правила, ответственность, проверку данных, цифровую память и обучение на опыте.

В таблице 5.5 раскрыты диагностические домены ИЦСК. Для каждого домена указаны содержание, индикаторы, источники данных и возможные управленческие решения.

Таблица 5.5 – Домены индекса цифрового сознания команды

Домен	Содержание	Индикаторы	Источники данных	Управленческое решение
Цифровая координация задач	Как команда распределяет и отслеживает цифровую работу.	Единый маршрут задач, статусность, отсутствие серых зон.	Опрос, доски задач, протоколы.	Настроить единые правила управления задачами.
Совместная работа с документами и	Качество совместного редактирования	Общие пространства, версии,	Аудит цифровых артефактов.	Ввести стандарт общего рабочего пространства.

Домен	Содержание	Индикаторы	Источники данных	Управленческое решение
артефактами	я, версионности и хранения материалов.	прослеживаемость изменений.		
Прозрачность процессов	Видимость хода работы и оснований решений.	Документированные решения, доступность логики, журнал решений.	Интервью, документы, цифровые следы процессов.	Закрепить порядок фиксации решений.
Цифровая дисциплина	Соблюдение принятых цифровых правил.	Единые каналы, сроки, правила именования и версий.	Наблюдение, аудит артефактов.	Провести командную ретроспективу и уточнить нормы.
Командная коммуникация	Качество цифрового взаимодействия.	Ясность, уважение, выбор канала, фиксация договоренностей.	Опрос, взаимная оценка, анализ сообщений.	Ввести коммуникационный протокол.
Управление знаниями	Сохранение и передача командного знания.	База знаний, инструкции, шаблоны, материалы адаптации.	База знаний, интервью.	Провести спринт управления знаниями.
Распределение цифровых ролей	Ясность ответственности за данные, ИИ, документы и безопасность.	Назначенные ответственные и резервные роли.	Матрица ролей, интервью.	Уточнить зоны ответственности.
Коллективная ответственность	Готовность отвечать за общий цифровой результат.	Нет перекладывания на ИИ, ИТ-службу или отдельного эксперта.	Интервью, ретроспективы.	Ввести разбор ошибок без поиска виновного.
Командная проверка данных и ИИ	Наличие взаимной проверки и человеческого контроля.	Двухэтапная проверка, контроль источников, проверка ИИ-результатов.	Артефакты, рецензии, протоколы.	Утвердить протокол проверки данных и ИИ.
Безопасность командной работы	Командная кибергигиена и безопасный	Правила доступа, безопасная передача файлов,	Журналы инцидентов, опрос.	Усилить правила доступа и обмена.

Домен	Содержание	Индикаторы	Источники данных	Управленческое решение
	обмен.	реагирование на инциденты.		
Цифровая память проекта	Сохранение истории проекта и логики решений.	Протоколы, журнал решений, архивы, карта изменений.	Документы и системы.	Ввести шаблон цифровой памяти проекта.
Обучение и корректировка практик	Способность команды учиться на цифровом опыте.	Регулярные обзоры, фиксация уроков, изменение правил после ошибок.	Ретроспективы, интервью.	Проводить регулярные сессии командного обучения.

Источник: составлено авторами на основе [44; 85; 123; 147].

Данные таблицы показывают, что ИЦСК оценивает устойчивость командной практики: координацию, коммуникацию, проверку данных, распределение ролей, безопасность, цифровую память и обучение.

Интерпретация ИЦСК должна учитывать профиль команды. В таблице 5.6 предложена шкала интерпретации, связывающая числовой результат с типовыми управленческими выводами.

Таблица 5.6 – Шкала интерпретации индекса цифрового сознания команды

Значение ИЦСК	Уровень	Диагностический смысл	Рекомендуемое действие
0–20	Фрагментарная команда	Работа ведется в разрозненных каналах, решения теряются, проверка данных и ИИ отсутствует.	Настройка базовых правил, общего пространства и ответственных ролей.
21–40	Базовая команда	Есть отдельные правила и цифровые инструменты, но их применение нестабильно.	Закрепление цифровой дисциплины, общих шаблонов и протокола решений.
41–60	Функциональная команда	Команда способна работать в общей цифровой среде, но проверка данных и обучение нерегулярны.	Введение взаимной проверки, цифровой памяти и регулярных ретроспектив.
61–80	Согласованная команда	Практики устойчивы, роли понятны, данные и ИИ проверяются, решения фиксируются.	Развитие командного наставничества и обмена лучшими практиками.
81–100	Развивающаяся команда	Команда не только применяет правила, но и улучшает их, обучает других	Распространение практик на другие команды и участие в организационном

Значение ИЦСК	Уровень	Диагностический смысл	Рекомендуемое действие
		и управляет цифровыми рисками.	управлении.

Источник: составлено авторами.

Данные таблицы показывают, что командный индекс интерпретируется как состояние совместной практики, а не как сумма индивидуальных умений.

Таким образом, ИЦСК позволяет выявить скрытые разрывы координации, которые не видны при индивидуальной оценке. Он особенно важен для проектных групп, подразделений, команд внедрения ИИ, аналитических команд и управленческих контуров, где качество результата зависит от совместной проверки данных, ясности ролей и коллективной ответственности.

5.4. ИНДЕКС ОРГАНИЗАЦИОННОГО ЦИФРОВОГО СОЗНАНИЯ

Индекс организационного цифрового сознания (ИОЦС) описывает состояние организации как коллективного субъекта цифровой среды. Его задача – оценить не количество цифровых сервисов, а согласованность стратегии, данных, ИИ, архитектуры, культуры, безопасности, развития персонала, цифрового доверия и организационной рефлексии.

ИОЦС ближе к оценке зрелости управления, чем к проверке отдельных компетенций. Он опирается на логику систем управления, управления информационной безопасностью, управления ИИ, цифровой зрелости и организационного обучения [81–83; 101; 102]. Поэтому организационный индекс должен строиться на анализе документов, процессов, ролей, данных, практик, инцидентов, программ обучения, управленческой аналитики и обратной связи стейкхолдеров.

Расчет ИОЦС допускает несколько моделей взвешивания. Универсальная равновесная модель удобна для первичной диагностики. Стратегически взвешенная модель усиливает вклад стратегии, данных, культуры и развития персонала. Риск-ориентированная модель повышает вес управления данными, управления ИИ, безопасности и этики. Отраслевая модель позволяет адаптировать веса под профиль рисков конкретной организации.

$$\text{ИОЦС} = (\sum w_j \times O_j / \sum w_j \times O_{\max}) \times 100$$

где O_j – доменная оценка организационного цифрового сознания; w_j – вес домена; $O_{\max}$ – максимальный балл по домену. Значение индекса переводится в шкалу 0–100 и интерпретируется с учетом профиля рисков организации.

На рисунке 5.4 представлена структура ИОЦС как системы двенадцати организационных доменов. Рисунок помогает увидеть, что организационная

диагностика должна охватывать не только ИТ-инфраструктуру, но и культуру, доверие, обучение, этику, управление ИИ и рефлекссию.



Рисунок 5.4 – Индекс организационного цифрового сознания

Источник: составлено авторами на основе [81–83; 101; 102; 109].

Рисунок 5.4 раскрывает ИОЦС как многодоменную оценку организации: стратегию, данные, ИИ, архитектуру, персонал, культуру, безопасность, этику, аналитику, внешнее взаимодействие, доверие и рефлекссию.

В таблице 5.7 дана диагностическая карта ИОЦС. Она показывает домены организационного уровня, управленческие индикаторы, источники данных, документы и риски дефицита.

Таблица 5.7 – Домены индекса организационного цифрового сознания

Домен	Содержание	Документы и механизмы	Источники данных	Риск дефицита
Стратегический контур	Наличие цифровой стратегии, связанной с миссией,	Цифровая стратегия, дорожная карта, протоколы управления	Стратегия, интервью, протоколы.	Разрозненные цифровые инициативы.

Домен	Содержание	Документы и механизмы	Источники данных	Риск дефицита
	результатами и ответственность ю.	портфелем.		
Управление данными	Политики, владельцы данных, качество, доступ, жизненный цикл и каталог данных.	Политика данных, реестр данных, каталог, правила качества.	Аудит данных, документы, интервью.	Ошибочные решения и низкое доверие к аналитике.
Управление ИИ	Правила выбора, тестирования, применения, контроля и объяснимости ИИ.	Политика применения ИИ, реестр ИИ-сценариев, карта рисков.	Реестр сценариев, документы, экспертная оценка.	Теневое применение ИИ, предвзятость, галлюцинации.
Цифровая архитектура и сервисы	Интеграция, совместимость, устойчивость и пользовательская пригодность сервисов.	Архитектурные принципы, карта систем, сервисные стандарты.	ИТ-аудит, карты процессов, аналитика сервисов.	Фрагментация, технический долг, перегрузка пользователей.
Развитие персонала и команд	Система обучения, сопровождения изменений и ролевых траекторий.	Политика обучения, программы развития, карта компетенций.	Данные обучения, опросы, планы развития.	Отставание навыков от цифровой стратегии.
Цифровая культура	Нормы использования цифровых инструментов, данных и ИИ.	Кодекс цифрового поведения, коммуникационные нормы.	Опросы, интервью, фокус-группы.	Формализм и имитация цифровизации.
Цифровая безопасность	Встроенность защиты информации в процессы организации.	Политики безопасности, планы реагирования, матрица доступа.	Журналы инцидентов, аудит, документы.	Утечки данных и нарушения режима доступа.
Этика и ответственность	Этические рамки, процедуры оценки риска и справедливости	Политика цифровой этики, процедура этической экспертизы.	Документы, экспертные заключения.	Репутационные, правовые и социальные риски.

Домен	Содержание	Документы и механизмы	Источники данных	Риск дефицита
	цифровых решений.			
Управленческая аналитика	Качество использования данных в управленческих решениях.	Положение об аналитике, протоколы решений, аналитические панели.	Панели, протоколы, интервью.	Декоративная аналитика без управленческого действия.
Внешнее цифровое взаимодействие	Качество цифровых сервисов и каналов для внешних стейкхолдеров.	Регламенты сервиса, стандарты обратной связи.	Отзывы, обращения, данные пользовательского опыта.	Потеря доверия и сервисные провалы.
Цифровое доверие	Доверие сотрудников и внешних участников к цифровому контуру организации.	Политики прозрачности, коммуникации о данных и ИИ.	Опросы, жалобы, интервью.	Сопротивление и обход систем.
Организационная рефлексивность	Способность пересматривать цифровые практики на основе опыта.	Порядок регулярных обзоров, отчеты об уроках, план корректировок.	Ретроспективы, отчеты, решения комитетов.	Повторение одних и тех же ошибок.

Источник: составлено авторами на основе [56; 81–83; 101; 102; 109].

Таблица 5.7 раскрывает ИОЦС как инструмент оценки управляемости цифрового развития организации. Важен не отдельный документ, а связность стратегии, данных, ИИ, архитектуры, культуры, безопасности и рефлексии.

Выбор весов ИОЦС должен быть прозрачным и документированным. В таблице 5.8 представлены возможные модели взвешивания доменов.

Таблица 5.8 – Модели взвешивания доменов ИОЦС

Модель	Логика взвешивания	Когда применять	Преимущества	Ограничение
Универсальная равновесная	Все домены имеют одинаковый вес.	Первичная диагностика организации; сравнение динамики во времени.	Простота и прозрачность.	Может недооценивать высокорисковые домены.

Модель	Логика взвешивания	Когда применять	Преимущества	Ограничение
Стратегически взвешенная	Приоритет получают стратегия, данные, культура и развитие персонала.	Организации, проходящие этап стратегической цифровой трансформации.	Связь индекса с целями развития.	Риск недооценить безопасность и этику.
Риск-ориентированная	Повышенный вес у управления данными, ИИ, безопасности и этики.	Организации с чувствительными данными, автоматизированными решениями и высокими требованиями надежности.	Лучше отражает критичные риски.	Требует экспертной оценки профиля риска.
Отраслевая	Веса корректируются с учетом отрасли, правового режима и характера цифровых решений.	Бизнес, публичное управление, медицина, промышленность, научные и проектные организации.	Повышает применимость модели.	Снижает сопоставимость между отраслями.
Адаптивная	Веса пересматриваются после пилота и анализа результатов.	Организации, внедряющие модель поэтапно.	Позволяет уточнять диагностику на основе опыта.	Требует строгой фиксации изменений методики.

Источник: составлено авторами.

Таблица 5.8 показывает, что индекс может быть адаптирован к профилю организации, но любые изменения весов должны быть заранее описаны и одинаково применяться в рамках одной волны диагностики.

Таким образом, ИОЦС позволяет оценить цифровое сознание организации как управляемую систему. Его следует использовать не для построения внешнего рейтинга, а для выбора приоритетов развития, настройки управления данными и ИИ, усиления цифровой культуры, повышения безопасности и организации цикла рефлексии.

5.5. УРОВНИ ЦИФРОВОЙ ЗРЕЛОСТИ ОРГАНИЗАЦИИ

Уровни цифровой зрелости в логике настоящего пособия не должны сводиться к количеству внедренных сервисов или степени автоматизации

процессов. Цифровая зрелость понимается как согласованность стратегии, данных, ИИ, архитектуры, культуры, безопасности, персонала и рефлексивного управления. В этой логике цифровое сознание выступает смысловой и управленческой основой зрелости.

Пятиуровневая шкала зрелости переводит результаты ИОЦС из числового значения в содержательную интерпретацию. Она позволяет понять, на каком уровне организация находится: фрагментарном, базовом, координируемом, интегрированном или адаптивно-рефлексивном. Переход между уровнями связан не с механическим приростом баллов, а с качественным изменением управляемости цифровой среды.

На рисунке 5.5 представлена траектория цифровой зрелости организации в логике цифрового сознания. Схема показывает движение от разрозненных цифровых практик к управляемой, интегрированной и рефлексивной организации.

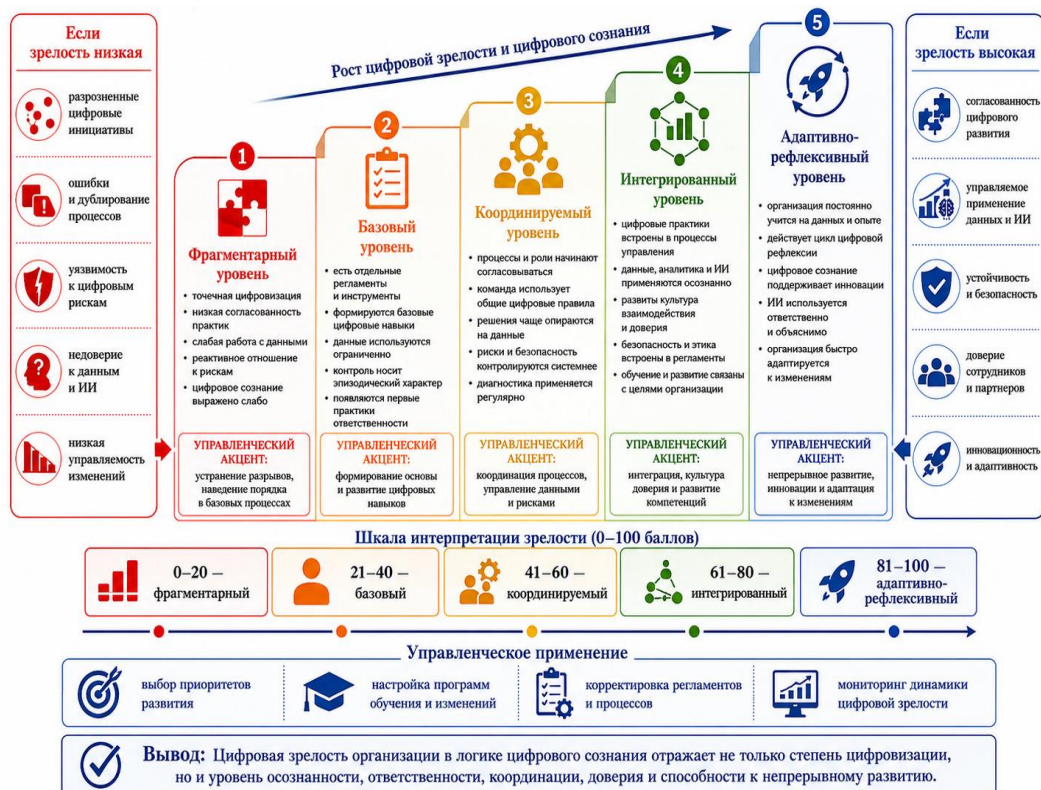


Рисунок 5.5 – Уровни цифровой зрелости организации в логике цифрового сознания

Источник: составлено авторами на основе [82; 83; 85; 101; 102].

Рисунок 5.5 демонстрирует пять уровней зрелости. Чем выше уровень, тем сильнее организация связывает цифровые решения с целями, данными, безопасностью, культурой, доверием и обучением.

Содержательная характеристика уровней представлена в таблице 5.9. Она помогает интерпретировать результаты ИОЦС и формулировать задачи перехода к следующему уровню.

Таблица 5.9 – Уровни цифровой зрелости организации в логике цифрового сознания

Уровень	Общая характеристика	Типичные признаки	Типичные риски	Задача перехода
Фрагментарный	Цифровые средства используются эпизодично и несогласованно.	Набор инициатив без общего контура; данные разрознены; ИИ случайный; безопасность реактивная.	Технический хаос, теневые сервисы и ИИ, повторение ошибок.	Сформировать базовый контур правил, ролей, данных и ответственности.
Базовый	Основные цифровые процессы присутствуют, но в основном инструментальны.	Есть цифровые цели, базовые платформы и правила, но слабая интеграция с управлением.	Декларативная цифровизация, формальное обучение, слабая проверка данных.	Зафиксировать роли, минимальные стандарты, базовую карту данных и сценариев ИИ.
Координируемый	Цифровые практики становятся управляемыми и сопоставимыми.	Стратегия связана с процессами; команды работают по единым правилам; безопасность встроена в ключевые процессы.	Застывание на уровне пилотов, локальные контуры без системной интеграции.	Перейти к интеграции стратегии, данных, ИИ, архитектуры и культуры.
Интегрированный	Стратегия, данные, ИИ, архитектура и культура связаны.	Управление данными и ИИ формализовано; цифровые сервисы прозрачны;	Инерция модели и недостаточная адаптивность.	Усилить организационную рефлексию, обратную связь и обновление правил.

Уровень	Общая характеристика	Типичные признаки	Типичные риски	Задача перехода
		обучение ролевое; ответственность устойчива.		
Адаптивно-рефлексивный	Организация учится на данных о собственных цифровых практиках.	Стратегия корректируется на основе доказательств; архитектура гибкая; доверие стейкхолдеров высокое; обучение непрерывное.	Самодовольство, усложнение модели, чрезмерная зависимость от метрик.	Поддерживать баланс инноваций, безопасности, этики и человеческой ответственности.

Источник: составлено авторами на основе [82; 83; 85; 101; 102].

Таблица 5.9 связывает уровни зрелости с признаками цифрового поведения, рисками и задачами развития. Она показывает, что зрелость является качественной характеристикой организации, а не только баллом.

Для практического использования полезно соотнести диапазоны ИОЦС с уровнями зрелости и управленческими действиями. Такое соотнесение представлено в таблице 5.10.

Таблица 5.10 – Интерпретация ИОЦС через уровни цифровой зрелости

Значение ИОЦС	Уровень зрелости	Диагностический профиль	Приоритетное управленческое действие
0–20	Фрагментарный	Разрозненные сервисы, неясные роли, слабое управление данными и ИИ.	Базовый аудит цифровых сервисов, данных, ИИ-сценариев и рисков.
21–40	Базовый	Есть отдельные регламенты и обучение, но практики нестабильны.	Стандартизация правил, назначение владельцев данных и ответственных за ИИ.
41–60	Координируемый	Процессы и команды согласованы частично; цифровая культура развивается.	Интеграция регламентов, командных практик, аналитики и программ развития.
61–80	Интегрированный	Контур стратегии, данных, ИИ, архитектуры и культуры связаны.	Развитие адаптивности, цифрового доверия и организационной

Значение ИОЦС	Уровень зрелости	Диагностический профиль	Приоритетное управленческое действие
			рефлексии.
81–100	Адаптивно-рефлексивный	Организация управляет цифровой средой на основе данных, этики, доверия и обучения.	Поддержание непрерывного улучшения и распространение практик в экосистеме.

Источник: составлено авторами.

Таблица 5.10 превращает индекс в управленческий ориентир: каждому диапазону соответствует не оценочный ярлык, а задача развития.

Таким образом, уровни зрелости позволяют интерпретировать ИОЦС не как абстрактный балл, а как состояние организации. Главная ценность шкалы состоит в определении следующего шага: от базовой стандартизации к координации, от координации к интеграции, от интеграции к рефлексивному развитию.

5.6. МЕТОДЫ СБОРА ДАННЫХ: ОПРОСЫ, КЕЙСЫ, ЦИФРОВОЙ СЛЕД, АНАЛИТИКА, ЭКСПЕРТНАЯ ОЦЕНКА

Диагностика цифрового сознания требует смешанной методологии. Самооценка показывает субъективное восприятие, но не доказывает реальное поведение. Кейсовое задание показывает способность применить знание, но зависит от качества сценария. Экспертная оценка дает профессиональную интерпретацию, но требует единой рубрики. Цифровой след дает поведенческие признаки, но может быть неправильно истолкован и создает этические риски. Поэтому ни один метод не должен использоваться изолированно.

Ключевым методическим правилом выступает триангуляция данных. Под триангуляцией в настоящей главе понимается сопоставление нескольких источников для подтверждения одного диагностического вывода. Например, вывод о слабой командной цифровой дисциплине должен опираться не только на жалобы руководителя, но и на анализ артефактов, интервью, наблюдение процесса и, при необходимости, ограниченные агрегированные данные цифровой среды.

На рисунке 5.6 представлена модель триангуляции. Она показывает, какие типы данных должны соединяться при диагностике и почему итоговый вывод должен быть подтвержден несколькими источниками.

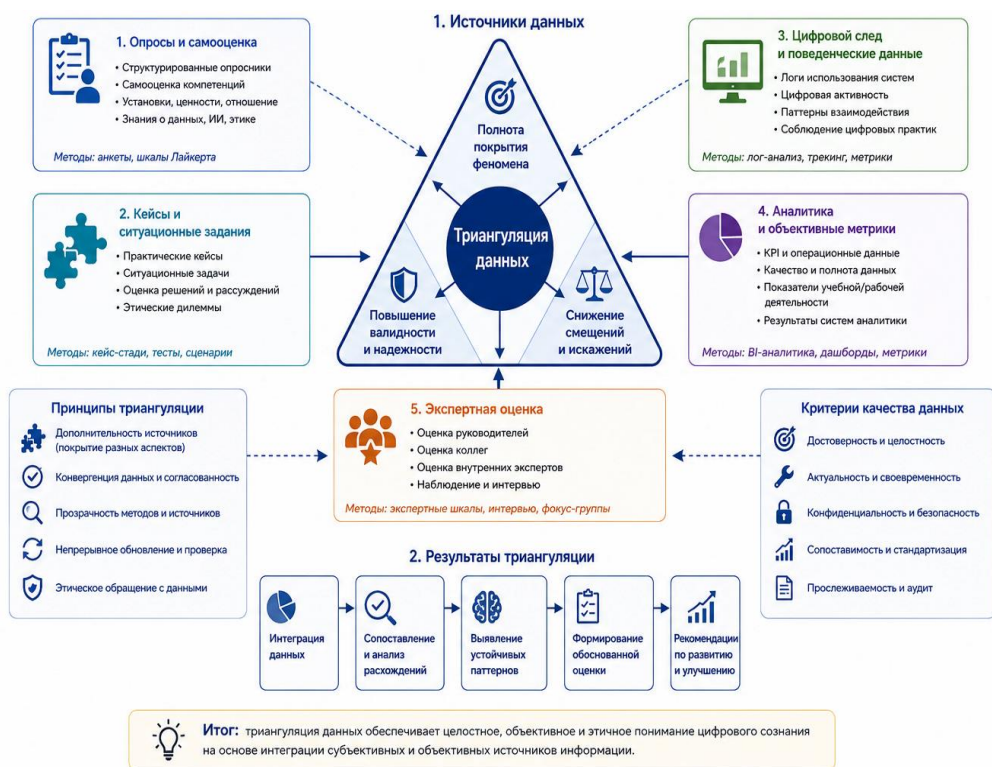


Рисунок 5.6 – Триангуляция данных в диагностике цифрового сознания

Источник: составлено авторами на основе [42; 44; 58; 86; 99].

Рисунок 5.6 показывает, что достоверный диагностический вывод формируется через сопоставление самооценки, кейсов, экспертной оценки, цифровых артефактов, интервью и аналитики.

В таблице 5.11 представлены основные методы сбора данных. Для каждого метода указаны объект измерения, преимущества, ограничения, этические условия и рекомендуемое сочетание с другими методами.

Таблица 5.11 – Методы сбора данных для диагностики цифрового сознания организации

Метод	Что измеряет	Преимущество	Ограничение	Этическое условие	Как сочетать
Анкетирование	Установки, самооценка, восприятие норм.	Быстро, масштабируемо, удобно для мониторинга.	Не показывает реальное поведение.	Ясные цели, конфиденциальность, запрет санкций по одному опросу.	Сочетать с кейсами и артефактами.
Самооценки	Рефлексивность	Поддержива	Завышение	Нельзя	Сочетать с

Метод	Что измеряет	Преимущество	Ограничение	Этическое условие	Как сочетать
а	ть и субъективная уверенность.	ет развитие и индивидуальный отчет.	или занижение результата.	использовать как единственное основание решений.	ситуационными заданиями.
Экспертная оценка	Профессиональная интерпретация практики.	Учитывает контекст и качество действия.	Требует подготовки экспертов и рубрик.	Прозрачные критерии и независимая оценка там, где возможно.	Сочетать с документами и кейсами.
Оценка руководителей	Видимость цифрового поведения в работе.	Связана с рабочим контекстом.	Может быть искажена отношениями.	Не должна подменять всю диагностику.	Сочетать с взаимной оценкой и кейсами.
Взаимная оценка	Качество совместной работы в команде.	Хорошо выявляет командные практики.	Риск групповой лояльности и конформизма.	Анонимизация и правила обратной связи.	Сочетать с артефактами и интервью.
Кейсовые задания	Способность применять знания в ситуации.	Ближе к реальному действию.	Требуют разработки банка кейсов.	Пропорциональность сложности и роли.	Сочетать с экспертным оцениванием.
Ситуационные тесты	Выбор решения в типовой цифровой ситуации.	Полезны для ИИ, данных, этики и безопасности.	Могут стимулировать угадывание ответа.	Четкие критерии и последующее обсуждение.	Сочетать с интервью.
Анализ цифровых артефактов	Реальные продукты деятельности: документы, записи решений, шаблоны.	Высокая прикладная валидность.	Трудоемкость и риск случайной выборки.	Исключение лишних персональных данных.	Сочетать с экспертной оценкой.
Анализ цифрового следа	Агрегированные паттерны использования систем.	Дает поведенческие признаки.	Активность не равна качеству.	Прозрачность, минимизация, запрет скрытого контроля.	Только в составе триангуляции.
Интервью	Контекст,	Позволяет	Сложно	Добровольность	Проводить

Метод	Что измеряет	Преимущество	Ограничение	Этическое условие	Как сочетать
	причины дефицитов, мотивация.	объяснить цифры.	масштабировать.	и конфиденциальность.	после первичного анализа.
Фокус-группы	Нормы и коллективные смыслы.	Полезны для культуры и доверия.	Риск давления активных участников.	Безопасная модерация.	Сочетать с предварительными выводами.
Аудит документов	Формализованный контур управления.	Показывает наличие ролей и регламентов.	Документы могут быть формальными.	Проверка практики исполнения.	Сочетать с интервью и анализом инцидентов.
Анализ инцидентов	Реальные сбои, ошибки и риски.	Высокая практическая значимость.	Инциденты не покрывают всю систему.	Ненаказательный подход к разбору.	Сочетать с безопасностью и управлением ИИ.
Аналитические панели	Динамика процессов и показателей.	Удобны для мониторинга.	Фокус на легко измеряемом.	Не подменять смысловую диагностику метриками.	Сочетать с качественным разбором.

Источник: составлено авторами на основе [42; 44; 58; 86; 99].

Таблица 5.11 показывает, что надежная диагностика требует смешанных методов. Количественные данные должны дополняться качественным контекстом, а цифровой след не может быть единственной основой вывода.

Практическое правило триангуляции можно зафиксировать в виде таблицы 5.12. Она показывает, какой вклад вносит каждый тип источника и какую ошибку он помогает предотвратить.

Таблица 5.12 – Принцип триангуляции в диагностике цифрового сознания

Источник	Диагностический вклад	Какую ошибку предотвращает	Правило применения
Самооценка	Показывает субъективное восприятие и готовность к рефлексии.	Иллюзия компетентности или занижение собственных возможностей.	Не использовать отдельно от кейсов и артефактов.
Кейсовое задание	Показывает способность действовать в моделируемой	Декларативное знание без применения.	Оценивать по единой рубрике.

Источник	Диагностический вклад	Какую ошибку предотвращает	Правило применения
	ситуации.		
Экспертная оценка	Дает профессиональное суждение о качестве действия.	Поверхностная интерпретация результатов.	Использовать нескольких экспертов в спорных случаях.
Цифровой артефакт	Показывает реальный продукт деятельности.	Отрыв диагностики от практики.	Минимизировать персональные данные.
Аналитика процесса	Показывает динамику и повторяемость поведения.	Опора только на впечатления.	Не приравнивать активность к качеству.
Интервью или фокус-группа	Показывает причины, барьеры и контекст.	Механическое толкование числового результата.	Проводить в безопасной и конфиденциальной форме.

Источник: составлено авторами.

Таблица 5.12 фиксирует эпистемологическую логику диагностики: разные источники дают разные типы знания, поэтому вывод должен строиться на их сопоставлении.

Особого регулирования требует цифровой след. Он действительно может быть полезен для понимания повторяемых ошибок, перегрузки, соблюдения маршрутов работы и причин инцидентов. Однако цифровой след легко превращается в инструмент скрытого наблюдения. Поэтому в таблице 5.13 разграничены допустимые и недопустимые практики.

Таблица 5.13 – Допустимое и недопустимое использование цифрового следа

Допустимо	Недопустимо
Анализ агрегированной активности команды для выявления узких мест процессов.	Скрытый индивидуальный мониторинг без информирования участников.
Анализ соблюдения согласованного маршрута работы, версионности и сроков.	Тотальный контроль рабочего времени и микроповедения ради наказания.
Подсчет прохождения обязательных модулей по безопасности и грамотности в области ИИ.	Выводы о личности, лояльности или потенциале человека только по логам.
Анализ обращений к базе знаний для проектирования обучения.	Непрозрачные рейтинги активности как суррогат качества работы.
Анализ причин инцидентов на уровне команд или процессов.	Автоматические кадровые решения без человеческой проверки.
Проверка наличия маршрута согласования	Оценка по приватной переписке или

Допустимо	Недопустимо
документов и взаимной проверки.	личным аккаунтам.
Использование обезличенных данных для организационной диагностики и улучшения процессов.	Сбор данных «на всякий случай» и повторное использование вне исходной цели.

Источник: составлено авторами на основе [86; 152].

Таблица 5.13 служит этическим фильтром работы с цифровым следом. Она показывает, что цифровой след может применяться только открыто, ограниченно, пропорционально цели диагностики и в сочетании с другими источниками.

Таким образом, диагностика цифрового сознания организации должна строиться как смешанное исследование, соединяющее количественные и качественные данные. Ни самооценка, ни цифровой след, ни экспертное мнение не могут быть абсолютным источником истины. Достоверность возникает через триангуляцию, прозрачность критериев и управленческую интерпретацию результата.

5.7. ЭТИЧЕСКИЕ ОГРАНИЧЕНИЯ ДИАГНОСТИКИ И НЕДОПУСТИМОСТЬ ЦИФРОВОГО НАДЗОРА

Этические ограничения являются не внешним дополнением к диагностике, а частью ее методологии. Чем больше организация использует данные, цифровой след, аналитические панели и ИИ для оценки собственных практик, тем выше риск превращения диагностики в скрытый контроль. Поэтому глава завершает диагностическую модель прямым запретом цифрового надзора под видом развития.

Под цифровым надзором в контексте главы понимается скрытое, непропорциональное или непрозрачное отслеживание цифрового поведения сотрудников, команд или пользователей с последующим ранжированием, профилированием или санкциями без понятных критериев, человеческой проверки и права на объяснение. Такая практика разрушает доверие и противоречит самой идее цифрового сознания.

На рисунке 5.7 представлены границы допустимого и недопустимого использования диагностических данных. Схема показывает, что этическая диагностика должна строиться вокруг развития, минимизации данных, прозрачности и человеческой проверки.

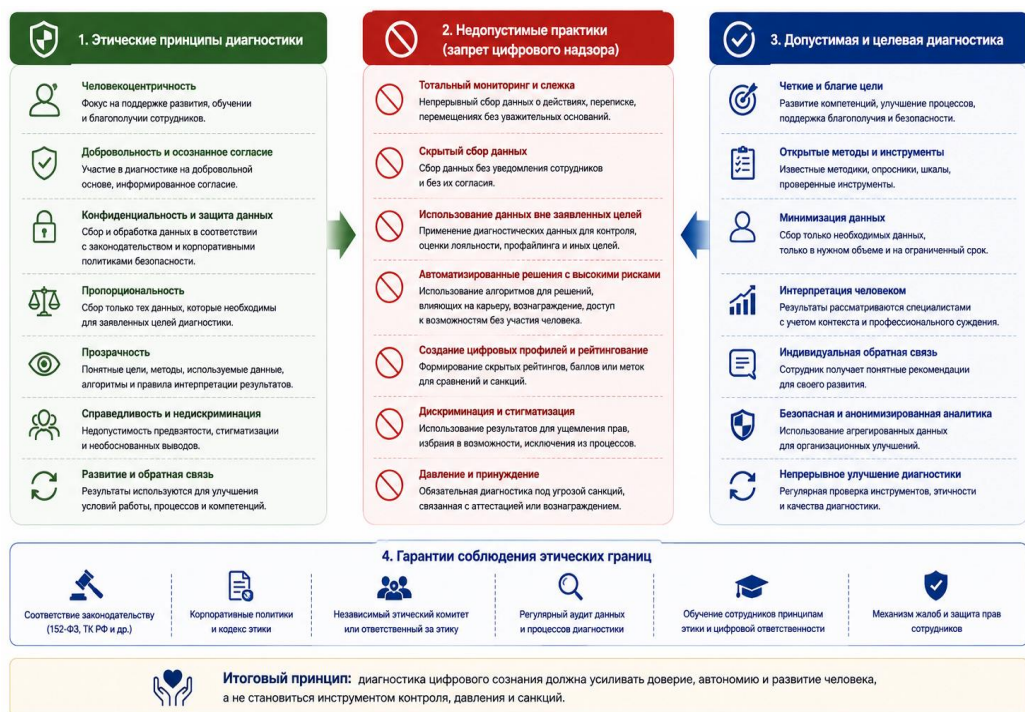


Рисунок 5.7 – Этические границы диагностики и запрет цифрового надзора

Источник: составлено авторами на основе [18; 86; 137; 152].

Рисунок 5.7 противопоставляет развивающую диагностику скрытому надзору. Допустимыми являются открытые цели, минимизация данных, агрегирование и обратная связь; недопустимыми – скрытый мониторинг, автоматические санкции и профилирование.

В таблице 5.14 раскрыты основные этические риски диагностики и меры их предотвращения. Таблица может использоваться как чек-лист при проектировании локального положения о диагностике.

Таблица 5.14 – Этические риски диагностики и меры предотвращения

Этический риск	Как проявляется	Возможный ущерб	Мера предотвращения
Цифровой надзор	Диагностика превращается в постоянное наблюдение за поведением.	Недоверие, сопротивление, правовые риски.	Явный запрет скрытого мониторинга.
Скрытый сбор данных	Данные собираются без понятного уведомления участников.	Нарушение автономии и доверия.	Информирование и политика прозрачности.

Этический риск	Как проявляется	Возможный ущерб	Мера предотвращения
Профилирование сотрудников	По цифровому следу строятся скрытые профили личности или лояльности.	Стигматизация и дискриминация.	Запрет высокорискового профилирования.
Автоматические кадровые решения	Индекс используется как триггер санкций без человеческой проверки.	Ошибочные и несправедливые решения.	Обязательная человеческая проверка значимых выводов.
Манипуляция метриками	Участники подстраивают активность под показатели.	Имитация развития вместо реального изменения.	Баланс метрик, кейсов и содержательной оценки.
Формальное ранжирование	Появляются рейтинги лучших и худших без объяснения методики.	Подрыв командной культуры.	Агрегированные отчеты и развивающая обратная связь.
Нарушение конфиденциальности	Широкий доступ к персональным результатам.	Психологический, репутационный и правовой вред.	Ролевая модель доступа и сроки хранения.
Использование вне цели	Данные диагностики применяются для иных задач.	Этический и правовой риск.	Ограничение цели и повторное согласование.
Дискриминация	Индикаторы не учитывают различия ролей и условий деятельности.	Систематическая несправедливость.	Ролевые нормы и проверка справедливости модели.
Стигматизация низких результатов	Низкий балл трактуется как цифровая непригодность.	Демотивация и защитное поведение.	Конфиденциальная обратная связь и план роста.

Источник: составлено авторами на основе [18; 86; 137; 152].

Таблица 5.14 показывает, что этическая защита должна быть встроена во все этапы диагностики: от выбора данных до интерпретации индексов и управленческих решений.

Итоговая диагностическая рамка главы представлена на рисунке 5.8. Она объединяет принципы, индексы, методы, шкалы, этические ограничения и

управленческие решения в единую систему оценки цифрового сознания организации.



Рисунок 5.8 – Диагностическая рамка оценки цифрового сознания организации
Источник: составлено авторами.

Рисунок 5.8 фиксирует итоговую логику главы: диагностика начинается с принципов, проходит через индексы и методы, интерпретируется через шкалы зрелости, ограничивается этическим контуром и завершается управленческими решениями.

Для практического применения важно связать индексы с управленческими действиями. Такая связь представлена в таблице 5.15.

Таблица 5.15 – Связь индексов, методов и управленческих решений

Инструмент	Уровень применения	Что показывает	Какое решение поддерживает
ИЦСС	Сотрудник	Индивидуальный профиль цифрового поведения: дееспособность, критичность, данные и ИИ, безопасность, этика,	Индивидуальный план развития, наставничество, обучение, включение в командные практики.

Инструмент	Уровень применения	Что показывает	Какое решение поддерживает
		коммуникация, рефлексия.	
ИЦСК	Команда	Согласованность совместной цифровой деятельности: координация, общие данные, проверка ИИ, цифровая память, командное обучение.	Командная ретроспектива, настройка правил, распределение ролей, протоколы проверки и коммуникации.
ИОЦС	Организация	Состояние стратегии, управления данными и ИИ, архитектуры, культуры, безопасности, доверия и рефлексивности.	Корректировка стратегии, регламентов, архитектуры, программ обучения и контуров управления рисками.
Шкала зрелости	Организация в целом	Интерпретация индекса как уровня цифровой зрелости: от фрагментарного до адаптивно-рефлексивного.	Выбор приоритетов развития и мониторинг динамики по годовым циклам.
Триангуляция	Все уровни	Проверка достоверности вывода через несколько источников данных.	Повышение надежности диагностики и снижение риска ошибочных управленческих решений.
Этический контур	Все уровни	Ограничения использования данных, цифрового следа и результатов диагностики.	Поддержание доверия, правомерности и развивающего характера диагностики.

Источник: составлено авторами.

Таблица 5.15 показывает, что диагностика имеет смысл только тогда, когда каждый индекс и метод связан с конкретным управленческим действием: обучением, корректировкой правил, управлением рисками или развитием культуры.

Таким образом, этические ограничения являются условием доверия к диагностике. Без них оценка цифрового сознания может превратиться в механизм контроля и давления. С этическими ограничениями она становится инструментом развития, обучения, управления рисками и повышения цифровой зрелости организации.

5.8. МЕТОДИЧЕСКИЙ АЛГОРИТМ ПРИМЕНЕНИЯ РЕЗУЛЬТАТОВ ДИАГНОСТИКИ

После расчета индексов диагностическая работа не завершается. Организация должна перевести результаты в управленческий цикл: обсудить дефициты, определить приоритеты, назначить ответственных, запланировать обучение, уточнить локальные документы и установить сроки повторной оценки. Именно на этом этапе диагностика становится инструментом цифровой зрелости, а не статистическим упражнением. Если результаты остаются в виде отчета без управленческих решений, организация получает видимость контроля, но не получает развития.

На рисунке 5.9 представлен методический алгоритм применения результатов диагностики.

Первый шаг применения результатов – подготовка диагностического отчета. Он должен содержать не только итоговые значения ИЦСС, ИЦСК и ИОЦС, но и профиль доменов: какие компоненты развиты, какие находятся в зоне риска, какие требуют дополнительной проверки. В индивидуальном отчете нежелательно показывать сравнительный рейтинг сотрудников. Более корректно показывать личный профиль развития: сильные стороны, зоны поддержки, рекомендуемые модули обучения, практические задания и форму обратной связи.

Второй шаг – управленческое обсуждение результатов на уровне команды и организации. Для командного уровня полезны не индивидуальные фамилии, а агрегированный профиль совместной практики: где команда теряет решения, как работает с данными, есть ли взаимная проверка результатов ИИ, фиксируются ли цифровые договоренности, как сохраняется цифровая память проекта. Такая форма обсуждения снижает защитную реакцию и переводит разговор из поиска виновных в улучшение процесса.

Третий шаг – классификация дефицитов. Дефициты цифрового сознания бывают разной природы. Одни связаны с недостатком знаний: сотрудник не понимает, как проверить результат ИИ. Другие связаны с отсутствием правил: команда не знает, где фиксировать решение. Третьи обусловлены архитектурой: данные находятся в разных системах и не имеют владельца. Четвертые являются культурными: сотрудники не сообщают об ошибках, потому что опасаются санкций. Для каждого типа дефицита нужны разные управленческие действия.



Рисунок 5.9 – Методический алгоритм применения результатов диагностики

Четвертый шаг – перевод дефицита в решение. Если проблема находится на уровне знаний, выбирается обучение. Если она связана с отсутствием правил, разрабатывается регламент или чек-лист. Если причина в архитектуре, корректируются сервисы, доступы, интеграции и данные. Если дефицит культурный, необходимы коммуникации, безопасное обсуждение ошибок, работа руководителей и изменение норм взаимодействия. Поэтому диагностический отчет должен содержать не только оценку, но и матрицу «дефицит – причина – действие – ответственный – срок».

Пятый шаг – назначение владельцев изменений. Диагностика часто оказывается бесполезной, если результаты распределены между подразделениями, но ни одно из них не отвечает за интегральное изменение. Например, дефицит грамотности в области ИИ может требовать участия цифрового подразделения, юридической службы, службы безопасности, службы персонала и руководителей процессов. Поэтому по итогам диагностики целесообразно формировать межфункциональную рабочую группу или комитет по развитию цифрового сознания.

Шестой шаг – формирование карты быстрых и системных действий. Быстрые действия устраняют очевидные разрывы: обновление памятки по ИИ, настройка доступа, запуск короткого инструктажа, введение шаблона проверки данных. Системные действия требуют большего времени: разработка политики управления данными, создание реестра ИИ-сценариев, перестройка цифровой архитектуры, изменение программы развития управленческих команд. Диагностика должна помогать различать эти два горизонта.

Седьмой шаг – повторная оценка. Цифровое сознание не формируется в результате одной диагностической волны. Организация должна устанавливать регулярность: базовая оценка, промежуточная оценка после управленческих действий и итоговая оценка по результатам цикла. Между волнами методика должна сохранять сопоставимость, иначе динамика окажется недостоверной. Изменение вопросов, шкал и весов допускается только с фиксацией причины и пересчетом сопоставимости.

Восьмой шаг – закрепление результатов в организационной памяти. Итоги диагностики, принятые решения, извлеченные уроки, улучшенные регламенты и успешные кейсы должны быть сохранены в базе знаний. Иначе организация будет повторять одинаковые ошибки при каждой новой технологической волне. Цифровая память должна включать не только технические инструкции, но и методические разборы: почему решение было принято, какие риски учитывались, какие эффекты получены и что было изменено.

Девятый шаг – связь диагностики с цифровой стратегией. Если диагностика показывает низкую готовность к управлению данными и ИИ, организация не должна запускать высокорисковые ИИ-проекты без предварительной подготовки. Если выявлено низкое цифровое доверие, необходимо сначала объяснить правила работы с данными и цифровым следом. Если слабым звеном является командная координация, развитие индивидуальных навыков не даст результата без изменения совместных процессов.

Десятый шаг – публичная управленческая коммуникация. Руководство должно объяснить, зачем проводится диагностика, какие выводы сделаны на агрегированном уровне, какие действия будут предприняты и какие данные не будут использоваться для санкций. Такая коммуникация снижает опасения

сотрудников и формирует доверие к модели. В отсутствие коммуникации даже корректная диагностика может восприниматься как скрытый контроль.

Для практического применения целесообразно различать три типа диагностических отчетов. Первый – индивидуальный отчет сотрудника, предназначенный для саморазвития и конфиденциальной обратной связи. Второй – командный отчет, предназначенный для совместной ретроспективы и настройки правил взаимодействия. Третий – организационный отчет, предназначенный для управленческой команды и проектирования изменений в стратегии, архитектуре, управлении данными, ИИ, безопасности и обучении.

Индивидуальный отчет должен быть лаконичным и понятным. Он может содержать профиль по семи компонентам, короткое объяснение уровня, рекомендации по развитию, примеры практических действий и перечень образовательных модулей. Недопустимо превращать его в «паспорт цифровой пригодности». Сотрудник должен понимать, что результат показывает текущую траекторию развития, а не фиксирует окончательное качество личности или профессиональной ценности.

Командный отчет должен показывать не среднюю оценку участников, а качество совместной цифровой практики. В нем целесообразно выделять зоны согласованности и зоны разрыва: где нет единого маршрута задач, где не фиксируются решения, где отсутствует взаимная проверка данных, где используются разные каналы коммуникации, где цифровая память проекта зависит от отдельных людей. Такой отчет лучше обсуждать в формате командной ретроспективы.

Организационный отчет должен быть связан с управленческими решениями. В нем недостаточно указать общий ИОЦС. Необходимо показать доменный профиль: стратегия, управление данными, управление ИИ, архитектура, культура, безопасность, развитие персонала, аналитика, доверие и рефлексия. Для каждого домена должны быть указаны дефициты, возможные причины, рекомендуемые действия, ответственные подразделения и срок повторной проверки.

Диагностика также должна учитывать различие ролей. Требования к рядовому сотруднику, руководителю, аналитику, специалисту по безопасности, владельцу данных, участнику ИИ-проекта и члену управленческой команды не могут быть одинаковыми. Базовые принципы общие, но индикаторы должны быть ролевыми. Например, сотруднику достаточно знать правила допустимого применения ИИ, а руководитель должен понимать контур ответственности, риски делегирования и порядок проверки результатов.

При проектировании ролевых профилей важно не усложнить модель чрезмерно. Рекомендуется выделить базовый профиль для всех сотрудников и специальные модули для групп повышенной ответственности: руководители,

владельцы данных, пользователи ИИ в значимых процессах, аналитики, специалисты по персоналу, специалисты по информационной безопасности и участники цифровых проектов. Такой подход сохраняет универсальность и одновременно учитывает риски.

Отдельного внимания требует диагностическая коммуникация. Участникам нужно объяснить, что именно измеряется: не личная «технологическая продвинутость», а готовность действовать осознанно, безопасно и ответственно в цифровой среде. Нужно также объяснить, какие данные собираются, кто их увидит, как долго они хранятся, какие результаты будут агрегированы и какие решения могут последовать. Без этого доверие к диагностике будет низким.

Принцип обратной связи должен быть обязательным. Если человек или команда участвуют в диагностике, они должны получить результат в понятной форме. Отсутствие обратной связи превращает диагностику в извлечение данных, а не в развивающую практику. Обратная связь может быть индивидуальной, командной или организационной, но она должна объяснять смысл результата, его ограничения и следующие шаги.

Интерпретация индексов должна избегать ложной точности. Разница между 63 и 66 баллами не всегда управленчески значима. Значимым является профиль доменов, динамика по сравнению с предыдущей волной, подтверждение несколькими источниками и связь с реальными изменениями. Поэтому в отчетах следует использовать диапазоны, уровни и качественные комментарии, а не только точные числовые значения.

Сильный диагностический инструмент всегда имеет ограничение. Он показывает часть реальности, но не исчерпывает ее. Поэтому модель должна предусматривать процедуру апелляции, уточняющего интервью или дополнительной экспертной проверки в спорных случаях. Особенно это важно там, где результат может повлиять на обучение, распределение ролей, допуск к цифровым проектам или оценку готовности команды к работе с ИИ.

Еще одно ограничение связано с динамикой технологий. То, что сегодня является продвинутой практикой, через год может стать базовой цифровой нормой. Поэтому диагностические индикаторы не должны быть заморожены. Необходимо ежегодно проверять актуальность компонентов, формулировок, кейсовых заданий, перечня рисков и шкал. При этом ядро модели – критичность, этика, безопасность, ответственность и рефлексия – должно сохраняться.

Кейсовые задания должны строиться на типовых ситуациях организации. Универсальные примеры полезны на старте, но диагностическая точность возрастает, когда кейсы отражают реальные процессы: подготовку аналитической записки, проверку ИИ-ответа, работу с чувствительными данными, согласование цифрового документа, выбор канала коммуникации,

реагирование на инцидент или оценку цифрового сервиса. Это делает диагностику ближе к практике.

При разработке кейсов важно не подталкивать участника к очевидному ответу. Хороший кейс содержит неоднозначность: полезность цифрового инструмента сочетается с риском данных, скорость решения – с необходимостью проверки, автоматизация – с ответственностью человека, интерес организации – с правами участника. Именно такие ситуации позволяют увидеть цифровое сознание как способность взвешивать альтернативы, а не как знание правильной инструкции.

Опросные вопросы должны быть сформулированы так, чтобы снижать социально желательные ответы. Вопрос «соблюдаете ли вы правила безопасности?» менее информативен, чем вопрос о конкретном поведении: проверяет ли участник адрес отправителя, использует ли утвержденные каналы обмена, знает ли порядок сообщения об инциденте. Поведенческая формулировка повышает диагностическую ценность анкеты и облегчает последующую проверку.

Экспертная оценка требует подготовки экспертов. Эксперт должен понимать авторскую модель цифрового сознания, уровни шкалы, критерии оценки и этические ограничения. Если разные эксперты по-разному понимают, что такое «осознанный уровень» или «рефлексивная готовность», результаты будут несопоставимы. Поэтому перед диагностикой необходима калибровочная сессия, на которой эксперты оценивают пробные кейсы и согласуют критерии.

Для организаций с высоким уровнем цифровых рисков полезно вводить отдельный протокол оценки ИИ-сценариев. Он должен включать описание цели применения ИИ, типа данных, степени влияния на человека, необходимости человеческой проверки, требований к объяснимости, порядка журналирования и процедуры пересмотра решения. Такой протокол связывает диагностику цифрового сознания с практикой управления ИИ и цифровой ответственностью.

Важной частью применения диагностики является связь с обучением. Индекс без образовательной траектории создает тревогу, но не создает развития. Поэтому для каждого уровня должны быть подготовлены образовательные действия: базовые модули для фрагментарного уровня, практикумы для базового уровня, кейс-семинары для функционального уровня, наставничество для осознанного уровня и участие в проектировании практик для развивающего уровня.

Диагностика должна быть полезна и руководителям. Управленческая команда получает не только информацию о дефицитах персонала, но и зеркало собственных управленческих решений: насколько ясны правила, понятны ли роли, доступны ли данные, не перегружена ли цифровая среда, доверяют ли сотрудники цифровым практикам, есть ли механизм исправления ошибок.

Поэтому результаты должны обсуждаться на уровне стратегического управления.

Организация может использовать диагностику для выбора пилотных подразделений. Более зрелые команды целесообразно включать в пилоты новых цифровых решений, а команды с фрагментарным уровнем сначала поддерживать обучением, настройкой процессов и нормами безопасности. Такой подход снижает риск провала пилота и показывает, что диагностика является инструментом управляемого внедрения, а не только описанием текущего состояния.

Еще одно направление применения – управление цифровыми рисками. Если диагностика показывает низкую кибергигиену, высокую зависимость от внешних ИИ-сервисов, отсутствие проверки данных или низкое понимание правовых границ, организация должна не просто обучить сотрудников, но и пересмотреть правила доступа, список разрешенных инструментов, порядок работы с конфиденциальной информацией и контуры реагирования на инциденты.

Результаты диагностики должны быть сопоставлены с цифровой архитектурой. Иногда низкие показатели связаны не с нежеланием сотрудников, а с неудобством систем, дублированием каналов, отсутствием интеграции, устаревшими интерфейсами или противоречивыми регламентами. Цифровое сознание организации предполагает честное признание того, что поведение людей формируется не только обучением, но и качеством цифровой среды.

В годовом цикле управления диагностика может быть связана с планированием бюджета цифрового развития. Если данные показывают, что организация не готова к масштабированию ИИ из-за слабого управления данными, средства следует направить не только на закупку моделей, но и на качество данных, обучение, регламенты и безопасность. Это делает диагностику инструментом рационального распределения ресурсов.

Наконец, диагностика должна поддерживать цифровое доверие. Сотрудники и команды будут участвовать в ней осознанно только тогда, когда понимают ее развивающий смысл и видят реальные изменения после предыдущих волн. Если результаты игнорируются, доверие снижается. Если на основе диагностики улучшаются процессы, снижается перегрузка, появляются понятные правила и поддержка, цифровое сознание становится частью культуры организации.

Таким образом, методический алгоритм применения результатов диагностики включает восемь обязательных действий: подготовку отчета, обсуждение на соответствующем уровне, классификацию дефицитов, перевод дефицитов в решения, назначение владельцев изменений, разделение быстрых и системных действий, повторную оценку и закрепление результатов в

организационной памяти. Эта последовательность обеспечивает переход от оценки к формированию цифрового сознания.

5.9. МЕТОДИЧЕСКИЕ ТРЕБОВАНИЯ К РАЗРАБОТКЕ ДИАГНОСТИЧЕСКИХ ИНСТРУМЕНТОВ

Разработка диагностических инструментов должна начинаться с описания конструкта. Для каждого индекса необходимо определить, какие компоненты входят в оценку, какие признаки наблюдаемы, какие данные могут быть использованы, какие ограничения действуют и какие управленческие решения допустимы. Без такого описания анкета или кейс превращаются в набор разрозненных вопросов, не связанных с общей методологией пособия.

Каждый диагностический вопрос должен быть привязан к компоненту модели. Например, вопрос о проверке источников относится к информационно-аналитической критичности, вопрос о запрете передачи конфиденциальных данных во внешние сервисы – к безопасности и этике, вопрос о фиксации решений – к командной цифровой дисциплине. Такая привязка нужна для содержательной валидности инструмента и последующей интерпретации результатов.

Вопросы анкеты целесообразно формулировать через конкретное действие, а не через самооценочный образ. Формулировка «я цифрово компетентен» методически слаба, поскольку участники вкладывают в нее разные смыслы. Более надежна формулировка «перед использованием данных я проверяю источник, дату обновления и ограничения интерпретации». Она описывает наблюдаемую практику и может быть сопоставлена с кейсом или артефактом.

Для каждого компонента желательно иметь не менее трех типов индикаторов: когнитивный, поведенческий и рефлексивный. Когнитивный индикатор показывает понимание правила, поведенческий – применение правила в ситуации, рефлексивный – способность объяснить последствия и изменить практику. Такая структура особенно важна для цифрового сознания, поскольку оно не сводится к знанию инструкции.

Кейсовые задания должны проходить экспертную проверку. Эксперты оценивают, соответствует ли кейс компоненту, реалистична ли ситуация, есть ли неоднозначность, не содержит ли задание подсказки правильного ответа, не дискриминирует ли оно участников с разными ролями. После пилотирования кейсы следует корректировать на основе анализа ответов: слишком легкие, слишком сложные или двусмысленные кейсы снижают качество диагностики.

Шкалы оценивания должны быть описаны до начала диагностики. Участники и эксперты должны понимать, чем отличается базовый уровень от функционального, функциональный от осознанного, а осознанный от

рефлексивного. Если шкала не описана, экспертная оценка становится субъективной, а результаты разных подразделений несопоставимыми.

При проектировании ИЦСС необходимо учитывать, что не все сотрудники работают с одинаковым уровнем цифровой сложности. Для базовых ролей достаточно общего профиля, но для ролей повышенной ответственности нужны дополнительные блоки: управление данными, работа с ИИ, анализ цифровых рисков, управление доступом, подготовка аналитических материалов, принятие решений с цифровой поддержкой. Это позволяет избежать несправедливой оценки.

При проектировании ИЦСК важно фиксировать реальный объект оценки: команда, подразделение, проектная группа, рабочая группа или управленческий контур. Команды различаются по длительности существования, степени формализации, составу и задачам. Для временной проектной группы важна цифровая память и передача знаний, для постоянного подразделения – устойчивость процессов и цифровая дисциплина.

При проектировании ИОЦС необходимо определить границы организации. В крупных организациях целесообразно проводить оценку как по организации в целом, так и по ключевым подразделениям. Это позволяет выявить неоднородность: одна часть организации может иметь развитую цифровую архитектуру, а другая оставаться на уровне ручных практик. Итоговый ИОЦС без профиля подразделений может скрыть важные различия.

Пилотирование диагностического инструмента является обязательным этапом. На пилоте проверяются понятность формулировок, время прохождения, устойчивость шкал, качество кейсов, техническая удобность процедуры, уровень доверия участников и корректность интерпретации. После пилота необходимо провести сессию обратной связи и исправить вопросы, вызывающие непонимание или не дающие полезной диагностической информации.

Оценка надежности должна включать несколько направлений. Для анкет – проверку внутренней согласованности компонентов после накопления достаточного массива данных. Для экспертной оценки – проверку согласованности экспертов. Для повторной диагностики – сопоставление результатов во времени с учетом проведенных управленческих действий. Для кейсов – анализ того, различают ли они уровни цифрового сознания.

Содержательная валидность обеспечивается экспертной процедурой. Экспертам предлагается оценить, насколько каждый пункт соответствует компоненту модели, насколько он понятен, необходим и не дублирует другие пункты. Пункты с низкой экспертной оценкой исключаются или перерабатываются. Такая процедура особенно важна, поскольку цифровое сознание является авторским метаконструктом и требует аккуратной операционализации.

Конструктивная валидность может проверяться после накопления эмпирических данных. На этом этапе возможно изучать, действительно ли вопросы группируются в ожидаемые компоненты, как компоненты связаны между собой, отличаются ли индивидуальный, командный и организационный уровни, как индексы связаны с показателями цифровой зрелости, безопасностью, качеством данных, доверием и результатами обучения.

Нельзя смешивать диагностические и мотивационные задачи. Если организация хочет стимулировать участие, можно использовать общую коммуникацию, сертификаты, образовательные рекомендации и признание командных улучшений. Но нельзя превращать индекс в соревнование за высокий балл. В противном случае участники начнут отвечать стратегически, подстраивая поведение под метрику, а не развивая цифровое сознание.

В диагностике важно учитывать цифровую нагрузку. Слишком длинные анкеты, сложные кейсы и множественные процедуры могут сами стать источником перегрузки и сопротивления. Поэтому диагностическая волна должна быть разумной по времени. Лучше проводить несколько коротких и содержательных процедур, чем один большой опрос, который участники проходят формально.

Техническая среда диагностики должна быть безопасной и понятной. Если используется цифровая платформа, нужно обеспечить контроль доступа, корректное хранение результатов, возможность выгрузки агрегированных данных, отсутствие лишнего сбора информации, понятный интерфейс и возможность получить обратную связь. Техническая организация процедуры сама становится проявлением цифрового сознания.

Документирование методики должно включать описание целей, уровней, индексов, шкал, источников данных, правил интерпретации, этических ограничений, ролей участников, порядка хранения данных, способов обратной связи и сроков повторной оценки. Такой документ защищает организацию от произвольного применения диагностики и повышает доверие к результатам.

При работе с персональными результатами необходимо соблюдать принцип минимальной достаточности. Руководителю не всегда нужны детальные ответы сотрудника по каждому вопросу. Чаще достаточно агрегированного профиля и рекомендации по развитию. Детальные персональные данные должны быть доступны только тем, кто отвечает за конфиденциальную обратную связь и сопровождение обучения.

Командные результаты рекомендуется обсуждать в формате фасилитируемой сессии. На такой сессии команда не выясняет, кто «испортил» общий показатель, а анализирует практики: где теряются решения, почему не проверяются данные, как распределяется ответственность, какие правила

избыточны, какие отсутствуют. Это переводит диагностику в режим организационного обучения.

Организационные результаты должны быть представлены в форме карты приоритетов. Для каждого домена указывается текущий уровень, желаемый уровень, разрыв, риск, требуемое действие, ответственный, срок и показатель повторной проверки. Такая карта связывает ИОЦС с цифровой стратегией и делает диагностику инструментом управляемой трансформации.

Методика должна предусматривать процедуру обновления. Раз в год целесообразно пересматривать перечень ИИ-сценариев, типовые риски, образовательные модули, кейсовые задания и ролевые профили. При этом изменения должны фиксироваться, чтобы не разрушить сопоставимость динамики. Если шкалы существенно изменились, результаты разных лет нужно сравнивать с осторожностью.

В организациях с высоким уровнем регулирования необходима правовая экспертиза диагностики. Она должна проверить основания обработки данных, категории собираемой информации, сроки хранения, доступ, порядок обезличивания, возможность отзыва согласия для чувствительных процедур и пределы использования результатов. Такой шаг особенно важен при анализе цифрового следа и применении ИИ в самой диагностике.

Если диагностика проводится внешними экспертами, организация должна сохранить контроль над целями, данными и интерпретацией. Внешний эксперт может обеспечить методическую независимость, но не должен получать избыточный доступ к персональным данным и не должен подменять управленческую ответственность организации. Результаты должны возвращаться в организацию в форме, пригодной для развития.

Для устойчивого применения методики необходимо подготовить внутренних модераторов диагностики. Они должны понимать модель цифрового сознания, уметь объяснять цели участникам, проводить командные обсуждения, фиксировать результаты, соблюдать конфиденциальность и переводить выводы в планы развития. Это снижает зависимость организации от внешних процедур и укрепляет собственную субъектность.

Итоговое требование к диагностическим инструментам можно сформулировать следующим образом: они должны быть достаточно строгими, чтобы давать надежные управленческие выводы, и достаточно гуманными, чтобы поддерживать развитие, доверие и ответственность. Именно этот баланс отличает диагностику цифрового сознания от простого контроля цифровой активности.

При итоговой редакции диагностического инструмента полезно сохранять журнал изменений методики. В нем фиксируются версии анкеты, изменения шкал, замены кейсов, корректировки весов, причины этих изменений и дата

введения новой версии. Такой журнал необходим для сопоставимости динамики и для защиты результатов от произвольного толкования.

Еще одно условие качества – обучение участников чтению результатов. Сотрудник, команда или руководитель могут неправильно понять индекс, если видят только число. Поэтому к каждому отчету следует прикладывать пояснение: что означает уровень, какие ограничения есть у оценки, как читать профиль, какие действия рекомендуются и куда обратиться за консультацией.

Диагностика цифрового сознания не должна конкурировать с действующими системами оценки персонала, качества или информационной безопасности. Напротив, она должна связывать их. Результаты могут использоваться для уточнения программ обучения, корректировки цифровых регламентов, разработки карт рисков и улучшения сервисов, но не должны подменять профессиональную оценку деятельности.

Важна и языковая ясность диагностических материалов. Термины «данные», «цифровой след», «управление ИИ», «человеческая проверка», «этический риск», «инцидент», «цифровая память» должны быть объяснены в глоссарии. Непонятный язык снижает доверие к диагностике и провоцирует формальные ответы.

Организация может начинать с упрощенной диагностической модели, но должна сохранять целевую архитектуру. На первом этапе достаточно базовой анкеты, нескольких кейсов и экспертной оценки ключевых регламентов. На втором этапе добавляется командная диагностика. На третьем – организационный индекс, цифровая зрелость, триангуляция и годовой цикл улучшений.

Следовательно, разработка диагностических инструментов является не технической процедурой, а частью методологии формирования цифрового сознания. Способ измерения влияет на то, как организация понимает цифровое развитие, какие нормы закрепляет и какие действия считает приоритетными.

Для пилотного внедрения целесообразно выбирать не самую проблемную и не самую сильную команду, а подразделение со средней цифровой готовностью и мотивированным руководителем. Это позволяет проверить методику в реалистичных условиях, не искажая результаты экстремальными факторами.

После пилота следует провести методическую сессию с участниками. На ней обсуждаются понятность вопросов, справедливость кейсов, достаточность обратной связи, продолжительность процедуры и доверие к интерпретации. Эти данные важны не меньше, чем сами баллы, потому что они показывают качество диагностической среды.

Если организация планирует использовать диагностику ежегодно, необходимо закрепить календарь. В нем указываются период подготовки, информирование участников, сбор данных, обработка, обсуждение результатов,

утверждение планов развития, реализация действий и промежуточная проверка. Регулярность делает диагностику частью организационного управления.

Индикаторы цифрового сознания должны быть связаны с реальными цифровыми рисками. Если в организации часто возникают утечки, ошибки в данных, спорные ИИ-ответы, перегрузка каналов или потеря цифровых артефактов, эти ситуации должны быть отражены в кейсах и диагностических вопросах. Тогда оценка становится практически значимой.

Наконец, в диагностике следует сохранять пространство для качественного суждения. Число помогает увидеть контур проблемы, но окончательный управленческий вывод требует контекста: роли сотрудника, зрелости команды, состояния архитектуры, характера процессов и уже реализованных изменений. Поэтому индекс должен быть началом разговора, а не его завершением.

Данный подход делает главу 5 методическим мостом между моделью цифрового сознания и последующей технологией внедрения. Он показывает, что измерение не является самостоятельной целью: оно нужно для того, чтобы организация научилась лучше видеть себя в цифровой среде и осознанно управлять собственным развитием.

ИТОГИ ГЛАВЫ

Диагностическая рамка объединяет ИЦСС, ИЦСК и ИОЦС, пятиуровневую шкалу зрелости и методы триангуляции данных. Индексы предназначены для выявления дефицитов, выбора мер развития и мониторинга динамики, а не для автоматического ранжирования сотрудников или подразделений.

Управленческий переход к главе 6: результаты диагностики становятся основанием для выбора приоритетов, проектирования пилота, распределения ответственности и решения о корректировке либо масштабировании.

***Интерактивное сопровождение.** В цифровом руководстве размещены онлайн-диагностика, калькуляторы индексов, рубрики оценивания, формы обратной связи и шаблоны диагностического отчета.*

ГЛАВА 6. УПРАВЛЕНИЕ ВНЕДРЕНИЕМ МОДЕЛИ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

«Инновация – это идея, практика или объект, воспринимаемые как новые отдельным человеком или другой единицей принятия».

Эверетт Роджерс

Управленческий вопрос главы. Как перевести методологическую модель в контролируемую программу изменений с понятными этапами, ответственными, ресурсами и критериями решений?

Управленческий результат главы. Цикл внедрения от подготовки и входной диагностики до пилотирования, мониторинга, масштабирования и институционализации, описанный через цели, роли, обязательные артефакты, показатели и критерии перехода (рисунок 6.1).

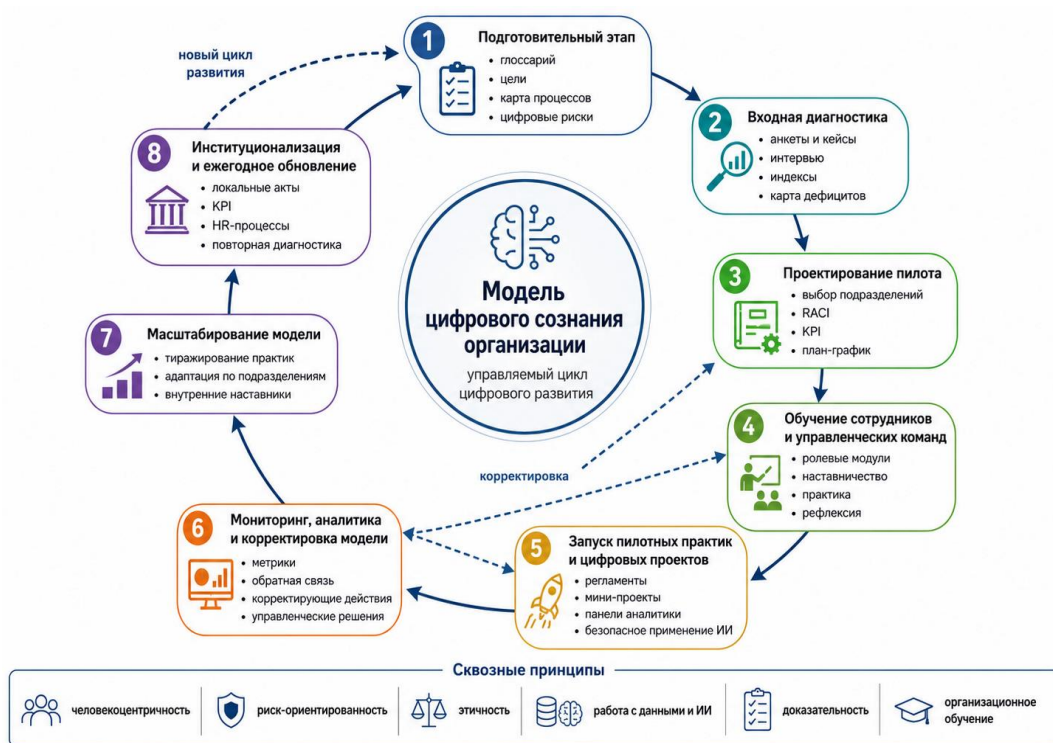


Рисунок 6.1 – Цикл внедрения модели цифрового сознания организации

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рисунок 6.1 представляет внедрение как замкнутый управленческий цикл. Переход между этапами допускается только после проверки артефактов и принятия управленческого решения; результаты мониторинга возвращаются в подготовительный и диагностический контуры.

6.1. ПОДГОТОВИТЕЛЬНЫЙ ЭТАП: ГЛОССАРИЙ, ЦЕЛИ, КАРТА ПРОЦЕССОВ И ЦИФРОВЫХ РИСКОВ

Подготовительный этап определяет качество всей последующей работы. Если организация начинает с обучения отдельным сервисам или с запуска показательного проекта, не согласовав понятия, цели и границы ответственности, внедрение быстро распадается на несвязанные инициативы. Поэтому первая задача – сформировать единый язык проекта. Рабочий глоссарий должен содержать операциональные определения цифрового сознания, цифровой зрелости, цифровой дееспособности, цифрового следа, цифрового риска, управления данными, управления ИИ и цифрового доверия. Термины фиксируются не ради академической полноты, а для предотвращения управленческих конфликтов: одинаковые слова должны обозначать одинаковые объекты и процедуры [80; 82].

Второй результат подготовки – формальный мандат внедрения. Руководитель организации назначает спонсора, утверждает куратора, состав межфункциональной рабочей группы и границы проекта. В рабочую группу включаются представители руководства, проектного офиса, кадровой функции, корпоративного обучения, ИТ, информационной безопасности, аналитики и данных, юридической службы, а также руководители потенциальных пилотных подразделений. Такая композиция исключает подмену модели ИТ-проектом либо учебной кампанией. Структура подготовительного этапа и его обязательные результаты представлены на рисунке 6.2.

Цели внедрения должны формулироваться как ожидаемые организационные результаты. Недостаточно поставить цель «повысить цифровую грамотность». Корректная постановка включает объект изменения, желаемое поведение, управленческий эффект, ограничения и горизонт измерения. Например: повысить качество проверки ИИ-результатов в аналитических документах; снизить долю несанкционированных цифровых сервисов; сформировать владельцев критичных данных; сократить коммуникационную перегрузку; внедрить регулярный разбор цифровых инцидентов. Для каждой цели задаются исходное значение, целевое значение, владелец и источник данных.

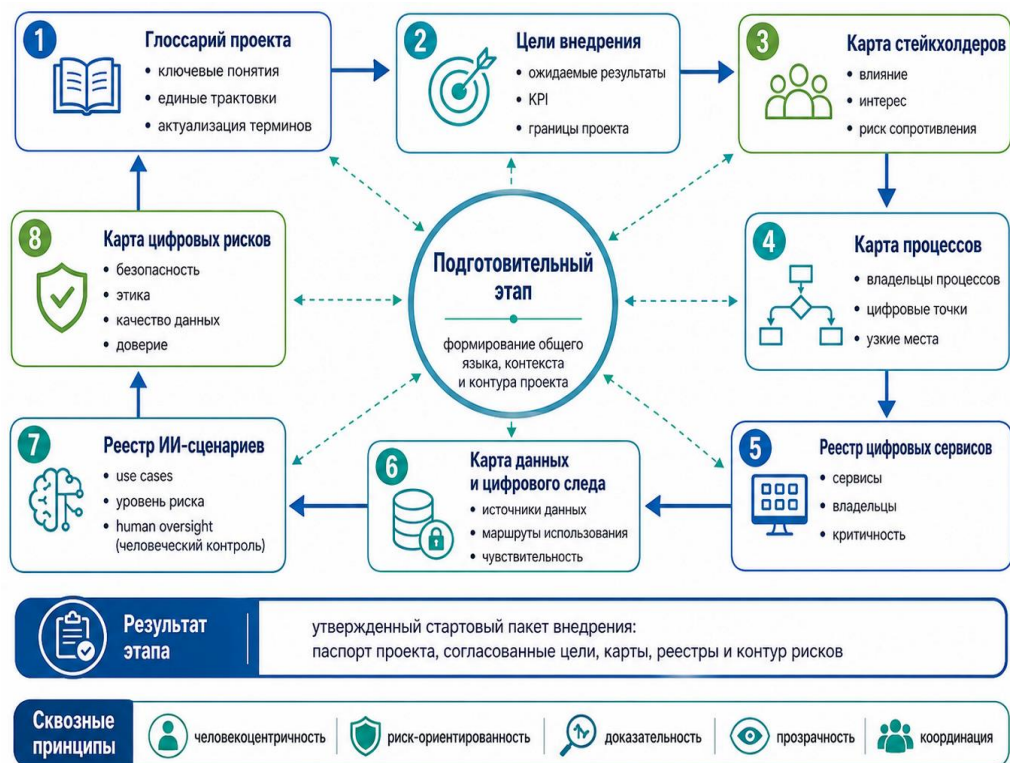


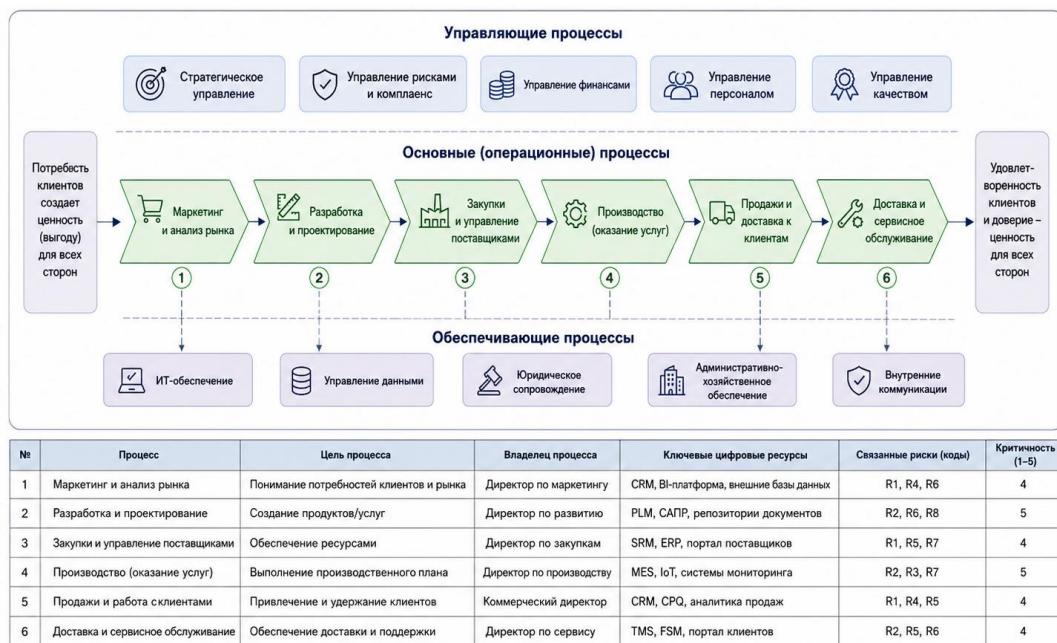
Рисунок 6.2 – Структура подготовительного этапа внедрения модели цифрового сознания организации

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рисунок 6.2 показывает состав подготовительного этапа: согласование понятий, постановку целей, картирование процессов и первичную оценку цифровых рисков.

Цели внедрения должны формулироваться как ожидаемые организационные результаты. Недостаточно поставить цель «повысить цифровую грамотность». Корректная постановка включает объект изменения, желаемое поведение, управленческий эффект, ограничения и горизонт измерения. Например: повысить качество проверки ИИ-результатов в аналитических документах; снизить долю несанкционированных цифровых сервисов; сформировать владельцев критичных данных; сократить коммуникационную перегрузку; внедрить регулярный разбор цифровых инцидентов. Для каждой цели задаются исходное значение, целевое значение, владелец и источник данных.

Карта процессов связывает модель цифрового сознания с реальной деятельностью. Пример построения карты процессов организации представлен на рисунке 6.3.



Коды рисков (Пример): R1 – информационная безопасность; R2 – ошибки данных; R3 – сбои ИТ-систем; R4 – недостаточная аналитика; R5 – риски поставщиков; R6 – недостаточное требование; R7 – репутационные риски; R8 – киберриски; R9 – недоступность ресурсов.

Рисунок 6.3 – Пример карты процессов организации
 Источник: составлено авторами на основе [75; 81; 84; 101; 122]

Рисунок 6.3 показывает, как ключевой процесс раскрывается через этапы, участников, цифровые сервисы, данные, ИИ-сценарии, риски и контрольные точки. Карта связывает диагностику цифрового сознания с конкретной деятельностью организации.

Для каждого ключевого процесса фиксируются владелец, входы и выходы, цифровые сервисы, используемые данные, ИИ-сценарии, точки принятия решений, потенциальные риски и проблемные зоны. На этой основе становится видно, где дефицит цифрового сознания проявляется как операционная потеря: дублирование действий, некачественные данные, некритичное использование ИИ, неясная ответственность, ошибки доступа или цифровая перегрузка.

Реестр цифровых сервисов необходим для выявления официальной и теневой цифровой инфраструктуры. Пример структуры реестра цифровых сервисов представлен на рисунке 6.4.

№	Цифровой сервис	Назначение	Владелец сервиса	Пользователи	Ключевые данные	Критичность	Основные риски	Статус	Потенциал ИИ
1	CRM-система	Управление клиентами	Директор по продажам	Отдел продаж, маркетинг	Данные клиентов, сделки	высокая	Утечка данных, дублирование	действует	рекомендации, прогноз продаж
2	ERP-система	Управление ресурсами	Финансовый директор	Финансы, закупки, склад, производство	Финансы, запасы, заказы	высокая	Сбои процессов, ошибки данных	действует	прогноз спроса, оптимизация
3	Система электронного документооборота	Создание и согласование документов	Юридический директор	Все подразделения, партнёры	Документы, договоры	высокая	Потеря документов, доступ	требует обновления	классификация, извлечение данных
4	Корпоративный портал	Единая точка доступа к сервисам	Директор по информационным технологиям	Все сотрудники	Новости, политики, регламенты	средняя	Устаревшая информация	частично интегрирован	поиск, ассистент
5	Система управления задачами и проектами	Планирование и контроль работ	Операционный директор	Руководители, команды проектов	Задачи, сроки, статусы	средняя	Срывы сроков, некорректные оценки	пилот	прогноз сроков, приоритизация
6	Платформа бизнес-аналитики	Анализ и визуализация данных	Директор по аналитике	Руководство, аналитики	В-отчёты, KPI, витрины данных	средняя	Качество данных, интерпретации	действует	поиск аномалий, аналитика
7	HRM-система	Управление персоналом	Директор по персоналу	HR, руководители, сотрудники	Данные сотрудников, компетенции	средняя	Доступ к данным, актуальность	требует обновления	прогноз текучести, рекомендации
8	Сервис коммуникаций и видеосвязи	Коммуникации и совместная работа	Директор по информационным технологиям	Все сотрудники, партнёры	Сообщения, звонки, файлы	средняя	Безопасность, зависимость от сети	частично интегрирован	ассистент, перевод речи, резюме встреч



Легенда статусов:

действует
 требует обновления
 пилот
 частично интегрирован

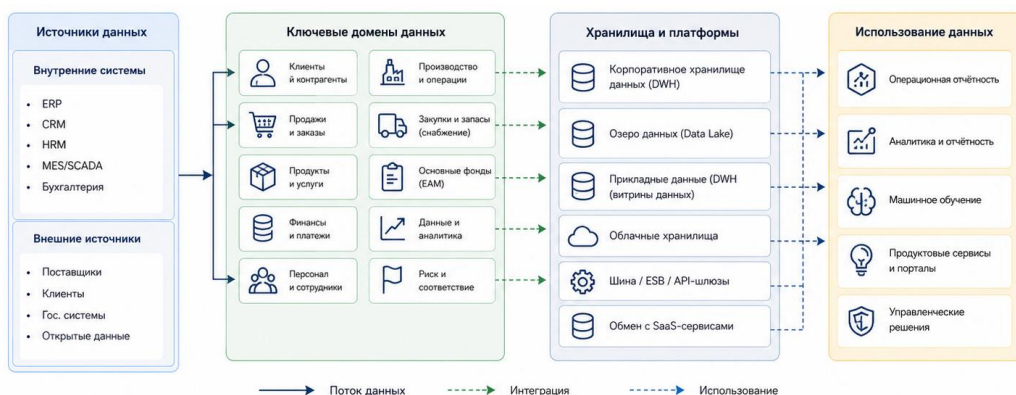
Рисунок 6.4 – Пример реестра цифровых сервисов организации

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рисунок 6.4 демонстрирует структуру реестра цифровых сервисов: назначение, владельцев, пользователей, категории данных, критичность, статус и технический долг. Реестр позволяет выявлять дублирование, теневые инструменты и инфраструктурные зависимости.

В нем указываются назначение сервиса, владелец, группы пользователей, интеграции, критичность, категории данных, условия поддержки и известные риски. Отдельно фиксируются внешние сервисы и личные инструменты сотрудников. Это позволяет обнаружить теневые ИТ- и ИИ-практики до того, как они станут источником утечки данных или разрыва процессов. В международных системах управления ИТ, информационной безопасностью и ИИ инвентаризация активов и контекста выступает исходным условием управляемости [81; 83; 102].

Карта данных описывает источники, потоки, владельцев, качество, чувствительность, сроки хранения и ограничения использования. Пример карты данных организации представлен на рисунке 6.5.



Класс данных	Примеры данных	Уровень чувствительности	Правила доступа	Срок хранения	Ответственный
Персональные данные	ФИО, контактные данные, документы	Высокий	Ролевой доступ, шифрование	По законодательству	Директор по персоналу
Коммерческие данные	Договоры, цены, условия, клиенты	Высокий	Ролевой доступ, NDA	5 лет	Коммерческий директор
Финансовые данные	Платежи, отчетность, бюджеты	Высокий	Ролевой доступ, контроль изменений	7 лет	Финансовый директор
Производственные данные	Параметры, смены, оборудование	Средний	Доступ по ролям	3 года	Директор по производству
Операционные данные	Заявки, заказы, статусы	Средний	Доступ по ролям	2 года	Руководитель процессов
Неиссущественные данные	Справочники, публичные данные	Низкий	Открытый доступ	Без ограничений	Владелец данных

NDA – соглашение о неразглашении информации | EAM – управление активами предприятия | ESB – корпоративная сервисная шина | API – программный интерфейс приложений

Рисунок 6.5 – Пример карты данных организации
Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рисунок 6.5 систематизирует категории данных, их источники, владельцев, характеристики качества, правовой режим, сроки хранения и ограничения использования. Карта служит основой управления данными и оценки связанных с ними рисков. Реестр ИИИ-сценариев дополняет ее сведениями о цели применения ИИИ, типе входных данных, ожидаемом результате, способе проверки, уровне риска и ответственном лице. Важно фиксировать не только утвержденные, но и фактически используемые сценарии. Пример реестра ИИИ-сценариев представлен на рисунке 6.6.

№	Наименование ИИ-сценария	Цель и бизнес-ценность	Данные и источники	Модель / подход	Ответственный	Этап внедрения	Риски (коды)	Ожидаемый эффект (KPI)
1	Прогноз спроса	Повышение точности планирования и сокращение излишков и дефицита	История продаж (ERP, CRM), календарные данные, маркетинг	ML: модели временных рядов (Prophet, XGBoost, Recurrent NN)	Директор по коммерции (финансы)	Пилот	R2, R4, R6	Снижение отклонений прогноза на 20%
2	Сегментация клиентов	Персонализация предложений и рост конверсии	CRM, история покупок, поведение на сайте	ML: кластеризация (K-means)	Директор по маркетингу	Пилот	R1, R4	Рост конверсии на 10%
3	Рекомендательная система	Увеличение среднего чека и кросс-продажи	CRM, каталог, покупки, поведение	ML: коллаборативная фильтрация	Коммерческий директор	Внедрение	R1, R4	Рост среднего чека на 12%
4	Распознавание документов	Автоматизация обработки договоров и счетов	Сканы документов, ЭДО, почта	NLP + OCR, классификация	Директор по ОЦО	Пилот	R1, R2, R6	Сокращение ручной обработки на 60%
5	Интеллектуальный чат-ассистент	Снижение нагрузки на сотрудников поддержки	База знаний, регламенты, история обращений	LLM (RAG), контролируемые диалоги	Руководитель службы поддержки	Внедрение	R1, R5, R6	Снижение времени ответа на 30%
6	Анализ рисков поставщиков	Повышение надежности и снижение сбоя поставок	Данные поставщиков, финансы, новости, реестры	ML: классификация (GBM, XGBoost)	Директор по закупкам	Пилот	R2, R5	Снижение простоев поставок на 15%
7	Прогноз оттока сотрудников	Снижение текучести и удержание ключевых специалистов	HRIS, оценки, опросы, активности	ML: классификация (Logistic Regression, GBM)	Директор по персоналу	Внедрение	R1, R5	Снижение текучести на 8%
8	Обнаружение аномалий в платежах	Повышение финансовой безопасности и снижение мошенничества	Платежи, транзакции, история инцидентов	ML: детекция аномалий (Autoencoder, Isolation Forest)	Руководитель финансового контроля	Внедрение	R1, R2, R6	Снижение мошеннических операций на 25%
9	Классификация обращений	Автоматизация маршрутизации и приоритезация заявок	Тексты обращений, теги, история	NLP: классификация (BERT, FastText)	Руководитель службы поддержки	Пилот	R1, R4	Рост доли корректной маршрутизации до 90%
10	Мониторинг репутации бренда	Вовремя выявлять негатив и управлять репутацией	Соцсети, СМИ, отзывы, форумы	NLP: анализ тональности и тем (BERT, LDA)	Директор по маркетингу	Пилот	R1, R5	Сокращение времени реакции на негатив на 40%

Коды рисков см. в Карте рисков (раздел 6.1). Этапы внедрения: пилот – пилот, внедрение – масштабирование, эксплуатация – эксплуатация.

R1 – информационная безопасность **R2** – качество и достоверность данных **R3** – этика и предвзятость **R4** – непрозрачность алгоритмов
R5 – риск поставщиков **R6** – несоответствие требованиям **R7** – технологические сбои **R8** – утечка данных **R9** – нарушение условий договоров

Рисунок 6.6 – Пример реестра ИИ-сценариев

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рисунок 6.6 показывает, как фиксируются цель ИИ-сценария, входные данные, ожидаемый результат, способ проверки, уровень риска и ответственное лицо. Реестр обеспечивает прозрачность и управляемость фактического применения ИИ.

Карта цифровых рисков формируется на пересечении процессов, данных, сервисов, ИИ и человеческого поведения. Пример карты цифровых рисков организации представлен на рисунке 6.7.

Риски оцениваются по вероятности и влиянию, после чего назначаются владельцы и меры контроля. Минимальный перечень включает риски некачественных данных, несанкционированного использования ИИ, утечки информации, алгоритмической ошибки, цифрового надзора, коммуникационной перегрузки, зависимости от поставщика, отсутствия владельца решения и сопротивления изменениям.

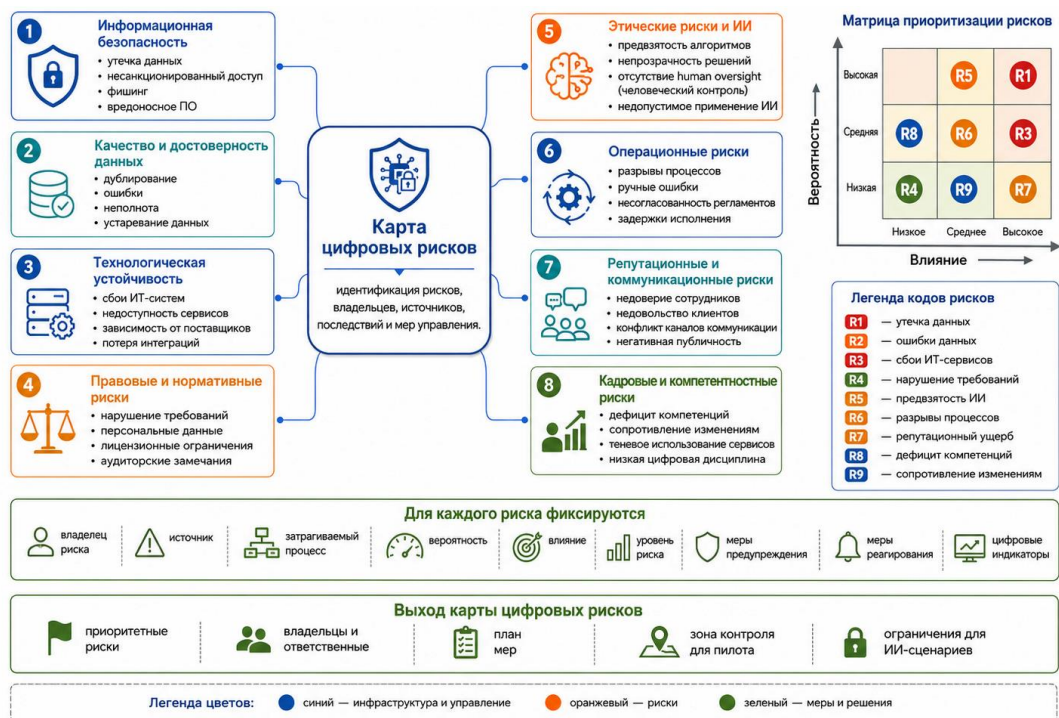


Рисунок 6.7 – Пример карты цифровых рисков организации
Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рисунок 6.7 объединяет источники цифровых рисков, их индикаторы, вероятность и последствия, меры контроля и владельцев. Карта используется для приоритизации профилактических и корректирующих действий.

Для приоритизации может применяться показатель $R = P \times I$, где P – оценка вероятности по шкале 1–5, I – оценка влияния по шкале 1–5. Значения 1–5 трактуются как низкий риск, 6–12 – средний, 15–25 – высокий.

Риск-карта не подменяет экспертное обсуждение. Высокая числовая оценка требует проверки причин, затрагиваемых стейкхолдеров и возможных вторичных последствий. Для сценариев, связанных с правами людей, персональными данными, значимыми финансовыми или кадровыми решениями, применяется повышенный уровень контроля независимо от средней расчетной оценки.

Подготовительный этап завершается комплектом артефактов: паспортом проекта, глоссарием, картой стейкхолдеров, картой процессов, реестром сервисов, картой данных, реестром ИИ-сценариев, картой цифровых рисков и коммуникационным сообщением сотрудникам. Критерием перехода к диагностике является не наличие черновиков, а подтвержденная полнота: назначены владельцы, согласованы цели, определены ограничения использования данных, утвержден порядок доступа к результатам диагностики.

Коммуникация на старте должна прямо объяснять развивающий характер проекта. Сотрудники должны знать, что диагностика не предназначена для скрытого ранжирования или дисциплинарных санкций, какие данные будут собираться, кто получит доступ, как результаты будут агрегироваться и каким образом они будут использованы для обучения и улучшения процессов. Доверие на подготовительном этапе является не «мягким» условием, а ресурсом достоверности последующей диагностики.

6.2. ВХОДНАЯ ДИАГНОСТИКА ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

Входная диагностика фиксирует исходное состояние, относительно которого будут оцениваться результаты пилота и последующего масштабирования. Она опирается на методику главы 5 и сохраняет три уровня измерения: сотрудник, команда, организация. Индивидуальный индекс цифрового сознания сотрудника рассчитывается по формуле $ИЦСС = (\sum w_i \times C_i / \sum w_i \times C_{max}) \times 100$. Командный индекс: $ИЦСК = (\sum D_j / D_{max}) \times 100$. Организационный индекс: $ИОЦС = (\sum w_j \times O_j / \sum w_j \times O_{max}) \times 100$. На этапе внедрения индексы используются не как рейтинги, а как базовые профили дефицитов и сильных сторон.

Единая шкала интерпретации 0–100 позволяет сопоставлять уровни: 0–20 – фрагментарный; 21–40 – базовый; 41–60 – функциональный или координируемый; 61–80 – осознанный или интегрированный; 81–100 – трансформационный, адаптивно-рефлексивный. При интерпретации нельзя ограничиваться средним баллом: одинаковый итоговый индекс может скрывать разные конфигурации дефицитов.

Диагностика строится на триангуляции. Опросы и самооценка выявляют установки и субъективную уверенность; кейсовые задания показывают способность действовать; интервью раскрывают контекст; аудит документов и процессов фиксирует формальную и фактическую институционализацию; экспертная оценка помогает интерпретировать сложные сценарии; ограниченный цифровой след подтверждает отдельные поведенческие паттерны. Значимый вывод должен подтверждаться как минимум двумя разнородными источниками.

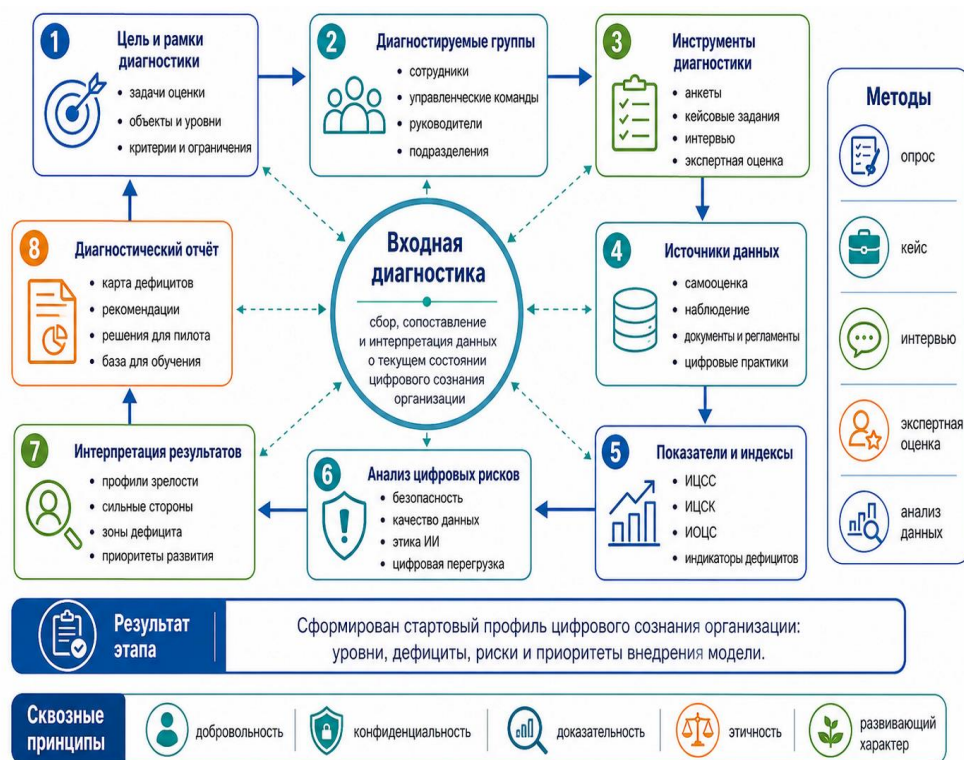


Рисунок 6.8 – Входная диагностика цифрового сознания организации

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рисунок 6.8 отражает последовательность входной диагностики: подготовку выборки, сбор и сопоставление данных, расчёт показателей и обсуждение результатов.

Выборка должна охватывать критические роли, типы подразделений и уровни управления. Если организация мала, возможна сплошная диагностика; в крупной организации используется стратифицированная выборка. Необходимо отдельно включать руководителей, владельцев процессов, специалистов по данным и ИИ, сотрудников с высокой цифровой нагрузкой и участников процессов с повышенным уровнем риска.

Диагностический паспорт содержит: цель измерения; уровни и компоненты; индикаторы; методы; выборку; сроки; правила конфиденциальности; порядок расчета; ограничения интерпретации; правила обратной связи. До запуска инструменты проходят содержательную экспертизу и пилотирование. Для опросников оценивается внутренняя согласованность, для экспертных шкал – межэкспертная согласованность, для кейсов – однозначность рубрик. Методическая надежность особенно важна, поскольку ошибочная диагностика может направить ресурсы в неверную область.

Цифровой след используется только как вторичный источник. Допустимы агрегированные данные о соблюдении рабочих маршрутов, использовании баз знаний, прохождении обязательного обучения, наличии процедур проверки и частоте инцидентов. Недопустимы скрытый мониторинг частной переписки, непрозрачное профилирование, выводы о лояльности и автоматические кадровые решения.

Результаты представляются в трех формах. Индивидуальная форма содержит конфиденциальный профиль развития сотрудника. Командная форма отражает согласованность цифровых практик, роли, коммуникацию, проверку данных и способность к обучению. Организационная форма показывает состояние стратегии, управления данными и ИИ, архитектуры, культуры, безопасности, развития персонала и рефлексивности. Для руководства формируется карта сильных сторон, критических дефицитов и рисков.

Приоритет пилота определяется не только по минимальным значениям. В расчет принимаются стратегическая значимость процесса, уровень риска, готовность руководителя, возможность измерить эффект и переносимость результата. Дефицит с низким баллом, но слабой связью со стратегией может быть отложен; дефицит со средним баллом, но высоким риском для данных или доверия получает высокий приоритет.

Диагностический отчет включает описание методики, охват, ограничения, значения индексов, профили компонентов, расхождения между источниками, карту рисков и рекомендации. Обязателен раздел «что диагностика не позволяет утверждать», предотвращающий чрезмерные выводы. Управленческое обсуждение проводится с участием руководства, рабочей группы и представителей подразделений. Результатом становится решение о целях пилота, критериях выбора подразделений и наборе мер поддержки.

Входная диагностика завершается формированием baseline – исходной линии. Она должна быть воспроизводимой: повторная оценка использует сопоставимые инструменты, периоды и правила расчета. Изменение индекса рассматривается вместе с изменением поведения, рисков и процессов; рост самооценки без подтверждения кейсами или практикой не считается достаточным доказательством эффекта.

6.3. ПРОЕКТИРОВАНИЕ ПИЛОТА И ВЫБОР ПОДРАЗДЕЛЕНИЙ

Пилотирование представляет собой контролируемое внедрение ограниченного набора практик в выбранном организационном контуре. Его задача – проверить не абстрактную применимость модели, а конкретные причинно-следственные связи: приводит ли обучение и изменение правил к улучшению цифрового поведения; уменьшаются ли риски; повышается ли качество решений; сохраняется ли доверие; воспроизводим ли результат. Пилот

должен иметь границы, срок, владельца, измеримые исходы и условия остановки.

Критерии выбора подразделения включают управленческую готовность руководителя, наличие реальных цифровых задач, стратегическую значимость, типичность процессов, измеримость результатов, допустимость риска, готовность сотрудников, наличие сервисов и данных, а также возможность масштабирования опыта. Оптимальным является подразделение с реальной проблемой и достаточной готовностью, но без критически высокой цены ошибки. Логика проектирования пилота и выбора подразделения представлена на рисунке 6.9



Рисунок 6.9 – Проектирование пилота и выбор подразделений

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рисунок 6.9 раскрывает логику выбора пилотного контура: определение задачи, подразделения, участников, ограничений, ресурсов и критериев завершения.

Для сравнительной оценки подразделений может применяться интегральный рейтинг готовности пилота: $G_p = \sum a_k \times g_k / \sum a_k$, где g_k – оценка критерия по шкале 0–5, a_k – вес критерия. Рекомендуемая интерпретация: менее 2,0 – пилот нецелесообразен без предварительной подготовки; 2,0–3,4 – условная

готовность; 3,5–4,2 – высокая готовность; более 4,2 – приоритетная зона пилота. Отдельный запрет применяется к подразделениям, где риск для прав, безопасности или непрерывности деятельности невозможно снизить до приемлемого уровня.

Паспорт пилота фиксирует проблему, цель, гипотезу ценности, границы, состав участников, перечень практик, исходные и целевые показатели, роли, риски, ресурсы, коммуникационный план, порядок мониторинга и критерии решения о масштабировании. Гипотеза формулируется проверяемо: «если внедрить ролевое обучение, чек-лист проверки ИИ и обязательное экспертное подтверждение, то доля непроверенных ИИ-результатов снизится не менее чем на 30 % за три месяца».

Ролевая матрица RACI предотвращает размывание ответственности. Для каждого действия определяется исполнитель (R), лицо, несущее итоговую ответственность (A), консультируемые участники (C) и информируемые лица (I). Спонсор отвечает за ресурс и приоритет; куратор – за сквозную координацию; руководитель подразделения – за внедрение в процесс; HR и обучение – за развитие компетенций; ИТ, ИБ, данные, ИИ и юристы – за специализированные контроли; наставники – за повседневную поддержку.

В пилоте необходимо различать показатели деятельности и показатели результата. К первым относятся участие в обучении, число консультаций, доля обновленных документов. Ко вторым – изменение качества проверки данных, снижение инцидентов, сокращение времени процесса без потери качества, повышение доверия, устойчивое соблюдение новых норм. Решение о масштабировании не может приниматься только по показателям активности.

Коммуникационный план пилота описывает аудитории, ключевые сообщения, каналы, периодичность, ответственных и механизм обратной связи. Сотрудникам объясняются цели, ожидаемые изменения, границы цифрового мониторинга, способы обращения за поддержкой и возможность сообщать о проблемах. Руководителям – критерии успеха, необходимость выделения времени и запрет на использование диагностических данных для неоговоренных кадровых решений.

Риск-журнал пилота ведется с первого дня. Он содержит риск, триггер, вероятность, влияние, владельца, профилактику, план реагирования и статус. Особое внимание уделяется формализации, перегрузке, сопротивлению среднего звена, некачественным данным, теневому ИИ, цифровому надзору и зависимости результата от одного лидера или эксперта.

Пилот должен включать контрольные точки: готовность к обучению; готовность к запуску; промежуточный обзор; итоговую оценку. На каждой точке возможны решения «продолжить», «скорректировать», «приостановить», «закрыть». Принцип поэтапного допуска снижает риск масштабирования

ошибочной практики. Ошибка в пилоте рассматривается как источник обучения при условии, что она своевременно обнаружена, не скрыта и не повлекла недопустимого ущерба.

Критерий успешности пилота – не максимальный рост всех показателей, а доказанная полезность, безопасность и воспроизводимость. Пилот считается готовым к масштабированию, если достигнуты ключевые результаты, отсутствуют неустраненные критические риски, понятны условия переноса, подготовлены методические материалы и назначены владельцы дальнейшего распространения.

6.4. ОБУЧЕНИЕ СОТРУДНИКОВ И УПРАВЛЕНЧЕСКИХ КОМАНД

Обучение является центральным механизмом внедрения, но не заменяет изменение процессов и правил. Его задача – сформировать знания, навыки, установки и поведенческие нормы, необходимые для конкретных ролей. Универсальный курс для всех категорий участников методически слаб: сотруднику нужны безопасные сценарии цифрового действия, руководителю – качество решений и управление рисками, наставнику – сопровождение и фасилитация, специалистам ИТ, ИБ, данных и ИИ – проектирование контролей и пользовательской поддержки.

Ролевая модель обучения строится на диагностических профилях. Для сотрудников базовые модули включают цифровую дееспособность, критическую работу с информацией, грамотность в области данных и ИИ, цифровую этику, безопасность, коммуникацию и рефлекссию. Для руководителей добавляются цифровое лидерство, интерпретация аналитики, управление ИИ, оценка последствий, цифровая нагрузка и организация обратной связи. Ролевая модель обучения сотрудников и управленческих команд представлена на рисунке 6.10.

Программа обучения строится по циклу «знание – практика – рефлексия – закрепление». Знание дает общие правила и понятия; практика переносит их в реальные задачи; рефлексия позволяет разобрать ошибки и последствия; закрепление встраивает новую норму в процесс, чек-лист, шаблон или роль. Отсутствие любого элемента снижает эффект: знание без практики остается декларацией, практика без рефлексии воспроизводит ошибки, рефлексия без закрепления не меняет организационную систему.



Рисунок 6.10 – Обучение сотрудников и управленческих команд

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Рекомендуются короткие модули, кейсовые задания, тренажеры, рабочие лаборатории, наставничество и групповые разборы. Материал должен опираться на реальные процессы и риски организации. Например, модуль по ИИ включает классификацию данных, проверку фактов, фиксацию человеческого решения и анализ сценария утечки; модуль по цифровой коммуникации – правила каналов, фиксации решений и снижения уведомительной нагрузки.

Индивидуальный план развития связывает диагностический дефицит с конкретным действием, сроком и способом подтверждения. Командный план развития фиксирует общие правила: где хранятся документы, кто проверяет данные, как применяется ИИ, как оформляется решение, когда проводится ретроспектива. Планы не должны превращаться в бюрократический отчет; их назначение – обеспечить перенос обучения в работу.

Для оценки результата обучения используется многоуровневая логика: реакция участников; освоение знаний и кейсов; изменение поведения; организационный эффект. Показатель результативности переноса может рассчитываться как $K_{пер} = N_{п} / N_{о} \times 100 \%$, где $N_{п}$ – число освоенных практик,

подтвержденных в работе, Но – число запланированных практик. Значение ниже 50 % указывает на слабый перенос, 50–74 % – частичный, 75–89 % – устойчивый, 90–100 % – высокий.

Цифровые наставники обеспечивают повседневную поддержку. Их функция – не выполнять работу за коллег, а помогать применять правила, разбирать затруднения, направлять к специалистам и фиксировать повторяющиеся барьеры. Наставники проходят отдельную подготовку по фасилитации, этике помощи, границам ответственности, работе с сопротивлением и передаче обратной связи рабочей группе.

Чтобы институт наставничества не стал формальным, определяются нагрузка, время, каналы консультации, супервизия и показатели качества. Количество консультаций само по себе не является результатом: рост обращений может отражать как полезность поддержки, так и плохой дизайн процесса. Поэтому анализируются темы запросов, повторяемость проблем, скорость решения и снижение потребности в помощи по типовым действиям.

Управленческая команда обучается через стратегические сессии и разбор решений. Руководители рассматривают реальные кейсы качества данных, ИИ-рекомендаций, цифрового следа, безопасности и доверия; формируют правила эскалации и распределения ответственности. Важно, чтобы руководитель демонстрировал требуемое цифровое поведение: проверял основания, признавал неопределенность, не требовал скрытого мониторинга и выделял ресурсы на обучение.

Обучение завершается оценкой готовности к запуску практик. Участники должны не только пройти модули, но и выполнить практические задания, знать каналы поддержки, понимать ограничения данных и ИИ, уметь применять чек-листы и объяснять собственную ответственность. Управленческое решение о запуске принимается при подтвержденной готовности ключевых ролей и наличии организационных условий.

6.5. ЗАПУСК ПИЛОТНЫХ ПРАКТИК И ЦИФРОВЫХ ПРОЕКТОВ

На этапе запуска цифровое сознание превращается из учебного содержания в измененный способ работы. Каждая пилотная практика должна быть встроена в конкретный процесс и иметь владельца, рабочий регламент, инструменты поддержки, критерии качества и способ фиксации отклонений. Типовые практики включают проверку ИИ-результатов, единый порядок работы с документами, командные правила цифровой коммуникации, ведение реестра данных и ИИ-сценариев, безопасное использование внешних сервисов, регулярный разбор цифровых ошибок и мониторинг нагрузки.

Пилотные практики могут оформляться как мини-проекты. Карточка практики содержит проблему, новое правило, целевую группу, владельца,

необходимые сервисы, данные, риски, показатели, срок и способ обратной связи. Такой формат делает изменения наблюдаемыми и управляемыми. Последовательность запуска пилотных практик и цифровых проектов представлена на рисунке 6.11.

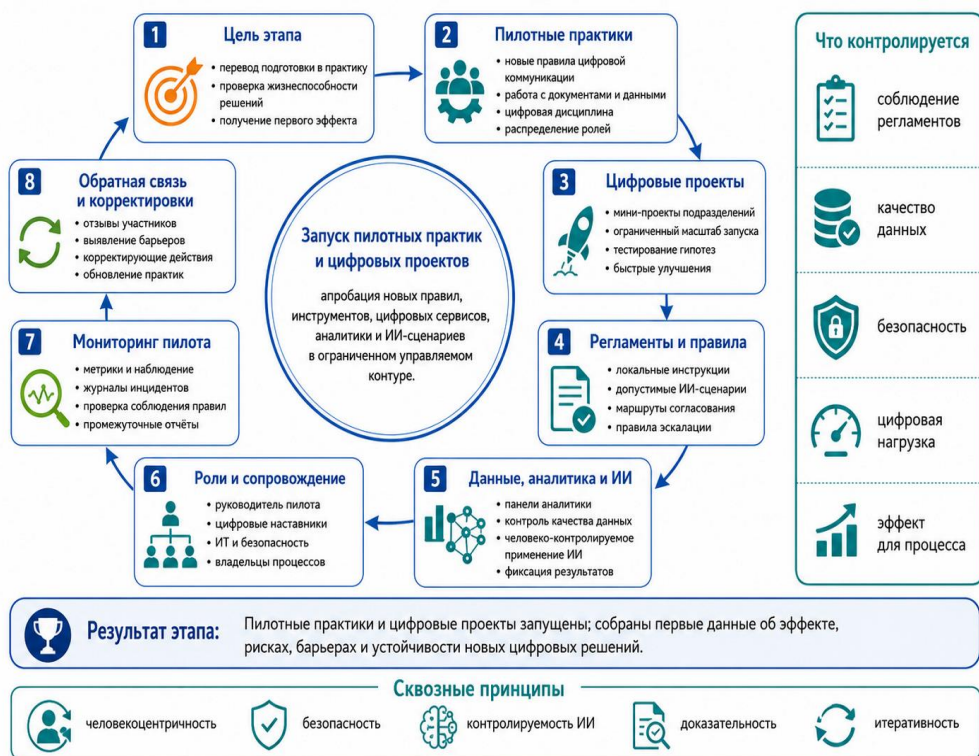


Рисунок 6.11 – Запуск пилотных практик и цифровых проектов

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Представленная схема показывает запуск пилота как управляемый эксперимент с утверждёнными сценариями, ответственными лицами, мерами безопасности и каналами обратной связи.

Диагностический дефицит переводится в управленческую гипотезу. Например, низкая информационно-аналитическая критичность переводится в практику обязательного указания источников и ограничений в аналитических записках; слабая командная цифровая память – в единый журнал решений и шаблон передачи знаний; высокий риск теневого ИИ – в список разрешенных инструментов, безопасную среду и процедуру регистрации сценариев.

Регламентные проекты должны избегать «бумажного» результата. Локальный документ считается внедренным, если сотрудники понимают правило, имеют удобный инструмент исполнения, получают поддержку, а соблюдение проверяется пропорционально и прозрачно. Если правило

невозможно выполнить в реальном процессе, оно требует корректировки, а не формального усиления контроля.

Для ИИ-проектов обязательны реестр сценариев, оценка риска, описание входных данных, критерии качества, человеческая проверка, журналирование и мониторинг последствий. Значимый ИИ-результат не считается готовым без подтверждения компетентным человеком. Доля проверенных результатов может использоваться как показатель: $K_{\text{проверки}} = N_{\text{провер}} / N_{\text{знач}} \times 100 \%$. Для высокорисковых сценариев целевое значение должно составлять 100 %.

Для проектов по данным назначаются владельцы, правила качества и порядок исправления дефектов. Показатели качества включают полноту, точность, актуальность, непротиворечивость и доступность. Решения на основе данных с критическими дефектами приостанавливаются до устранения проблемы.

Проекты цифровой коммуникации направлены на снижение шума и восстановление ясности. Устанавливаются назначение каналов, правила срочности, окна тишины, порядок фиксации решений, шаблоны совещаний и требования к передаче знаний. Эффект оценивается не количеством сообщений, а временем поиска информации, долей потерянных решений, нагрузкой встреч и удовлетворенностью команд.

Проекты безопасности сочетают технические контроли и поведенческие практики: многофакторную аутентификацию, классификацию данных, тренировки распознавания атак, понятный канал сообщения об инцидентах и разбор без обвинительной культуры. Снижение инцидентов анализируется вместе с готовностью сообщать о проблемах; искусственное уменьшение зарегистрированных событий может означать не улучшение, а потерю доверия.

В ходе пилота рабочая группа ведет журнал затруднений и инцидентов. Запись включает событие, контекст, последствия, первичную реакцию, коренную причину, корректирующее действие и урок для модели. Журнал используется не для поиска виноватых, а для улучшения процесса, обучения и обновления регламентов.

Запуск практик завершается промежуточным обзором. Анализируется, выполняются ли правила, создают ли они ценность, не возникли ли непредвиденные нагрузки, насколько достаточна поддержка, какие данные надежны. По итогам часть практик продолжается, часть упрощается или усиливается, а неэффективные решения прекращаются. Способность остановить неработающую практику является признаком цифрового сознания, а не неудачей проекта.

6.6. МОНИТОРИНГ, АНАЛИТИКА И КОРРЕКТИРОВКА МОДЕЛИ

Мониторинг обеспечивает управляемость внедрения и превращает пилот в цикл организационного обучения. Его задача – не собирать максимум показателей, а своевременно обнаруживать отклонения, риски и эффекты, требующие решения. Система мониторинга объединяет активность, качество практик, поведение, риски, обучение, управленческий эффект, цифровую нагрузку, доверие и безопасность. Для каждого показателя определяются владелец, источник, периодичность, допустимый диапазон и действие при отклонении.

Показатели активности отвечают на вопрос, что было сделано; показатели качества – насколько правильно; показатели результата – что изменилось; показатели устойчивости – сохраняется ли эффект. Например, число прошедших обучение относится к активности, балл кейса – к качеству освоения, доля проверенных ИИ-результатов – к поведению, снижение повторяющихся ошибок – к результату, сохранение эффекта через шесть месяцев – к устойчивости. Контур мониторинга, аналитики и корректировки модели представлен на рисунке 6.12.

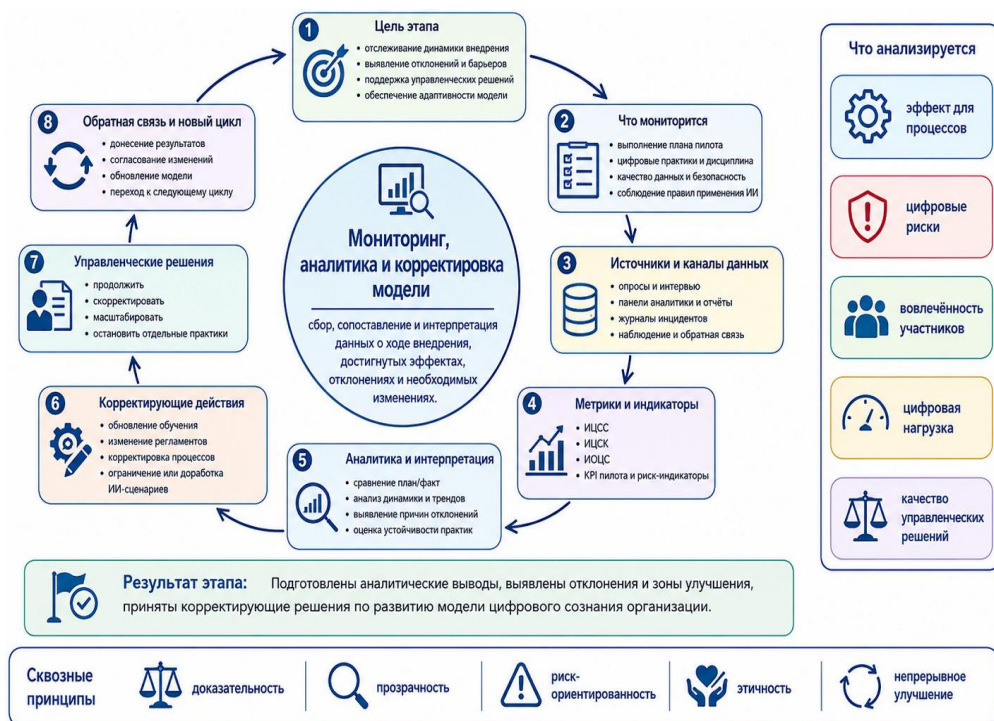


Рисунок 6.12 – Мониторинг, аналитика и корректировка модели

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Интегральный коэффициент реализации пилота может рассчитываться как $K_{пил} = 0,2A + 0,3Q + 0,3E + 0,2S$, где A – нормированная активность, Q – качество практик, E – организационный эффект, S – устойчивость и безопасность. Весовая схема является рекомендуемой и подлежит адаптации. Значение менее 50 баллов указывает на необходимость пересборки; 50–69 – частичный результат; 70–84 – достаточный результат при корректировках; 85–100 – высокая готовность к масштабированию.

Числовая оценка дополняется интерпретационным обзором. Команда мониторинга обсуждает причины изменений, качество данных, расхождения между источниками, непредвиденные последствия и обратную связь сотрудников. Такой обзор предотвращает управление по удобным метрикам, когда рост показателя скрывает ухудшение доверия или перегрузку.

Аналитическая панель пилота должна быть компактной. Она включает: динамику ИЦСС, ИЦСК и выбранных доменов ИОЦС; выполнение ключевых практик; качество данных; ИИ-контроли; инциденты; обучение и перенос; цифровую нагрузку; доверие; статус корректирующих действий. Персональные данные выводятся только там, где это необходимо и правомерно; для управленческого анализа предпочтительны агрегированные значения.

Особое внимание уделяется ведущим индикаторам – ранним сигналам будущего результата. К ним относятся снижение участия, рост повторяющихся вопросов, задержки решений, падение качества данных, увеличение обходных практик, жалобы на перегрузку и снижение готовности сообщать об ошибках. Реагирование на ведущие индикаторы дешевле и безопаснее, чем исправление уже наступившего ущерба.

Корректирующее действие оформляется карточкой: выявленная проблема; доказательства; коренная причина; предлагаемая мера; владелец; срок; ресурс; критерий закрытия. Закрытие подтверждается не отчетом о выполнении, а проверкой изменения. Если мера не дала эффекта, рабочая группа пересматривает гипотезу, а не продолжает действие автоматически.

Периодичность мониторинга зависит от риска и темпа изменений. Операционные показатели могут обновляться еженедельно, управленческий обзор проводится ежемесячно, а комплексная промежуточная диагностика – по завершении ключевой фазы. Высокорисковые ИИ- и информационные сценарии требуют более частого контроля.

Корректировка модели может затрагивать инструменты, обучение, роли, регламенты, архитектуру, показатели и саму диагностическую методику. Например, устойчивое расхождение самооценки и кейсов указывает на необходимость изменить обучение и интерпретацию ИЦСС; конфликт между подразделениями – пересмотреть командные роли; рост теневого ИИ – улучшить легитимные инструменты и поддержку.

Итоговый мониторинговый отчет должен отвечать на пять вопросов: что изменилось; чем это подтверждается; какие причины выявлены; какие риски остаются; какое решение требуется. Отчет, не приводящий к управленческому решению, не выполняет функции мониторинга. По итогам принимается решение о продлении пилота, корректировке, масштабировании либо прекращении отдельных практик.

6.7. МАСШТАБИРОВАНИЕ И ИНСТИТУЦИОНАЛИЗАЦИЯ МОДЕЛИ

Масштабирование начинается после доказательной оценки пилота. Оно не означает механического копирования практик во все подразделения. Каждая функция имеет собственные процессы, данные, риски и профессиональные нормы; поэтому перенос требует адаптации неизменного ядра и переменных элементов. К ядру относятся принципы, диагностическая логика, роли ответственности, этические ограничения и цикл мониторинга. К адаптируемым элементам – состав модулей, конкретные практики, показатели и локальные документы.

Перед масштабированием проводится оценка переносимости: какие условия обеспечили успех пилота, какие ресурсы уникальны, насколько результат зависит от конкретного руководителя, какие данные и сервисы доступны в других подразделениях, какие новые риски появятся. Практика, успех которой нельзя воспроизвести без уникального энтузиаста, требует дополнительной институционализации. Переход от пилотирования к масштабированию и институционализации представлен на рисунке 6.13.



Рисунок 6.13 – Масштабирование и институционализация модели

Источник: составлено авторами на основе [75; 81; 84; 101; 122].

Дорожная карта масштабирования группирует подразделения по типам и волнам. Первая волна включает наиболее готовые и сходные подразделения; вторая – зоны со средней готовностью; третья – сложные и высокорисковые процессы после накопления опыта. Для каждой волны определяются обучение, поддержка, сроки, владельцы, показатели и контрольные точки.

Внутренние тренеры и наставники снижают зависимость от внешней поддержки. Подготовка включает методику обучения, супервизию, стандарты консультаций и механизм обновления материалов. Сообщество практиков аккумулирует кейсы, шаблоны, ошибки и решения; тем самым формируется организационная память внедрения.

Институционализация означает встраивание модели в систему управления. Обязательный пакет может включать положение о цифровом сознании и цифровом развитии; политику применения ИИ; политику управления данными; кодекс цифрового поведения; порядок диагностики; положение о цифровых наставниках; регламент мониторинга и ежегодного отчета. Документы должны быть согласованы между собой и встроены в реальные процессы.

Интеграция в кадровые процессы включает адаптацию новых сотрудников, ролевые профили компетенций, индивидуальные планы развития, подготовку кадрового резерва и обучение руководителей. При этом индексы цифрового сознания не должны автоматически превращаться в кадровые рейтинги. Они используются для развития, а решения с существенными последствиями требуют комплексной оценки и человеческого рассмотрения.

Связь с KPI требует осторожности. Показатели цифрового сознания могут включаться в цели подразделений и руководителей как развитие практик, качество данных, выполнение контроля ИИ, снижение рисков, обновление знаний и доверие. Нельзя стимулировать «гонку за индексом», когда сотрудники оптимизируют ответы вместо поведения. Поэтому количественные показатели дополняются качественной экспертизой и проверкой реального результата.

Постоянный контур управления включает совет или комитет, ответственный за ежегодную диагностику, обновление реестров, пересмотр ИИ-сценариев, мониторинг рисков, актуализацию программ обучения и согласование значимых цифровых решений. Состав комитета должен оставаться межфункциональным; доминирование одной функции воспроизводит фрагментарность.

Повторная диагностика проводится по сопоставимой методике. Динамика индексов анализируется вместе с результатами процессов, рисками, доверием и устойчивостью поведения. Годовой отчет содержит изменения ИЦСС, ИЦСК и ИОЦС, выполненные программы, ключевые инциденты и уроки, статус локальных актов, новые риски и план следующего цикла.

Завершение первого цикла внедрения не означает завершение формирования цифрового сознания. Технологии, регуляторные требования, риски и компетенции меняются; поэтому институционализированная модель должна включать ежегодный пересмотр. В этом состоит переход от проекта к организационной способности: организация не только внедряет цифровые практики, но и регулярно осмысляет, корректирует и обновляет собственный цифровой способ действия.

Масштабирование и институционализация завершают первоначальный цикл внедрения модели цифрового сознания организации, но не прекращают её развитие. После закрепления доказавших результативность практик в регламентах, кадровых процессах, программах обучения, системе показателей и управленческой отчётности организация переходит к регулярной повторной диагностике и обновлению модели. Таким образом, технология внедрения приобретает циклический характер: результаты каждого периода становятся исходными данными для следующего этапа организационного развития.

Последовательность этапов внедрения, обязательные результаты и управленческие решения систематизированы в сокращённой дорожной карте (таблица 6.1).

Дорожная карта внедрения модели цифрового сознания организации на 12–18 месяцев

В печатной версии дорожная карта отражает управленческую последовательность этапов, обязательных результатов и решений о переходе. Полная детализированная форма с ответственными ролями, документами, показателями, сроками контроля и заполняемыми полями размещена в интерактивном научно-методическом руководстве.

Таблица 6.1 – Дорожная карта внедрения модели цифрового сознания организации на 12–18 месяцев

№	Этап и срок	Ключевая задача	Обязательный результат	Решение о переходе
1	Инициация и подготовка 1–2 мес.	Согласовать цель, контур управления, границы проекта, процессы, сервисы, данные и риски.	Паспорт проекта; рабочая группа; глоссарий; карты процессов, сервисов, данных и рисков.	Допуск к входной диагностике.
2	Входная диагностика 2–3 мес.	Зафиксировать исходное состояние сотрудников, команд и организации, выявить риски и зоны развития.	Диагностический отчёт; профили ИЦСС, ИЦСК и ИОЦС; перечень приоритетных разрывов.	Утверждение приоритетов и зоны пилота.
3	Проектирование	Сформировать	Паспорт пилота;	Допуск к

№	Этап и срок	Ключевая задача	Обязательный результат	Решение о переходе
	пилота 3–4 мес.	ограниченный, безопасный и измеримый организационный эксперимент.	матрица ролей; показатели; реестр рисков; критерии остановки.	подготовке участников.
4	Ролевое обучение 4–5 мес.	Подготовить сотрудников, руководителей и специалистов сопровождения к работе по новым правилам.	Программы обучения; кейсы; чек-листы; подтверждение готовности ключевых ролей.	Разрешение на запуск пилота.
5	Пилотные практики 5–8 мес.	Встроить цифровые и ИИ-практики в реальные процессы при контролируемом уровне риска.	Работающие практики; журналы проверок; реестры инцидентов и ИИ-сценариев; обратная связь.	Продолжение, корректировка или остановка пилота.
6	Мониторинг и корректировка 5–9 мес., параллельно	Ежемесячно сопоставлять результативность, риски, нагрузку, качество данных и доверие.	Аналитическая панель; промежуточные отчёты; карточки корректирующих действий.	Корректировка состава практик и мер контроля.
7	Итоговая оценка пилота 9 мес.	Сопоставить исходное и достигнутое состояние, прямые эффекты, побочные последствия и риски.	Итоговый отчёт; анализ «до/после»; извлечённые уроки; рекомендации.	Масштабировать, повторить пилот или прекратить решение.
8	Масштабирование 10–14 мес.	Перенести подтверждённые практики в другие процессы и подразделения с учётом контекста.	Дорожная карта масштабирования; адаптированные пакеты; сеть цифровых наставников.	Переход к институционализации.
9	Институционализация 12–17 мес.	Закрепить модель в управлении, локальных актах, кадровых процессах, работе с данными и ИИ.	Локальные акты; утверждённые роли; показатели; ежегодный цикл оценки и развития.	Перевод модели в регулярное управление.
10	Повторная диагностика 18 мес. и далее	Оценить динамику, актуализировать риски, правила,	Ежегодный аналитический отчёт; обновлённая карта	Запуск нового цикла развития.

№	Этап и срок	Ключевая задача	Обязательный результат	Решение о переходе
	ежегодно	обучение и портфель цифровых инициатив.	рисков; план следующего цикла.	

Источник: составлено авторами на основе исследовательской базы главы 6.

Таблица 6.8 объединяет десять взаимосвязанных этапов – от формирования стартового управленческого контура до повторной диагностики. Переход между этапами определяется подтверждённой организационной готовностью, а не только календарным сроком.

Подготовка, диагностика, проектирование пилота, обучение и запуск образуют последовательную часть внедрения; мониторинг, корректировка, масштабирование и повторная диагностика – контур непрерывного улучшения.

Мониторинг начинается до завершения обучения и продолжается на всех последующих этапах. Институционализация частично совмещается с масштабированием: уже доказавшие результативность практики закрепляются в локальных документах, программах обучения и кадровых процессах, не ожидая завершения распространения модели по всей организации.

Контрольные точки внедрения

Переход между этапами осуществляется не автоматически, а после прохождения управленческой контрольной точки.

1. **Контрольная точка 1 – готовность к диагностике:** утверждены паспорт проекта, рабочая группа, глоссарий, карты процессов, данных, сервисов и рисков.

2. **Контрольная точка 2 – готовность к пилоту:** результаты диагностики приняты, определены дефициты, риски и приоритетные подразделения.

3. **Контрольная точка 3 – готовность участников:** сотрудники, руководители и наставники выполнили практические задания и понимают правила работы с данными и ИИ.

4. **Контрольная точка 4 – жизнеспособность пилота:** зафиксированы изменения поведения и процессов, подтверждённые несколькими источниками данных.

5. **Контрольная точка 5 – готовность к масштабированию:** эффект воспроизводим, риски контролируются, результат не зависит исключительно от одного руководителя или эксперта.

6. **Контрольная точка 6 – институциональная устойчивость:** модель закреплена в стратегии, локальных актах, HR-процессах, обучении, показателях и ежегодной диагностике.

Система показателей дорожной карты

Показатели следует объединить в девять блоков, предусмотренных исследовательской базой:

- **охват:** доля сотрудников, команд и подразделений, включённых в программу;
- **диагностическая динамика:** изменение ИЦСС, ИЦСК и ИОЦС;
- **качество цифровых практик:** соблюдение правил работы с данными, документами, коммуникациями и ИИ;
- **изменение поведения:** доля проверяемых ИИ-результатов, качество аналитических выводов, дисциплина хранения данных;
- **снижение рисков:** динамика инцидентов, ошибок данных, теневого использования сервисов и ИИ;
- **результативность обучения:** результаты кейсов, практических заданий и перенос обучения в рабочие процессы;
- **управленческий эффект:** скорость и обоснованность решений, прозрачность проектов, использование аналитических панелей;
- **цифровая нагрузка:** число дублирующих сервисов и каналов, продолжительность совещаний, объём уведомлений;
- **доверие и безопасность:** готовность сообщать о проблемах, восприятие справедливости диагностики, уровень психологической и информационной безопасности.

Роль архитектуры

Руководитель организации утверждает цели, ресурсы и решения о масштабировании.

Куратор цифровой трансформации отвечает за сквозную координацию дорожной карты.

Проектный офис ведёт график, документы, риски, показатели и контрольные точки.

HR-служба и корпоративное обучение отвечают за диагностику компетенций, программы развития и интеграцию модели в кадровые процессы.

ИТ-служба, информационная безопасность, специалисты по данным и ИИ обеспечивают цифровую инфраструктуру, качество данных, контроль ИИ-сценариев и безопасность.

Руководители подразделений переводят модель в реальные процессы.

Цифровые наставники обеспечивают повседневное сопровождение и горизонтальное распространение практик.

Сотрудники участвуют в апробации, обратной связи и совершенствовании модели. Такое распределение ответственности должно сохраняться после завершения пилота, поскольку институционализация предполагает постоянный, а не временный контур управления.

Описание дорожной карты

Представленная дорожная карта показывает последовательный переход от концептуальной модели к устойчивой организационной практике. Подготовительный этап формирует язык и управленческую инфраструктуру проекта; диагностика задаёт исходное состояние; пилотирование позволяет проверить модель в ограниченном контуре; обучение обеспечивает ролевую готовность; пилотные практики переводят знания в поведение; мониторинг обеспечивает доказательную корректировку; масштабирование распространяет результат с учётом специфики подразделений; институционализация закрепляет модель в стратегии, регламентах, кадровых процессах и системе управления. Повторная диагностика замыкает цикл и запускает следующий этап развития.

Таким образом, дорожная карта должна применяться не как жёсткий линейный график, а как управляемая система этапов и обратных связей. Масштабирование допустимо только после подтверждения эффекта пилота, а институционализация – после закрепления владельцев, регламентов, показателей, образовательных механизмов и ежегодного цикла оценки. Именно такой подход предотвращает подмену цифрового сознания разовым обучением, формальной цифровизацией или набором несвязанных ИТ-проектов.

ИТОГИ ГЛАВЫ

Внедрение модели цифрового сознания представляет собой цикл, включающий подготовку, диагностику, проектирование пилота, обучение, запуск практик, мониторинг, корректировку, масштабирование и институционализацию. Каждый этап завершается проверяемыми артефактами и управленческим решением.

Управленческий переход к главе 7: после подтверждения ценности пилота и приемлемого риска устойчивость обеспечивается через лидерство, работу с сопротивлением и институционализацию цифровой культуры.

***Интерактивное сопровождение.** В цифровом руководстве размещены конструктор дорожной карты, паспорт пилота, реестры сервисов, данных и ИИ-сценариев, карта рисков и формы мониторинга.*

ГЛАВА 7. УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ИНСТИТУЦИОНАЛИЗАЦИЯ ЦИФРОВОЙ КУЛЬТУРЫ ОРГАНИЗАЦИИ

«Культура изменяется только после того, как вам удалось изменить действия людей».

Джон Коттер

Управленческий вопрос главы. Почему цифровые инициативы сталкиваются с сопротивлением и как превратить успешные пилоты в устойчивые нормы, практики и элементы организационной культуры?

Управленческий результат главы. Система управления изменениями, объединяющая лидерство, коммуникацию, работу с сопротивлением, профессиональные сообщества, наставничество, мотивацию, нормативное закрепление и ежегодный цикл развития.



Рисунок 7.1 – Гуманитарно-управленческий контур цифровой трансформации

Источник: составлено авторами на основе [53; 55; 75; 84; 100; 119; 139].

Представленная схема показывает, что семь контуров образуют единую систему формирования цифровой культуры. Центральным результатом выступает не интенсивность использования технологий, а ответственное цифровое поведение организации, поддерживаемое лидерством, диалогом, обучением, институциональными правилами и ежегодной рефлексией.

Как показано на рисунке 7.1, контуры не образуют линейную последовательность. Лидерство задает смысл и границы, коммуникация превращает смысл в коллективное понимание, работа с сопротивлением возвращает в проект данные о рисках и барьерах, сообщества и наставники обеспечивают горизонтальное обучение, мотивационный контур поддерживает

участие, институциональный закрепляет нормы, а ежегодный цикл пересматривает всю систему. Такое построение соответствует логике управляемой адаптации: организация не «внедряет культуру» одновременно, а воспроизводит ее через повторяющиеся управленческие практики.

Сравнительная применимость базовых теорий и моделей к задачам формирования цифрового сознания систематизирована в таблице 7.1.

Таблица 7.1 – Сравнительная применимость теорий и моделей к формированию цифрового сознания

Подход или модель	Ключевая идея	Методическое применение	Ограничение	Адаптация к среде ИИ
Фазовая модель изменений	Подготовка, переход, закрепление	Построение логики перехода от прежних норм к новым цифровым практикам	Слабо отражает постоянную технологическую турбулентность	Добавляется ежегодный цикл пересмотра данных, рисков, навыков и правил
Модель Коттера	Коалиция, видение, коммуникация, быстрые результаты, закрепление	Лидерство, мобилизация и институционализация	Риск линейности и чрезмерной директивности	Включаются голос сотрудников, совместное проектирование и управление ИИ
ADKAR	Осведомленность, желание, знание, способность, закрепление	Диагностика индивидуальной готовности и проектирование обучения	Недостаточно раскрывает власть, культуру и надзор	Добавляются ИИ-грамотность, этика, защита данных и право на вопрос
Модель перехода Бриджеса	Завершение, нейтральная зона, новое начало	Работа с тревогой, идентичностью и потерей привычных ролей	Менее операциональна для систем управления	Учитываются страх замещения ИИ и изменение профессионального статуса
Организационная культура Шейна	Артефакты, провозглашаемые ценности, базовые допущения	Выявление расхождения между цифровой декларацией и реальной практикой	Глубинные допущения трудно диагностировать	Анализируются представления о данных, ИИ, наблюдении и справедливости
Организационное обучение	Одиная и двойная петля; коллективное знание	Разбор ошибок, пересмотр правил, обновление программ	Требует психологической безопасности и	Включается аудит человеко-алгоритмических решений и

Подход или модель	Ключевая идея	Методическое применение	Ограничение	Адаптация к среде ИИ
			времени	право оспаривания
Теории принятия технологий	Полезность, простота, социальное влияние и условия поддержки	Диагностика барьеров использования сервисов	Недостаточно учитывают этику и власть	Добавляются доверие к ИИ, приватность, прозрачность и режим данных
JD-R и психологическая безопасность	Баланс требований и ресурсов; безопасность межличностного риска	Профилактика перегрузки, цифровой тревоги и скрытия ошибок	Могут оставаться локальными без изменений процессов	Учитываются постоянные прерывания, алгоритмическое давление и гарантии от санкций
Сообщества практики	Знание распространяется через совместную практику	Наставничество, база кейсов, горизонтальное обучение	Риск превращения в клуб без влияния на решения	Сообщество связывается с HR, ИТ, безопасностью и обновлением регламентов

Данные таблицы показывают, что ни одна теория не охватывает все аспекты цифрового изменения. Для формирования цифрового сознания необходима композиция подходов, соединяющая структуру перехода, культурное закрепление, поддержку человека, этические ограничения и организационное обучение.

7.1. ЦИФРОВОЕ ЛИДЕРСТВО И РОЛЬ РУКОВОДИТЕЛЯ

Цифровое лидерство определяется как способность руководителя создавать стратегический смысл цифровых изменений, обеспечивать межфункциональную координацию, формировать условия безопасного освоения технологий и сохранять человеческую ответственность за решения, принимаемые с использованием данных и ИИ. Это определение принципиально шире личной цифровой компетентности. Руководитель может не быть наиболее опытным пользователем конкретного сервиса, но обязан понимать цели, риски, организационные последствия и границы делегирования алгоритму [23; 78; 93; 112].

Роль руководителя целесообразно раскрывать в трех взаимосвязанных измерениях: носитель смысла, архитектор условий и гарант ответственности. Как носитель смысла он связывает цифровую трансформацию с миссией,

качеством деятельности и развитием сотрудников. Как архитектор условий он распределяет ресурсы, время, роли и полномочия, устраняет барьеры между функциями и обеспечивает доступ к легитимным инструментам. Как гарант ответственности он устанавливает этические границы, требует проверки значимых ИИ-результатов и не допускает переноса ответственности на систему.

Первой функцией цифрового лидера является формирование понятного образа целевого состояния. Сотрудникам необходимо знать не только, какой сервис вводится, но и какую организационную проблему он решает, какие действия изменятся, какие действия сохранятся и по каким признакам будет оценен эффект. Абстрактное требование «работать более цифровым способом» создает неопределенность. Операционализированное видение показывает связь между задачей, процессом, данными, ролями, рисками и ожидаемым результатом.

Вторая функция – создание коалиции изменений. В цифровой трансформации недостаточно передать проект ИТ-службе или HR. Руководитель должен сформировать устойчивый межфункциональный контур, в котором HR отвечает за развитие и справедливость кадровых процедур, ИТ – за архитектуру и доступность сервисов, служба безопасности – за риск-контроль и реагирование на инциденты, владельцы процессов – за рабочий результат, а представители сотрудников – за обратную связь и легитимацию. Куратор цифровой трансформации обеспечивает координацию, но не подменяет ответственность руководителя организации.

Третья функция – защита времени и ресурсов для освоения нового. Обучение, участие в пилоте, подготовка кейсов и наставничество требуют рабочего времени. Если организация добавляет новые требования поверх прежней нагрузки, цифровое развитие воспринимается как дополнительная повинность. Руководитель должен перераспределять приоритеты, сокращать дублирующие процедуры, устанавливать реалистичные сроки и контролировать не только темп внедрения, но и цифровую нагрузку [48; 96; 151].

Четвертая функция – формирование психологической безопасности. В цифровой и ИИ-насыщенной среде сотрудники должны иметь возможность сообщить, что они не понимают инструмент, обнаружили ошибку модели, не согласны с автоматизированной рекомендацией или видят риск для данных. Если вопрос воспринимается как признак нелояльности, организация получает ложное согласие, скрытое использование сервисов и позднее обнаружение инцидентов. Поэтому лидер публично нормализует обоснованное сомнение, демонстрирует собственную готовность пересматривать решения и отделяет сообщение о проблеме от дисциплинарной ответственности за умышленное нарушение.

Пятая функция – личное моделирование ответственного цифрового поведения. Руководитель не должен требовать от сотрудников соблюдения правил, которые сам систематически обходит. Использование неутвержденных сервисов, передача конфиденциальных данных через удобные каналы, некритичное цитирование ИИ или управление исключительно по цифровым показателям разрушает легитимность правил. Поведенческий пример руководителя является культурным сигналом сильнее любой инструкции.

Шестая функция – обеспечение человеческого контроля. Руководитель определяет категории решений, в которых ИИ может готовить вариант, но не принимать окончательное решение. Для значимых кадровых, финансовых, правовых, медицинских, образовательных, клиентских и безопасностных решений должны быть установлены компетентный проверяющий, критерии верификации, право остановить использование результата и порядок оспаривания. Формальное присутствие человека без времени, компетентности и полномочий не является человеческим контролем [67; 83; 100; 101].

Седьмая функция – управление цифровой нагрузкой и справедливостью. Руководитель обязан оценивать, не превращает ли новая система прозрачность процесса в микроконтроль, не переносит ли ошибки данных на отдельных работников, не усиливает ли цифровое неравенство между подготовленными и неподготовленными сотрудниками. Справедливость означает доступность обучения, разумный переходный период, понятные критерии и возможность исправить данные или объяснить контекст [71; 97].

Восьмая функция – организация обратной связи и корректирующих решений. Лидер не ограничивается публичным запуском проекта, а устанавливает регулярный обзор вопросов, барьеров, инцидентов, цифровой нагрузки и результатов обучения. Обратная связь становится управленческой только тогда, когда по ней принимаются решения, назначаются владельцы и сообщается, что именно изменено. Иначе участие сотрудников превращается в символическую процедуру.

Девятая функция – развитие распределенного лидерства. Руководитель организации не способен лично сопровождать все цифровые практики. Он создает многоуровневую систему: руководители подразделений переводят общую стратегию в процессы; проектные лидеры управляют пилотами; цифровые наставники оказывают горизонтальную помощь; профессиональные сообщества аккумулируют кейсы; неформальные лидеры нормализуют ответственное поведение. При этом полномочия и границы каждой роли должны быть определены, чтобы распределенность не превратилась в размывание ответственности.

Десятая функция – институционализация. Руководитель обеспечивает включение цифрового сознания в стратегию, программы обучения, регламенты,

систему управления рисками, кадровые процессы и ежегодную отчетность. Институционализация не равна росту количества документов: ее признаком является устойчивость практик при смене отдельных сотрудников и проектов. Новая норма должна поддерживаться ресурсами, сервисами, владельцами, обратной связью и механизмом пересмотра.

Предполагается, что чем выше согласованность смысловой, ресурсной, этической и рефлексивной функций руководителя, тем устойчивее переход от индивидуального использования цифровых инструментов к организационному цифровому сознанию. При этом личная техническая продвинутость руководителя без архитектуры ответственности может усиливать технологический волюнтаризм, а развитая архитектура без видимого лидерского поведения – формализм.

Ролевое содержание цифрового лидерства и взаимосвязь функций руководителя представлены на рисунке 7.2.



Рисунок 7.2 – Руководитель как носитель, архитектор и гарант цифрового сознания

Источник: составлено авторами на основе [55; 64; 78; 91; 93; 100].

Представленная схема показывает, что десять функций цифрового руководителя объединены вокруг трех базовых ролей: смыслового носителя, архитектора организационных условий и гаранта ответственности. Красная нижняя граница подчеркивает недопустимость скрытого мониторинга, делегирования ответственности алгоритму и принуждения к использованию ИИ без обучения и правил.

Представленная схема показывает, что цифровое лидерство проявляется прежде всего в устройстве среды. Руководитель задает цели, но HR превращает

их в справедливые программы развития; ИТ обеспечивает сервисы, но не определяет кадровые последствия; служба безопасности устанавливает контроль рисков, но не должна подменять собой коммуникацию и обучение; наставники помогают, но не оценивают лояльность; профессиональные сообщества создают знание, но не принимают управленческие решения. Четкое разграничение функций снижает типичный риск «расслоения трансформации», когда каждая функция действует по собственной логике.

Распределение ответственности между основными участниками формирования цифровой культуры представлено в таблице 7.2.

Таблица 7.2 – Разграничение функций участников формирования цифровой культуры

Субъект	Основная ответственность	Что субъект обязан делать	Что не входит в функцию	Ключевой результат
Руководитель организации	Стратегия, мандат, ресурсы и этические границы	Объяснять смысл, утверждать цели и ограничения, принимать решения по рискам и масштабу	Передавать итоговую ответственность ИТ, HR или алгоритму	Легитимный и ресурсно обеспеченный контур изменений
Куратор цифровой трансформации	Межфункциональная координация портфеля изменений	Вести дорожную карту, соединять функции, готовить обзоры и эскалации	Подменять владельцев процессов и руководителя организации	Согласованность инициатив, ролей и корректирующих действий
Руководитель подразделения	Перевод стратегии в рабочие практики	Убирать локальные барьеры, перераспределять нагрузку, обсуждать ошибки, обеспечивать обратную связь	Требовать использования ИИ ради статистики или вводить цифровой микроконтроль	Устойчивое изменение процесса и безопасная вовлеченность команды
HR-служба и корпоративное обучение	Развитие, справедливость и поддержка людей	Диагностировать потребности, проектировать	Устанавливать техническую архитектуру или	Доступное развитие, прозрачные кадровые

Субъект	Основная ответственность	Что субъект обязан делать	Что не входит в функцию	Ключевой результат
		обучение, выделять траектории, защищать некарательный характер оценки	самостоятельно оценивать киберриски	процедуры и снижение тревоги
ИТ-служба	Архитектура, интеграции, доступность и поддержка сервисов	Предлагать легитимные инструменты, обеспечивать жизненный цикл, удобство и техническую поддержку	Определять профессиональную ценность, этическую допустимость и кадровые санкции	Надежная, удобная и управляемая цифровая среда
Служба информационно й безопасности	Классификация рисков, защитные меры и реагирование	Устанавливать правила доступа и данных, консультировать, проводить анализ инцидентов и безопасный дизайн	Использовать безопасность как универсальный запрет или скрытый контроль продуктивности	Снижение рисков при сохранении работоспособности и доверия
Цифровой наставник	Горизонтальная помощь и эскалация барьеров	Консультировать, демонстрировать практики, помогать освоению, пополнять базу знаний	Оценивать лояльность, принимать кадровые решения, заменять техподдержку	Рост уверенности и перенос обучения в рабочую практику
Профессиональное сообщество	Обмен знаниями, стандартизация практик и рефлексия	Разбирать кейсы, формировать рекомендации, выявлять повторяющиеся барьеры	Выдавать обязательные управленческие распоряжения или вести персональный контроль	Организационное знание и распространение проверенных практик

Таблица 7.2 представляет фиксирует функциональные границы. Руководитель сохраняет стратегическую и этическую ответственность; HR отвечает за развитие и справедливость; ИТ – за сервисы; служба безопасности –

за риск-контроль; наставник – за помощь; профессиональное сообщество – за коллективное знание.

Диагностические признаки цифрового лидерства, источники данных и развивающие решения систематизированы в таблице 7.3.

Таблица 7.3 – Диагностические индикаторы цифрового лидерства

Направление	Наблюдаемый индикатор	Источник данных	Развивающее решение	Недопустимая трактовка
Смысл и последовательность	Сотрудники одинаково понимают цель изменения, а решения руководителей ей не противоречат	Опрос, интервью, анализ сообщений и решений	Уточнение карты сообщений, стратегическая сессия руководителей	Поиск «нелояльных» сотрудников по степени согласия
Ресурсная поддержка	Для обучения и пилотов выделены время, доступ и помощь; дублирующая нагрузка сокращается	План ресурсов, аудит нагрузки, обратная связь	Перераспределение задач и сроков	Требование осваивать изменения исключительно во внерабочее время
Психологическая безопасность	Сотрудники сообщают об ошибках и рисках без страха автоматического наказания	Пульс-опрос, кейсы инцидентов, интервью	Обучение руководителей обратной связи, безобвинительный разбор	Отождествление сообщения о проблеме с виновностью
Ответственное применение ИИ	Определены зоны человеческой проверки, владельцы решений и порядок оспаривания	Регламенты, реестр ИИ-сценариев, выборочный аудит	Уточнение процедур и обучение проверяющих	Оценка руководителя по количеству внедренных ИИ-сервисов
Обратная связь и корректировка	Вопросы сотрудников получают ответ, а принятые изменения публикуются	Журнал вопросов, протоколы обзоров, план корректировок	Назначение владельцев и сроков	Сбор предложений без обязательства рассматривать их

Направление	Наблюдаемый индикатор	Источник данных	Развивающее решение	Недопустимая трактовка
Управление нагрузкой	Отслеживаются цифровые прерывания, число каналов и перегрузка изменениями	Аудит рабочего дня, опрос, карта сервисов	Сокращение каналов и инициатив, изменение темпа	Персональное ранжирование по времени онлайн

Индикаторы, приведенные в таблице 7.3, оценивают качество управленческой среды и поведения руководителя, а не степень безусловного согласия сотрудников. Результаты используются для коучинга, корректировки процессов и ресурсных решений, но не для карательной аттестации.

Таким образом, цифровой лидер является не главным пользователем технологии, а носителем смысла, архитектором условий и гарантом ответственности. Его результат оценивается по качеству среды: ясности целей, доступности ресурсов, безопасности критического диалога, управляемости ИИ, снижению перегрузки и способности организации корректировать решения.

7.2. КОММУНИКАЦИОННАЯ СТРАТЕГИЯ ФОРМИРОВАНИЯ ЦИФРОВОГО СОЗНАНИЯ

Коммуникационная стратегия формирования цифрового сознания – это система целей, аудиторий, сообщений, каналов, форматов участия и обратной связи, обеспечивающая коллективное понимание цифровых изменений и легитимность новых практик. Ее предметом является не продвижение технологии, а совместное осмысление того, зачем организация меняется, какие последствия ожидаются, как распределяется ответственность и какие гарантии получает сотрудник [51; 52; 55; 64].

В традиционном проекте коммуникация нередко рассматривается как вспомогательное информирование: сообщить о решении, сроках запуска и инструкции. Для цифрового сознания этого недостаточно. Новые системы и ИИ меняют не только последовательность операций, но и профессиональные роли, режим работы с данными, степень прозрачности, критерии качества и границы автономии. Поэтому коммуникация должна включать объяснение смысла, обсуждение рисков, ответы на опасения, участие в проектировании и публичное сообщение о корректировках.

Первая задача стратегии – сформировать единый «дом сообщений». Он должен содержать ответы минимум на двенадцать вопросов: какую проблему решает изменение; почему выбран именно этот путь; что меняется в деятельности; что не меняется; какие данные используются; где применяется ИИ; кто проверяет результат; кто отвечает за решение; какие риски признаны;

как защищаются права и конфиденциальность; где получить помощь; как задать вопрос, оспорить решение или сообщить о проблеме. Отсутствие хотя бы части ответов заполняется слухами и неформальными версиями.

Вторая задача – сегментировать аудитории. Высшему руководству необходимы данные о ценности, рисках и соответствии стратегии. Руководителям среднего звена – понятные полномочия, ресурсы и сценарии работы с командами. Сотрудникам – конкретное описание изменений, гарантии, обучение и каналы помощи. ИТ, службе безопасности и юристам – реестры сценариев, требования и порядок эскалации. Наставникам – границы роли и регулярная методическая поддержка. Представителям работников – прозрачность показателей, режима данных и кадровых последствий.

Третья задача – соединить нисходящую коммуникацию с голосом сотрудников. Голос сотрудников означает возможность безопасно выражать вопросы, предложения, сомнения и несогласие с последующим рассмотрением. Он не равен опросу удовлетворенности и не исчерпывается анонимной формой. Развитая система включает открытые обсуждения, фокус-группы, каналы конфиденциального сообщения о рисках, участие в рабочих группах, публикацию ответов и обратное информирование о принятых решениях [52; 97].

Четвертая задача – организовать совместное придание смысла. В логике К. Вейка сотрудники принимают изменение не только через получение фактов, но и через коллективную интерпретацию: что это означает для нашей работы, профессионального статуса, отношений с клиентами и ответственности. Руководитель выполняет функцию смыслового направления, но смысл не может быть навязан односторонне. Он уточняется в диалоге, где организационные цели сопоставляются с реальными практиками и профессиональным опытом [55].

Пятая задача – обеспечить последовательность сообщений и действий. Доверие разрушается, когда публично заявляется человекоцентричность, а фактически вводится скрытый мониторинг; обещается снижение рутины, но растет число отчетов; декларируется право на ошибку, но первая же ошибка используется для наказания. Поэтому коммуникационный аудит должен сопоставлять слова, управленческие решения, настройки систем и фактические кадровые практики.

Шестая задача – управлять неопределенностью честно. Руководство не обязано иметь готовый ответ на все вопросы, особенно при пилотировании ИИ. Однако оно обязано различать известное, предполагаемое и еще не решенное. Формула «все будет только лучше» снижает доверие, поскольку игнорирует реальные риски. Более зрелая позиция: организация объясняет гипотезы, критерии пилота, условия остановки и порядок пересмотра.

Седьмая задача – обеспечивать доступность. Сообщения должны быть понятны людям с разным уровнем цифровой готовности, не перегружены

техническим жаргоном и доступны через привычные каналы. Для сложных понятий необходимы краткие определения, примеры и визуальные схемы. Признанные англоязычные термины вводятся однократно с русским пояснением; далее используется русская формулировка. Такая языковая дисциплина сама по себе является частью цифровой культуры.

Восьмая задача – предотвратить коммуникационную перегрузку. Парадокс цифровых изменений состоит в том, что организация может сопровождать их чрезмерным количеством писем, чатов, презентаций и совещаний. В результате важные сообщения теряются, а у сотрудников формируется усталость. Коммуникационная стратегия должна задавать ритм, приоритетность, единый источник актуальной информации и правила прекращения устаревших каналов [48; 96].

Предполагается, что доверие к цифровым изменениям определяется не объемом сообщений, а соответствием четырех условий – смысловой ясности, признания рисков, реальной возможности участия и видимости корректирующих решений. При отсутствии любого из условий коммуникация воспринимается как формальная и не переводит технологическое решение в разделяемую организационную практику.

Последовательность коммуникационного сопровождения цифровых изменений представлена на рисунке 7.3.



Результат: сотрудники понимают цель изменений, знают границы применения ИИ и видят, как их обратная связь влияет на решение.

Рисунок 7.3 – Коммуникационный цикл цифровых изменений

Источник: составлено авторами на основе [51; 52; 55; 64].

Представленная схема показывает, что коммуникация разворачивается как цикл: объяснение смысла, раскрытие последствий, диалог, участие, обратная

связь и корректировка. Центральным условием выступает пространство доверия, в котором вопрос или критическое замечание не влечет автоматической санкции.

На рисунке 7.3 важно различать обратную связь и корректировку. Получение вопросов еще не означает диалога. Диалог возникает тогда, когда организация интерпретирует сигнал, принимает решение и возвращает сотрудникам объяснение. Поэтому коммуникационный контур должен иметь владельца, реестр вопросов, сроки ответа и правила эскалации вопросов о данных, ИИ, безопасности и кадровых последствиях.

Соответствие аудиторий, сообщений, каналов и механизмов обратной связи раскрыто в таблице 7.4.

Таблица 7.4 – Матрица коммуникационной стратегии формирования цифрового сознания

Аудитория	Основные опасения	Ключевое сообщение	Каналы	Обратная связь	Ответственный
Высшее руководство	Ценность, риски, регулирование, репутация	Цифровое сознание – условие устойчивого эффекта, а не второстепенная культурная тема	Стратегические сессии, аналитическая записка, квартальный обзор	Обсуждение портфеля, риск-обзор, решение по ресурсам	Руководитель организации и куратор трансформации
Руководители среднего звена	Рост нагрузки, потеря управляемости, неясность полномочий	Изменение сопровождается ресурсами, обучением, понятными ролями и правом корректировать процесс	Управленческие брифинги, FAQ, взаимное обучение руководителей	Пульс-опросы, встречи, разбор локальных барьеров	Куратор, HR и руководители функций
Сотрудники	Потеря работы, ошибки, слежка, непонятные KPI, утечка данных	ИИ не снимает человеческую ответственность; действуют прозрачные правила, обучение и	Общие встречи, интранет, база знаний, короткие памятки	Форма вопросов, очные обсуждения, конфиденциальный канал рисков	Внутренние коммуникации и руководители подразделений

Аудитория	Основные опасения	Ключевое сообщение	Каналы	Обратная связь	Ответственный
		право задавать вопросы			
ИТ-служба	Теневые сервисы, интеграции, нагрузка на поддержку	Развитие идет через реестр сервисов, архитектурные правила и пользовательскую обратную связь	Архитектурные обзоры, рабочие группы, каталог сервисов	Журнал запросов, анализ причин обходных практик	ИТ-руководитель и куратор
Служба безопасности и комплаенс	Утечки, нарушения требований, неконтролируемый ИИ	Риск-контроль соединяется с легитимным и инструментами, обучением и понятной эскалацией	Комитет по рискам, тематическое инструктаж и, база допустимых сценариев	Журнал инцидентов и прединцидентов, консультации	Служба безопасности и юридическая функция
Цифровые наставники	Размытость роли, перегрузка, ожидание универсальной помощи	Наставничество – помощь и передача практик, а не оценка и скрытый контроль	Сообщество наставников, супервизии, методические сессии	Журнал обезличенных запросов, ретроспективы	HR и корпоративное обучение
Профессиональные сообщества	Отсутствие влияния, формальность встреч	Сообщество формирует проверенные практики и передает системные предложения владельцам решений	Регулярные встречи, демонстрации кейсов, база знаний	Протокол рекомендаций, ответ владельца процесса	Модератор сообщества и куратор
Представители и работников	Справедливость, использование данных,	Нет скрытых рейтингов и автоматических кадровых	Консультации, совместные комиссии,	Протокол замечаний и обязательный ответ	HR, комплаенс и руководитель

Аудитория	Основные опасения	Ключевое сообщение	Каналы	Обратная связь	Ответственный
	кадровые последствия	решений; есть объяснение, пересмотр и минимизация данных	письменные разъяснения		организации

Матрица, представленная в таблице 7.4, обеспечивает соответствие сообщения реальным опасениям каждой аудитории и закрепляет владельца обратной связи. Она предотвращает сведение коммуникации к единому массовому сообщению, которое не учитывает различие ролей, рисков и уровней ответственности.

Таким образом, коммуникационная стратегия формирует не информационную осведомленность, а коллективное понимание и легитимность цифровых изменений. Ее обязательные элементы – честное объяснение смысла и рисков, сегментация аудиторий, голос сотрудников, видимые корректировки, единый источник актуальной информации и отсутствие репрессивной реакции на обоснованные вопросы.

7.3. ПРЕОДОЛЕНИЕ СОПРОТИВЛЕНИЯ ЦИФРОВЫМ ИЗМЕНЕНИЯМ

Соппротивление цифровым изменениям определяется как совокупность когнитивных, эмоциональных, поведенческих и организационных реакций, указывающих на несогласие, тревогу, дефицит ресурсов, несоответствие решения профессиональной логике или недоверие к способу внедрения. Такое определение исключает трактовку сопротивления как личного недостатка сотрудника. Сигнал может быть непродуктивным, но он всегда требует диагностики причин до выбора управленческого ответа [48; 75; 84; 111; 149] [62].

Для методической работы необходимо различать четыре формы реакции. Конструктивная критика указывает на реальный риск, несоответствие процесса или нарушение прав. Тревога возникает при неопределенности, угрозе статуса и недостатке информации. Дефицит готовности связан с навыками, временем, доступом и поддержкой. Саботаж предполагает сознательное нарушение согласованных правил после того, как цели, ресурсы и границы были объяснены. Смещение этих форм приводит к наказанию критиков, игнорированию тревоги и неэффективному обучению там, где проблема находится в дизайне процесса.

Модели принятия технологий TAM (модель принятия технологии) и UTAUT (унифицированная теория принятия и использования технологии) показывают значение воспринимаемой полезности, простоты, социального влияния и условий поддержки. Однако в ИИ-насыщенной среде этих факторов недостаточно. Сотрудник оценивает не только удобство, но и доверие к алгоритму, прозрачность использования данных, справедливость, влияние на автономию и возможность оспорить результат [71; 97].

Модель рабочих требований и ресурсов JD-R (модель баланса рабочих требований и ресурсов) позволяет объяснить цифровую усталость и сопротивление перегруженной команды. Новая система увеличивает требования: нужно учиться, менять привычки, заполнять новые поля, проверять ИИ, работать в нескольких каналах. Если одновременно не появляются ресурсы – время, обучение, упрощение процесса, поддержка и управленческая ясность, – изменение закономерно усиливает стресс. Следовательно, преодоление сопротивления начинается с перерасчета баланса требований и ресурсов, а не с усиления мотивационных лозунгов.

Организационная справедливость является следующим объяснительным фактором. Сотрудники оценивают, справедливо ли распределена нагрузка, понятны ли критерии, могут ли они влиять на процесс, одинаково ли правила применяются к руководителям и подчиненным, можно ли исправить неверные данные. Непрозрачная аналитика, «невидимые» рейтинги и автоматическое ранжирование создают недоверие даже при технически корректной системе [54; 97].

Страх потери работы и профессионального статуса должен обсуждаться прямо. Массовое распространение ИИ одновременно создает новые роли и меняет содержание существующих. Отказ признавать возможное перераспределение задач снижает доверие. Организация должна показывать карту ролей, сценарии переобучения, временной горизонт и критерии принятия кадровых решений. Принуждение по формуле «либо используете ИИ, либо становитесь ненужными» является методически неприемлемым и разрушает внутреннюю мотивацию [78; 151].

Страх ошибки ИИ имеет рациональное основание. Сотрудник может опасаться использовать инструмент, если не понимает, как проверить результат и кто отвечает за последствия. Управленческий ответ – не требование «доверять технологии», а правила человеческой проверки, учебные кейсы, понятная маркировка, допустимые сценарии и возможность эскалации сомнительного результата. Рост доли проверенных ИИ-результатов является более содержательным показателем, чем рост числа пользователей.

Потеря автономии проявляется, когда система детализирует поведение, задает жесткие шаблоны или превращает цифровой след в постоянный

микроконтроль. В этом случае сопротивление защищает профессиональную субъектность. Организация должна пересмотреть, какие решения действительно требуют стандартизации, а где необходима зона профессионального суждения. Технологическая прозрачность процесса не должна автоматически означать прозрачность каждого действия человека.

Цифровая перегрузка является системной причиной. Новые каналы, уведомления, панели, согласования и учебные задания нередко добавляются без отмены прежних процедур. В результате сотрудники сопротивляются не цели, а накопившейся сложности. Для диагностики используется аудит нагрузки: количество параллельных систем, повторный ввод, число прерываний, совещаний и каналов, доля времени на вспомогательные цифровые операции. Решением может быть не дополнительное обучение, а упрощение архитектуры и процесса [48; 96].

Несогласованность руководителей создает политическое сопротивление. Если один руководитель требует использовать ИИ, другой запрещает, ИТ предлагает сервис без согласования с безопасностью, а HR вводит показатели без объяснения, сотрудник выбирает стратегию ожидания или обхода. Поэтому до массовой коммуникации необходимо провести выравнивание управленческой позиции, утвердить единые определения, роли и правила исключений.

Скрытый мониторинг и непрозрачная HR-аналитика являются отдельной причиной недоверия. Организация обязана заранее определить, какие данные собираются, зачем, кто имеет доступ, как долго они хранятся и какие решения на их основе запрещены. Персональный цифровой след не может использоваться вне объявленной цели, а результаты самооценки – для автоматических санкций. Эти гарантии должны быть закреплены в локальных актах и коммуникации [54; 83; 97; 139].

Алгоритм работы с сопротивлением включает семь действий: фиксацию сигнала; отделение симптома от причины; определение уровня – индивидуального, командного, управленческого или организационного; проверку факторов навыков, нагрузки, справедливости, данных и доверия; выбор меры; согласование с затронутыми участниками; оценку эффекта. Важный принцип – мера должна быть соразмерна причине. Недостаток навыка требует обучения, неудобный сервис – доработки, конфликт ролей – RACI, скрытый мониторинг – прекращения практики, а умышленное нарушение – отдельной правовой процедуры.

Предполагается, что сопротивление становится ресурсом развития, если организация обладает безопасным каналом выражения, диагностической методикой и полномочиями корректировать проект. При отсутствии этих условий сопротивление либо подавляется и уходит в тень, либо накапливается в форме цинизма, обходных практик и скрытия ошибок.

Логика преобразования сопротивления в диагностический сигнал и управленческое решение представлена на рисунке 7.4.

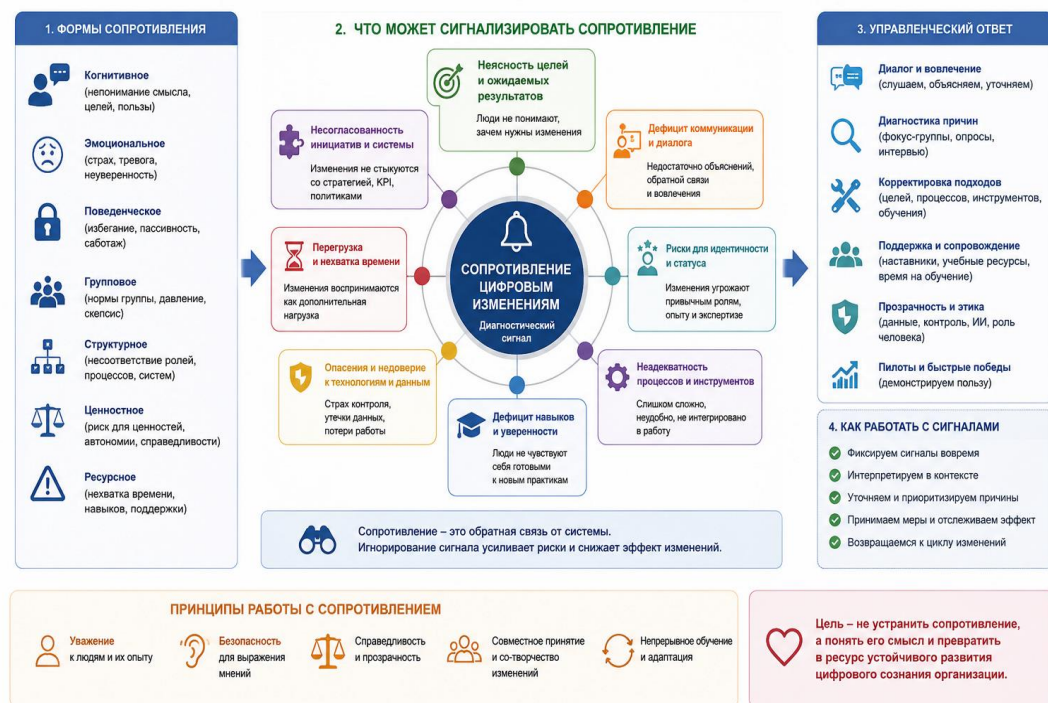


Рисунок 7.4 – Сопротивление цифровым изменениям как диагностический сигнал

Источник: составлено авторами на основе [48; 96; 97; 111; 149].

Рисунок 7.4 показывает, что сигнал проходит через разъяснение, диагностику причин, выбор управленческого ответа и проверку эффекта. Нижние блоки разграничивают допустимые меры и недопустимые реакции, включая угрозы замещением ИИ, скрытые рейтинги и добавление обучения поверх прежней нагрузки. Понятие «преодоление сопротивления» из логики подавления переводится в логику организационной диагностики. Сопротивление считается преодоленным не тогда, когда исчезают критические высказывания, а тогда, когда снижены объективные барьеры, восстановлено доверие, сотрудник понимает правила и способен безопасно действовать в новом процессе.

Основные причины сопротивления и соразмерные управленческие инструменты сопоставлены в таблице 7.5.

Таблица 7.5 – Причины сопротивления цифровым изменениям и управленческие инструменты

Причина	Уровень и проявление	Диагностика	Управленческий инструмент	Недопустимая реакция	Индикатор улучшения
Страх потери работы	Индивидуальный: пассивность, слухи, отказ обсуждать будущее	Интервью, пульс-опрос, вопросы на встречах	Прозрачная карта ролей, переобучение, карьерные сценарии	Угрозы и формула «ИИ или увольнение»	Снижение тревоги и рост участия в развитии
Дефицит навыков	Индивидуальный: избегание сервисов, зависимость от коллег	Самооценка, кейсовые задания, наблюдение	Ролевое обучение, наставник, песочница	Стыжение за отставание, публичное ранжирование	Рост уверенности и корректного применения
Страх ошибок ИИ	Индивидуальный и командный: отказ от допустимых сценариев	Разбор кейсов и вопросов к регламенту	Правила проверки, экспертная поддержка, журналирование	Принуждение без критериев верификации	Рост доли проверенных результатов и снижение ошибок
Потеря автономии	Командный: жалобы на микроконтроль, обход системы	Фокус-группа, анализ процесса, интервью	Пересмотр зон решения, профессиональные исключения	Усиление контроля и детализация наблюдения	Рост индекса автономии и снижение обходных практик
Конфликт ролей	Управленческий: споры HR, ИТ, безопасности и бизнеса	Процессный аудит, анализ эскалаций	Матрица RACI, владелец решения, проектный офис	Размывание ответственности и кулуарные договоренности	Снижение ролевых конфликтов и сроков согласования
Цифровая перегрузка	Командный и организационный: усталость, снижение качества,	Аудит нагрузки, карта сервисов, опрос	Бюджет времени, сокращение каналов и дублирования, изменение	Добавление обучения поверх прежней нагрузки	Снижение перегрузки, прерываний и

Причина	Уровень и проявление	Диагностика	Управленческий инструмент	Недопустимая реакция	Индикатор улучшения
	отказ учиться		темпа		повторного ввода
Несо согласованность руководителя	Управленческий: противоречивые сигналы и ожидание	Коммуникационный аудит, анализ решений	Единый дом сообщений, обзор исключений, управленческая сессия	Параллельные несовместимые указания	Рост понятности целей и правил
Скрытый мониторинг	Организационный: недоверие, скрытие ошибок, саботаж	Аудит цифрового следа, HR-аналитики и локальных актов	Прекращение непрозрачной практики, минимизация данных, право на объяснение	Невидимые рейтинги и автоматические санкции	Рост доверия и готовности сообщать о проблемах

Таблица 7.5 разграничивает причины и соразмерные меры. Она может использоваться как рабочая карта руководителя и HR при анализе барьеров. Столбец недопустимых реакций фиксирует границы: сопротивление не должно автоматически вести к наказанию, усилению слежки или стигматизации сотрудника.

Таким образом, сопротивление является многослойным сигналом о качестве проекта, ресурсов, справедливости, коммуникации и доверия. Его преодоление предполагает не подавление критики, а диагностику причин и корректировку условий. Карательная реакция допустима только в рамках отдельной процедуры при доказанном умышленном нарушении, но не как ответ на вопрос, тревогу, дефицит навыка или обоснованное несогласие.

7.4. ПРОФЕССИОНАЛЬНЫЕ СООБЩЕСТВА И ВНУТРЕННЯЯ СЕТЬ ЦИФРОВЫХ НАСТАВНИКОВ

Профессиональное сообщество цифровых практик определяется как устойчивое объединение сотрудников и экспертов, совместно решающих повторяющиеся профессиональные задачи, обменивающихся проверенными цифровыми решениями и формирующих организационное знание. Цифровой наставник – это подготовленный сотрудник, оказывающий коллегам горизонтальную помощь в освоении инструментов, правил и ответственных сценариев применения данных и ИИ. Эти определения подчеркивают практический и развивающий характер ролей [50; 64; 73; 76].

Профессиональное сообщество отличается от формальной рабочей группы. Рабочая группа создается для выполнения конкретного задания и действует в рамках мандата. Сообщество поддерживает длительный обмен практиками, выявляет повторяющиеся затруднения, сравнивает решения и превращает индивидуальный опыт в общую базу знаний. Оно также отличается от канала новостей: ценность возникает не из публикации материалов, а из совместного анализа реальных кейсов.

Наставничество необходимо потому, что формальное обучение не обеспечивает автоматического переноса знаний в рабочую ситуацию. После курса сотрудник сталкивается с конкретным документом, ограничением данных, непривычной системой, ошибкой ИИ или конфликтом требований. Наставник помогает интерпретировать правило, найти легитимный инструмент, выполнить действие и при необходимости эскалировать системный барьер. Эта работа сокращает дистанцию между обучением и практикой.

Роль наставника должна иметь жесткие границы. Он не оценивает лояльность, не принимает кадровых решений, не ведет скрытый мониторинг, не заменяет руководителя и не является универсальным техническим специалистом. Если проблема связана с доступом, интеграцией или сбоем, запрос передается ИТ. Если затрагивается риск утечки или нарушение режима данных – службе безопасности. Если необходима кадровая траектория – HR. Если требуется профессиональное решение – владельцу процесса. Наставник помогает правильно маршрутизировать запрос, но не подменяет функции.

Профессиональное сообщество также не должно превращаться в неформальный орган контроля. Его участники обсуждают типовые ситуации в обезличенном или разрешенном формате, формируют рекомендации и передают их владельцам решений. Персональные данные, оценки коллег и конфиденциальные материалы не могут свободно циркулировать внутри сообщества. Правила сообщества должны включать конфиденциальность, уважение, фиксацию источников и границы публикации кейсов.

Организационная сеть поддержки включает несколько ролей. Координационный центр соединяет HR, корпоративное обучение, ИТ, безопасность, специалистов по данным и ИИ, наставников и профессиональные сообщества. HR отвечает за отбор, обучение, время и признание наставников. ИТ обеспечивает сервисы, доступ и технические материалы. Служба безопасности готовит правила безопасного поведения и участвует в разборе рисков. Эксперты по данным и ИИ консультируют по качеству, ограничениям и проверке сценариев. Сообщества накапливают кейсы, а наставники поддерживают применение в подразделениях.

Практика AI@EC Европейской комиссии показывает важность соединения сети экспертов, ИИ-чемпионов, портала знаний, ролевого обучения и

межфункционального управления. Программы цифровых чемпионов в системе здравоохранения Великобритании демонстрируют эффективность длительного сопровождения, групп практического обучения и взаимной поддержки. Общий вывод состоит в том, что горизонтальная инфраструктура работает только при наличии мандата, времени, методической поддержки и канала влияния на решения [64; 73; 76].

Отбор наставников не следует строить только по уровню технической компетентности. Значимы способность объяснять без стигматизации, понимание границ роли, готовность признавать неопределенность, умение слушать, знание организационных правил и способность эскалировать риск. Технически сильный сотрудник, который демонстрирует превосходство или нарушает конфиденциальность, не создает доверия.

Подготовка наставника включает пять модулей: методика консультации; цифровые и ИИ-сценарии; безопасность и данные; работа с сопротивлением и тревогой; фиксация и обобщение запросов. Дополнительно необходима супервизия – регулярный разбор сложных случаев с методологом, HR, ИТ и службой безопасности. Супервизия защищает наставника от перегрузки и помогает отличать индивидуальный вопрос от системной проблемы.

Журнал запросов наставника должен быть минимизирован и по возможности обезличен. Его назначение – увидеть типовые барьеры, обновить инструкции, курсы и сервисы. Он не должен становиться персональным досье сотрудников. Допустимы категории запроса, подразделение, время решения, маршрут эскалации и результат. Недопустимы субъективные оценки личности, рейтинги «цифровой слабости» и использование обращений как негативного кадрового сигнала.

Профессиональное сообщество нуждается в паспорте: цель, участники, модератор, периодичность, правила работы, каналы, продукты и связь с управленческим контуром. Продуктами могут быть библиотека проверенных сценариев, чек-листы, краткие стандарты, разборы инцидентов, предложения по улучшению и обновленные учебные кейсы. Для каждого предложения должен быть определен адресат и порядок ответа.

Показатели сети должны оценивать не число встреч, а полезность и организационный эффект: долю решенных запросов, время снятия типового барьера, повторяемость проблем, вклад в базу знаний, число принятых улучшений, оценку полезности помощи, снижение цифровой тревоги и рост качества практик. Эти показатели применяются к системе поддержки, а не к персональному ранжированию наставников и пользователей.

Предполагается, что профессиональные сообщества и наставники становятся механизмом цифрового сознания, когда выполняются три условия – четкая ролевая граница, связь с формальным управлением и превращение запросов в

обновление организационных практик. Без этих условий сеть вырождается либо в клуб энтузиастов, либо в неформальную техподдержку, либо в скрытый контроль.

Организационная архитектура внутренней сети цифровых наставников и профессиональных сообществ представлена на рисунке 7.5.



Рисунок 7.5 – Внутренняя сеть цифровых наставников и профессиональных сообществ

Источник: составлено авторами на основе [50; 64; 73; 76].

Рисунок 7.5 показывает, что координационный центр соединяет функции HR, ИТ, безопасности, экспертов по данным и ИИ, наставников и профессиональные сообщества. Нижняя граница роли фиксирует, что наставник не оценивает лояльность, не принимает кадровых решений, не заменяет техническую поддержку и не выступает скрытым контролером. Также показана двунаправленность сети. Центральные функции передают наставникам правила, инструменты и обучение. Наставники и сообщества возвращают агрегированные данные о барьерах, типовых ошибках и потребностях. Благодаря этому горизонтальная помощь становится источником организационного обучения, а не параллельной неформальной системой.

Роли, границы полномочий и результаты деятельности участников сети поддержки систематизированы в таблице 7.6.

Таблица 7.6 – Роли внутренней сети поддержки цифрового сознания

Роль	Назначение	Границы роли	Основные инструменты	Показатели системы
Координационный центр	Согласование функций, приоритетов и эскалаций	Не заменяет владельцев процессов и руководителя	Карта ролей, обзор запросов, план улучшений	Сроки решений, доля закрытых системных барьеров
Цифровой наставник	Помощь в освоении инструментов и правил	Не оценивает лояльность, не принимает кадровых решений, не ведет скрытый контроль	Консультация, демонстрация, маршрутизация, база ответов	Полезность, решенные запросы, снижение повторяемости проблем
Цифровой лидер подразделения	Локальная координация практик и связь с руководителем	Не заменяет ИТ, HR и службу безопасности	Командные соглашения, локальные обзоры, план улучшений	Внедренные улучшения, качество обратной связи
Специалист технической поддержки	Устранение технических сбоев и проблем доступа	Не отвечает за развитие цифрового поведения и профессиональную методику	Система заявок, инструкции, диагностика	SLA, доступность, удовлетворенность пользователей
Эксперт по данным	Консультация по качеству, источникам и интерпретации	Не принимает бизнес-решение вместо владельца процесса	Каталог данных, методики показателей, проверка качества	Снижение дефектов данных и спорных интерпретаций
Эксперт по ИИ	Поддержка выбора сценария, ограничений и проверки	Не заменяет юридическую, этическую и управленческую экспертизу	Реестр сценариев, оценка риска, шаблоны проверки	Корректность сценариев, число своевременных эскалаций
Служба безопасности	Консультация по данным, доступу и рискам	Не использует обращения для скрытой оценки продуктивности	Классификация данных, чек-листы, разбор инцидентов	Снижение нарушений при росте своевременных сообщений

Роль	Назначение	Границы роли	Основные инструменты	Показатели системы
Модератор профессионального сообщества	Организация обмена практиками и коллективной рефлексии	Не является неформальным начальником или персональным оценщиком	Встречи, кейс-база, протокол рекомендаций	Активность, качество материалов, принятые предложения
HR и корпоративное обучение	Отбор, подготовка, время, признание и развитие сети	Не подменяет техническую и риск-экспертизу	Программа наставников, супервизия, траектории развития	Устойчивость сети, удержание наставников, перенос в практику

Таблица 7.6 представляет разграничивает роли внутри сети поддержки. Ее центральный принцип – помощь не должна превращаться в контроль, а консультационный запрос не должен создавать негативных кадровых последствий. Системные показатели используются для улучшения обучения, сервисов и регламентов.

Таким образом, наставники и профессиональные сообщества обеспечивают перевод формального обучения в повседневную практику и формируют горизонтальный контур организационного знания. Их эффективность зависит от времени, подготовки, ролевых границ, супервизии и способности влиять на обновление процессов. Наставничество несовместимо со скрытой оценкой сотрудников.

7.5. МОТИВАЦИЯ СОТРУДНИКОВ К РАЗВИТИЮ ЦИФРОВОГО СОЗНАНИЯ

Мотивация к развитию цифрового сознания определяется как устойчивая готовность сотрудника и команды осваивать ответственные цифровые практики, применять их в работе, делиться опытом и участвовать в улучшении организационной среды. Мотивационный результат не равен принужденному использованию сервиса. Он проявляется в осмысленном действии, соблюдении границ, критической проверке результатов и готовности сообщать о рисках.

Теория самодетерминации связывает устойчивую внутреннюю мотивацию [142] с удовлетворением потребностей в автономии, компетентности и связанности. В цифровой трансформации автономия означает возможность понимать и обсуждать способ действия, а не слепо следовать алгоритму. Компетентность требует обучения и практики. Связанность обеспечивается поддержкой руководителя, наставников и сообщества. Если изменение строится только на внешнем давлении, мотивация становится краткосрочной и стимулирует формальное поведение.

Мотивационный контур целесообразно строить как последовательность «смысл – возможность – поддержка – признание – развитие». Смысл отвечает на вопрос, зачем новое поведение нужно организации и сотруднику. Возможность включает время, доступ и удобные легитимные инструменты. Поддержка дает обучение, наставника и безопасный канал вопроса. Признание делает вклад видимым. Развитие связывает практику с проектами, сертификацией, профессиональной мобильностью и новыми ролями.

Выделенное рабочее время является базовым мотиватором. Требование постоянно учиться без изменения нагрузки воспринимается как перекалывание стоимости трансформации на сотрудника. Организация должна планировать время на освоение, практические задания, участие в сообществе и наставничество. Для ролей с дополнительной нагрузкой необходимы формальное закрепление функций, ограничение объема и компенсация.

Возможность пользоваться утвержденным и удобным инструментом также влияет на мотивацию. Если корпоративный сервис медленнее, сложнее или недоступнее внешнего, запретительная политика стимулирует теневые практики. Поэтому ИТ и служба безопасности должны совместно создавать безопасные пользовательские сценарии, а не только фиксировать нарушения. Мотивация к безопасному поведению повышается, когда правильный путь является понятным и практически доступным.

Признание должно быть связано с качеством вклада. Организация может отмечать разработку полезного кейса, помощь команде, выявление риска, улучшение процесса, создание шаблона проверки или участие в пилоте. Недопустимо поощрять число запросов к ИИ, время нахождения в системе, количество сообщений или демонстративную «цифровую активность». Такие метрики легко имитируются и искажают цель.

Командное признание предпочтительно там, где результат создается совместно. Соревнование подразделений по числу внедренных сервисов может снижать обмен знаниями и стимулировать скрытие проблем. Командная номинация за ответственное улучшение процесса подчеркивает сотрудничество, качество данных, снижение риска и ценность для пользователя.

Карьерная мобильность является сильным развивающим механизмом. Участие в пилотах, наставничестве и профессиональных сообществах может учитываться при формировании кадрового резерва, проектных ролей и индивидуальных планов развития. При этом критерии должны быть прозрачными, доступ к возможностям – открытым, а отказ от дополнительной роли не должен интерпретироваться как низкая лояльность.

Материальное стимулирование допустимо для дополнительной ответственности: ведение сообщества, разработка программы, наставническая нагрузка, управление рискованной пилотом. Однако премия не должна заменять

смысл, время и поддержку. Система, в которой сотруднику платят за количество формальных действий, создает игровое поведение и не формирует цифровое сознание.

Экономическая аргументация развития навыков важна, но требует осторожности. Исследования рынка труда показывают рост спроса на ИИ-компетенции и необходимость массового переобучения. Для организации это не означает автоматического сокращения персонала. Более зрелая стратегия связывает обучение с перераспределением задач, внутренней мобильностью и повышением качества работы [23; 74; 117; 151].

Мотивация к сообщению о рисках требует отдельной защиты. Сотрудник не будет информировать об ошибке ИИ, подозрительном сервисе или утечке, если ожидает наказания за сам факт обнаружения. Безобвинительный первичный разбор не отменяет ответственности за умышленное нарушение, но отделяет добросовестное сообщение и обучение от дисциплинарной процедуры. Это критично для безопасности и организационной рефлексии.

Предполагается, что устойчивая мотивация к развитию цифрового сознания возникает при совпадении пяти условий – понятного смысла, реальной возможности, доступной поддержки, справедливого признания и перспективы развития. Изолированное материальное стимулирование или давление KPI без этих условий увеличивает формализм и теневое поведение.



Рисунок 7.6 – Мотивационный контур развития цифрового сознания

Источник: составлено авторами на основе [73; 74; 117; 151].

Рисунок 7.6 показывает, что ответственное цифровое поведение помещено в центр пяти взаимосвязанных факторов: смысла, возможности, поддержки, признания и развития. Нижний блок фиксирует баланс стимулов: материальная компенсация возможна за дополнительный вклад, но не за формальное количество цифровых действий. Также рисунок 7.6 служит картой проектирования мотивационной среды. Если сотрудник понимает смысл, но не имеет времени, мотивационный контур неполон. Если есть обучение, но отсутствуют легитимные инструменты, знания не переносятся в практику. Если вклад признается только индивидуально, командное обучение ослабевает. Поэтому мотивация оценивается как конфигурация условий, а не как личное качество работника.

Механизмы мотивации, критерии их применения и ограничения обобщены в таблице 7.7.

Таблица 7.7 – Механизмы мотивации к развитию цифрового сознания

Механизм	Целевая группа	Развиваемое поведение	Условия применения	Риск искажения	Развивающий показатель
Выделенное время на обучение	Все сотрудник и и руководители	Регулярное освоение и перенос практик	Обучение встроено в рабочий план, прежняя нагрузка пересмотрена	Формальное прохождение без применения	Доля участников, применивших практику в рабочем кейсе
Доступ к легитимным инструментам	Пользователи данных и ИИ	Безопасный выбор утвержденного сервиса	ИТ и безопасность обеспечиваются доступностью и понятными сценарии	Теневое использование из-за неудобства	Снижение обходных практик и времени на типовую задачу
Наставничество и взаимная помощь	Новые пользователи, команды пилота	Запрос помощи, проверка результата, обмен опытом	Есть подготовленные наставники, время и границы роли	Зависимость от отдельных энтузиастов	Полезность помощи и снижение повторных барьеров
Признание цифровых улучшений	Команды, наставники, авторы	Инициативность, качество, обмен знаниями	Прозрачные критерии и командный	Куль героев, конкуренция	Число принятых улучшений

Механизм	Целевая группа	Развиваемое поведение	Условия применения	Риск искажения	Развиваемый показатель
	кейсов		акцент	и имитация активности	и их эффект
Участие в пилотах и проектах	Сотрудник и с интересом к развитию	Ответственность, экспериментирование, межфункциональность	Открытый отбор и безопасный контур пилота	Элитарность и перегрузка участников	Доля практик, перенесенных в регулярный процесс
Сертификация и кадровый резерв	Специалисты и руководители	Закрепление компетенций и готовность к новым ролям	Связь с реальными задачами, прозрачные критерии	Бюрократизация сертификатов	Внутренняя мобильность и качество выполнения новых ролей
Материальная компенсация дополнительной роли	Наставники, модераторы, авторы программ	Устойчивое выполнение дополнительной функции	Формально закрепленная нагрузка и измеримый вклад	Подмена смысла премией и гонка показателей	Удержание сети и выполнение согласованных функций
Культура сообщения о рисках	Все участники цифровых процессов	Раннее сообщение, рефлексия, предотвращение ущерба	Разделение добросовестного сообщения и умышленного нарушения	Скрытие ошибок из-за страха санкций	Рост ранних сообщений при снижении тяжести инцидентов

Таблица 7.7 механизмы направлены на качество цифрового поведения и среды. Процессные показатели рассматриваются только вместе с переносом в практику, снижением барьеров и эффектом для процессов. Само участие в обучении или частота использования ИИ не являются достаточным основанием для вознаграждения.

Таким образом, мотивация к развитию цифрового сознания создается организационной средой, а не извлекается из сотрудника давлением. Смысл, время, легитимные инструменты, обучение, наставничество, справедливое признание и карьерная перспектива должны действовать совместно. КРІ мотивации не могут поощрять цифровую активность ради активности.

7.6. ВКЛЮЧЕНИЕ ЦИФРОВОГО СОЗНАНИЯ В КРІ, РЕГЛАМЕНТЫ И КАДРОВУЮ ПОЛИТИКУ

Институционализация цифрового сознания определяется как закрепление ответственного цифрового поведения в стратегии, ролях, регламентах, показателях, кадровых процессах, обучении и механизмах управления рисками. Ее задача – сделать новые практики устойчивыми и воспроизводимыми, не превращая цифровую культуру в систему тотального контроля. Поэтому институционализация должна одновременно усиливать управляемость и устанавливать ограничения на сбор данных, автоматизированную оценку и кадровые решения [67; 83; 93; 97; 100; 139].

Ключевой методический вопрос состоит не в том, нужны ли показатели, а в том, что именно они измеряют и какие решения запускают. Необходимо различать цифровую активность, цифровую компетентность, качество цифрового поведения, командную практику, управленческую ответственность и организационную зрелость. Количество входов в систему, сообщений, запросов к ИИ и пройденных модулей отражает активность, но не доказывает критичность, этичность, безопасность и результативность.

Допустимый КРІ цифрового сознания должен отвечать пяти требованиям. Во-первых, быть связанным с организационной целью и качеством процесса. Во-вторых, иметь понятную методику и владельца. В-третьих, использовать минимально необходимый объем данных. В-четвертых, допускать объяснение, контекст и человеческий пересмотр. В-пятых, вести преимущественно к развивающему решению: обучению, изменению процесса, ресурса, сервиса или регламента.

Недопустимыми являются скрытые показатели, о которых сотрудник не информирован; автоматические кадровые решения без содержательного человеческого пересмотра; непрозрачное ранжирование; использование самооценки для санкций; выводы о качестве труда только по времени онлайн, числу кликов или объему коммуникации; сбор цифрового следа вне заявленной цели; использование данных обращения к наставнику как негативного кадрового сигнала [54; 97].

На уровне сотрудника предпочтительны качественные и кейсовые индикаторы: умеет ли он проверить ИИ-результат, правильно классифицировать данные, объяснить ограничение инструмента, вовремя сообщить о риске, использовать утвержденное хранилище. Такие индикаторы применяются для развития и допуска к отдельным сценариям, но не образуют скрытый рейтинг личности. Ошибка в учебном кейсе рассматривается как основание обучения, а не санкции.

На уровне команды оцениваются согласованность правил, качество совместной работы с данными, фиксация решений, вклад в базу знаний, способность обсуждать ошибки и снижать цифровую нагрузку. Командный уровень снижает риск индивидуализации системных проблем. Если несколько сотрудников допускают одну ошибку, сначала проверяются инструкция, интерфейс, процесс и обучение.

На уровне руководителя оцениваются не количество внедренных сервисов, а качество лидерской среды: ясность смысла, выделение ресурсов, доступность обратной связи, снижение барьеров и перегрузки, обеспечение человеческой проверки, выполнение корректирующих действий. Такой подход удерживает ответственность за результат на управленческом уровне и не позволяет переложить неудачу цифрового проекта на «неподготовленных пользователей».

На организационном уровне учитываются наличие и актуальность политик по данным и ИИ, реестр сценариев, зрелость наставнической сети, регулярность анализа рисков, динамика доверия, выполнение плана развития и результативность ежегодного цикла. Здесь KPI выступают инструментом управления системой, а не наблюдения за каждым сотрудником.

Роль HR-службы состоит в проектировании справедливых кадровых процедур, ролевых моделей компетенций, обучения, адаптации, развития и признания. HR не должен самостоятельно интерпретировать технические данные как показатели эффективности труда. Любая HR-аналитика, связанная с цифровым следом, требует цели, правового основания, проверки качества данных, оценки влияния, минимизации и объяснения сотрудникам.

Роль ИТ-службы – обеспечить надежную архитектуру, доступность, интеграции, журналирование безопасности и корректность технических метрик. ИТ не принимает решения о компетентности или лояльности сотрудников. Технический лог показывает событие в системе, но не раскрывает контекст работы, мотивы, качество профессионального суждения и скрытую нагрузку.

Служба информационной безопасности отвечает за классификацию данных, контроль доступа, оценку цифровых и ИИ-рисков, реагирование и профилактику. Ее показатели должны отражать своевременность сообщения, устойчивость и снижение ущерба, а не число наказанных нарушителей. Культура безопасности развивается, когда раннее сообщение считается полезным действием и не скрывается из-за страха.

Наставники и профессиональные сообщества не включаются в персональный контроль. Их данные используются агрегированно: типы запросов, повторяющиеся барьеры, востребованные темы, время решения, потребность в доработке сервиса. Персональный журнал консультаций хранится только в минимально необходимом объеме и не передается в кадровую оценку без отдельного законного и заранее объявленного основания.

Пакет локальных нормативных актов должен быть согласованным. Положение о формировании цифрового сознания задает общую рамку; кодекс цифровой этики – ценностные границы; политика управления данными – владельцев и режимы; регламент применения ИИ – допустимые сценарии и проверку; правила цифровой коммуникации – каналы и нагрузку; положение о наставничестве – роль и гарантии; порядок диагностики – методику и ограничения; регламент ежегодного отчета – цикл решений. Документы не должны дублировать друг друга или содержать противоречивые определения.

Предполагается, что включение цифрового сознания в KPI и HR-политику повышает устойчивость цифровой культуры только при действии этического шлюза. Если показатели прозрачны, минимизированы, объяснимы, пересматриваются человеком и ведут к развитию, они поддерживают обучение. Если эти условия нарушены, те же показатели создают надзор, игровое поведение, снижение доверия и скрывание ошибок.

Этическая архитектура применения показателей и диагностики цифрового сознания представлена на рисунке 7.7.



Рисунок 7.7 – Этическая архитектура KPI и диагностики цифрового сознания

Источник: составлено авторами на основе [54; 67; 83; 97; 100; 139].

Рисунок 7.7 показывает, что пирамида разводит процессные метрики, качество поведения, командную практику, управленческую ответственность и организационный результат. Нижние блоки задают этические гарантии и прямо запрещают скрытый мониторинг, автоматические кадровые решения, непрозрачные рейтинги и санкции по самооценке. Также показывается принцип приоритетности. Процессные метрики находятся в основании и имеют ограниченную интерпретацию. Качественные выводы возникают только при их соединении с поведением, командным контекстом и управленческой ответственностью. Организационный результат нельзя напрямую приписывать отдельному сотруднику по техническому следу.

Допустимые показатели цифрового сознания, источники данных и этические ограничения представлены в таблице 7.8.

Таблица 7.8 – Матрица допустимых показателей цифрового сознания

Уровень	Допустимый показатель	Источник данных	Периодичность	Развивающее решение	Этическое ограничение
Сотрудник	Качество проверки ИИ-результатов в учебном или рабочем кейсе	Кейс, самоотчет, экспертная выборочная проверка	По этапам обучения или допуска	Обучение, уточнение чек-листа, консультации	Не используется для скрытого рейтинга и автоматической санкции
Сотрудник	Соблюдение правил работы с данными и утвержденными сервисами	Инциденты, кейсы, подтвержденные факты	Квартал и по событию	Разбор причины, обучение, корректировка процесса	Цифровой след не является единственным доказательством вины
Команда	Согласованность правил цифровой коммуникации и применения ИИ	Командная самооценка, анализ артефактов, ретроспектива	Квартал	Командное соглашение, настройка процесса	Оценивается среда и практика, а не «слабые» участники
Команда	Вклад в базу знаний и взаимное обучение	Обезличенный журнал сообщества, продукты команды	Квартал	Поддержка сообщества, выделение времени	Количество публикаций не заменяет оценку полезности
Руководитель	Качество обратной	Опрос, 360 градусов,	Полугодие	Коучинг, изменение	Критика руководителя

Уровень	Допустимый показатель	Источник данных	Периодичность	Развивающее решение	Этическое ограничение
	связи и снятия цифровых барьеров	протоколы решений		роли, ресурсное решение	защищена от ответных санкций
Руководитель	Снижение цифровой нагрузки и рисков при сохранении результата	Аудит нагрузки, реестр рисков, показатели процесса	Квартал	Пересмотр сервисов, сроков, ресурсов и правил	Нельзя повышать результат за счет скрытого переноса нагрузки
Организация	Наличие и актуальность политик по данным, ИИ, безопасности, коммуникации и диагностике	Реестр локальных актов и аудит применения	Год	Ревизия управления и обучение владельцев	Наличие документа не считается достаточным без проверки практики
Организация	Выполнение плана развития цифрового сознания и динамика индексов	Годовой отчет, триангуляция данных	Год	Обновление стратегии, бюджета и программы развития	Диагностика не используется для персональных санкций
Организация	Доверие и готовность сообщать о рисках	Анонимный опрос, фокус-группы, анализ ранних сообщений	Полугодие	Корректировка коммуникации и гарантий	Не допускается поиск авторов анонимной критики

Таблица 7.8 представляет связывает показатель с источником, периодичностью и развивающим решением. Этическое ограничение является частью паспорта показателя. Если ограничение невозможно обеспечить, показатель исключается из системы.

Состав и назначение локальных нормативных документов формирования цифровой культуры приведены в таблице 7.9.

Таблица 7.9 – Пакет локальных нормативных документов формирования цифровой культуры

Документ	Предмет регулирования	Владелец	Обязательные положения	Риск формализации
Положение о формировании цифрового сознания	Цели, принципы, роли, контуры и ежегодный цикл	Руководитель организации и куратор	Человекоцентричность, некарательность, распределение функций, отчетность	Декларация без ресурсов и владельцев
Кодекс цифровой этики	Права, справедливость, прозрачность, человеческая ответственность	Комплаенс и этический орган	Право на объяснение, пересмотр, маркировка ИИ, запрет дискриминации	Общие лозунги без процедур
Политика управления данными	Владение, качество, доступ, хранение и использование данных	Владелец данных и ИТ	Каталог данных, классификация, минимизация, сроки, качество	Отсутствие связи с процессами и ИИ-сценариями
Регламент применения ИИ	Допустимые сценарии, риски, проверка и ответственность	Куратор, ИТ, безопасность, юридическая функция	Реестр сценариев, человеческая проверка, запрещенные данные, журналирование	Запреты без легитимных альтернатив и обучения
Правила цифровой коммуникации	Каналы, фиксация решений, сроки ответа и цифровая нагрузка	Внутренние коммуникации и руководители подразделений	Назначение каналов, единый источник, режим срочности, право на отключение	Документ не поддержан поведением руководителей
Положение о цифровом наставничестве	Назначение, отбор, время, границы и поддержка	HR и корпоративное обучение	Неоценочная роль, конфиденциальность, супервизия, эскалация	Подмена наставника техподдержкой или

Документ	Предмет регулирования	Владелец	Обязательные положения	Риск формализации
	наставников			контролером
Порядок диагностики цифрового сознания	Цели, методы, данные, права участников и использование результатов	HR, аналитическая функция и комплаенс	Добровольность где возможно, минимизация, агрегирование, запрет санкций	Скрытая аттестация и сбор избыточного следа
Регламент ежегодного аналитического отчета	Структура, сроки, ответственные и управленческие решения	Куратор и проектный офис	Динамика индексов, риски, нагрузка, доверие, обучение, корректировки	Отчетность без бюджета и решений

Таблица 7.9 пакет документов должен использовать единый глоссарий и не дублировать нормы. Операциональность проверяется по наличию владельцев, процедур, ресурсов, примеров и механизма обновления. Формальный документ без изменения практики не повышает цифровую зрелость.

Индекс управляемости изменений и цифровой культуры

Для интегральной оценки предлагается индекс управляемости изменений и цифровой культуры (ИУИЦК). Он не заменяет индексы цифрового сознания сотрудника, команды и организации, введенные в главе 5, а оценивает качество культурно-управленческого сопровождения. Индекс рассчитывается по семи контурам: лидерство, коммуникация, работа с сопротивлением, наставничество и сообщества, мотивация, институционализация, ежегодный цикл.

Каждый контур включает набор индикаторов, оцениваемых по шкале от 0 до 4: 0 – практика отсутствует; 1 – носит эпизодический характер; 2 – формально определена, но применяется неравномерно; 3 – системно применяется и контролируется; 4 – интегрирована, доказательно оценивается и регулярно совершенствуется. Субиндекс контура определяется по формуле:

$$C_k = (\sum r_{ki} / (4 \times n_k)) \times 100,$$

где C_k – субиндекс k-го контура; r_{ki} – оценка i-го индикатора от 0 до 4; n_k – число индикаторов контура; 4 – максимальная оценка.

Интегральный индекс рассчитывается как взвешенная сумма субиндексов. Рекомендуемые веса отражают повышенную значимость лидерства и институционализации: лидерство – 0,18; коммуникация – 0,14; работа с сопротивлением – 0,14; наставничество и сообщества – 0,12; мотивация – 0,12; институционализация – 0,18; ежегодный цикл – 0,12. Организация может изменить веса до диагностики, если документирует отраслевое обоснование.

$$\text{ИУИЦК} = \sum (w_k \times C_k), \text{ при } \sum w_k = 1,$$

где w_k – вес k -го контура; C_k – его субиндекс в диапазоне 0–100.

Числовой результат применяется только совместно с профилем контуров, качественными данными и этическим коэффициентом допустимости. Высокий средний балл не должен скрывать провал отдельного критического контура. Например, развитое наставничество не компенсирует скрытый мониторинг, а качественная коммуникация не компенсирует отсутствие человеческого пересмотра кадрового решения.

Для проверки этической допустимости системы показателей вводится коэффициент этической допустимости (КЭД). Оцениваются шесть бинарных гарантий: прозрачность цели и методики; минимизация данных; право на объяснение; человеческий пересмотр; развивающее назначение; отсутствие скрытого мониторинга. Каждая гарантия принимает значение 1 при подтверждении и 0 при отсутствии.

$$\text{КЭД} = (\sum e_j / 6) \times 100,$$

где e_j – наличие j -й этической гарантии. Значение КЭД ниже 84 баллов означает отсутствие как минимум одной из шести обязательных гарантий.

Применяется правило этического шлюза: при КЭД ниже 84 баллов организация не может быть отнесена к интегрированному или адаптивно-рефлексивному уровню независимо от значения ИУИЦК. Если отсутствует запрет скрытого мониторинга, право на объяснение или человеческий пересмотр, система диагностики должна быть перепроектирована до использования результатов в управлении.

Уровни управляемости изменений и цифровой культуры и критерии их интерпретации представлены в таблице 7.10.

Таблица 7.10 – Шкала интерпретации индекса управляемости изменений и цифровой культуры

Диапазон ИУИЦК	Уровень	Характеристика	Приоритетное решение	Этическое условие
0–20	Критически фрагментарный	Контуров отсутствуют или действуют как разовые несвязанные меры; высок риск недоверия и теневых практик	Остановить формальное масштабирование, определить роли, гарантии и базовую коммуникацию	Провести этический аудит; персональные выводы запрещены
21–40	Начальный	Есть отдельные лидеры, обучение и документы, но практика зависит от энтузиастов и	Создать межфункциональный контур, сеть поддержки и карту барьеров	Обеспечить минимум данных и право на вопрос

Диапазон ИУИЦК	Уровень	Характеристика	Приоритетное решение	Этическое условие
		неравномерна		
41–60	Управляемый	Основные процессы определены, однако обратная связь и институционализация неполны	Связать КРІ с качеством среды, усилить корректировки и ежегодный цикл	КЭД должен быть не ниже 84 для дальнейшего роста
61–80	Интегрированный	Контуры согласованы, роли разделены, показатели ведут к развитию, практики масштабируются	Улучшать качество данных, доверие, перенос обучения и межфункциональное обучение	Все шесть гарантий подтверждены и периодически проверяются
81–100	Адаптивно-рефлексивный	Организация регулярно пересматривает нормы, учится на сигналах и сохраняет ответственность в среде ИИ	Поддерживать двойную петлю обучения, отраслевую адаптацию и внешний обмен практиками	КЭД = 100; любые исключения требуют отдельного публичного обоснования

Таблица 7.10 содержит интерпретирует не «качество сотрудников», а зрелость системы управления изменениями. Переход между уровнями требует подтверждения практики несколькими источниками и соблюдения этического шлюза. Индекс используется для приоритизации развития, а не для рейтинга подразделений без учета контекста.

Таким образом, институционализация цифрового сознания требует показателей, документов и кадровых процедур, но их допустимость определяется этическими гарантиями. КРІ должны оценивать качество поведения, командных практик, управленческой ответственности и организационной среды. Скрытый мониторинг, автоматические кадровые решения, непрозрачные рейтинги и санкции по самооценке исключаются.

7.7. ЕЖЕГОДНЫЙ ЦИКЛ ОЦЕНКИ И РАЗВИТИЯ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

Ежегодный цикл оценки и развития цифрового сознания определяется как институционализированная последовательность диагностики, анализа, коллективной рефлексии, управленческих решений, обучения, изменения практик, мониторинга и повторной оценки. Его назначение состоит не в подготовке формального отчета, а в обновлении стратегии, ролей, регламентов, сервисов и программ развития на основе доказательств и опыта организации.

Цикл продолжает логику главы 5, где диагностика рассматривалась как развивающая процедура, и главы 6, где внедрение было представлено как управляемый процесс. В главе 7 диагностика включается в организационное обучение. Это означает, что результатом оценки становится не только балл, но и изменение управленческого решения: выделение ресурсов, пересмотр процесса, обновление программы, изменение правил данных и ИИ, поддержка наставников или прекращение неэффективной практики.

Теория одинарной и двойной петли обучения позволяет различить два типа корректировки. В одинарной петле организация устраняет отклонение, сохраняя исходное правило: например, проводит дополнительное обучение при ошибках пользователей. В двойной петле она пересматривает само основание: возможно, сервис неудобен, показатель неверно спроектирован, роль не обеспечена ресурсом или правило стимулирует обход. Цифровое сознание требует сочетания обеих петель [55; 75; 119].

Первый этап – подготовка. До сбора данных утверждаются цели, индикаторы, этические ограничения, состав участников, источники и порядок использования результатов. Сотрудники информируются о том, какие данные собираются, как обеспечивается конфиденциальность и какие решения не могут приниматься автоматически. Изменение методики в течение цикла документируется, чтобы сохранялась сопоставимость.

Второй этап – диагностика. Используются опросы, кейсовые задания, интервью, экспертная оценка, анализ документов, агрегированная аналитика процессов и данные о рисках. Применяется триангуляция: ни один источник не считается достаточным сам по себе. Цифровой след используется только при заранее определенной цели, минимизации и контекстной интерпретации. Самооценка отражает восприятие и потребность в развитии, но не является доказательством фактической компетентности или нарушения.

Третий этап – аналитическая интерпретация. Рассчитываются индексы, строятся профили контуров, сопоставляются количественные и качественные данные. Анализируется динамика относительно предыдущего периода, но сравнение подразделений проводится осторожно, с учетом функций, уровня риска, цифровой инфраструктуры и характера работы. Методологически неверно объявлять подразделение «отстающим» только по среднему баллу без анализа условий.

Четвертый этап – коллективная рефлексия. Результаты обсуждаются с руководством, подразделениями, наставниками, профессиональными сообществами, HR, ИТ, службой безопасности и представителями сотрудников. Задача обсуждения – проверить интерпретацию, выявить причины и отделить системные дефициты от локальных. Участникам должна быть доступна возможность уточнить данные и оспорить вывод.

Пятый этап – управленческое решение. По каждому приоритету определяются владелец, ресурс, срок, ожидаемый эффект и показатель проверки. Решение может относиться к обучению, процессу, сервису, архитектуре, нагрузке, коммуникации, безопасности, регламенту или структуре ролей. Если единственным решением по всем дефицитам является курс обучения, цикл считается методически неполным.

Шестой этап – развитие и изменение практик. Запускаются ролевые программы, наставничество, командные соглашения, доработка сервисов, пересмотр доступа, обновление реестров данных и ИИ, коммуникационные меры и пилоты. Развитие должно быть связано с конкретными рабочими ситуациями. Общий курс без последующего применения не закрывает диагностический разрыв.

Седьмой этап – мониторинг. Отслеживаются выполнение решений, изменение поведения, качество процессов, риски, нагрузка, доверие и обратная связь. Мониторинг не должен превращаться в непрерывное наблюдение за сотрудником. Предпочтительны агрегированные показатели, выборочные проверки, ретроспективы и анализ инцидентов. Персональный контроль допускается только при ясном основании, пропорциональности и установленной процедуре.

Восьмой этап – повторная оценка и обновление. Организация проверяет, какие решения дали эффект, какие создали побочные последствия и какие предпосылки необходимо пересмотреть. Обновляются методика, приоритеты, локальные документы, карта рисков и программа развития. Завершение цикла становится началом нового, что обеспечивает адаптивность в условиях изменения технологий и требований.

Годовой аналитический отчет должен содержать не менее двенадцати блоков: методика и ограничения; динамика ИЦСС, ИЦСК, ИОЦС и ИУИЦК; профиль цифровой культуры; результаты обучения; деятельность наставников и сообществ; состояние данных; использование ИИ; цифровые риски и инциденты; цифровая нагрузка; доверие и голос сотрудников; результаты пилотов и улучшений; план корректирующих действий. В отчете отдельно фиксируется соблюдение этических гарантий.

Годовой отчет не должен включать списки «цифрово слабых» сотрудников, рейтинги обращений к наставникам, необъяснимые интегральные оценки и выводы о лояльности. Персональные данные приводятся только при необходимости и правовом основании, преимущественно в обезличенном виде. Основная единица анализа – контур, процесс, команда или организационная практика.

Предполагается, что ежегодный цикл становится механизмом организационного цифрового сознания, если результаты диагностики связаны с

бюджетом, ответственными решениями и проверкой эффекта, а участники имеют право на объяснение и корректировку интерпретации. Без этой связи цикл деградирует в отчетность и снижает доверие к диагностике.

Последовательность ежегодного цикла оценки и развития цифрового сознания организации представлена на рисунке 7.8.



Рисунок 7.8 – Ежегодный цикл оценки и развития цифрового сознания организации

Источник: составлено авторами на основе [55; 74; 75; 100; 119; 151].

Рисунок 7.8 показывает, что восемь этапов замыкаются вокруг организационного обучения и обновления. Красная методическая оговорка подчеркивает: повторная диагностика предназначена для оценки динамики, приоритизации развития и проверки управленческих решений, а не для персональных санкций. Так же, демонстрируется, что цикл не является календарной формальностью. Он содержит две обязательные обратные связи: от рефлексии к интерпретации и от мониторинга к управленческим решениям. Это позволяет не только исправлять отдельные отклонения, но и пересматривать правила, на которых построена цифровая практика.

Содержание этапов ежегодного цикла, ответственные и контрольные точки систематизированы в таблице 7.11.

Таблица 7.11 – Этапы ежегодного цикла оценки и развития цифрового сознания

Этап	Цель	Ключевые действия	Ответственные	Артефакт	Контрольная точка
1. Подготовка	Зафиксировать цели, методику и гарантии	Утверждение индикаторов, источников, состава участников, порядка информирования и использования данных	Руководитель, куратор, HR, комплаенс, аналитики	Паспорт цикла и информационный лист	Методика прозрачна, этический шлюз пройден
2. Диагностика	Получить сопоставимые данные о контурах и практиках	Опросы, кейсы, интервью, документы, агрегированная аналитика, экспертная оценка	HR, аналитики, эксперты, представители подразделений	Массив данных и протокол ограничений	Данные достаточны и не основаны на одном источнике
3. Анализ	Выявить динамику, сильные стороны, дефициты и риски	Расчет индексов, профиль контуров, сравнение с предыдущим периодом, анализ контекста	Аналитическая группа и куратор	Проект аналитического отчета	Выводы подтверждены триангуляцией
4. Рефлексия	Проверить интерпретацию и выявить причины	Обсуждения с командами, наставникам и, сообществам и и функциями; право на уточнение	Руководители, HR, ИТ, безопасность, представители сотрудников	Протокол уточнений и причин	Участники могут объяснить и оспорить вывод
5. Решение	Перевести выводы в управленческий план	Выбор приоритетов, владельцев, ресурсов, сроков и ожидаемого эффекта	Руководитель и управленческая команда	План корректирующих действий	Каждый приоритет имеет владельца и ресурс

Этап	Цель	Ключевые действия	Ответственные	Артефакт	Контрольная точка
6. Развитие	Изменить компетенции, процессы, сервисы и нормы	Обучение, наставничество, доработка сервисов, обновление регламентов и коммуникации	HR, ИТ, безопасность, владельцы процессов, наставники	Программы, обновленные процессы и документы	Меры соответствуют диагностированной причине
7. Мониторинг	Проверить исполнение, эффект и побочные последствия	Агрегированные метрики, выборочные проверки, ретроспективы, анализ рисков и нагрузки	Куратор, проектный офис, аналитики и владельцы	Панель мониторинга и журнал решений	Мониторинг не превращен в персональный надзор
8. Обновление	Закрепить уроки и запустить новый цикл	Повторная оценка, пересмотр методики, стратегии, рисков, обучения и документов	Координационный орган и руководитель	Годовой отчет и план следующего периода	Проверен эффект решений и обновлены приоритеты

Таблица 7.11 задает управленческую технологию ежегодного цикла. Переход между этапами осуществляется после контрольной точки. Диагностика не является финалом; она ценна только тогда, когда приводит к ресурсному решению, изменению практики и последующей проверке эффекта.

Интегральная ролевая архитектура управления изменениями

Для практического применения главы необходима матрица RACI (распределение ролей по признакам: выполняет, несет итоговую ответственность, консультирует, информируется). В русской интерпретации используются обозначения: И – исполняет действие; О – несет итоговую ответственность; К – консультирует; У – уведомляется. Матрица не заменяет должностные полномочия, а показывает межфункциональное взаимодействие в формировании цифровой культуры.

Принципиальное разграничение состоит в следующем. Руководитель организации отвечает за стратегию, ресурсы и этические границы. HR отвечает за людей, обучение, справедливость и прозрачность кадровых процедур. ИТ отвечает за сервисы, интеграции, доступность и технические данные. Служба

безопасности отвечает за риск-контроль, данные, доступ и инциденты. Цифровые наставники исполняют горизонтальную поддержку, но не оценивают сотрудников. Профессиональные сообщества обеспечивают обмен знаниями и рефлексия, но не принимают обязательных кадровых и технических решений.

Распределение ролей по модели RACI в управлении изменениями и развитии цифровой культуры представлено в таблице 7.12.

Таблица 7.12 – Матрица RACI управления изменениями и развитием цифровой культуры

Процесс	Руководитель	HR / обучение	ИТ	Служба безопасности	Наставники	Профессиональные сообщества
Стратегия цифровой культуры и этические рамки	О	К	К	К	У	К
Коммуникационная стратегия и голос сотрудников	О	И	К	К	К	К
Диагностика потребностей и развивающая оценка	У	О / И	К	К	К	К
Архитектура сервисов и легитимные инструменты	У	К	О / И	К	К	К
Классификация данных, рисков и ИИ-сценариев	У	К	И	О / И	К	К
Рольное обучение и программы развития	У	О / И	К	К	И	К
Повседневная консультационная поддержка	У	О	К	К	И	К
Обмен кейсами и организационное знание	У	К	К	К	И	О / И
Корректировка	О	К	К	К	К	К

Процесс	Руководитель	HR / обучение	ИТ	Служба безопасности	Наставники	Профессиональные сообщества
процессов и распределение нагрузки						
Разбор цифрового или ИИ-инцидента	У	К	И	О / И	К	К
Ежегодный отчет и план развития	О	И	К	К	К	К
Кадровое решение, связанное с цифровой ролью	О	И	У	К	У	У

Таблица 7.12 представляет исключает функциональную подмену. ИТ и служба безопасности предоставляют техническую и риск-экспертизу, но не принимают кадровых решений; HR организует развитие, но не интерпретирует технический лог без контекста; наставники и сообщества помогают и обучают, но не оценивают лояльность.

Система диагностических вопросов, индикаторов, методов и управленческих решений обобщена в таблице 7.13.

Таблица 7.13 – Система диагностических индикаторов управления изменениями и цифровой культуры

Контур	Ключевой диагностический вопрос	Индикаторы	Методы	Тип управленческого решения
Лидерство	Создает ли руководство смысл, ресурсы, безопасность и ответственность?	Ясность целей; выделенное время; человеческий контроль; выполненные корректировки; снижение перегрузки	Опрос, 360 градусов, документы, интервью, анализ решений	Коучинг, перераспределение ресурсов, изменение роли и портфеля
Коммуникация	Понимают ли участники цели, риски,	Понятность сообщений; охват	Опрос, коммуникационный аудит,	Обновление сообщений, каналов, FAQ и

Контур	Ключевой диагностический вопрос	Индикаторы	Методы	Тип управленческого решения
	правила и каналы влияния?	аудиторий; сроки ответов; доля реализованных предложений	журнал вопросов	процедуры участия
Соппротивление	Выявляются ли причины и корректируются ли условия?	Уровень тревоги; барьеры навыков и нагрузки; доверие; число системных корректировок	Интервью, фокус-группы, аудит нагрузки, анализ барьеров	Обучение, доработка сервиса, RACI, изменение темпа и правил
Наставничество и сообщества	Работает ли горизонтальная инфраструктура без контрольной функции?	Полезность консультации; время решения; повторяемость запросов; принятые предложения	Обезличенный журнал, опрос, анализ базы знаний	Подготовка наставников, супервизия, обновление сервисов и обучения
Мотивация	Есть ли смысл, возможность, поддержка, признание и развитие?	Выделенное время; доступ; участие в проектах; внутренние переходы; качество признанных кейсов	Опрос, HR-данные, интервью, анализ проектов	Ресурсное решение, карьерные маршруты, изменение стимулов
Институционализация	Закреплены ли практики в документах, KPI и кадровых процессах этично?	Актуальность актов; прозрачность показателей; КЭД; отсутствие запрещенных практик	Аудит документов и процессов, интервью, выборочная проверка	Ревизия KPI, политики данных, ИИ, диагностики и кадровых процедур
Ежегодный цикл	Связана ли диагностика с	Выполнение плана;	Годовой отчет, индексы,	Новый план развития,

Контур	Ключевой диагностический вопрос	Индикаторы	Методы	Тип управленческого решения
	решениями и проверкой эффекта?	динамика индексов; закрепление действий; обновление стратегии и обучения	протоколы, ретроспективы	бюджет, пересмотр методики и приоритетов

Система индикаторов, представленная в таблице 7.13, охватывает все семь контуров и связывает диагностику с типом решения. Показатели интерпретируются в контексте и не используются как автоматический рейтинг сотрудников или подразделений.

Интегральная взаимосвязь субъектов, контуров и результатов управления изменениями представлена на рисунке 7.9.



Рисунок 7.9 – Интегральная модель управления изменениями и развития цифровой культуры

Источник: составлено авторами.

Рисунок 7.9 показывает, что функциональные субъекты воздействуют на шесть контуров, которые создают организационные результаты: доверие, ответственность, освоение ИИ, снижение рисков, организационное обучение и цифровую зрелость. Все связи проходят через этический шлюз, запрещающий скрытые рейтинги и карательную диагностику.

Интегральная модель на рисунке 7.9 завершает логику главы. Она показывает, что результат не принадлежит одной функции. Руководитель гарантирует рамку; HR, ИТ и безопасность создают специализированные условия; наставники и сообщества поддерживают горизонтальное освоение. Семь контуров переводят эти функции в устойчивую культуру, а этический шлюз ограничивает способы измерения и управления.

Таким образом, ежегодный цикл превращает цифровую культуру в адаптивную систему. Его эффективность определяется не регулярностью опроса, а способностью связывать данные, рефлексию, ресурсы, изменение практик и повторную проверку эффекта. Разграничение ролей и этические гарантии защищают цикл от формализма и цифрового надзора.

Методический алгоритм закрепления результатов управления изменениями

Практическое закрепление результатов главы целесообразно организовать как десятишаговый алгоритм, встроенный в ежегодный цикл (рисунок 7.10).



Рисунок 7.10 – Методический алгоритм закрепления результатов управления изменениями

Источник: составлено авторами.

Первый шаг – подтвердить стратегический смысл: управленческая команда формулирует, какую организационную ценность должны поддерживать цифровые практики и какие этические границы не подлежат пересмотру. Второй шаг – верифицировать роли: для каждого решения определяются итогового ответственный руководитель, исполнители, консультанты и участники обратной связи.

Третий шаг – сопоставить формальные правила с реальной практикой. Анализируются не только положения и регламенты, но и фактические каналы, обходные действия, неформальные ИИ-сценарии, нагрузка и способы проверки результатов. Расхождение рассматривается как сигнал к изменению процесса или документа, а не как автоматическое основание обвинить сотрудника. Четвертый шаг – провести этический шлюз показателей и аналитики: подтвердить прозрачность цели, минимизацию данных, право на объяснение, человеческий пересмотр, развивающее назначение и отсутствие скрытого мониторинга.

Пятый шаг – определить приоритетные барьеры по семи контурам. Организация выбирает ограниченное число проблем, по которым возможен измеримый управленческий эффект. Шестой шаг – подобрать меру, соответствующую причине: обучение применяется при дефиците знания; наставничество – при затруднении переноса; доработка сервиса – при неудобстве; пересмотр RACI – при конфликте ролей; сокращение каналов – при перегрузке; прекращение практики – при нарушении этических гарантий.

Седьмой шаг – обеспечить ресурсное решение. Для каждой меры фиксируются время, бюджет, владелец, поддержка ИТ и безопасности, ожидаемый результат и контрольная точка. Восьмой шаг – провести совместное проектирование с затронутыми сотрудниками и профессиональными сообществами. Совместное проектирование не означает передачу управленческой ответственности, но позволяет проверить применимость решения и заранее обнаружить побочные последствия.

Девятый шаг – внедрить изменение в ограниченном и наблюдаемом контуре, собрать обратную связь и проверить влияние на качество процесса, риски, нагрузку и доверие. Десятый шаг – закрепить доказавшую результативность практику в документах, обучении, базе знаний и регулярном управлении, одновременно установив срок ее следующего пересмотра. Алгоритм завершается не фиксацией «лучшей практики навсегда», а включением результата в новый цикл организационного обучения.

Методическое значение алгоритма состоит в защите от двух крайностей. Первая – культурный декларативизм, когда организация обсуждает доверие и ценности, но не меняет роли, сервисы и ресурсы. Вторая – административный технократизм, когда новые показатели и регламенты вводятся без участия, объяснения и этических гарантий. Последовательность десяти шагов соединяет смысл, ответственность, данные, участие и институционализацию в единую управленческую процедуру.

ИТОГИ ГЛАВЫ

Управление изменениями обеспечивает культурное и организационное закрепление цифрового сознания. Его результат зависит от согласованности лидерства, коммуникации, работы с сопротивлением, профессиональных сообществ, мотивации, институционализации и ежегодного цикла развития.

Управленческий переход к главе 8: диагностика сохраняет развивающий характер, а сопротивление используется как информация о барьерах. Далее универсальный контур переводится в отраслевые профили управления.

Интерактивное сопровождение. В цифровом руководстве размещены план коммуникаций, карта причин сопротивления, модель сети цифровых наставников, этический шлюз KPI и шаблон ежегодного цикла развития.

ГЛАВА 8. ОТРАСЛЕВАЯ АДАПТАЦИЯ МОДЕЛИ УПРАВЛЕНИЯ ФОРМИРОВАНИЕМ ЦИФРОВОГО СОЗНАНИЯ ОРГАНИЗАЦИИ

«Только разнообразие может уничтожить разнообразие».

Уильям Росс Эшби

Управленческий вопрос главы. Какие элементы методологии должны оставаться универсальными, а какие требуют настройки под отраслевые цели, процессы, данные, риски и контуры ответственности?

Управленческий результат главы. Алгоритм отраслевой адаптации и профили для образовательных, коммерческих, государственных, медицинских, научно-экспертных и социальных организаций с обязательной экспертной проверкой, пилотированием и пересмотром.

Общая архитектура отраслевой адаптации представлена на рисунке 8.1. Она показывает соотношение единого методологического ядра и шести отраслевых профилей, рассматриваемых в главе.



Рисунок 8.1 – Единое методологическое ядро и отраслевые профили

Источник: составлено авторами на основе [41; 83; 90; 100; 102; 109; 136; 140].

Рисунок 8.1 показывает, что отраслевые профили не являются самостоятельными моделями. Образование, коммерческая сфера, публичное управление, медицина 4.0, наука и экспертиза, социальная сфера и НКО сохраняют общие уровни, компоненты, организационные контуры, диагностическую логику и критические ограничения, изменяя содержательные акценты и набор прикладных инструментов.

Теоретико-методологические основания отраслевой адаптации систематизированы в таблице 8.1. Их сопоставление позволяет определить назначение каждого подхода и границы его применения.

Таблица 8.1 – Теоретико-методологические основания отраслевой адаптации

Подход	Ключевая идея	Методическое применение	Ограничение
Контекстная обусловленность	Организационная конфигурация зависит от миссии, среды, масштаба и риска.	Обосновывает различие отраслевых профилей и отказ от единого шаблона.	Риск оправдания любых различий без общих ограничений.
Социотехнический подход	Люди, технологии, процессы и нормы оптимизируются совместно.	Требуется связывать цифровые сервисы с ролями, обучением и ответственностью.	Сложность межфункциональной координации.
Институциональный подход	Организация действует в системе права, профессиональных норм и легитимности.	Определяет отраслевые требования к данным, ИИ, обжалованию и раскрытию.	Подмена развития формальным соответствием.
Процессный подход	Индикаторы и технологии привязываются к реальным процессам и результатам.	Предотвращает цифровизацию ради инструмента и показатели без владельца.	Недооценка культуры и доверия.
Компетентностный подход	Способность к действию выражается в знаниях, умениях, установках и поведении.	Позволяет создавать ролевые программы обучения и отраслевые задания.	Сведение цифрового сознания только к навыкам.
Модели зрелости	Развитие описывается последовательными уровнями и доменами.	Сохраняет общую шкалу и позволяет строить отраслевые проявления уровней.	Иллюзия линейного и одинакового темпа развития.
Контекстное проектирование	Решение строится на понимании реальной практики пользователей.	Используется при пилоте, интервью, карте сценариев и доработке индикаторов.	Высокая трудоёмкость и риск локальной переадаптации.

Подход	Ключевая идея	Методическое применение	Ограничение
Динамические способности	Организация распознаёт изменения, использует возможности и перестраивает ресурсы.	Обосновывает адаптивно-рефлексивный уровень зрелости.	Сложность прямого измерения способности к перестройке.
Ответственное проектирование	Изменения оцениваются по последствиям, участию, прозрачности и отзывчивости.	Задаёт этический шлюз, валидацию стейкхолдерами и запрет цифрового надзора.	Замедление решений при формальном применении процедур.

Таблица 8.1 показывает, что отраслевая адаптация не может опираться на одну теорию. Контекстная обусловленность объясняет различия, социотехнический и процессный подходы связывают изменения с деятельностью, институциональная логика учитывает право и профессиональные нормы, а модели зрелости и ответственное проектирование сохраняют сопоставимость и этические границы.

8.1. ПРИНЦИПЫ АДАПТАЦИИ УНИВЕРСАЛЬНОЙ МОДЕЛИ ПОД КОНКРЕТНУЮ СФЕРУ

Отраслевая адаптация начинается с разграничения близких понятий. Конкретизация уточняет язык, примеры и роли, но не меняет диагностическую архитектуру. Локализация привязывает методику к юрисдикции, языку и действующему праву. Контекстуализация описывает особенности конкретной организации. Кастомизация настраивает инструменты и форматы внедрения под заказчика. Отраслевая адаптация объединяет эти действия в повторяемую процедуру, но дополнительно меняет профиль рисков, индикаторы, веса, критические минимумы и управленческую конфигурацию. Поэтому она не может быть сведена к замене слов «клиент» на «обучающийся» или «гражданин».

Инвариантное ядро методологии включает шесть групп элементов. Первая – определение цифрового сознания как способности осознанно, критично, этично, безопасно и результативно действовать в цифровой и ИИ-насыщенной среде. Вторая – пять уровней проявления. Третья – семь компонентов сотрудника и управленческой команды. Четвёртая – шесть организационных контуров. Пятая – диагностическая логика, включающая индексы, триангуляцию и повторную оценку. Шестая – обязательные принципы: человекоцентричность,

прозрачность, объяснимость, риск-ориентированность, человеческий контроль и запрет цифрового надзора [83; 100; 102; 109].

Изменять в отраслевом контексте допустимо терминологию, описание миссии, набор стейкхолдеров, карту процессов, классификацию данных, реестр сценариев ИИ, профиль рисков, индикаторы компонентов, относительные веса, отраслевые минимумы, содержание программ обучения, состав координационного органа, формат пилота и критерии масштабирования. Однако любое изменение должно быть документировано и обосновано: организация обязана показать, почему показатель значим именно для этой сферы и каким источником данных он подтверждается.

Первый принцип адаптации – методологическая целостность. Отраслевой профиль не должен исключать неудобные компоненты. Например, коммерческая организация не может отказаться от этики в пользу клиентской ценности, научная – от безопасности в пользу открытости, образовательная – от критичности в пользу цифровой педагогики. Перераспределение веса допустимо, но превращение одного компонента в «нулевой» разрушает смысл модели.

Второй принцип – отраслевая релевантность. Индикатор должен отражать реальный результат и риск сферы. Количество используемых ИИ-сервисов почти ничего не говорит о качестве образования, законности публичного решения, достоверности исследования или безопасности социальной помощи. В каждой сфере требуется собственная связка «миссия – процесс – данные – решение – последствия – доверие».

Третий принцип – сопоставимость. Все отраслевые индексы сохраняют шкалу от 0 до 100, одинаковые определения уровней зрелости и общую семикомпонентную структуру. Благодаря этому возможен анализ динамики и сравнение конфигураций без ложного ранжирования. Сопоставимость означает единый язык, но не одинаковые веса и не единые нормативы для разных процессов.

Четвёртый принцип – некомпенсируемость критических минимумов. Если нарушены законность, безопасность, академическая или исследовательская добросовестность, защита уязвимых групп либо право на человеческий пересмотр, высокий общий балл не может переводить организацию на интегрированный или адаптивно-рефлексивный уровень. Этот принцип продолжает этический шлюз главы 7 и согласуется с риск-ориентированными рамками NIST, ISO и регулированием ИИ [67; 83; 100].

Пятый принцип – доказательность настройки. Веса, пороги и индикаторы рассматриваются как исследовательские гипотезы до полевой проверки. Их нельзя объявлять «объективными» только потому, что они выражены числом. Требуются экспертная оценка, анализ данных пилота, проверка надёжности

инструментов, обсуждение с участниками и повторная калибровка. В этом смысле отраслевой профиль является не завершённым стандартом, а управляемой версией модели.

Шестой принцип – участие стейкхолдеров. В адаптацию должны быть включены не только руководители и ИТ-специалисты, но и представители профессиональных ролей, владельцы процессов и данных, службы безопасности, юридической функции, сотрудники, пользователи и группы, на которых цифровые решения могут повлиять. Участие не отменяет управленческую ответственность, но позволяет увидеть риски, незаметные из центра организации.

Седьмой принцип – реализуемость. Отраслевой профиль должен учитывать ресурсы, масштаб и цифровую инфраструктуру. Модель, требующая от небольшой НКО такого же комплекса комитетов, как от крупной корпорации, формально точна, но практически непригодна. Поэтому функции могут объединяться, а инструменты – упрощаться, если сохраняются ответственность, прозрачность и контроль критических рисков.

Предполагается, что устойчивость отраслевой модификации возрастает, когда организация сначала описывает миссию, стейкхолдеров, процессы, данные, сценарии ИИ и риски, а уже затем настраивает индикаторы и веса. Обратная последовательность повышает вероятность инструментализма, когда показатели подбираются под имеющиеся технологии, а не под значимые результаты и последствия.

Практическая процедура включает десять этапов. На первом определяется тип организации, её миссия и основной результат. На втором строится карта стейкхолдеров и критериев доверия. На третьем описываются основные, обеспечивающие и управляющие процессы. На четвёртом формируется карта данных и цифровых сервисов. На пятом – реестр действующих и планируемых сценариев ИИ. На шестом – карта отраслевых рисков и ранних сигналов. На седьмом настраиваются индикаторы, веса и минимумы. На восьмом проектируются обучение, наставничество и пилот. На девятом проводится экспертная и стейкхолдерская валидация. На десятом результаты пилота используются для повторной настройки и институционализации.

Последовательность разработки и проверки отраслевого профиля представлена на рисунке 8.2. Схема переводит общие принципы адаптации в воспроизводимый организационный алгоритм.



Рисунок 8.2 – Алгоритм отраслевой адаптации методологии цифрового сознания организации

Источник: составлено авторами на основе [16; 77; 83; 100; 109; 129].

Представленная схема отражает строгую последовательность действий. Миссия и стейкхолдеры определяют процессы; процессы – данные, сервисы и сценарии ИИ; только после оценки рисков настраиваются индикаторы и веса. Завершающие этапы включают пилот, валидацию и повторную калибровку. Нижний блок фиксирует запрет компенсировать этические и безопасностные дефекты высокой эффективностью.

Разграничение инвариантного ядра и допустимых параметров отраслевой настройки представлено в таблице 8.2. Она используется для проверки того, не разрушает ли предлагаемая модификация методологическую целостность модели.

Таблица 8.2 – Инвариантное ядро и допустимые параметры отраслевой настройки

Элемент	Инвариантное содержание	Допустимая настройка	Изменять нельзя
Рабочее определение	Осознанность, критичность, этичность, безопасность и результативность.	Отраслевые примеры и язык описания.	Исключение этики, критичности или безопасности.
Пять уровней	Сотрудник, команда, управление,	Детализация ролей и стейкхолдеров.	Удаление уровня или сведение модели к

Элемент	Инвариантное содержание	Допустимая настройка	Изменять нельзя
	организация, экосистема.		индивидуальным навыкам.
Семь компонентов	Дееспособность, критичность, грамотность в области данных и ИИ, этика, безопасность, коммуникация, рефлексивность.	Относительные веса и отраслевые проявления.	Нулевой вес критического компонента.
Шесть контуров	Стратегия; данные, аналитика и ИИ; архитектура и сервисы; культура, доверие и безопасность; развитие персонала; рефлексивность.	Секторные индикаторы и владельцы.	Фрагментация и отказ от контура данных или культуры.
Диагностика	Индексы, триангуляция, повторность, развивающая интерпретация.	Инструменты сбора данных, вопросы, отраслевые пороги.	Оценка по одному источнику или карательное использование.
Этические ограничения	Прозрачность, минимизация данных, объяснение, человеческий пересмотр, отсутствие скрытого мониторинга.	Процедуры реализации и состав гарантий.	Невидимые рейтинги, автоматические санкции, цифровой надзор.

Таблица 8.2 отделяет неизменяемые основания методологии от параметров, подлежащих отраслевой настройке. Такое разграничение предотвращает две крайности: формальное копирование универсальной модели без учета контекста и создание несопоставимых отраслевых систем под общим названием.

Структура паспорта отраслевой адаптации приведена в таблице 8.3. Паспорт фиксирует обязательные характеристики профиля и обеспечивает воспроизводимость решений рабочей группы.

Таблица 8.3 – Паспорт отраслевой адаптации методологии цифрового сознания

Поле паспорта	Что необходимо зафиксировать
Тип организации и миссия	Отраслевая принадлежность, назначение, общественный или коммерческий результат.
Ключевые стейкхолдеры	Сотрудники, пользователи, клиенты, граждане, обучающиеся, доноры, регуляторы и другие затронутые

Поле паспорта	Что необходимо зафиксировать
	группы.
Процессы	Основные, обеспечивающие, управляющие, аналитические и коммуникационные процессы.
Данные и цифровые сервисы	Категории данных, владельцы, правовой режим, цифровые платформы, интеграции и цифровой след.
Сценарии ИИ	Текущие и планируемые сценарии, ценность, риск, владелец и обязательный человеческий контроль.
Отраслевые риски	Возможный вред, ранние сигналы, профилактика, реагирование и недопустимые практики.
Профиль компонентов	Приоритетные компоненты, веса, критические минимумы и источники данных.
Уровни зрелости	Отраслевые проявления пяти уровней и критерии перехода.
Обучение и наставничество	Рольевые программы, практические форматы, сообщества и поддержка.
Управление и документы	Координационный орган, владельцы, локальные акты, цикл пересмотра.
Пилотирование	Площадка, срок, ограничения, показатели, участники валидации.
Масштабирование	Условия расширения, контрольные точки, доказательства ценности и отсутствия неприемлемого вреда.

Таблица 8.3 представляет паспорт отраслевой адаптации как обязательный комплект сведений о миссии, стейкхолдерах, процессах, данных, ИИ-сценариях, рисках, индикаторах, ролях и порядке пересмотра. Заполненный паспорт становится основанием для экспертной проверки и пилота.

Рольевая архитектура отраслевой адаптации должна быть сформирована до настройки индикаторов. Руководитель организации утверждает миссию, границы и некомпенсируемые минимумы; методологическая группа отвечает за сохранение ядра и сопоставимость шкал; владельцы процессов описывают реальную деятельность; HR-служба формирует рольевые профили и программы развития; ИТ-служба предоставляет данные об архитектуре и сервисах; служба безопасности классифицирует риски; юридическая функция проверяет нормативную применимость; представители стейкхолдеров участвуют в проверке приемлемости. Ни одна функция не должна единолично создавать отраслевой профиль, поскольку это приводит к функциональному смещению модели.

Методологическая группа формирует журнал решений об адаптации. В нем фиксируются исходный элемент универсальной модели, отраслевое основание

изменения, использованные данные, экспертное обоснование, ожидаемое влияние на сопоставимость и дата следующего пересмотра. Такой журнал позволяет отличить обоснованную настройку от смыслового дрейфа. Например, увеличение веса безопасности в коммерческой сфере может быть связано с клиентскими данными и цепочками поставок; исключение этики из индекса не может быть обосновано отраслевой спецификой.

Экспертная валидация проводится в два контура. Внутренний контур проверяет соответствие миссии, процессам и ресурсам организации. Внешний контур оценивает соответствие отраслевым нормам, профессиональной этике и ожиданиям затронутых групп. Для высокорисковых профилей дополнительно применяется проверка сценариями: участникам предлагаются реальные ситуации использования данных и ИИ, после чего анализируется, позволяют ли индикаторы различить ответственное, ошибочное и недопустимое действие.

Качество адаптации оценивается по восьми критериям: целостность, релевантность, сопоставимость, нормативная применимость, практическая реализуемость, диагностируемость, этическая допустимость и масштабируемость. Каждый критерий должен иметь доказательство. Целостность подтверждается сохранением ядра; релевантность – связью с процессами; сопоставимость – общей шкалой; применимость – правовой экспертизой; реализуемость – ресурсным планом; диагностируемость – доступными источниками данных; этическая допустимость – прохождением шлюза; масштабируемость – результатами пилота.

Типовые ошибки отраслевой адаптации образуют четыре группы. Первая – терминологическая: замена понятий без изменения содержания. Вторая – технологическая: построение профиля вокруг набора сервисов. Третья – измерительная: назначение весов без данных и экспертного обоснования. Четвертая – нормативная: перенос практики из другой сферы без учета прав, ответственности и профессиональной этики. Для каждой ошибки в паспорте адаптации следует предусмотреть ранний сигнал и корректирующее действие.

Итогом является не готовый отраслевой индекс, а верифицированный проект профиля. Он включает паспорт, карту стейкхолдеров, процессов, данных и ИИ-сценариев, реестр рисков, проект индикаторов и весов, этические минимумы, модель управления, программу пилота и протокол валидации. Только полный комплект позволяет перейти от концептуальной настройки к практическому применению в конкретной сфере.

Таким образом, отраслевая адаптация является управляемой перенастройкой прикладной конфигурации, а не созданием новой модели. Её качество обеспечивается сохранением инвариантов, последовательным анализом контекста, некомпенсируемыми минимумами, валидацией и пилотированием.

Практическим результатом параграфа выступают десятишаговый алгоритм и паспорт отраслевого профиля.

8.2. АДАПТАЦИЯ МОДЕЛИ ДЛЯ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Образовательная организация представляет собой особый тип социально-цифровой системы, в которой цифровые решения непосредственно влияют на развитие личности, качество обучения, способы оценивания, академическую добросовестность и доступность образовательной среды. Поэтому отраслевой профиль не может быть построен как простая замена общей терминологии педагогическими примерами. Он должен перенастраивать универсальную модель под педагогическую миссию, образовательные результаты, возрастные и статусные различия участников, режим образовательных данных и повышенную ответственность за решения, влияющие на траекторию обучающегося [94; 110; 118; 135; 136].

В образовательной сфере цифровое сознание организации определяется как способность осознанно проектировать и применять цифровые технологии, данные и ИИ так, чтобы они усиливали обучение, сохраняли субъектность преподавателя и обучающегося, обеспечивали справедливость оценивания, защищали персональные данные и поддерживали инклюзивность. Существенным является различие цифровой поддержки обучения и цифровой подмены обучения. Первая расширяет обратную связь, доступность и возможности практики; вторая заменяет самостоятельную мыслительную деятельность готовым машинным результатом и тем самым разрушает целевой образовательный эффект.

Педагогический дизайн становится центральным механизмом адаптации. Решение о применении ИИ должно исходить не из доступности инструмента, а из образовательной цели: какую деятельность должен выполнить обучающийся, какой способ мышления сформировать, какие доказательства освоения представить и какая помощь допустима. Поэтому отраслевой профиль связывает ИИ-сценарий с результатами обучения, формой задания, критериями оценивания, правилами раскрытия использования ИИ и процедурой апелляции.

Особую зону образуют образовательные данные. В организации накапливаются сведения о результатах обучения, посещаемости, активности в LMS, коммуникации, цифровом следе, индивидуальных траекториях и затруднениях. Эти данные могут поддерживать педагогические решения, но не должны превращаться в непрозрачное профилирование обучающихся и работников. Для каждого аналитического сценария необходимы законная цель, минимизация данных, описание методики, проверка качества, ограничение доступа и человеческий пересмотр значимого вывода [87; 136].

Карта стейкхолдеров образовательной организации строится вокруг трех центров доверия. Первый – доверие к профессиональному педагогическому суждению преподавателя. Второй – доверие к процедурам оценивания и академической честности. Третий – доверие к защите образовательных данных. Нарушение любого центра снижает легитимность цифрового решения: даже удобный сервис не будет принят, если обучающийся не понимает критерии оценки, преподаватель лишен возможности профессионального решения, а данные используются вне заявленной цели.

Эмпирические материалы OECD TALIS показывают одновременный рост использования ИИ педагогами и выраженный дефицит знаний, необходимых для его педагогически обоснованного применения. Значительная доля педагогов связывает генеративный ИИ с риском подмены авторства и академической честности. Эти данные подтверждают, что образовательная адаптация должна соединять доступ к инструментам с ролевым обучением, правилами оценивания, обсуждением этических дилемм и организационным управлением ИИ [108; 110].

Приоритетными компонентами образовательного профиля являются грамотность в области данных и ИИ, информационно-аналитическая критичность, цифровая этика и ответственность, безопасность образовательных данных и рефлексивность. Цифровая дееспособность остается необходимой, но высокий уровень владения инструментами не компенсирует дефицит академической добросовестности или защиты данных. Поэтому в индексе вводятся некомпенсируемые минимумы по этике, безопасности и академической честности.

Предполагается, что цифровое сознание образовательной организации развивается устойчиво, если ИИ и аналитика проектируются одновременно как педагогический, этический и управленческий объект. Если внедрение оценивается только по числу сервисов, пользователей или сгенерированных материалов, оно повышает цифровую активность, но не гарантирует качества обучения и может усиливать генеративную подмену.

Практическим форматом адаптации является ограниченный пилот в одной образовательной программе, структурном подразделении или контуре оценивания. Пилот включает правила использования ИИ, переработку заданий с учетом генеративных возможностей, обучение преподавателей, информирование обучающихся, защиту данных, канал апелляции и повторную диагностику после завершения периода. Масштабирование допускается только при подтверждении образовательной ценности и отсутствии критических этических последствий.

Кейсы Khanmigo и институциональных образовательных пилотов показывают значимость контролируемого внедрения, оценки восприятия и поддержки уязвимых групп [60]. Негативный опыт крупного школьного чат-

бота LAUSD демонстрирует, что привлекательность продукта не компенсирует риски поставщика, неустойчивость проекта и неопределенность судьбы данных обучающихся [63]. Следовательно, управление поставщиком является частью образовательного цифрового сознания.

Структура образовательного отраслевого профиля представлена на рисунке 8.3. Она связывает педагогическую миссию, данные, ИИ-сценарии, доверие, риски и механизмы организационного закрепления.



Рисунок 8.3 – Отраслевой профиль цифрового сознания образовательной организации

Источник: составлено авторами на основе [87; 94; 110; 135; 136].

Рисунок 8.3 показывает, что центром образовательного профиля выступают качество образования и развитие личности. Педагогический дизайн, академическая добросовестность, образовательные данные, ИИ, инклюзивность и профессиональная ответственность образуют взаимосвязанный контур, в котором технология оценивается по педагогическому результату.

Содержательные параметры адаптации образовательной организации систематизированы в таблице 8.4. Таблица используется как рабочий паспорт при проектировании локальной версии методологии.

Таблица 8.4 – Паспорт адаптации методологии для образовательной организации

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
Миссия и результат	Качество обучения, развитие личности,	Карта образовательных	Подмена образовательной

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
	доступность, академическая добросовестность	результатов и цифровой миссии	цели технологической активностью
Субъекты	Обучающиеся, педагоги, научно-педагогические работники, администрация, родители, работодатели	Карта ролей и стейкхолдеров	Исключение голоса обучающихся и уязвимых групп
Критические данные	Персональные данные, результаты обучения, цифровой след, аналитика LMS	Карта данных, правила доступа и хранения	Непрозрачное профилирование и утечка данных
Сценарии ИИ	Подготовка материалов, обратная связь, персонализация, библиографический поиск, аналитика риска	Реестр ИИ-сценариев и карта педагогической применимости	Генеративная подмена обучения и ошибочная автоматическая оценка
Приоритетные компоненты	Критичность, грамотность в области данных и ИИ, этика, безопасность, рефлексивность	Отраслевой профиль компетенций	Сведение развития к освоению сервисов
Критические минимумы	Этика не ниже 50; безопасность не ниже 50; академическая честность не ниже 50	Этический шлюз индекса	Компенсация нарушений высокими баллами по цифровому дизайну
Локальные документы	Политика ИИ в обучении и оценивании, кодекс академической честности, регламент аналитики обучения	Согласованный пакет локальных актов	Противоречивые правила для преподавателей и обучающихся
Обучение	Цифровая педагогика, ИИ-грамотность, защита данных, инклюзивность	Методические семинары, клиника ИИ, взаимная экспертиза заданий	Формальные курсы без изменения оценивания
Пилот	Одна программа или контур оценивания, ограниченный набор	Паспорт пилота и журнал педагогических	Массовое внедрение без апробации

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
	инструментов	эффектов	
Масштабирование	Расширение после проверки качества, доверия, доступности и нагрузки	Контрольные точки готовности	Тиражирование единой практики без учета дисциплин и возрастных групп

Таблица 8.4 показывает, что образовательная адаптация охватывает миссию, образовательные процессы, данные, ИИ-сценарии, академическую честность, инклюзивность, роли и механизмы обратной связи. Паспорт используется для согласования решений администрации, преподавателей, ИТ-службы и участников образовательного процесса.

Для диагностики образовательного профиля целесообразно применять индикаторы, представленные в таблице 8.5. Они оценивают качество среды и практик, а не цифровую активность отдельных участников.

Таблица 8.5 – Диагностические индикаторы образовательного отраслевого профиля

Направление	Диагностический вопрос	Индикатор	Источник данных	Развивающее решение
Педагогическая обоснованность	Связан ли ИИ-сценарий с результатом обучения?	В паспортах заданий указаны цель, допустимая помощь ИИ и критерии самостоятельности	Экспертиза программ, заданий и курсов	Переработка дизайна задания и методическая консультация
Академическая честность	Понятны ли правила авторства и раскрытия ИИ?	Действуют единые правила маркировки, проверки и апелляции	Локальные акты, кейсы нарушений, опрос	Уточнение правил, обучение и redesign оценивания
Защита данных	Обосновано ли использование образовательного следа?	Определены цель, минимальный набор данных, доступ и срок хранения	Карта данных, аудит LMS, интервью	Минимизация данных и изменение аналитического сценария
Инклюзия	Доступны ли сервисы участникам с разными возможностями?	Проводится оценка доступности и предусмотрены альтернативные	Тестирование доступности, обратная связь	Доработка интерфейса и поддержка пользователей

Направление	Диагностический вопрос	Индикатор	Источник данных	Развивающее решение
		форматы		
Человеческий пересмотр	Можно ли оспорить автоматизированный вывод?	Назначен компетентный проверяющий и описана процедура апелляции	Регламент, журнал обращений	Уточнение полномочий и обучение проверяющих
Развитие педагогов	Переносится ли обучение в практику?	Преподаватели перерабатывают задания и делятся проверенными кейсами	Портфолио практик, наблюдение, сообщества	Наставничество и выделение времени на методическую работу

Таблица 8.5 связывает диагностические признаки с развивающими действиями. Количество сервисов, запросов к ИИ или время работы в цифровой среде не рассматриваются как самостоятельное доказательство зрелости без оценки качества обучения, самостоятельности мышления, честности и безопасности.

Ролевая архитектура образовательной адаптации должна исключать передачу всей ответственности ИТ-службе или отдельному преподавателю. Руководитель образовательной организации утверждает цели и гарантии; коллегиальный орган или методический совет определяет педагогические правила; руководители программ переводят их в результаты обучения и оценивание; ИТ обеспечивает утвержденную среду; ответственный за данные контролирует правомерность аналитики; преподаватель принимает педагогическое решение; обучающийся получает понятные правила и возможность апелляции.

Отдельным практическим инструментом является паспорт цифрового задания. В нем указываются образовательная цель, допустимые и недопустимые формы помощи ИИ, требования к самостоятельному вкладу, источники данных, способ раскрытия использования ИИ, критерии проверки и порядок обсуждения спорного результата. Паспорт снижает неопределенность и позволяет рассматривать академическую честность не только как запрет, но и как проектируемое условие обучения.

Диагностический цикл образовательного профиля должен включать анализ локальных документов, экспертизу заданий, опрос преподавателей и обучающихся, сценарные кейсы, выборочную проверку аналитики LMS и обсуждение результатов с академическим сообществом. Самооценка преподавателя показывает потребность в развитии, но не заменяет анализа

практики. Цифровой след обучающегося не используется как единственное доказательство нарушения или низкой вовлеченности.

Критерием успешного масштабирования является не доля дисциплин, применяющих ИИ, а доля практик, для которых доказаны педагогическая ценность, понятность правил, доступность, безопасность данных и качество человеческой обратной связи. При расширении профиля следует учитывать различия уровней образования, дисциплин и типов заданий. Практика, полезная для проектной работы, может быть недопустима при проверке базовых профессиональных знаний.

Ежегодный пересмотр образовательного профиля должен учитывать изменения инструментов, форм оценивания, рисков генеративной подмены и требований к защите данных. Методический совет анализирует не только нарушения, но и успешные способы поддерживать самостоятельность мышления. Тем самым организация формирует не культуру запрета ИИ, а культуру ответственного педагогического проектирования.

Таким образом, образовательная адаптация строится вокруг качества обучения, академической добросовестности, педагогического суждения, инклюзии и защиты образовательных данных. ИИ допустим как средство поддержки, но не как необъяснимая замена обучения или профессионального решения. Пилотирование, человеческий пересмотр и некомпенсируемые минимумы по этике, безопасности и честности являются обязательными условиями.

8.3. АДАПТАЦИЯ МОДЕЛИ ДЛЯ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

В коммерческой организации цифровое сознание связано с созданием клиентской ценности, устойчивостью бизнес-модели, качеством продукта, эффективностью процессов и цифровой репутацией. Однако отраслевой профиль не должен сводиться к возврату инвестиций или скорости автоматизации. Экономический эффект становится устойчивым только при наличии управления данными, ИИ, киберрисками, поставщиками и человеческой ответственностью [37; 83; 100; 102; 109].

Цифровое сознание коммерческой организации можно определить как способность создавать экономическую и клиентскую ценность посредством данных, цифровых сервисов и ИИ, сохраняя управляемость, безопасность, справедливость и доверие клиентов, работников, партнеров и инвесторов. В таком определении соединены внешнее и внутреннее измерения. Внешнее касается качества продукта, прозрачности решений и защиты клиентских данных; внутреннее – условий работы сотрудников, допустимости аналитики труда и отсутствия цифрового микроконтроля.

Критические данные включают клиентские, финансовые, коммерческие, кадровые, производственные и поведенческие сведения, интеллектуальную собственность и данные цепочки поставок. Их ценность определяется не объемом, а качеством, правомерностью, доступностью для решений и защищенностью. Поэтому отраслевой профиль требует владельцев данных, каталога критичных наборов, правил качества, контроля доступа и оценки внешних поставщиков.

Типовые ИИ-сценарии охватывают маркетинг, продажи, клиентскую поддержку, прогнозирование спроса, управление запасами, контроль качества, разработку продуктов, управление персоналом и кибербезопасность. Каждый сценарий должен проходить двойной фильтр: проверку ценности и проверку риска. Сценарий, демонстрирующий локальную экономию, не может считаться успешным, если он снижает качество обслуживания, усиливает дискриминацию, ухудшает условия труда или создает неприемлемую зависимость от поставщика.

Данные Eurostat свидетельствуют о быстром росте использования ИИ европейскими предприятиями и одновременно о значительном разрыве между крупными и небольшими организациями. Для отраслевой адаптации это означает необходимость учитывать масштаб и ресурсную обеспеченность: малой организации не требуется копировать сложную архитектуру корпорации, но минимальные правила данных, ИИ, безопасности и ответственности должны сохраняться независимо от размера [69].

Клиентское доверие формируется через надежность сервиса, понятность правил данных, отсутствие манипулятивной персонализации и наличие механизма исправления ошибки. Решение по делу *Moffatt v. Air Canada* показало, что организация отвечает за информацию, которую ее цифровой агент сообщает клиенту [98]. Следовательно, чат-бот или ИИ-помощник не является автономным субъектом: его ответы должны быть включены в контур контроля контента, эскалации и компенсации ущерба.

Внутреннее доверие требует запрета на скрытое наблюдение за сотрудниками. Технические журналы, показатели активности и коммуникационный след не раскрывают полностью профессионального контекста и не могут автоматически использоваться как оценка труда или лояльности. Допустимая аналитика должна иметь заявленную цель, минимальный состав данных, понятную методику, право на объяснение и человеческий пересмотр.

Предполагается, что устойчивый экономический эффект цифровизации положительно связан не с максимальным уровнем автоматизации, а с согласованностью четырех элементов – ценности, управления данными и ИИ, доверия и организационной устойчивости. Дефицит любого элемента повышает вероятность того, что краткосрочный эффект будет нейтрализован репутационным, правовым или операционным ущербом.

Пилот коммерческой адаптации целесообразно проводить в одном процессе с измеримым результатом: клиентское обслуживание, прогнозирование, контроль качества, подготовка коммерческих материалов или внутренний сервис. Паспорт пилота должен содержать исходную метрику, ожидаемую ценность, карту данных, владельца, человеческий резервный сценарий, критерии остановки, журнал рисков и оценку клиентского либо пользовательского опыта.

В отраслевом индексе повышаются веса грамотности в области данных и ИИ, безопасности и рефлексивности. Вместе с тем этика и ответственность не исключаются из-за коммерческой ориентации. Рекомендуемые минимумы составляют 45 баллов по этике и ответственности и 50 баллов по безопасности. Ни высокий финансовый эффект, ни рост производительности не могут компенсировать нарушение этих порогов.

Логика коммерческого отраслевого профиля представлена на рисунке 8.4. Она показывает, что клиентская ценность создается только при согласовании цифрового продукта, управления данными и ИИ, доверия и устойчивости.



Рисунок 8.4 – Контур ценности, управления, доверия и устойчивости коммерческой организации

Источник: составлено авторами на основе [69; 83; 100; 102; 109; 151].

Рисунок 8.4 показывает, что коммерческий профиль строится вокруг взаимосвязанных элементов: клиентской ценности, управляемого применения данных и ИИ, доверия и организационной устойчивости. Экономический эффект признается результатом только при соблюдении требований безопасности, прозрачности и ответственности.

Содержательная настройка коммерческой организации представлена в таблице 8.6. Она используется при подготовке корпоративного паспорта отраслевой адаптации.

Таблица 8.6 – Паспорт адаптации методологии для коммерческой организации

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
Миссия и результат	Клиентская ценность, выручка, качество продукта, инновации, устойчивость и репутация	Карта ценности и портфель цифровых инициатив	Оптимизация локальной метрики в ущерб клиенту и устойчивости
Субъекты	Собственники, совет директоров, руководство, сотрудники, клиенты, партнеры, инвесторы, регуляторы	Карта стейкхолдеров и распределения ответственности	Игнорирование интересов работников и клиентов
Критические данные	Клиентские, коммерческие, финансовые, кадровые, производственные данные и интеллектуальная собственность	Каталог данных и матрица доступа	Утечки, некорректная аналитика и потеря интеллектуальных прав
Сценарии ИИ	Маркетинг, продажи, поддержка, прогнозирование, качество, HR, кибербезопасность	Реестр сценариев, оценка ценности и риска	Манипулятивная персонализация, предвзятость, ошибочная автоматизация
Поставщики	Облачные сервисы, модели, платформы и подрядчики	Оценка поставщика, договорные требования, план выхода	Зависимость от поставщика и непрозрачная цепочка данных
Критические минимумы	Этика не ниже 45; безопасность не ниже 50	Этический и риск-шлюз	Компенсация нарушения прав финансовым эффектом
Локальные документы	Политика ИИ, управление данными, модельные риски, конфиденциальность, кибербезопасность	Корпоративный пакет политик	Несо согласованность функций бизнеса, ИТ, безопасности и HR
Обучение	Грамотность в области данных и ИИ, клиентская аналитика, кибергигиена,	Микромодули, лаборатории решений,	Обучение сервисам без понимания бизнес-

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
	риск поставщиков	практические руководства	процесса
Пилот	Один бизнес-процесс с измеримым ценностным результатом и человеческим резервом	Паспорт ценности, журнал рисков, контроль качества	Массовая автоматизация до подтверждения качества
Масштабирование	Расширение после доказательства повторяемого эффекта, безопасности и доверия	Порог готовности и архитектурный обзор	Тиражирование технического долга и ошибочной модели

Таблица 8.6 представляет коммерческий паспорт как средство согласования бизнес-результата и ответственного цифрового управления. Он не позволяет свести цифровое сознание к финансовой эффективности и требует учитывать клиентский опыт, качество данных, риски ИИ, киберустойчивость и репутационные последствия.

Управление коммерческим профилем распределяется между советом директоров или высшим руководством, владельцами бизнес-процессов, функцией данных, ИТ, безопасностью, юридической службой, HR и владельцами продуктов. Руководство утверждает приемлемый риск; владелец процесса отвечает за ценность; владелец данных – за качество и режим; ИТ – за архитектуру; безопасность – за защиту; юридическая функция – за правомерность; HR – за справедливость кадровых практик. Алгоритм не может быть признан владельцем решения.

Для каждого корпоративного ИИ-сценария рекомендуется оформлять карточку ценности и риска. Она содержит описание проблемы, затронутые группы, данные, поставщика, ожидаемый эффект, ограничения модели, способ человеческой проверки, показатели качества, риск недобросовестного поведения, план реагирования и критерии прекращения. Карточка делает видимыми предпосылки эффекта и препятствует запуску сценариев только из-за технологической привлекательности.

Для малых и средних организаций применяется принцип пропорциональности: структура управления может быть компактной, но функции должны быть распределены. Один сотрудник может совмещать несколько ролей, если исключен конфликт интересов и сохраняется независимая проверка высокорискового решения. Допустимы отраслевые ассоциации, совместные центры компетенций и типовые политики, однако ответственность за конкретное применение остается у организации.

Диагностика коммерческого профиля сочетает финансовые и процессные данные с показателями качества, жалобами, инцидентами, интервью сотрудников, оценкой поставщиков и анализом клиентского пути. Рост скорости обработки не считается положительным эффектом, если увеличиваются повторные обращения, ошибки или необходимость человеческого исправления. Аналогично снижение затрат не является устойчивым, если оно достигнуто скрытым переносом нагрузки на клиента или сотрудника.

Корректирующее решение выбирается по причине дефицита. Низкое качество модели требует пересмотра данных и алгоритма; неудобство сервиса – изменения пользовательского пути; теневое использование ИИ – предоставления легитимного инструмента и обучения; дискриминационный результат – приостановки сценария и независимой экспертизы; зависимость от поставщика – архитектурного плана выхода. Универсальная рекомендация «обучить сотрудников» не заменяет изменение системы.

Таким образом, в коммерческой организации цифровое сознание соединяет клиентскую ценность, управление данными и ИИ, безопасность, доверие и устойчивость. Экономический эффект рассматривается совместно с качеством сервиса, правами клиентов и сотрудников, рисками поставщиков и человеческой ответственностью. Пилот должен иметь не только показатель выгоды, но и контур исправления ошибки и безопасного возврата к человеческому процессу.

8.4. АДАПТАЦИЯ МОДЕЛИ ДЛЯ ОРГАНА ГОСУДАРСТВЕННОГО ИЛИ МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ

Для органа государственного или муниципального управления цифровое сознание должно быть связано прежде всего с общественной ценностью, законностью, доступностью, подотчетностью и доверием граждан. В публичной сфере эффективность не может быть единственным критерием: цифровое решение легитимно только тогда, когда оно улучшает исполнение публичной функции, не нарушает права, остается объяснимым и допускает человеческий пересмотр [33; 106; 107; 140; 150].

Цифровое сознание публичной организации можно определить как способность использовать данные, цифровые сервисы и ИИ для создания общественной ценности при соблюдении закона, равного доступа, прозрачности, безопасности и ответственности перед гражданами. В отличие от клиента коммерческой организации гражданин часто не может свободно отказаться от взаимодействия с государственным сервисом. Это усиливает обязанность органа обеспечить альтернативный канал, понятное объяснение и процедуру обжалования.

Карта стейкхолдеров включает руководство, государственных и муниципальных служащих, граждан, организации, подведомственные

учреждения, контрольно-надзорные органы, общественные объединения и представителей уязвимых групп. При проектировании цифрового сервиса необходимо анализировать не только основного пользователя, но и тех, кто может быть исключен из-за возраста, состояния здоровья, территории, уровня цифровой грамотности или отсутствия доступа к инфраструктуре.

Критическими являются государственные информационные ресурсы, персональные, социальные, финансовые и геопространственные данные, сведения об обращениях и межведомственном взаимодействии. Низкое качество реестров или несогласованность данных способно привести не просто к ошибке аналитики, а к неправомерному решению в отношении гражданина. Поэтому управление качеством данных и порядок исправления ошибочной записи включаются в профиль как самостоятельные индикаторы.

Типовые ИИ-сценарии охватывают обработку обращений, поиск по документам, прогнозирование, выявление рисков, поддержку решений, чат-боты, интеллектуальную маршрутизацию и анализ общественной обратной связи. Для каждого сценария должны быть определены правовое основание, класс риска, компетентный владелец, зона человеческой проверки, доступ гражданина к объяснению и условия приостановки.

Международные обзоры UN E-Government Survey и World Bank GovTech Maturity Index фиксируют рост цифровой зрелости государств, но одновременно показывают неравномерность институциональных возможностей [140; 150]. Методический вывод состоит в том, что зрелость публичного сектора определяется не количеством электронных услуг, а согласованностью стратегии, институтов, данных, компетенций, безопасности и механизмов участия.

Некритичное применение алгоритмов в публичных решениях может масштабировать несправедливость. Поэтому законность, этика и право на обжалование являются некомпенсируемыми минимумами. Для профиля рекомендуется порог не ниже 55 баллов по законности, этике и ответственности, не ниже 50 по безопасности и не ниже 50 по механизму пересмотра. При недостижении любого порога высокий показатель скорости сервиса не повышает итоговый уровень зрелости.

Проверяемое положение 8.4: общественное доверие к цифровому государству зависит от согласованности пяти условий – законности, доступности, качества данных, объяснимости и реального механизма обжалования. Технологическая надежность без этих условий формирует работоспособный, но не легитимный цифровой контур.

Пилот публичной адаптации целесообразно проводить в одном массовом сервисе или межведомственном процессе. Помимо процессных показателей необходимо оценивать понятность интерфейса и решения, долю успешных обращений, доступность альтернативного канала, качество данных, число

исправлений, обращения по поводу ошибок и способность работников объяснить участие ИИ.

Позитивные примеры цифрового государства показывают значение интероперабельности и принципа однократного предоставления данных. Негативные кейсы алгоритмических ошибок в социальной сфере демонстрируют, что автоматизация властного решения без достаточных правовых гарантий способна разрушить доверие на системном уровне. Следовательно, публичный профиль должен включать процедуру остановки алгоритмического сценария до завершения расследования.

Профиль цифрового сознания органа государственного или муниципального управления представлен на рисунке 8.5. Схема связывает общественную ценность с законностью, доступностью, качеством данных, объяснимостью и возможностью человеческого пересмотра.



Рисунок 8.5 – Профиль цифрового сознания органа государственного или муниципального управления

Источник: составлено авторами на основе [67; 105–107; 140; 150].

Рисунок 8.5 показывает, что центральным результатом публичного профиля является общественная ценность. Ее обеспечивают законность, доступность, качество государственных данных, прозрачность, человеческий пересмотр, межведомственная согласованность и подотчетность.

Рабочая конфигурация публичного профиля приведена в таблице 8.7. Она задает минимальный набор параметров для государственного или муниципального органа.

Таблица 8.7 – Паспорт адаптации методологии для публичного управления

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
Миссия и результат	Общественная ценность, законность, качество услуг, доступность и доверие	Карта публичной ценности и результатов сервиса	Подмена общественного результата ведомственной эффективностью
Субъекты	Служащие, руководство, граждане, организации, подведомственные учреждения и контрольные органы	Карта стейкхолдеров и уязвимых групп	Цифровое исключение участников с ограниченным доступом
Критические данные	Государственные реестры, персональные, социальные, финансовые и геоданные	Паспорт реестра, правила качества и межведомственного обмена	Неправомерное решение из-за ошибочных или несогласованных данных
Сценарии ИИ	Обращения, аналитика, прогнозирование, поддержка решений, чат-боты, умный город	Реестр сценариев и правовая экспертиза	Автоматизация властного решения без человеческого контроля
Доверие	Понятность сервиса, прозрачность правил, возможность альтернативного канала	Стандарт сервиса и протокол объяснения	Недоверие и невозможность воспользоваться правом
Критические минимумы	Законность и этика не ниже 55; безопасность не ниже 50; пересмотр не ниже 50	Правовой и этический шлюз	Компенсация нарушения прав высокой скоростью услуги
Локальные документы	Стратегия цифровой трансформации, правила обмена данными, политика ИИ, доступность, обжалование	Согласованный пакет публичного управления	Формальные акты без работающей процедуры
Обучение	Управление публичными данными, объяснимость, права граждан, доступность, межведомственная работа	Кейс-обучение и лаборатории дизайна услуг	Техническое обучение без правовой и сервисной логики
Пилот	Один массовый сервис или межведомственный процесс	Паспорт пилота, правовая экспертиза,	Масштабирование непрозрачного решения

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
		общественная проверка	
Масштабирование	Расширение после проверки доступности, качества данных, обжалования и устойчивости	Контрольные точки публичной готовности	Тиражирование межведомственных несогласованностей

Таблица 8.7 показывает, что законность, права граждан, объяснимость и механизм обжалования включаются в конструкцию цифрового сознания публичной организации. Эффективность цифровой услуги не может компенсировать нарушение этих требований.

Ролевая архитектура публичного профиля должна обеспечивать разделение политической, административной, технической и контрольной ответственности. Руководитель органа утверждает публичную цель и принимает решение о риске; владелец услуги отвечает за результат для гражданина; владелец реестра – за качество данных; ИТ – за инфраструктуру; юридическая функция – за законность; служба безопасности – за защиту; подразделение по работе с обращениями – за доступный механизм пересмотра. Межведомственный сценарий требует соглашения о владельцах и порядке исправления данных.

Для высокочащного сценария применяется оценка воздействия. Она описывает затронутые права, категории граждан, используемые данные, возможные ошибки, риск исключения, доступность альтернативы, степень автоматизации, компетентность проверяющего и порядок уведомления. Оценка проводится до пилота и повторяется после существенного изменения модели, источника данных или масштаба применения.

Проектирование публичного сервиса целесообразно вести с участием пользователей. Наблюдение за реальным прохождением услуги, интервью, тестирование понятности и работа с представителями уязвимых групп позволяют выявить барьеры, которые не видны из ведомственного процесса. Участие не означает передачу государственно-властной ответственности, но делает решение более применимым и легитимным.

Показатели публичного профиля разделяются на четыре группы: общественный результат, качество услуги, права и доверие, институциональная устойчивость. Время обработки и доля электронных заявлений относятся только ко второй группе. Они интерпретируются вместе с долей успешного завершения, доступностью, числом исправленных ошибок, результатами обжалования, удовлетворенностью понятностью и устойчивостью межведомственного обмена.

Ежегодный пересмотр должен включать публично значимые результаты: какие цифровые решения введены, какие данные используются, какие риски выявлены, сколько обращений привело к корректировке и какие практики приостановлены. Прозрачность не требует раскрытия защищенной технической информации, но требует объяснения целей, ответственности и способов защиты прав.

Таким образом, в публичном управлении цифровое сознание измеряется способностью создавать общественную ценность при сохранении законности, доступности, объяснимости и права гражданина на пересмотр. Электронная услуга или ИИ-сценарий не могут считаться зрелыми, если их результат нельзя понять, исправить или оспорить. Критические правовые и этические минимумы не компенсируются процессной эффективностью.

8.5. АДАПТАЦИЯ МОДЕЛИ ДЛЯ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ В КОНТЕКСТЕ МЕДИЦИНЫ 4.0

Медицинская организация относится к высокорисковым социально-цифровым системам: цифровое решение способно одновременно повысить доступность и качество помощи и создать прямой риск для здоровья, безопасности, конфиденциальности или непрерывности лечения. Поэтому отраслевой профиль должен связывать технологии не с количеством внедренных сервисов, а с клинической целесообразностью, безопасностью пациента, качеством медицинской помощи, преемственностью наблюдения, соблюдением прав пациента и персональной ответственностью медицинского работника [153–156].

В настоящем пособии медицина 4.0 понимается как пациентоцентричная социотехническая модель, объединяющая электронные медицинские данные, подключённые медицинские изделия, телемедицинские технологии, дистанционный мониторинг, искусственный интеллект, роботизированные и аддитивные технологии, облачные и периферийные вычисления в управляемые клинические и организационные процессы. Технологическая связанность является средством, а не самостоятельным результатом: её ценность определяется улучшением исходов, доступности, безопасности и непрерывности помощи. Обследование 50 государств Европейского региона ВОЗ показывает, что внедрение ИИ в здравоохранение развивается неравномерно и по-прежнему сопровождается разрывами в управлении, готовности персонала, регулировании и управлении данными [162].

Миссия медицинского профиля цифрового сознания состоит в безопасном и доказательном использовании цифровых технологий для профилактики, диагностики, лечения, реабилитации, мониторинга состояния пациента и управления медицинской организацией. ISO 7101:2023 ориентирует систему

управления качеством здравоохранения на пациентоцентричность, управление рисками, безопасность пациентов и работников, измерение клинических и неклинических результатов и постоянное улучшение [160]. Следовательно, цифровая зрелость медицинской организации оценивается через качество помощи и клиническую безопасность, а не через инфраструктурную насыщенность.

Карта стейкхолдеров включает пациента и его законных представителей, врачей, средний медицинский персонал, диагностические и фармацевтические подразделения, службу записи и маршрутизации, службу качества и безопасности медицинской деятельности, ИТ- и кибербезопасность, владельцев данных, страховые организации, регуляторов, разработчиков медицинских изделий и поставщиков ИИ-систем. Для каждого сценария фиксируются права, профессиональные полномочия, информационные потребности, риски и порядок пересмотра решения. Пациент не должен превращаться в пассивный объект алгоритмической обработки.

Управление медицинскими данными охватывает электронную медицинскую документацию, результаты лабораторных и инструментальных исследований, медицинские изображения, генетические сведения, данные назначений, подключенных устройств и дистанционного мониторинга. Для каждого набора данных определяются происхождение, целостность, актуальность, клинический контекст, семантическая совместимость, владелец, режим доступа, журналирование, срок хранения и допустимые вторичные цели. Данные, пригодные для непосредственного оказания помощи, не автоматически пригодны для обучения модели, исследования или оценки работника [153; 154; 158].

Интероперабельность в медицине имеет не только техническое, но и клиническое содержание. Передача показателя между системами должна сохранять идентичность пациента, единицы измерения, время получения, метод исследования, референтный диапазон и клинический контекст. Технически успешный обмен при утрате смысла данных создает риск ошибочного решения. Поэтому архитектурно-сервисный контур медицины 4.0 должен включать управление медицинскими справочниками, терминологиями, версиями интерфейсов и качеством межсистемного обмена.

Сценарии применения ИИ целесообразно классифицировать по клиническому риску. К низкому риску относятся подготовка обезличенных информационных материалов, ресурсное планирование и классификация документов без влияния на медицинское решение. Умеренный риск характерен для маршрутизации пациентов, аналитики потоков, предварительной обработки исследований и дистанционного мониторинга при наличии установленных порогов эскалации. Высокий риск возникает при интерпретации

диагностических данных, прогнозировании ухудшения, поддержке выбора терапии и дозирования, клинической сортировке и иных действиях, способных изменить лечение. Для высокорискового сценария обязательны клиническая валидация, описание назначения и ограничений, применимость к локальной популяции, управление версиями, проверка компетентным медицинским работником и мониторинг после внедрения [155–157; 161].

Принцип «человек в контуре решения» в медицине должен быть клиническим, а не формальным. Специалисту необходимы достаточная квалификация, доступ к исходным данным, понимание ограничений модели, время на проверку, полномочие отклонить рекомендацию и возможность зафиксировать основание решения. Если интерфейс создает давление в пользу алгоритмического ответа или медицинский работник не способен проверить его, присутствие человека не обеспечивает реального контроля.

Подключенные медицинские изделия и дистанционный мониторинг требуют отдельного контура надежности. Организация проверяет точность и стабильность измерений, идентификацию пациента и устройства, качество связи, обработку пропусков, приоритет тревожных сообщений, риск ложных срабатываний и наличие резервного клинического маршрута. Цифровое наблюдение не должно создавать иллюзию непрерывного медицинского контроля, если фактически отсутствуют ответственный специалист, регламент реакции или гарантированный канал связи.

Кибербезопасность медицинской организации является частью безопасности пациента. Недоступность медицинской информационной системы, подмена данных, компрометация учетной записи, нарушение работы оборудования или атака на поставщика способны прервать лечение и повлиять на клиническое решение. Поэтому планы непрерывности должны включать резервирование, сегментацию, управление доступом, контроль поставщиков, восстановление, ручные клинические процедуры и регулярные учения [81; 101; 154].

Этико-правовой контур включает информирование пациента о существенном применении ИИ, защиту медицинской тайны, оценку справедливости и доступности, контроль предвзятости по отношению к возрастным, социальным и клиническим группам, право на понятное объяснение и человеческий пересмотр. Точность модели в среднем по выборке не отменяет анализа ее влияния на уязвимые группы и редкие клинические ситуации [155; 157].

Развитие персонала строится по ролевому принципу. Врачу необходимы критическая оценка доказательств и результатов ИИ, понимание границ автоматизации и документирование решения; среднему медицинскому персоналу – безопасная работа с устройствами, данными и тревожными сигналами; руководителю – управление качеством, рисками, данными,

поставщиками и ответственностью; ИТ- и инженерным специалистам – понимание клинического процесса и последствий отказа. Обучение должно включать сценарные задания, симуляции, разбор инцидентов и практику остановки небезопасного решения.

Управление медицинским профилем требует межфункционального органа или устойчивого координационного контура. В него входят клинический руководитель, служба качества и безопасности медицинской деятельности, ИТ, информационная безопасность, защита данных, юридическая и этическая экспертиза, владельцы процессов и представители пользователей. Для медицинского изделия с ИИ дополнительно проверяются регистрационный статус, клиническая оценка, условия эксплуатации, изменения версии и пострегистрационный мониторинг.

В диагностической модели повышенный вес получают цифровая безопасность, этика и право, грамотность в области данных и ИИ и информационно-аналитическая критичность. Некомпенсируемыми минимумами являются безопасность пациента, клиническая валидация, конфиденциальность медицинских данных, реальный человеческий контроль, прослеживаемость решения и непрерывность медицинской помощи. Высокая оценка сервисов, коммуникации или автоматизации не может компенсировать нарушение любого из этих требований.

Структура медицинского отраслевого профиля представлена на рисунке 8.6. Она связывает клиническую миссию, данные, ИИ, подключенные устройства, безопасность, этику, персонал и управление качеством.



Рисунок 8.6 – Отраслевой профиль цифрового сознания медицинской организации в контексте медицины 4.0

Источник: составлено авторами на основе [153–162].

Рисунок 8.6 показывает, что зрелость медицины 4.0 определяется согласованием клинической ценности, качества медицинских данных, клинической валидации ИИ, надежности подключенных устройств, киберустойчивости и человеческой ответственности. Центральным критерием остается безопасность пациента.

Параметры адаптации медицинской организации систематизированы в таблице 8.8. Таблица используется как рабочий паспорт при проектировании локального профиля медицины 4.0.

Таблица 8.8 – Паспорт адаптации методологии для медицинской организации в контексте медицины 4.0

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
Миссия и результат	Безопасность пациента, качество, доступность, непрерывность и клиническая результативность помощи	Карта клинической ценности и результатов	Подмена клинического результата количеством цифровых сервисов
Субъекты и роли	Пациенты, врачи, средний медицинский персонал, диагностика, ИТ, качество, регуляторы и поставщики	Карта стейкхолдеров и клинико-цифровых ролей	Принятие решения без компетентного клинического участника
Критические данные	Электронная медицинская документация, изображения, лабораторные, генетические, лекарственные и сенсорные данные	Паспорт медицинских данных и карта происхождения	Клиническая ошибка из-за некачественных данных или неверной идентификации пациента
ИИ-сценарии	Классификация сценариев по клиническому риску и условиям человеческого контроля	Реестр ИИ-сценариев, клиническая валидация и журнал версий	Автоматизация ошибки и размывание ответственности

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
Подключенные изделия	Точность измерений, идентификация, связь, тревоги, резервный маршрут	Реестр устройств, приемочные испытания, мониторинг и резервные процедуры	Отказ устройства, пропущенная или ложная тревога
Этика и доверие	Медицинская тайна, информирование, справедливость, объяснение и пересмотр	Этико-клинический шлюз цифрового сценария	Предвзятость, скрытое применение ИИ и потеря доверия пациента
Безопасность и непрерывность	Киберустойчивость клинического процесса и сохранение помощи при отказе систем	План непрерывности, ручные процедуры, сегментация и учения	Прерывание лечения или недоступность критичных данных
Обучение	Рольевые программы для клиницистов, среднего персонала, руководителей, ИТ и инженеров	Симуляции, кейсы, разбор инцидентов и тренировки остановки	Обучение интерфейсу без клинической и риск-ориентированной подготовки
Управление	Межфункциональная клиничко-цифровая ответственность и контроль жизненного цикла	Комитет по цифровой медицине, владельцы сценариев и контур качества	Разрыв между клиническим, техническим и управленческим решениями
Пилот и масштабирование	Локальная валидация, стандартный процесс сравнения, критерии остановки и постмониторинг	Паспорт пилота, протокол оценки и решение о масштабировании	Преждевременное распространение решения без доказанной безопасности и ценности

Таблица 8.8 показывает, что медицинская адаптация охватывает клиническую миссию, данные, ИИ, подключенные изделия, непрерывность, обучение и межфункциональное управление. Ее центральный критерий – способность цифрового решения улучшать медицинскую помощь без снижения безопасности и профессиональной ответственности. Паспорт применяется до пилота и обновляется при изменении алгоритма, данных, клинического процесса или уровня риска.

Пилотирование медицинского сценария проводится в ограниченном клиническом процессе и начинается только после проверки правового статуса, качества данных, кибербезопасности, клинической валидации и готовности

персонала. До запуска фиксируются стандартный процесс сравнения, показатели клинической ценности и безопасности, ответственные лица, способ информирования пациента, критерии остановки и резервная процедура. После пилота оцениваются не только точность и скорость, но и ошибки, нагрузка, влияние на клиническое мышление, доступность, доверие и устойчивость процесса.

Предполагается, что цифровое сознание медицинской организации развивается устойчиво, если технологическая интеграция медицины 4.0 подчинена клинической целесообразности, безопасности пациента и доказательной оценке на протяжении жизненного цикла. Приоритет автоматизации без клинической валидации и реального человеческого контроля повышает цифровую активность, но не формирует медицинскую цифровую зрелость.

Таким образом, медицинская адаптация переводит универсальную модель в высокорисковый клинический контекст. Ее ядро образуют пациентоцентричность, качество медицинских данных, клиническая валидация ИИ, надежность подключенных устройств, киберустойчивость, этико-правовая ответственность, ролевое обучение и непрерывный мониторинг. Расширенные заполняемые формы медицинского профиля представлены в медицинском разделе интерактивного научно-методического руководства.

8.6. АДАПТАЦИЯ МОДЕЛИ ДЛЯ НАУЧНОЙ, ПРОЕКТНОЙ ИЛИ ЭКСПЕРТНОЙ ОРГАНИЗАЦИИ

Научная, проектная или экспертная организация создает знание, доказательства, модели, проектные решения и экспертные заключения. Поэтому центральным объектом отраслевой адаптации является эпистемическое качество – достоверность, прослеживаемость, воспроизводимость и обоснованность интеллектуального продукта. Цифровое сознание этой сферы должно защищать не только данные и инфраструктуру, но и процедуру производства знания [41; 65; 132; 138].

Цифровое сознание организации, производящей знания можно определить как способность использовать цифровые технологии, исследовательские данные и ИИ для ускорения создания знания при сохранении научной добросовестности, проверяемости источников, воспроизводимости, конфиденциальности и интеллектуальных прав. В проектной и экспертной работе к этим требованиям добавляются обязательства перед заказчиком, ограничения договора и прослеживаемость оснований рекомендации.

Критические данные включают исследовательские наборы, экспериментальные результаты, код, модели, проектную документацию, экспертные материалы, конфиденциальные данные заказчика и объекты

интеллектуальной собственности. Для них необходимы планы управления исследовательскими данными, правила доступа, версии, метаданные, резервирование и условия публикации. Принципы FAIR – находимость, доступность, совместимость и повторное использование – применяются там, где они совместимы с правом, безопасностью и договорными ограничениями [138].

ИИ-сценарии охватывают библиографический поиск, анализ данных, моделирование, помощь в программировании, визуализацию, управление знаниями, патентную аналитику и подготовку черновых материалов. Высокая скорость генерации создает особую опасность: правдоподобная форма способна скрыть вымышленные ссылки, несуществующие данные и незафиксированные преобразования. Поэтому результат ИИ не может включаться в доказательную цепочку без верификации и указания способа получения.

Научная добросовестность требует правил раскрытия использования ИИ. Организация должна различать техническую помощь, аналитическое преобразование, генерацию текста, генерацию кода и участие ИИ в экспертном выводе. Для каждого уровня определяется необходимая степень раскрытия, проверка источников, ответственность автора и допустимость использования в рецензировании или оценке.

Цифровое доверие в этой сфере является доверием к процедуре производства доказательств. Заказчик, рецензент, партнер и общество должны иметь возможность понять происхождение данных, ход преобразований, роль ИИ и пределы вывода. Если организация ускоряет подготовку текста, но теряет прослеживаемость и воспроизводимость, ее цифровая активность растет, а цифровое сознание снижается.

В отраслевом индексе повышаются веса критичности, грамотности в области данных и ИИ, этики и рефлексивности. Устанавливаются минимумы: научная добросовестность и раскрытие использования ИИ не ниже 55 баллов, безопасность не ниже 45. Высокая производительность или объем публикаций не компенсируют нарушение данных требований.

Предполагается, что ИИ повышает результативность организации, производящей знания только при сохранении прослеживаемой цепочки «источник – метод – преобразование – проверка – вывод – раскрытие». Разрыв любого звена увеличивает скорость производства цифрового артефакта, но снижает эпистемическую легитимность результата.

Пилот рекомендуется проводить в одной лаборатории, проектном офисе или экспертном центре и ограничивать несколькими сценариями: поиск, обработка данных, программный код или подготовка черновика. Для каждого сценария создается протокол раскрытия, журнал проверки, правила конфиденциальности и критерии воспроизводимости. Повторная оценка проводится не только по экономии времени, но и по качеству источников и числу исправленных ошибок.

Развитие AlphaFold и открытых инфраструктур белковых структур показывает потенциал соединения ИИ и качественных открытых данных [66]. Политики UKRI демонстрируют институционализацию правил использования генеративного ИИ в заявках и экспертных процедурах [134]. Оба направления подтверждают, что ответственная цифровая наука требует инфраструктуры и формализованных границ, а не только индивидуальной осторожности.

Логика научно-экспертного профиля представлена на рисунке 8.7 как цепочка производства проверяемого знания.



Рисунок 8.7 – Контур доказательности научной, проектной и экспертной организации

Источник: составлено авторами на основе [41; 65; 116; 132; 138].

Рисунок 8.7 показывает, что цепочка начинается с проверяемого источника и плана данных, проходит через метод, цифровое или ИИ-преобразование, экспертную проверку и раскрытие использования ИИ, а завершается воспроизводимым либо аудируемым результатом. Защитный контур охватывает конфиденциальность и интеллектуальные права.

Параметры адаптации научной, проектной или экспертной организации систематизированы в таблице 8.9. Они задают требования к доказательности, воспроизводимости и прозрачности использования данных и ИИ.

Таблица 8.9 – Паспорт адаптации методологии для научной, проектной или экспертной организации

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
Миссия и результат	Новое знание, проектное решение, экспертиза, доказательность и интеллектуальный продукт	Карта доказательственной цепочки	Производство убедительного, но недостоверного результата
Субъекты	Исследователи, аналитики, инженеры, эксперты, проектные менеджеры, заказчики, рецензенты	Карта ролей автора, владельца данных и проверяющего	Размывание авторства и ответственности
Критические данные	Исследовательские данные, код, модели, проектные документы, данные заказчика, интеллектуальная собственность	План управления данными и матрица доступа	Потеря воспроизводимости, утечка и конфликт прав
Сценарии ИИ	Поиск, анализ, моделирование, код, визуализация, управление знаниями, подготовка черновиков	Реестр сценариев и протокол раскрытия	Вымышленные источники и скрытое соавторство
Качество результата	Прослеживаемость, воспроизводимость, экспертная проверка и фиксация ограничений	Чек-лист доказательности и журнал преобразований	Невозможность повторить или проверить вывод
Критические минимумы	Добросовестность и раскрытие не ниже 55; безопасность не ниже 45	Эпистемический и этический шлюз	Компенсация недостоверности скоростью или числом публикаций
Локальные документы	Политика ИИ в исследованиях, авторство и раскрытие, управление данными, интеллектуальная собственность и конфиденциальность	Согласованный пакет исследовательского управления	Формальные правила без технической инфраструктуры
Обучение	Управление данными,	Лабораторные	Обучение генерации

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
	воспроизводимость, проверка источников, безопасный ИИ, интеллектуальные права	протоколы и практикумы воспроизводимости	без методологии проверки
Пилот	Одна лаборатория, проект или экспертная процедура и ограниченный набор сценариев	Протокол пилота, журнал проверки и раскрытия	Расширение ИИ-применения без доказательной валидации
Масштабирование	Расширение при сохранении аудируемости, безопасности и качества	Порог воспроизводимости и независимая экспертиза	Тиражирование непроверяемых практик

Таблица 8.9 переносит центр оценки с производительности инструментов на качество доказательственной процедуры. Основным результатом признается не объем сгенерированного материала, а обоснованное, проверяемое и воспроизводимое знание.

Роли научно-экспертного профиля должны быть связаны с доказательственной цепочкой. Руководитель исследования или проекта отвечает за замысел и итоговый вывод; владелец данных – за происхождение, качество и доступ; специалист по ИИ – за описание модели и ограничений; автор – за проверку текста и ссылок; независимый рецензент – за критическую оценку; организация – за правила раскрытия, конфиденциальности и интеллектуальной собственности.

План управления данными дополняется разделом об ИИ. В нем фиксируются модели и версии, внешние сервисы, категории передаваемых данных, способы предварительной обработки, сохранение запросов и результатов, критерии проверки, требования к воспроизводимости и условия публикации. Если полная воспроизводимость невозможна из-за закрытой модели, должен быть обеспечен достаточный аудиторский след и описано ограничение.

Для экспертного заключения рекомендуется матрица происхождения утверждений. Каждое значимое положение связывается с первичным источником, данными, методом анализа, возможной ролью ИИ и экспертом, подтвердившим вывод. Матрица особенно полезна при коллективной подготовке материалов и позволяет обнаружить ссылки, которые были сгенерированы, но не проверены.

Диагностика профиля включает аудит выборки проектов, проверку планов данных, анализ случаев исправления и отзыва материалов, опрос исследователей, оценку защищенности сред и разбор сценариев использования ИИ. Показатель количества публикаций, отчетов или сэкономленных часов не интерпретируется без оценки качества и воспроизводимости.

Организационное обучение строится вокруг безобвинительного разбора эпистемических ошибок. Целью является не сокрытие факта использования ИИ и не стигматизация пользователя, а уточнение протокола проверки. Умышленная фабрикация и добросовестная ошибка различаются процедурно. Такое различие повышает готовность сообщать о сомнительном результате до его внешнего распространения.

Таким образом, для научной, проектной и экспертной организации цифровое сознание выражается в способности ускорять интеллектуальную работу без разрушения достоверности, прослеживаемости, воспроизводимости и ответственности. Обязательны правила раскрытия использования ИИ, управление исследовательскими данными, защита интеллектуальной собственности и независимая проверка результата.

8.7. АДАПТАЦИЯ МОДЕЛИ ДЛЯ СОЦИАЛЬНОЙ И НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

Социальная и некоммерческая организация использует цифровые технологии для достижения общественно значимого результата, защиты прав, оказания помощи, вовлечения сообществ и обеспечения устойчивости программ. Поэтому цифровая трансформация здесь подчинена миссии социального воздействия, а не модернизации как самоцели. Отраслевой профиль должен учитывать ограниченность ресурсов и одновременно высокую чувствительность данных благополучателей [16; 90; 103].

Цифровое сознание социальной организации можно определить как способность применять данные, цифровые сервисы и ИИ для расширения социального эффекта, не причиняя дополнительного вреда уязвимым группам, сохраняя конфиденциальность, доступность, информированное участие и возможность человеческого пересмотра. Центральным принципом выступает этика заботы: эффективность рассматривается через влияние на конкретного человека и сообщество.

Стейкхолдеры образуют сложную конфигурацию: сотрудники, волонтеры, благополучатели, доноры, грантодатели, партнеры, общественность и государственные органы. Их ожидания могут не совпадать. Донору необходимы доказательства результата, благополучателю – безопасность и уважение, волонтеру – понятные инструменты, организации – устойчивость и экономия

ресурсов. Отраслевая адаптация должна открыто описывать эти напряжения и не подменять интересы благополучателя удобством отчетности.

Критические данные включают сведения о здоровье, социальном статусе, семейной ситуации, обращениях, пожертвованиях, волонтерах и результатах программ. Даже небольшой объем таких данных может иметь высокую чувствительность. Поэтому минимизация, информированное согласие, ограничение доступа и правила безопасного уничтожения информации являются базовыми требованиями, а не показателями поздних уровней зрелости.

ИИ-сценарии могут использоваться для первичной маршрутизации обращений, перевода и повышения доступности, поддержки коммуникации с донорами, подготовки грантовых материалов, аналитики социального эффекта и координации волонтеров. Недопустимо автоматическое распределение помощи или определение уязвимости без прозрачных критериев, компетентного человека и процедуры исправления.

Исследования Data Orchard показывают медленное повышение зрелости работы с данными в некоммерческом секторе при устойчивом дефиците грамотности [90]. Материалы NetHope подчеркивают недостаток ресурсов на киберзащиту в организациях, работающих с критически уязвимыми сообществами [103]. Следовательно, малый бюджет не снижает требования к безопасности, а требует коллективных решений, типовых защищенных инструментов и партнерской поддержки.

Цифровое доверие в социальной сфере имеет триадную структуру: доверие благополучателя, доверие донора и доверие сообщества. Благополучатель должен быть уверен, что данные не причинят вреда; донор – что отчетность доказательна; сообщество – что цифровой проект не исключает людей и не присваивает их голос. Поэтому открытость должна сочетаться с конфиденциальностью: публикация данных ради отчетности ограничивается принципом минимально достаточного раскрытия.

В отраслевом индексе повышаются веса этики и ответственности, безопасности и рефлексивности. Минимумы составляют 55 баллов по защите уязвимых групп и конфиденциальности и 45 баллов по безопасности. Если они не достигнуты, организация не может быть отнесена к интегрированному или адаптивно-рефлексивному уровню независимо от социального эффекта.

Предполагается, что цифровые технологии усиливают социальную миссию только при одновременном соблюдении четырех условий – минимизации данных, защиты уязвимых групп, доступности и участия сообщества. При отсутствии любого условия цифровизация способна увеличить масштаб программы и одновременно увеличить масштаб цифрового вреда.

Пилот целесообразно проводить в одной программе помощи или одном сервисе обращений. Он должен быть малобюджетным, но жестко защищенным:

ограниченный набор данных, ручной резервный маршрут, участие благополучателей в оценке, доступные каналы обратной связи и заранее определенная процедура реагирования на инцидент.

Программы TechSoup Europe показывают значение постепенного наращивания организационной способности, а не разовой закупки технологий [128]. Кейсы Ushahidi демонстрируют потенциал данных, создаваемых сообществами, для реагирования на кризисы и решения локальных проблем, но одновременно требуют контроля качества, безопасности участников и ответственного представления данных [141].

Социально-некоммерческий профиль представлен на рисунке 8.8. Он соединяет миссию, заботу, доверие, безопасность, доступность, данные и ограниченность ресурсов.



Рисунок 8.8 – Профиль цифровой устойчивости социальной и некоммерческой организации

Источник: составлено авторами на основе [16; 90; 103; 128; 141].

Рисунок 8.8 показывает, что в центре социально-некоммерческого профиля находится общественный эффект без дополнительного цифрового вреда. Защита уязвимых групп, доступность, минимизация данных, участие сообщества, безопасность и ресурсная соразмерность определяют границы допустимой цифровизации.

Параметры социальной и некоммерческой адаптации приведены в таблице 8.10. Они позволяют связать общественную миссию организации с этическими, безопасными и ресурсными ограничениями.

Таблица 8.10 – Паспорт адаптации методологии для социальной и некоммерческой организации

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
Миссия и результат	Социальный эффект, защита прав, благополучие, участие сообщества и устойчивость программ	Карта социального результата и цифрового влияния	Подмена миссии показателями цифрового охвата
Субъекты	Сотрудники, волонтеры, благополучатели, доноры, партнеры и уязвимые группы	Карта доверия и участия	Решения о людях без их голоса
Критические данные	Здоровье, социальный статус, обращения, пожертвования, волонтеры и результаты программ	Карта чувствительности, согласие и минимизация	Стигматизация, утечка и вторичное использование данных
Сценарии ИИ	Маршрутизация обращений, перевод, коммуникация, грантовая поддержка, аналитика эффекта	Реестр сценариев и человеческий пересмотр	Несправедливое распределение помощи
Доступность	Альтернативные форматы, понятный язык, поддержка пользователей	Проверка доступности по замыслу	Цифровое исключение благополучателей
Критические минимумы	Защита уязвимых групп и конфиденциальность не ниже 55; безопасность не ниже 45	Этический шлюз заботы	Компенсация вреда высоким социальным охватом
Локальные документы	Защита благополучателей, конфиденциальность и согласие, поведение волонтеров, данные доноров, реагирование	Набор простых типовых правил	Формальные документы, недоступные волонтерам и полевым работникам
Обучение	Конфиденциальность, защита, инклюзия, измерение воздействия, безопасные недорогие инструменты	Короткие модули и наставническая поддержка	Перегрузка малой команды сложными требованиями
Пилот	Одна программа или	Паспорт	Эксперимент на

Блок профиля	Отраслевая настройка	Практический инструмент	Критический риск
	сервис, ограниченный набор данных, ручной резерв	защищенного пилота	уязвимой группе без гарантий
Масштабирование	Расширение после оценки вреда, доверия, устойчивости и доступности	Порог социальной и киберготовности	Рост охвата быстрее способности защищать данные

Таблица 8.10 показывает, что ограниченность ресурсов не отменяет этических и безопасностных минимумов. Методология должна быть соразмерной масштабу организации, понятной исполнителям и выполнимой без создания избыточной цифровой нагрузки.

Ресурсно-пропорциональная модель управления допускает совмещение ролей, но сохраняет контрольные функции. Руководитель программы отвечает за социальный результат; ответственное лицо по защите благополучателей – за предотвращение вреда; владелец данных – за режим информации; ИТ-партнер – за техническую среду; координатор волонтеров – за доступность правил; коллегиальный орган или внешний эксперт рассматривает высокорисковые сценарии.

Практическим инструментом является карта цифрового вреда. Она фиксирует, кто может пострадать, через какой механизм, насколько обратим ущерб, какие ранние сигналы доступны, кто может остановить сценарий и какая поддержка предоставляется пострадавшему. Карта дополняет обычный реестр информационной безопасности социальными последствиями – стигмой, исключением, ошибочным отказом в помощи и потерей доверия.

Для волонтеров и временных участников правила должны быть особенно краткими и доступными. Необходимо определить разрешенные каналы, запрет на хранение данных в личных устройствах и облаках, порядок фото- и видеосъемки, использование переводчиков и ИИ, сообщение об инциденте и удаление данных после завершения роли. Формальное ознакомление не заменяет практический инструктаж.

Коллективная устойчивость может обеспечиваться через партнерские центры киберзащиты, общие лицензии, отраслевые базы знаний, типовые договоры и взаимное наставничество. Однако совместная инфраструктура не отменяет оценки конкретной программы. Организация должна понимать, какие данные она передает партнеру, какие гарантии получает и как продолжит работу при прекращении сервиса.

Оценка социального пилота включает не только количество обслуженных обращений, но и доступность для целевых групп, долю корректных маршрутов,

случаи ручного пересмотра, доверие пользователей, инциденты конфиденциальности и нагрузку команды. При выявлении вреда сценарий приостанавливается независимо от достигнутого охвата.

Таким образом, социальная и некоммерческая адаптация подчиняет цифровизацию миссии и принципу непричинения дополнительного вреда. Центральны защита уязвимых групп, минимизация данных, доступность, участие сообщества и киберустойчивость. Простота решения допустима, снижение этических гарантий – нет.

8.8. СРАВНИТЕЛЬНАЯ КАРТА ОТРАСЛЕВЫХ МОДИФИКАЦИЙ МОДЕЛИ

Сравнительная карта необходима для того, чтобы показать различия отраслевых профилей без превращения их в шесть автономных моделей. Единицей сравнения выступает не технологический набор, а конфигурация миссии, данных, ИИ-сценариев, рисков, ответственности, доверия, обучения и зрелости. Такой подход сохраняет научную сопоставимость и одновременно предотвращает механическое копирование решений.

Общим для всех сфер остается определение цифрового сознания, пятиуровневая архитектура, семь компонентов, шесть организационных контуров, диагностическая триангуляция, пятиуровневая шкала зрелости и запрет цифрового надзора. Различаются содержательные акценты. В образовании доминируют педагогическое качество и академическая честность; в бизнесе – клиентская ценность и устойчивость; в публичном управлении – законность и общественная ценность; в медицине – безопасность пациента, клиническая валидация и непрерывность помощи; в научной сфере – доказательность и воспроизводимость; в социальной – защита уязвимых групп и непричинение вреда.

Цифровое доверие также имеет отраслевую специфику. В образовании оно связано с честностью оценивания и защитой образовательных данных. В коммерческой сфере – с надежностью продукта, отношением к клиенту и отсутствием скрытого контроля работников. В публичной сфере – с законностью, объяснимостью и обжалованием. В медицине – с безопасностью пациента, сохранением медицинской тайны, клинической обоснованностью и правом на человеческий пересмотр. В научной сфере – с прослеживаемостью доказательств. В социальной – с непричинением дополнительного вреда, доступностью и участием сообщества.

Для сохранения единства индекса предлагается использовать общую формулу отраслевого индекса организационного цифрового сознания:

$$\text{ИОЦС}_s = (\sum w_{sj} \times O_j / \sum w_{sj} \times \text{Omax}) \times 100,$$

где $ИОЦС_s$ – индекс для сектора s ; w_{sj} – отраслевой вес j -го компонента; O_j – оценка компонента; O_{max} – максимальная оценка. Сумма весов для каждого профиля равна 100. Формула сохраняет общий диапазон 0–100 и позволяет сравнивать динамику организации во времени, но межотраслевое ранжирование допустимо только с учетом различий миссии и критических минимумов.

Некомпенсируемый минимум означает, что высокий балл по другим компонентам не устраняет критический дефицит. Математически применяется правило отраслевого шлюза: если хотя бы один критический показатель M_k ниже установленного порога T_{sk} , итоговый уровень не может превышать координируемый. После устранения дефицита уровень определяется по общей шкале. Такой механизм предотвращает ситуацию, когда интенсивное использование ИИ компенсирует отсутствие безопасности, законности или академической честности.

Предложенные веса и пороги являются авторскими исследовательскими гипотезами. До массового применения они проходят экспертную проверку, пилотную диагностику, анализ внутренней согласованности и сопоставление с качественными данными. Организация обязана утвердить веса до сбора данных; изменение коэффициентов после получения результата методологически недопустимо, поскольку создает возможность подгонки оценки.

Пятиуровневая шкала зрелости остается общей: фрагментарный, базовый, координируемый, интегрированный и адаптивно-рефлексивный уровни. Однако проявления уровней различаются. Интегрированная образовательная организация связывает аналитику обучения с этикой и инклюзией; интегрированный бизнес – клиентскую ценность с управлением данными и устойчивостью; публичный орган – межведомственные данные с правами граждан; научная организация – воспроизводимость с управлением знаниями; НКО – миссию с безопасной и доступной цифровой моделью.

Пакет документов также строится по принципу универсального ядра и специальных актов. Для всех сфер необходимы политика цифрового развития, управление данными, правила применения ИИ, информационная безопасность, цифровая коммуникация, обучение, карта рисков и порядок диагностики. Специальные документы отражают отраслевую ответственность: академическую честность; модельные и постмаркетинговые риски бизнеса; публичную подотчетность; клиническую валидацию, безопасность пациента и непрерывность медицинской помощи; научную добросовестность; защиту уязвимых групп.

Практическая проверка качества адаптации может быть проведена по десяти вопросам: сохранено ли определение; описана ли миссия; охвачены ли стейкхолдеры; картированы ли процессы и данные; учтены ли реальные ИИ-сценарии; определены ли критические риски; обоснованы ли веса и минимумы;

связаны ли индикаторы с решениями; предусмотрены ли пилот и валидация; сохранены ли этические запреты. Отрицательный ответ требует доработки профиля до институционализации.

Проверяемое положение 8.8: межатраслевая переносимость методологии обеспечивается не унификацией индикаторов, а стабильностью ядра и воспроизводимостью процедуры настройки. Чем прозрачнее переход от миссии и процессов к весам, рискам и инструментам, тем выше сопоставимость отраслевых версий и ниже риск методологического дрейфа.

Заполняемый шаблон расширенной отраслевой матрицы размещен в интерактивном научно-методическом руководстве. В главе приводится сравнительная версия, демонстрирующая логику применения, а цифровая форма предназначена для настройки под конкретную организацию.

Сравнительная логика отраслевых профилей представлена на рисунке 8.9. Схема показывает, какие смысловые центры и критические минимумы отличают шесть сфер при сохранении единого методологического ядра.



Рисунок 8.9 – Сравнительная карта отраслевых профилей цифрового сознания организации

Источник: составлено авторами.

Рисунок 8.9 показывает, что единое ядро соединено с шестью отраслевыми профилями. Каждый профиль получает собственный смысловой центр и критический минимум, но сохраняет общую архитектуру уровней, компонентов, контуров, диагностики и зрелости. Схема показывает адаптацию как конфигурацию, а не как создание конкурирующих моделей.

Рекомендуемые весовые гипотезы и критические минимумы представлены в таблице 8.11. Они предназначены для экспертной и пилотной настройки, а не для механического применения без проверки.

Таблица 8.11 – Отраслевая настройка весов компонентов цифрового сознания

Сектор	Дееспособность	Критичность	Данные и ИИ	Этика, право, ответственность	Безопасность	Коммуникация	Рефлексивность	Специальные минимумы
Образование	13	14	18	17	16	10	12	Этика ≥ 50 ; безопасность ≥ 50 ; академическая честность ≥ 50
Коммерческая сфера	14	13	18	12	18	9	16	Этика ≥ 45 ; безопасность ≥ 50
Публичное управление	11	14	12	20	18	10	15	Законность и этика ≥ 55 ; безопасность ≥ 50 ; пересмотр ≥ 50
Медицинская организация	10	16	17	18	20	8	11	Безопасность пациента ≥ 55 ; клиническая валидация ≥ 55 ; конфиденциальность ≥ 55 ; человеческий контроль ≥ 55 ; непрерывность помощи ≥ 55
Научно-	12	18	16	16	13	8	17	Добросовестность и

Сектор	Дееспособность	Критичность	Данные и ИИ	Этика, право, ответственность	Безопасность	Коммуникация	Рефлексивность	Специальные минимумы
экспертная сфера								раскрытие ≥ 55 ; безопасность ≥ 45
Социальная и НКО	12	12	12	20	18	10	16	Защита уязвимых групп и конфиденциальность ≥ 55 ; безопасность ≥ 45

Таблица 8.11 сумма весов в каждой строке равна 100. Весовые настройки сохраняют семь компонентов универсальной модели и меняют только их относительную значимость. Специальные минимумы являются этическим и отраслевым шлюзом, а не дополнительными баллами.

Общая шкала зрелости и ее отраслевые проявления сопоставлены в таблице 8.12.

Таблица 8.12 – Отраслевые проявления уровней цифровой зрелости

Уровень	Общая характеристика	Образование	Коммерческая сфера	Медицинская организация	Публичное управление	Научно-экспертная сфера	Социальная и НКО
Фрагментарный	Разрозненные практики, роли и границы ИИ не определены	Сервисы и запреты без педагогического дизайна	Локальная автоматизация ради экономии	Разрозненные сервисы и ИИ без клинической валидации и единого управления	Витринная цифровизация отдельных услуг	Личное применение ИИ без протокола	Стихийное использование бесплатных сервисов
Базовый	Есть начальные правила и ответственности	Правила ИИ, данных и честности	Базовые политики и данных и киберзащиты	Базовые правила данных, безопасности и применения	Портал, регламент и отдельные цифровые роли	Локальные правила раскрытия и данных	Базовые правила конфиденциальности и защиты

Уровень	Общая характеристика	Образование	Коммерческая сфера	Медицинская организация	Публичное управление	Научно-экспертная сфера	Социальная и НКО
	нные			ения ИИ; ответственность определяется по отдельным сценариям			
Координируемый	Появляются контуры управления и регулярная диагностика	Переработка, оценивания и ролевое обучение	Реестр ИИ, владельцы процессов и реагирование	Ведутся реестры ИИ и устройств, назначены владельцы данных, действует клиническая проверка и мониторинг инцидентов	Межведомственная координация и путь обжалования	Управление данными, политика ИИ, экспертная проверка	Управление данными доноров и благополучателей, протоколы волонтеров
Интегрированный	Стратегия, данные, культура и безопасность согласованы	Аналитика обучения связана с этикой и инклюзией	Ценность, управление данными, доверие и устойчивость соединения	Данные, устройства, клинические процессы, качество и безопасность согласованы в	Целостные государственные сервисы и интероперабельность	Воспроизводимость, FAIR и управление знаниями встроены	Цифровая модель подчинена миссии и устойчива

Уровень	Общая характеристика	Образование	Коммерческая сфера	Медицинская организация	Публичное управление	Научно-экспертная сфера	Социальная и НКО
				единой системе управления			
Адаптивно-рефлексивный	Организация учится, объясняет решения и переносится	ИИ усиливает обучение, не заменяя его	Ценность ИИ сбалансирована ответственностью и доверием	Организация учится на клинических результатах, обновляет модели и правила и поддерживает доверие пациентов	Проактивные человекоцентричные услуги с прозрачным надзором	Ответственный ИИ ускоряет знание, сохраняя добросовестность	Технологии расширяют инклюзию без вреда уязвимым группам

Таблица 8.12 показывает, что пятиуровневая шкала зрелости остается общей, тогда как признаки каждого уровня раскрываются через отраслевую миссию, тип результата и характер рисков. Это сохраняет методологическое единство без ложного сравнения организаций, создающих разные виды ценности.

Итоговая сравнительная матрица приведена в таблице 8.13. Она объединяет параметры шести профилей и служит методической основой интерактивного конструктора отраслевой адаптации.

Таблица 8.13 – Итоговая матрица отраслевой адаптации методологии цифрового сознания организации

Параметр	Образование	Коммерческая сфера	Медицинская организация	Публичное управление	Научная, проектная, экспертная сфера	Социальная и НКО
Миссия и результат	Обучение, развитие, честность, доступность	Клиентская ценность, качество, прибыль, устойчивость	Безопасная, качественная, доступная и непрерывная медицинская помощь	Общественная ценность, законность, доступность, доверие	Знание, доказательность, проектное и экспертное качество	Социальный эффект, защита прав и благополучие

Параметр	Образование	Коммерческая сфера	Медицинская организация	Публичное управление	Научная, проектная, экспертная сфера	Социальная и НКО
Критические данные	Образовательные данные и цифровой след	Клиентские, финансовые, кадровые, коммерческие данные	Электронная медицинская документация, изображения, лабораторные, генетические, лекарственные и сенсорные данные	Государственные реестры, персональные, социальные и геоданные	Исследовательские данные, код, модели, документы заказчика, интеллектуальная собственность	Данные благополучателей, здоровья, статуса, обращений и доноров
Типовые ИИ-сценарии	Материалы, обратная связь, персонализация, библиографический поиск	Маркетинг, продажи, поддержка, прогноз, качество, HR	Маршрутизация, мониторинг, анализ исследований, прогноз риска и поддержка клинических решений	Обращения, аналитика, поддержка решений, чат-боты, умный город	Поиск, анализ, моделирование, код, визуализация, управление знаниями	Маршрутизация, перевод, коммуникация, гранты, аналитика эффекта
Критический риск	Подмена обучения, непрозрачная оценка, утечка данных	Предвзятость, манипуляция, надзор, зависимость от поставщика	Клиническая ошибка, утечка медицинской тайны, отказ устройства, предвзятость и прерывание помощи	Нарушение прав, исключение, необъяснимое властное решение	Вымышленные доказательства, невоспроизводимость, утечка интеллектуальной собственности	Вред уязвимым группам, стигма, нарушение конфиденциальности
Цифровое доверие	Педагогическое суждение, честное оценивание, защита данных	Надежность продукта, уважение к клиенту и сотруднику	Безопасность пациента, клиническая обоснованность, конфиденциальность, объяснение и пересмотр	Законность, объяснимость, доступность и обжалование	Прослеживаемость, воспроизводимость и раскрытие ИИ	Непричинение вреда, согласие, участие и сохранность данных
Критические минимумы	Этика, безопасность и академическая честность	Этика и безопасность	Безопасность пациента, клиническая валидация, конфиденциальность, человеческий контроль и непрерывность ≥ 55	Законность, этика, безопасность и пересмотр	Добросовестность, раскрытие и безопасность	Защита уязвимых групп, конфиденциальность и безопасность
Обучение	Цифровая педагогика, ИИ-грамотность, аналитика, инклюзия	Данные и ИИ, клиентская аналитика, кибергигиена, риск поставщиков	Рольевые программы, симуляции, клинические кейсы и разбор инцидентов	Публичные данные, доступность, объяснимость, права и межведомственная работа	Управление данными, воспроизводимость, добросовестность, интеллектуальные права	Конфиденциальность, защита, доступность, оценка эффекта, безопасные недорогие инструменты
Управление	Методический совет, владельцы данных, ИИ и	Совет или комитет по данным и ИИ, владельцы	Межфункциональный клинико-цифровой контур	Руководитель органа, юридическая функция,	Научный руководитель, этический орган, владелец	Руководитель программы, ответственный за защиту и

Параметр	Образование	Коммерческая сфера	Медицинская организация	Публичное управление	Научная, проектная, экспертная сфера	Социальная и НКО
	оценивания	продуктов и рисков	качества, данных, ИИ и безопасности	владелец данных и сервиса	проекта и данных	благополучателей
Пилот	Одна программа или контур оценивания	Один процесс с измеримой ценностью и человеческим резервом	Локальная клиническая валидация, стандартный процесс сравнения, критерии остановки и резервный маршрут	Один массовый сервис или межведомственный процесс	Одна лаборатория, проект или экспертная процедура	Одна программа помощи или сервис обращений
Масштабирование	После проверки педагогической ценности, честности и инклюзии	После доказательства повторяемого эффекта, доверия и устойчивости	После подтверждения клинической ценности, безопасности, устойчивости и готовности персонала	После проверки прав, доступности, качества данных и обжалования	После подтверждения воспроизводимости, безопасности и аудируемости	После оценки вреда, доверия, доступности и киберустойчивости

Таблица 8.13 показывает единство структуры и отраслевое различие содержания. Во всех профилях присутствуют миссия, данные, ИИ, риск, доверие, обучение, управление, пилот и масштабирование, но их предметное наполнение определяется институциональной ответственностью отрасли.

Процедура эмпирической валидации весов включает четыре этапа. Сначала междисциплинарная группа оценивает содержательную значимость компонентов. Затем проводится пилотное обследование и анализ распределения ответов. После этого результаты сопоставляются с качественными признаками зрелости и известными рисками. Наконец, веса утверждаются на ограниченный срок и пересматриваются только в следующем цикле. Такой порядок снижает риск произвольной настройки индекса.

Сопоставимость результатов имеет три уровня. Внутри одной организации допустимо анализировать динамику по времени. Внутри отрасли возможно сравнение при одинаковой версии профиля и близком контексте. Между отраслями корректно сравнивать не итоговые баллы, а структуру дефицитов, соблюдение критических минимумов и способность к организационному обучению. Прямой рейтинг университета, предприятия и органа власти по одному числу методологически неверен.

Расширенная электронная матрица в интерактивном руководстве имеет четыре слоя: индикаторы и шкалы; источники данных и ограничения интерпретации; владельцы, документы и управленческие решения; красные

флаги, запрещенные практики и условия остановки. Такая структура превращает ее в рабочий инструмент аудита и пилотирования.

Организация может создавать подотраслевой профиль – например, для высшего образования, финансового бизнеса, муниципальных услуг или гуманитарной НКО. Подотраслевая настройка допустима, если она сохраняет вышестоящий отраслевой профиль и документирует дополнительные риски. Нельзя использовать подотраслевую специфику для удаления этических гарантий или для изменения общей шкалы после получения результата.

Ежегодный отчет по отраслевой адаптации должен содержать версию профиля, обоснование изменений, динамику индексов и минимумов, результаты пилотов, новые ИИ-сценарии, карту рисков, данные о доверии, обновленные программы обучения и план корректирующих действий. Отчет не включает скрытые персональные рейтинги и не использует самооценку как основание кадровой санкции.

Методология считается институционализированной, когда профиль встроен в стратегию, процессы, управление данными и ИИ, обучение, локальные документы, бюджет и цикл пересмотра. Наличие заполненной матрицы без владельцев и решений является только этапом описания. Устойчивость подтверждается тем, что организация способна объяснить отраслевую логику профиля, применить ее к новому сценарию и пересмотреть правила после обратной связи.

Методический вывод по параграфу 8.8. Сравнительная карта подтверждает принцип «единое ядро – отраслевые профили». Сопоставимость обеспечивается общей архитектурой и формулой, а релевантность – настройкой миссии, рисков, индикаторов, весов и критических минимумов. Отраслевая адаптация не является основанием для ранжирования несопоставимых организаций; ее назначение – построение доказательной траектории развития внутри конкретной сферы.

Методическая процедура применения итоговой отраслевой матрицы

Применение таблицы 8.13 начинается с фиксации версии универсального ядра и выбранного отраслевого профиля. Рабочая группа не заполняет матрицу по субъективному впечатлению, а прикладывает к каждой ячейке подтверждающие материалы: стратегический документ, карту процесса, описание данных, реестр ИИ-сценариев, результаты интервью, регламент, журнал рисков или иной проверяемый источник. Отсутствие доказательства отмечается как диагностический разрыв, а не заполняется предполагаемым значением.

На втором этапе проводится межфункциональная проверка. Владельцы процессов оценивают применимость индикаторов к реальной деятельности; HR проверяет ролевые и образовательные последствия; ИТ – архитектурную

реализуемость; служба безопасности – риски и режим данных; юридическая функция – правомерность; представители затронутых групп – понятность, доступность и доверие. Разногласия фиксируются в протоколе и не устраняются усреднением без содержательного обсуждения.

На третьем этапе определяется ограниченный набор приоритетов. Организация не должна одновременно устранять все выявленные дефициты. Сначала выбираются нарушения критических минимумов, затем риски высокой тяжести и только после этого – зоны, способные дать значимый эффект развития. Для каждого приоритета назначаются владелец, ресурс, срок, способ проверки и условие остановки. Обучение выбирается только тогда, когда причиной действительно является дефицит компетентности.

На четвертом этапе профиль проверяется в пилоте. В течение пилота ведется журнал решений, побочных последствий, нагрузки и обращений. Обратная связь собирается через безопасные каналы и анализируется агрегированно. Если участники вынуждены обходить правило, рабочая группа проверяет качество сервиса, процесса и коммуникации до вывода о недостаточной готовности персонала. Такой порядок сохраняет развивающий и некарательный характер методологии.

На пятом этапе проводится повторная диагностика и принимается решение о масштабировании. Сравниваются не только интегральные баллы, но и профиль компонентов, соблюдение минимумов, качество управленческих решений и изменение доверия. Успешная практика закрепляется в документах, обучении, архитектуре и бюджете с установленной датой пересмотра. Неуспешная практика корректируется или прекращается; ее остановка рассматривается как признак организационной рефлексивности, а не как провал цифровой трансформации.

ИТОГИ ГЛАВЫ

Отраслевая адаптация строится по принципу «единое методологическое ядро – различные профили». Сохраняются определение, уровни, компоненты, этические ограничения и развивающий характер диагностики; настройке подлежат миссия, индикаторы, веса, кейсы, риски и механизмы внедрения.

Отраслевая версия должна быть документирована, проверена экспертами и стейкхолдерами, апробирована в пилоте и регулярно пересматриваться. Некомпенсируемые минимумы по безопасности, законности, правам и человеческому контролю не могут отменяться отраслевой спецификой.

Интерактивное сопровождение. В цифровом руководстве размещены конструктор отраслевого профиля, паспорт адаптации, сравнительная матрица, весовые модели и заполняемые шаблоны для образовательных, коммерческих, государственных, медицинских, научных и социальных

организаций. Они применяются после выбора соответствующего отраслевого профиля и сохраняются как документированная версия локальной конфигурации методологии.

ЗАКЛЮЧЕНИЕ

Цифровая трансформация становится организационно значимой не вследствие самого факта внедрения технологий, а тогда, когда организация способна понимать цели, основания, ограничения и последствия их применения. В пособии эта способность раскрыта через категорию цифрового сознания организации.

Цифровое сознание организации определяется как интегральная способность коллективного субъекта осознанно, критично, этично, безопасно и результативно использовать цифровые технологии, данные и искусственный интеллект. Понятие имеет аналитический и управленческий статус и не предполагает наделения организации психологическим сознанием.

Авторская модель объединяет различие цифрового сознания 1.0 и 2.0, пять уровней его формирования и семь содержательных компонентов. Такой подход показывает, каким образом индивидуальные способности сотрудников преобразуются в командные нормы, управленческие решения, организационные процессы и доверие внешних стейкхолдеров.

Связь цифрового сознания с цифровой зрелостью раскрыта через шесть организационных контуров: стратегию; данные, аналитику и ИИ; архитектуру и сервисы; культуру, доверие и безопасность; развитие персонала и команд; организационную рефлексивность. Их согласованность отличает устойчивое цифровое развитие от формальной технологизации.

Диагностический блок включает модели ИЦСС, ИЦСК и ИОЦС, уровни зрелости и принцип триангуляции. Эти инструменты предназначены для развития и управления рисками. До эмпирической валидации они не должны использоваться как стандартизованные психометрические тесты или как основание для автоматических кадровых решений. Критические минимумы по законности, безопасности, этике, защите прав и человеческому контролю не компенсируются высоким интегральным баллом.

Технология внедрения строится как цикл от подготовки и входной диагностики до пилотирования, мониторинга, масштабирования и институционализации. Устойчивость изменений обеспечивается лидерством, коммуникацией, участием сотрудников, профессиональными сообществами, ролевым обучением и регулярной рефлексией. Отраслевая адаптация сохраняет единое методологическое ядро и изменяет только прикладную конфигурацию модели.

Научная значимость пособия состоит в системном соединении цифровой грамотности, организационной культуры, цифровой зрелости, управления данными и ИИ, информационной безопасности, этики и организационного обучения. Ограничения подхода связаны с новизной конструкта и

необходимостью дальнейшей эмпирической проверки индексов, весов и отраслевых профилей.

Публикуемое пособие фиксирует теоретическую и научно-методическую основу. Обновляемые опросники, калькуляторы, шаблоны, карты, реестры, отраслевые профили и учебные материалы размещаются в интерактивном научно-методическом руководстве. В его медицинском модуле представлены формы клинико-цифрового профиля медицины 4.0, паспорта данных и ИИ-сценариев, критерии клинической валидации, пилотирования и мониторинга.

Итоговый методологический вывод состоит в следующем: цифровая зрелость показывает степень встроенности технологий в деятельность организации, а цифровое сознание определяет, насколько организация способна управлять этой встроенностью как ответственным, доказательным и рефлексивным процессом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Акперов И. Г. Цифровое сознание и будущее образования: новые педагогические тренды в эпоху насыщенного искусственного интеллекта // Научные труды Нахчыванского института учителей. – 2023. – № 4 (74). – С. 30–34.
2. Акперов И. Г. Цифровое сознание как детерминанта управленческой парадигмы в условиях цифровой экономики // Интеллектуальные ресурсы – региональному развитию. – 2021. – № 2. – С. 242–246.
3. Акперов И. Г., Мартынов Б. В. Региональная образовательная экосистема: искусственный интеллект, цифровое сознание и управление процессами цифровой трансформации // Искусственный интеллект: от теории к практике : материалы Международной научной конференции, Нахичевань, 19–20 сентября 2024 г. – Нахичевань : Изд-во Нахчыванского государственного университета, 2024. – С. 8–16. – DOI: 10.5281/zenodo.13799811.
4. Акперов И. Г., Мартынов Б. В. Трансформация образовательной организации: цифровые инструменты и искусственный интеллект : учебно-методическое пособие. – Ростов н/Д : ЧОУ ВО ЮУ (ИУБиП), 2025. – 183 с. – EDN PTZFMО. – URL: <https://elibrary.ru/item.asp?id=82570679> (дата обращения: 12.07.2026).
5. Акперов И. Г., Мартынов Б. В. Цифровизация сознания как детерминанта управления трансформацией транспортных систем // Транспорт и логистика: пространственно-технологическая синергия развития : сборник научных трудов IV Международной научно-практической конференции, Ростов-на-Дону, 3–4 февраля 2020 г. – Ростов н/Д : РГУПС, 2020. – С. 22–25. – EDN NLMUJT.
6. Акперов И. Г., Мартынов Б. В., Прокопенко Е. С. Роль цифрового сознания в управлении изменениями // Вестник университета. – 2022. – № 11. – С. 5–10. – DOI: 10.26425/1816-4277-2022-10-5-10. – EDN NZWDSC.
7. Акперов И. Г., Мартынов Б. В., Прокопенко Е. С. Управление организацией в условиях насыщенного искусственного интеллекта // Энергетика транспорта. Актуальные проблемы и задачи : сборник научных трудов VII Международной научно-практической конференции, Ростов-на-Дону, 1–2 марта 2023 г. – Ростов н/Д : РГУПС, 2023. – С. 20–23. – EDN STLWIQ.
8. Акперов И. Г., Мартынов Б. В., Прокопенко Е. С. Цифровое сознание как фактор формирования человеческого капитала в реинтеграционных процессах // E-Management. – 2023. – Т. 6, № 3. – С. 32–38. – DOI: 10.26425/2658-3445-2023-6-3-32-38. – EDN OPKJGJ.
9. Аналитический центр при Правительстве Российской Федерации. Искусственный интеллект в России: тенденции применения и развития. – М. : Аналитический центр, 2024. – URL: <https://ac.gov.ru/> (дата обращения: 08.07.2026).
10. Бюндюгова Т. В., Акперов И. Г., Мартынов Б. В. Формирование цифрового сознания молодежи : учебное пособие. – Ростов н/Д : ИУБиП, 2022. – 212 с.
11. Выготский Л. С. Мышление и речь. – М. : Лабиринт, 1999. – 352 с.

12. ГОСТ Р 59276-2020. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения. – М. : Стандартинформ, 2021.

13. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М. : Стандартинформ, 2021.

14. Гретченко А. И., Гретченко А. А. Цифровая зрелость российских организаций: подходы к оценке и управлению развитием // Вестник РЭУ им. Г. В. Плеханова. 2023. Т. 20, № 5. С. 54–68.

15. Добросоцкая С. Ю., Мартынов Б. В. Формирование цифрового сознания посредством трансформации коммуникативной экосистемы на базе межвузовской научно-образовательной платформы для исследования проблем управления транспортными системами и подготовки специалистов // Шаг в будущее: искусственный интеллект и цифровая экономика. Революция в управлении: новая цифровая экономика или новый мир машин : материалы II Международного научного форума, Москва, 6–7 декабря 2018 г. – Вып. 3. – М. : Издательский дом ГУУ, 2018. – С. 142–148. – EDN YVXHEN.

16. Ефремова Е. Н., Сорокина В. Е., Фельдман М. А. Понятие цифровой зрелости организации и роль искусственного интеллекта в ее формировании // Креативная экономика. – 2025. – Т. 19, № 11. – С. 3053–3068. – DOI: 10.18334/ce.19.11.124198.

17. Журавлев А. Л. Психология совместной деятельности. – М. : Институт психологии РАН, 2005. – 640 с.

18. Индикаторы цифровой экономики: 2024 : статистический сборник / В. Л. Абашкин, Г. И. Абдрахманова, К. О. Вишневский [и др.]; под общ. ред. Н. Ю. Анисимова, Л. М. Гохберга, Я. И. Кузьмина [и др.]; Нац. исслед. ун-т «Высшая школа экономики». – М. : НИУ ВШЭ, 2024. – 276 с. – URL: <https://publications.hse.ru/books/888949257> (дата обращения: 12.07.2026).

19. Искусственный интеллект в России: разработка и применение / П. Б. Рудник (рук. авт. кол.), В. Л. Абашкин, Г. И. Абдрахманова [и др.]; под ред. Л. М. Гохберга, П. Б. Рудника, Г. И. Абдрахмановой; Нац. исслед. ун-т «Высшая школа экономики». – М. : ИСИЭЗ ВШЭ, 2025. – 86 с. – (Эмпирические исследования). – ISBN 978-5-7598-3038-2. – URL: <https://issek.hse.ru/mirror/pubs/share/1053986532.pdf> (дата обращения: 12.07.2026).

20. Кодекс этики в сфере искусственного интеллекта [Электронный ресурс]. – М., 2021. – URL: <https://a-ai.ru/ethics/> (дата обращения: 12.07.2026).

21. Кузнецов Н. В. Организационная культура цифровой трансформации: факторы и механизмы формирования // Вопросы инновационной экономики. 2022. Т. 12, № 4. С. 2261–2276.

22. Леонтьев А. Н. Деятельность. Сознание. Личность. – М. : Смысл; Академия, 2005. – 352 с.

23. Лукьянова А. Л., Талакаускас Д. С. Структурные парадоксы рынка ИИ-компетенций [Электронный ресурс]. – М. : ИСИЭЗ НИУ ВШЭ, 2026. – URL: <https://issek.hse.ru/news/1172434027.html> (дата обращения: 21.07.2026).

24. Мартынов Б. В. Интеллектуальная система управления третьей миссией университета на принципах нечеткой логики как инструмент формирования цифрового сознания // Эффективные системы менеджмента: качество и

цифровые интеллектуальные системы : материалы IX Международного научно-практического форума. – Казань, 2021. – С. 77–81. – URL: <https://elibrary.ru/item.asp?id=45732849> (дата обращения: 12.07.2026).

25. Мартынов Б. В. Региональная цифровая образовательная экосистема как основа формирования цифрового сознания молодежи // Интеллектуальные ресурсы – региональному развитию. – 2021. – № 2. – С. 82–86. – URL: <https://elibrary.ru/item.asp?id=46659134> (дата обращения: 12.07.2026).

26. Мартынов Б. В. Самоактуализация человека: обновляющееся понимание в изменяющихся условиях / Б. В. Мартынов; М-во образования и науки Рос. Федерации, Ин-т междунар. бизнеса. – Ростов н/Д : Ростиздат, 2005. – 179 с. – ISBN 5-7509-0324-9. – EDN QODSKD.

27. Мартынов Б. В. Формирование и капитализация цифрового сознания: экосистемный подход // Интеллектуальные ресурсы – региональному развитию. – 2019. – Т. 5, № 2. – С. 81–84.

28. Мартынов Б. В. Цифровое сознание как ядро компетентностной модели университета будущего: интеграция человеко-центрированных подходов в управлении искусственным интеллектом // Искусственный интеллект: от теории к практике : материалы Международной научной конференции, Нахичевань, 19–20 сентября 2024 г. – Нахичевань : Изд-во Нахчыванского государственного университета, 2024. – С. 420–427. – DOI: 10.5281/zenodo.14032009. – EDN MYCVDJ.

29. Мартынов Б. В., Прокопенко Е. С., Акперов И. Г. Гуманитарно-цифровые технологии проектирования интеллектуальных информационных систем управления бизнесом // Первый экономический журнал. – 2023. – № 1 (331). – С. 19–25.

30. О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию развития искусственного интеллекта на период до 2030 года : Указ Президента Российской Федерации от 15.02.2024 № 124 // Собрание законодательства Российской Федерации. – 2024. – № 8. – Ст. 1032. – URL: <http://www.kremlin.ru/acts/bank/50339> (дата обращения: 12.07.2026).

31. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента Российской Федерации от 07.05.2024 № 309 // Собрание законодательства Российской Федерации. – 2024. – № 20. – Ст. 2584. – URL: <http://www.kremlin.ru/acts/bank/50542> (дата обращения: 12.07.2026).

32. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31, ч. 1. – Ст. 3451.

33. Об утверждении стратегического направления в области цифровой трансформации государственного управления : распоряжение Правительства Российской Федерации от 16.03.2024 № 637-п // Официальный интернет-портал правовой информации. – URL: <https://publication.pravo.gov.ru/> (дата обращения: 12.07.2026).

34. Плотников В. А. Проблемы цифровой трансформации и концепция управления изменениями // Вопросы инновационной экономики. – 2021. – Т. 11, № 4. – С. 1403–1414.
35. Плотников В. А. Цифровая трансформация и управление изменениями в организациях // Экономика и управление. 2022. Т. 28, № 8. С. 801–812.
36. Рубинштейн С. Л. Основы общей психологии. – СПб. : Питер, 2002. – 720 с.
37. Сафрончук М. В. Искусственный интеллект и цифровая трансформация бизнеса: управленческие риски и возможности // Экономика. Налоги. Право. 2023. Т. 16, № 4. С. 89–99.
38. Цифровая трансформация: ожидания и реальность : доклад к XXIII Ясинской (Апрельской) международной научной конференции по проблемам развития экономики и общества, Москва, 2022 г. / Г. И. Абдрахманова, С. А. Васильковский, К. О. Вишневский [и др.]; рук. авт. кол. П. Б. Рудник, Т. С. Зинина. – М. : Издательский дом Высшей школы экономики, 2022. – 221 с. – ISBN 978-5-7598-2658-3. – URL: https://www.hse.ru/data/2024/03/01/2082502788/Цифровая%20трансформация_доклад_25.04.pdf (дата обращения: 12.07.2026).
39. Цифровая трансформация: эффекты и риски в новых условиях / рук. авт. кол. П. Б. Рудник, Т. С. Зинина; под ред. И. Р. Агамирзяна, Л. М. Гохберга, Т. С. Зининой, П. Б. Рудника; Нац. исслед. ун-т «Высшая школа экономики». – М. : ИСИЭЗ ВШЭ, 2024. – 156 с. – ISBN 978-5-7598-3009-2. – DOI: 10.17323/978-5-7598-3009-2. – URL: <https://publications.hse.ru/pubs/share/direct/943961082.pdf> (дата обращения: 12.07.2026).
40. Шейн Э. Х. Организационная культура и лидерство / пер. с англ. – СПб. : Питер, 2002. – 336 с.
41. ALLEA. The European Code of Conduct for Research Integrity. Revised edition. – Berlin : ALLEA, 2023. – URL: <https://allea.org/code-of-conduct/> (дата обращения: 12.07.2026).
42. American Educational Research Association, American Psychological Association, National Council on Measurement in Education. Standards for Educational and Psychological Testing. – Washington : AERA, 2014. – 230 p.
43. Argyris C. Organizational Learning: A Theory of Action Perspective / C. Argyris, D. A. Schön. – Reading, MA : Addison-Wesley, 1978. – 344 p.
44. Barends E., Rousseau D. M. Evidence-Based Management: How to Use Evidence to Make Better Organizational Decisions. – London : Kogan Page, 2018. – 336 p.
45. Bawden D. Origins and concepts of digital literacy / D. Bawden // Digital Literacies: Concepts, Policies and Practices / ed. by C. Lankshear, M. Knobel. – New York : Peter Lang, 2008. – P. 17–32.
46. Bender E. M. On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? / E. M. Bender, T. Gebru, A. McMillan-Major, S. Shmitchell // Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. – New York : ACM, 2021. – P. 610–623. – DOI: 10.1145/3442188.3445922.

47. Birken S. A. [et al.]. Organizational theory for implementation science // Implementation Science Communications. 2024. Vol. 5. DOI: 10.1186/s43058-024-00500-0.
48. Blanco Ameneiros C. The Never-Ending Workday in Flexible-Working Europe / C. Blanco Ameneiros, O. Vargas Llave [Электронный ресурс] // Eurofound. – 2026. – URL: <https://www.eurofound.europa.eu/en/publications/all/the-never-ending-workday-in-flexible-working-europe> (дата обращения: 12.07.2026).
49. Cao G. Organizational Culture, Digital Transformation, and Product Innovation / G. Cao, Y. Duan, J. S. Edwards // Information & Management. – 2025. – Vol. 62, no. 4. – Art. 104135. – DOI: 10.1016/j.im.2025.104135.
50. Catana G. C. The Communities of Practice Playbook: A Playbook to Collectively Run and Develop Communities of Practice / G. C. Catana [et al.]. – Luxembourg : Publications Office of the European Union, 2021. – DOI: 10.2760/443810. – URL: <https://publications.jrc.ec.europa.eu/repository/handle/JRC122830> (дата обращения: 12.07.2026).
51. CIPD. Employee communication : factsheet. – London : Chartered Institute of Personnel and Development, 2025. – URL: <https://www.cipd.org/en/knowledge/factsheets/employee-communication-factsheet/> (дата обращения: 12.07.2026).
52. CIPD. Employee Voice [Электронный ресурс]. – London : Chartered Institute of Personnel and Development, 2026. – URL: <https://www.cipd.org/uk/knowledge/factsheets/voice-factsheet/> (дата обращения: 21.07.2026).
53. CIPD. Organisational culture and cultural change : factsheet. – London : Chartered Institute of Personnel and Development, 2023. – URL: <https://www.cipd.org/en/knowledge/factsheets/organisation-culture-change-factsheet/> (дата обращения: 12.07.2026).
54. Commission nationale de l'informatique et des libertés. Employee Monitoring: CNIL Fines Amazon France Logistique €32 Million. – Paris : CNIL, 2024. – URL: <https://www.cnil.fr/en/employee-monitoring-cnil-fines-amazon-france-logistique-eu32-million> (дата обращения: 12.07.2026).
55. Cristofaro M. Organizational sensemaking: a systematic review and a co-evolutionary model // European Management Journal. – 2022. – Vol. 40, no. 3. – P. 393–405. – DOI: 10.1016/j.emj.2021.07.003.
56. DAMA International. DAMA-DMBOK: Data Management Body of Knowledge / ed. by S. Earley, D. Henderson. – 2nd ed. – Basking Ridge : Technics Publications, 2017. – 628 p.
57. Davenport T. H. Competing on Analytics: The New Science of Winning / T. H. Davenport, J. G. Harris. – Boston : Harvard Business School Press, 2007. – 240 p.
58. DeVellis R. F., Thorpe C. T. Scale Development: Theory and Applications. – 5th ed. – Thousand Oaks : SAGE, 2022. – 320 p.
59. DigComp 3.0: The Digital Competence Framework for Citizens / European Commission, Joint Research Centre. – 2025. – URL: <https://joint-research-centre.ec.europa.eu/> (дата обращения: 08.07.2026).

60. Digital Promise. Estudia Khanmigo: An Equity-Focused Pilot Exploration of AI-Assisted Learning. – Washington, DC : Digital Promise, 2024. – URL: <https://digitalpromise.org/wp-content/uploads/2024/09/SRM-Gates-Khanmigo-Report-Final.pdf> (дата обращения: 21.07.2026).
61. Dignum V. Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way / V. Dignum. – Cham : Springer, 2019. – 127 p. – DOI: 10.1007/978-3-030-30371-6.
62. Edmondson A. C., Bransby D. P. Psychological safety comes of age: observed themes in an established literature // Annual Review of Organizational Psychology and Organizational Behavior. – 2023. – Vol. 10. – P. 55–78. – DOI: 10.1146/annurev-orgpsych-120920-055217.
63. EdSurge. An Education Chatbot Company Collapsed. Where Did the Student Data Go? [Электронный ресурс]. – 2024. – URL: <https://www.edsurge.com/news/2024-07-15-an-education-chatbot-company-collapsed-where-did-the-student-data-go> (дата обращения: 12.07.2026).
64. European Commission. Artificial Intelligence in the European Commission (AI@EC): Communication and Internal Strategy. – Brussels : European Commission, 2024. – URL: https://commission.europa.eu/publications/artificial-intelligence-european-commission-aiec-communication_en (дата обращения: 12.07.2026).
65. European Commission. Living Guidelines on the Responsible Use of Generative AI in Research. – 3rd version. – Brussels : Directorate-General for Research and Innovation, 2026. – URL: https://research-and-innovation.ec.europa.eu/document/download/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en (дата обращения: 12.07.2026).
66. European Molecular Biology Laboratory. AlphaFold: Using Open Data and AI to Discover the 3D Protein Universe [Электронный ресурс]. – 2024. – URL: <https://www.embl.org/news/science/alphafold-using-open-data-and-ai-to-discover-the-3d-protein-universe/> (дата обращения: 12.07.2026).
67. European Parliament and Council. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence // Official Journal of the European Union. – 2024. – L 2024/1689. – URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата обращения: 12.07.2026).
68. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. – Athens : ENISA, 2024. – URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (дата обращения: 12.07.2026).
69. Eurostat. Use of Artificial Intelligence in Enterprises [Электронный ресурс]. – Luxembourg : European Commission, 2025. – URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises (дата обращения: 12.07.2026).
70. Floridi L. A unified framework of five principles for AI in society / L. Floridi, J. Cowls // Harvard Data Science Review. – 2019. – Vol. 1, № 1. – DOI: 10.1162/99608f92.8cd550d1.
71. Gillespie N., Lockey S., Ward T., Macdade A., Hassed G. Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025. – Melbourne : The University of Melbourne; KPMG, 2025. – DOI: 10.26188/28822919.

72. Gmyrek P. Generative AI and Jobs: A Refined Global Index of Occupational Exposure / P. Gmyrek, J. Berg, K. Kamiński [et al.] // ILO Working Paper. – Geneva : International Labour Organization, 2025. – No. 140. – DOI: 10.54394/HETP0387. – URL: <https://www.ilo.org/publications/generative-ai-and-jobs-refined-global-index-occupational-exposure> (дата обращения: 12.07.2026).
73. Good Things Foundation. Confidence and Engagement: Expert Overview [Электронный ресурс]. – London : Good Things Foundation, 2025. – URL: <https://www.goodthingsfoundation.org/policy-and-research/what-works-colab/confidence-and-engagement-briefing> (дата обращения: 21.07.2026).
74. Green A. Artificial Intelligence and the Changing Demand for Skills in the Labour Market // OECD Artificial Intelligence Papers. – Paris : OECD Publishing, 2024. – No. 14. – DOI: 10.1787/88684e36-en.
75. Harrison R., Fischer S., Walpola R. L. [et al.]. Where do models for change management, improvement and implementation meet? A systematic review of the applications of change management models in healthcare // BMC Health Services Research. – 2021. – Vol. 21. – Art. 1240. – DOI: 10.1186/s12913-021-07278-9.
76. Health Innovation North East and North Cumbria. Digital Champions [Электронный ресурс]. – URL: <https://healthinnovationnenc.org.uk/what-we-do/driving-digital-transformation/digital-champions/> (дата обращения: 21.07.2026).
77. Holtzblatt K. Contextual Design: Evolved / K. Holtzblatt, H. R. Beyer. – San Rafael, CA : Morgan & Claypool Publishers, 2014. – 91 p. – DOI: 10.2200/S00597ED1V01Y201409HCI024.
78. IBM Institute for Business Value. 6 Hard Truths CEOs Must Face: How to Leap Forward with Courage and Conviction in the Generative AI Era. – Armonk : IBM, 2024. – URL: <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ceo-generative-ai> (дата обращения: 12.07.2026).
79. IBM. Cost of a Data Breach Report 2025 [Электронный ресурс]. – Armonk : IBM, 2025. – URL: <https://www.ibm.com/reports/data-breach> (дата обращения: 12.07.2026).
80. ISO 31000:2018. Risk management – Guidelines. – Geneva : International Organization for Standardization, 2018.
81. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : International Organization for Standardization, 2022.
82. ISO/IEC 38500:2024. Information technology – Governance of IT for the organization. – Geneva : International Organization for Standardization, 2024.
83. ISO/IEC 42001:2023. Information technology – Artificial intelligence – Management system. – Geneva : International Organization for Standardization, 2023. – URL: <https://www.iso.org/standard/81230.html> (дата обращения: 12.07.2026).
84. Jääskä E. [et al.]. Bridging change management and project management: a systematic review // Project Leadership and Society. 2025. Vol. 6.
85. Jisc. Building Digital Capability [Электронный ресурс]. – Bristol : Jisc. – URL: <https://www.jisc.ac.uk/rd/projects/building-digital-capability> (дата обращения: 12.07.2026).

86. Jisc. Code of Practice for Learning Analytics [Электронный ресурс]. – Bristol : Jisc. – URL: <https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics> (дата обращения: 12.07.2026).
87. Jisc. Digital Transformation in Higher Education: Framework and Practice Resources [Электронный ресурс]. – Bristol : Jisc, 2024. – URL: <https://www.jisc.ac.uk/guides/digital-transformation> (дата обращения: 12.07.2026).
88. Jobin A. Artificial Intelligence: the global landscape of ethics guidelines / A. Jobin, M. Ienca, E. Vayena // *Nature Machine Intelligence*. – 2019. – Vol. 1. – P. 389–399. – DOI: 10.1038/s42256-019-0088-2.
89. Kane G. C. Strategy, not Technology, Drives Digital Transformation / G. C. Kane, D. Palmer, A. N. Phillips, D. Kiron, N. Buckley. – Cambridge : MIT Sloan Management Review; Deloitte University Press, 2015. – 27 p.
90. Khwaja H., Harkins L. State of the Sector: Data Maturity in the Nonprofit Sector 2024. – London : Data Orchard, 2024. – URL: <https://www.dataorchard.org.uk/resources/> (дата обращения: 12.07.2026).
91. Kotter. The 8 Steps for Leading Change. – 2025. – URL: <https://www.kotterinc.com/methodology/8-steps/> (дата обращения: 12.07.2026).
92. Long D. What is AI literacy? Competencies and design considerations / D. Long, B. Magerko // *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. – New York : ACM, 2020. – P. 1–16. – DOI: 10.1145/3313831.3376727.
93. McKinsey & Company. The State of AI in 2025: Agents, Innovation, and Transformation [Электронный ресурс]. – New York : McKinsey & Company, 2025. – URL: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai> (дата обращения: 12.07.2026).
94. Miao F., Shiohira K., Lao N. AI Competency Framework for Students. – Paris : UNESCO, 2024. – DOI: 10.54675/JKJB9835. – URL: <https://unesdoc.unesco.org/ark:/48223/pf0000391105> (дата обращения: 21.07.2026).
95. Microsoft. 2024 Work Trend Index Annual Report: AI at Work Is Here. Now Comes the Hard Part [Электронный ресурс]. – Redmond : Microsoft, 2024. – URL: <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part> (дата обращения: 12.07.2026).
96. Microsoft. 2025 Work Trend Index Annual Report: The Year the Frontier Firm Is Born. – Redmond : Microsoft, 2025. – URL: <https://www.microsoft.com/en-us/worklab/work-trend-index/> (дата обращения: 12.07.2026).
97. Milanez A. Algorithmic Management in the Workplace: New Evidence from an OECD Employer Survey / A. Milanez, A. Lemmens, C. Ruggiu // *OECD Artificial Intelligence Papers*. – Paris : OECD Publishing, 2025. – No. 31. – DOI: 10.1787/287c13c4-en.
98. Moffatt v. Air Canada, 2024 BCCRT 149 : Civil Resolution Tribunal Decision. – 2024. – URL: <https://decisions.civilresolutionbc.ca/crt/crtd/en/item/525448/index.do> (дата обращения: 12.07.2026).
99. Mokkink L. B. COSMIN Methodology for Systematic Reviews of Patient-Reported Outcome Measures / L. B. Mokkink [et al.]. – Amsterdam : COSMIN, 2018. – URL: <https://www.cosmin.nl/> (дата обращения: 12.07.2026).

100. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). – Gaithersburg : NIST, 2023. – DOI: 10.6028/NIST.AI.100-1.
101. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. – Gaithersburg : NIST, 2024. – DOI: 10.6028/NIST.AI.600-1. – URL: <https://www.nist.gov/itl/ai-risk-management-framework> (дата обращения: 12.07.2026).
102. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. – Gaithersburg : NIST, 2024. – DOI: 10.6028/NIST.CSWP.29. – URL: <https://www.nist.gov/cyberframework> (дата обращения: 12.07.2026).
103. NetHope. 2024 State of Humanitarian and Development Cybersecurity Report [Электронный ресурс]. – Washington, DC : NetHope, 2024. – URL: <https://nethope.org/toolkits/2024-state-of-humanitarian-and-development-cybersecurity-report/> (дата обращения: 12.07.2026).
104. Nonaka I. The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation / I. Nonaka, H. Takeuchi. – New York : Oxford University Press, 1995. – 284 p.
105. OECD. 2023 OECD Open, Useful and Re-usable Data (OURdata) Index. – Paris : OECD Publishing, 2023. – DOI: 10.1787/a37f51c3-en.
106. OECD. Digital Government Outlook 2026: From Foundations to Transformational Impact. – Paris : OECD Publishing, 2026. – 184 p. – DOI: 10.1787/0496b2bc-en.
107. OECD. Governing with Artificial Intelligence: Are Governments Ready? // OECD Artificial Intelligence Papers. – Paris : OECD Publishing, 2024. – No. 20. – DOI: 10.1787/26324bc2-en.
108. OECD. OECD Digital Education Outlook 2026: Exploring Effective Uses of Generative AI in Education. – Paris : OECD Publishing, 2026. – 247 p. – DOI: 10.1787/062a7394-en.
109. OECD. Recommendation of the Council on Artificial Intelligence [Электронный ресурс]. – Paris : OECD, 2019; updated 2024. – URL: <https://oecd.ai/en/ai-principles> (дата обращения: 12.07.2026).
110. OECD. Results from TALIS 2024: The State of Teaching. – Paris : OECD Publishing, 2025. – 306 p. – DOI: 10.1787/90df6235-en.
111. OECD. Using AI in the Workplace: Opportunities, Risks and Policy Responses // OECD Artificial Intelligence Papers. – Paris : OECD Publishing, 2024. – No. 11. – DOI: 10.1787/73d417f9-en.
112. Papagiannidis E. [et al.]. Responsible artificial intelligence governance: a review and research agenda // Technological Forecasting and Social Change. 2025. Vol. 210.
113. Papagiannidis E. Responsible Artificial Intelligence Governance: A Review and Research Framework / E. Papagiannidis, P. Mikalef, K. Conboy // The Journal of Strategic Information Systems. – 2025. – Vol. 34. – Art. 101885. – DOI: 10.1016/j.jsis.2024.101885.
114. Project Management Institute. The Standard for Program Management. – 5th ed. – Newtown Square, PA : PMI, 2024.

115. Prosci. The Prosci ADKAR Model. – 2025. – URL: <https://www.prosci.com/methodology/adkar> (дата обращения: 12.07.2026).
116. Purificato E. The Role of Artificial Intelligence in Scientific Research: A Science for Policy, European Perspective / E. Purificato, D. Bili, R. Jungnickel [et al.]. – Luxembourg : Publications Office of the European Union, 2025. – 123 p. – ISBN 978-92-68-31427-2. – DOI: 10.2760/7217497.
117. PwC. 2025 Global AI Jobs Barometer. – London : PricewaterhouseCoopers, 2025. – URL: <https://www.pwc.com/gx/en/issues/artificial-intelligence/job-barometer.html> (дата обращения: 12.07.2026).
118. Redecker C. European Framework for the Digital Competence of Educators: DigCompEdu / C. Redecker; Y. Punie (ed.). – Luxembourg : Publications Office of the European Union, 2017. – 95 p. – DOI: 10.2760/159770.
119. Reis J., Amorim M., Melão N., Cohen Y., Rodrigues M. Digital transformation: a meta-review and guidelines for future research // Heliyon. – 2023. – Vol. 9, no. 1. – Art. e12834. – DOI: 10.1016/j.heliyon.2023.e12834.
120. Royal Commission into the Robodebt Scheme. Report. – Canberra : Commonwealth of Australia, 2023. – URL: <https://robodebt.royalcommission.gov.au/publications/report> (дата обращения: 12.07.2026).
121. Schein E. H. Organizational Culture and Leadership / E. H. Schein. – 5th ed. – Hoboken : Wiley, 2017. – 416 p.
122. Schwaber K. The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game / K. Schwaber, J. Sutherland. – 2020. – URL: <https://scrumguides.org/> (дата обращения: 12.07.2026).
123. Senge P. M. The Fifth Discipline: The Art and Practice of the Learning Organization / P. M. Senge. – New York : Doubleday, 1990. – 424 p.
124. Shneiderman B. Human-Centered AI. – Oxford : Oxford University Press, 2022. – 400 p.
125. Škrinjaric B. Competence-based approaches in organizational and individual context // Humanities and Social Sciences Communications. – 2022. – Vol. 9. – Art. 214. – DOI: 10.1057/s41599-022-01228-8.
126. Stanford Institute for Human-Centered Artificial Intelligence. The 2025 AI Index Report [Электронный ресурс]. – Stanford : Stanford University, 2025. – URL: <https://hai.stanford.edu/ai-index/2025-ai-index-report> (дата обращения: 12.07.2026).
127. Stanford Institute for Human-Centered Artificial Intelligence. The 2026 AI Index Report [Электронный ресурс]. – Stanford : Stanford University, 2026. – URL: <https://hai.stanford.edu/ai-index/2026-ai-index-report> (дата обращения: 21.07.2026).
128. TechSoup Europe. Empowering Nonprofits Through Digital Transformation [Электронный ресурс]. – Warsaw : TechSoup Europe, 2024. – URL: <https://www.techsoupeurope.org/empowering-nonprofits-through-digital-transformation/> (дата обращения: 21.07.2026).
129. Teece D. J. Dynamic Capabilities: Foundational Concepts. – Cambridge : Cambridge University Press, 2025. – URL: <https://www.cambridge.org/core/elements/dynamic-capabilities/> (дата обращения: 12.07.2026).

130. Teece D. J. Explicating dynamic capabilities: the nature and microfoundations of sustainable enterprise performance / D. J. Teece // *Strategic Management Journal*. – 2007. – Vol. 28, № 13. – P. 1319–1350. – DOI: 10.1002/smj.640.
131. The Open Group. The TOGAF Standard. – 10th ed. – San Francisco : The Open Group, 2022. – URL: <https://www.opengroup.org/togaf> (дата обращения: 12.07.2026).
132. The Royal Society. Science in the Age of AI: How Artificial Intelligence Is Changing the Nature and Method of Scientific Research. – London : The Royal Society, 2024. – URL: <https://royalsociety.org/> (дата обращения: 12.07.2026).
133. Trist E. L. Some Social and Psychological Consequences of the Longwall Method of Coal-Getting / E. L. Trist, K. W. Bamforth // *Human Relations*. – 1951. – Vol. 4, № 1. – P. 3–38.
134. UK Research and Innovation. Generative Artificial Intelligence in Application and Assessment Policy. – Swindon : UKRI, 2024. – URL: <https://www.ukri.org/publications/generative-artificial-intelligence-in-application-and-assessment-policy/> (дата обращения: 12.07.2026).
135. UNESCO. AI Competency Framework for Teachers. – Paris : UNESCO, 2024. – URL: <https://unesdoc.unesco.org/ark:/48223/pf0000391104> (дата обращения: 12.07.2026).
136. UNESCO. Guidance for Generative AI in Education and Research. – Paris : UNESCO, 2023. – 44 p. – URL: <https://unesdoc.unesco.org/ark:/48223/pf0000386693> (дата обращения: 12.07.2026).
137. UNESCO. Readiness Assessment Methodology: A Tool of the Recommendation on the Ethics of Artificial Intelligence. – Paris : UNESCO, 2023. – URL: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics/readiness-assessment-methodology> (дата обращения: 12.07.2026).
138. UNESCO. Recommendation on Open Science. – Paris : UNESCO, 2021. – URL: <https://www.unesco.org/en/open-science/about> (дата обращения: 12.07.2026).
139. UNESCO. Recommendation on the Ethics of Artificial Intelligence. – Paris : UNESCO, 2021. – 43 p. – URL: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> (дата обращения: 21.07.2026).
140. United Nations. E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. – New York : United Nations Department of Economic and Social Affairs, 2024. – URL: <https://publicadministration.un.org/egovkb/> (дата обращения: 12.07.2026).
141. Ushahidi. Featured Case Studies [Электронный ресурс]. – Nairobi : Ushahidi, 2026. – URL: <https://www.ushahidi.com/in-action/case-studies> (дата обращения: 21.07.2026).
142. Vansteenkiste M. Basic Psychological Need Theory: Advancements, Critical Themes, and Future Directions / M. Vansteenkiste, R. M. Ryan, B. Soenens // *Motivation and Emotion*. – 2020. – Vol. 44. – P. 1–31. – DOI: 10.1007/s11031-019-09818-1.
143. Verhoef P. C., Broekhuizen T., Bart Y., Bhattacharya A., Dong J. Q., Fabian N., Haenlein M. Digital transformation: A multidisciplinary reflection and research

agenda // Journal of Business Research. – 2021. – Vol. 122. – P. 889–901. – DOI: 10.1016/j.jbusres.2019.09.022.

144. Verizon. 2026 Data Breach Investigations Report. 19th ed. [Электронный ресурс]. – New York : Verizon Business, 2026. – URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата обращения: 21.07.2026).

145. Vial G. Understanding Digital Transformation: A Review and a Research Agenda / G. Vial // The Journal of Strategic Information Systems. – 2019. – Vol. 28, № 2. – P. 118–144. – DOI: 10.1016/j.jsis.2019.01.003.

146. Vuorikari R. DigComp 2.2: The Digital Competence Framework for Citizens: With New Examples of Knowledge, Skills and Attitudes / R. Vuorikari, S. Kluzer, Y. Punie. – Luxembourg : Publications Office of the European Union, 2022. – 134 p. – DOI: 10.2760/115376. – URL: <https://publications.jrc.ec.europa.eu/repository/handle/JRC128415> (дата обращения: 12.07.2026).

147. Weick K. E. Sensemaking in Organizations / K. E. Weick. – Thousand Oaks : Sage Publications, 1995. – 248 p.

148. Westerman G. Leading Digital: Turning Technology into Business Transformation / G. Westerman, D. Bonnet, A. McAfee. – Boston : Harvard Business Review Press, 2014. – 292 p.

149. William Bridges Associates. Bridges Transition Model. – 2025. – URL: <https://wmbridges.com/about/what-is-transition/> (дата обращения: 12.07.2026).

150. World Bank. GovTech Maturity Index 2025: Tracking Public Sector Digital Transformation Worldwide. – Washington, DC : World Bank, 2025. – DOI: 10.1596/44136.

151. World Economic Forum. The Future of Jobs Report 2025. – Geneva : World Economic Forum, 2025. – URL: <https://www.weforum.org/publications/the-future-of-jobs-report-2025/> (дата обращения: 12.07.2026).

152. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. – New York : PublicAffairs, 2019. – 704 p.

153. Об основах охраны здоровья граждан в Российской Федерации : Федеральный закон от 21 ноября 2011 г. № 323-ФЗ (ред. по состоянию на дату обращения) [Электронный ресурс]. – URL: <https://pravo.gov.ru/> (дата обращения: 21.07.2026).

154. Об утверждении стратегического направления в области цифровой трансформации здравоохранения : распоряжение Правительства Российской Федерации от 17 апреля 2024 г. № 959-р [Электронный ресурс]. – URL: <https://government.ru/docs/all/153077/> (дата обращения: 21.07.2026).

155. World Health Organization. Ethics and Governance of Artificial Intelligence for Health: WHO Guidance. – Geneva : World Health Organization, 2021. – 150 p. – ISBN 978-92-4-002920-0. – URL: <https://www.who.int/publications/i/item/9789240029200> (дата обращения: 21.07.2026).

156. World Health Organization. Regulatory Considerations on Artificial Intelligence for Health. – Geneva : World Health Organization, 2023. – 61 p. – ISBN

978-92-4-007887-1. – URL: <https://www.who.int/publications/i/item/9789240078871> (дата обращения: 21.07.2026).

157. World Health Organization. Ethics and Governance of Artificial Intelligence for Health: Guidance on Large Multi-Modal Models. – Geneva : World Health Organization, 2025. – 98 p. – ISBN 978-92-4-008475-9. – URL: <https://www.who.int/publications/i/item/9789240084759> (дата обращения: 21.07.2026).

158. World Health Organization. Global Strategy on Digital Health 2020–2027. – Geneva : World Health Organization, 2025. – 60 p. – ISBN 978-92-4-011687-0. – URL: <https://www.who.int/publications/i/item/9789240116870> (дата обращения: 21.07.2026).

159. Haleem A. Medical 4.0 Technologies for Healthcare: Features, Capabilities, and Applications / A. Haleem, M. Javaid, R. P. Singh, R. Suman // Internet of Things and Cyber-Physical Systems. – 2022. – Vol. 2. – P. 12–30. – DOI: 10.1016/j.iotcps.2022.04.001.

160. ISO 7101:2023. Healthcare Organization Management – Management Systems for Quality in Healthcare Organizations – Requirements. – 1st ed. – Geneva : International Organization for Standardization, 2023. – 35 p. – URL: <https://www.iso.org/standard/81647.html> (дата обращения: 21.07.2026).

161. Topol E. J. High-Performance Medicine: The Convergence of Human and Artificial Intelligence / E. J. Topol // Nature Medicine. – 2019. – Vol. 25. – P. 44–56. – DOI: 10.1038/s41591-018-0300-7.

162. World Health Organization. Regional Office for Europe. Artificial Intelligence Is Reshaping Health Systems: State of Readiness across the WHO European Region. – Copenhagen : WHO Regional Office for Europe, 2025. – 56 p. – WHO/EURO:2025-12707-52481-81028. – URL: <https://www.who.int/europe/publications/i/item/WHO-EURO-2025-12707-52481-81028> (дата обращения: 21.07.2026).

Научно-методическое издание

Акперов Имран Гурруевич

Мартынов Борис Викторович

**УПРАВЛЕНИЕ ЦИФРОВЫМИ ИЗМЕНЕНИЯМИ:
МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ ЦИФРОВОГО СОЗНАНИЯ
ОРГАНИЗАЦИИ: НАУЧНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ**

Подписано в печать 28.08.26 Формат 60х84/16

Бумага газетная. Ризография. Усл.печ.л.

Тираж экз.100 Изд. № . Заказ

Редакционно-издательский центр ЮУ (ИУБиП)

Адрес университета:

344038, Ростов-на-Дону, пр. М. Нагибина 33А/47